Escuela Politécnica Superior

Desarrollo del Plan Director de Seguridad para la Asociación APSA

Máster Ciber Seg

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:
Jessica Alexandra Montero Valencia

Tutor/es:
José Vicente Berná Martinez

Septiembre 2019

Universitat d'Alacant
Universidad de Alicante

Resumen

El presente Trabajo Fin de Máster desarrolla un Plan Director de Seguridad para la asociación APSA en base a la metodología Magerit y la familia de normas ISO 27000. El plan director de seguridad consiste en un análisis y tratamiento de los riesgos que afecta a la asociación. El trabajo empieza con la creación del Inventario de activos que contiene los grupos: Datos/Información, Servicios, Aplicaciones, Equipos informáticos, Redes de comunicaciones, Soportes de información, Equipamiento auxiliar, Instalaciones y Personal. Definidos los activos se los valora en las 5 dimensiones de seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. Entonces, se determina las amenazas que afecta a cada activo y su frecuencia de ocurrencia, esto para calcular el valor del impacto y riesgo potencial. Teniendo los resultados del riesgo potencial se determina que todos los valores mayores a 4 serán riesgos graves, excepto para los Datos/Información, Servicios, Software y Redes de comunicaciones donde su valor de riesgo aceptable es menor. Definiendo los valores mínimos aceptados se caracterizan salvaguardas para mitigar, controlar o eliminar el riesgo de las amenazas. Las salvaguardas tendrán un grado o porcentaje de efectividad sobre las 5 dimensiones de seguridad y sobre la ocurrencia de las amenazas. Este porcentaje ayuda a determinar el impacto y riesgo residuales, obteniendo los resultados deseados de riesgo salvo en pocas excepciones donde exceden su valor mínimo, pero al no ser considerables, los riesgos son asumibles. Finalmente, los resultados se sintetizan con la creación de una herramienta ofimática del análisis de riesgos de la asociación y la elaboración de 5 planes de seguridad que quedan a disposición de APSA para su posterior implementación.

Motivación, justificación y objetivo general

Un Sistema de Gestión de Seguridad de la Información es importarte para una empresa, pues consigue: una mayor confianza en sus activos, tener una gestión estructurada de riesgos, posibilitar la mejora continua de la seguridad informática y lograr el cumplimiento de las obligaciones legales y reglamentarias. Tener un Sistema de Gestión de Seguridad organizado en un Plan Director de Seguridad de calidad, permite a una empresa tener un informe detallado del análisis de riesgos de todos sus activos y determinar cuáles son las medidas a considerarse para reducir su impacto. Los beneficios que se obtiene al implementar un Plan Director de Seguridad se reflejan en la mejora de la productividad y rentabilidad de la empresa. Y es lo que aprendí en la cátedra de Sistemas de Gestión de la Seguridad: cómo realizar un análisis de riesgos aplicando normas ISO de Sistemas de Gestión de Seguridad de la Información.

En la cátedra de Sistemas de Gestión de la Seguridad se trata inicialmente la importancia de una buena gestión de seguridad de la información en una organización, y en base a ello se estructuró un Plan Director de Seguridad. Todos los pasos que se desarrollan dentro del Plan Director de Seguridad están basados en la familia de las normas ISO27000, que es la norma establecida en España para la implementación de un Sistema de Gestión de Seguridad. Se usaron herramientas y metodologías utilizadas generalmente dentro de las empresas, y que son recomendadas en instituciones gubernamentales como el INCIBE.

Conociendo la importancia y la necesidad de una empresa de tener un sistema de gestión de Seguridad de la Información para proteger sus activos, acepté la oportunidad de desarrollar un Plan Director de Seguridad para la asociación APSA. Al conocer que APSA es una asociación sin fines de lucro que ayuda a muchas personas, me vi muy motivada para aportar en la mejora de su seguridad informática con los conocimientos que he adquirido en el Máster de Ciberseguridad aplicados al desarrollo de un Plan Director de Seguridad.

APSA es una organización que desde hace algunos años se está modernizando e integrando Tecnologías de la Información y Comunicación para ofrecer mejores servicios a sus usuarios. Al ser una Organización No Gubernamental para el Desarrollo (ONGD), APSA ha recibido ayuda de otras instituciones para este proceso de modernización. En 2017, con el apoyo de Aguas de Alicante y la Cátedra de Inclusión dirigida por el Vicerrectorado de Responsabilidad Social, Inclusión e Igualdad de la Universidad de Alicante, se llegó a un acuerdo importante de refuerzo en innovación de tecnologías de la información para mejorar y crecer en la oferta de servicios a sus asociados. (González Mataix, 2018, pp. 18-20)

El departamento TIC de APSA, consiente de la importancia de la seguridad de la información, han implementado políticas de seguridad según las necesidades y requerimientos de ley, que se han presentado con el tiempo. Esta metodología no es la adecuada y por el crecimiento de la asociación se requiere de un Sistema de Gestión de la Información estructurado y correctamente administrado, que no solo ayude a la situación actual, sino que sea el precedente para los próximos años en el área de seguridad de la información.

En consecuencia, el objetivo principal del presente trabajo es Desarrollar un Plan Director de Seguridad para la asociación APSA. Este es un largo trabajo que conlleva una gran responsabilidad pues es una organización real, pero en el que pondré todo mi esfuerzo para que los resultados sean apropiados y que APSA se vea realmente beneficiado con este trabajo. Además, sé que aportará mucho a mi formación profesional pues podré adquirir conocimientos que aplicaré durante el desarrollo del Plan Director de Seguridad de APSA y, que me servirá para profundizar en el tema de Gestión de la Información en el que tengo gran interés.

Agradecimientos

Agradezco primero a Dios por darme la vida y la oportunidad de cumplir con esta meta académica.

A mis padres, por su amor, apoyo incondicional y su esfuerzo para cursar mis estudios en España.

A mi hermana, por su amor, apoyo emocional, sus ánimos y consejos.

A mi Tutor, quien fue guía fundamental para el desarrollo de este trabajo pero también por su ayuda y consejos en otros sentidos de la vida.

A mi familia, en especial a mi tía Teresa.

Citas

“La máxima seguridad es tu comprensión de la realidad”

H. Stanley Judd

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

En los últimos años se ha extendido la integración de las Tecnologías de la Información y Comunicación (TIC) a los procesos de las empresas. La integración provoca, que a través de las TIC se gestione uno de activos más importantes para las empresas: los datos. Sin embargo, el uso de las TIC si bien ayudan al manejo de procesos y la información, pueden abrir nuevas brechas de seguridad, lo que conlleva a que la seguridad informática sea hoy en día una de las principales preocupaciones de las empresas.

Sin duda las tecnologías de la información han transformado a las empresas y su forma de manejar sus procesos, sus finanzas, el uso de datos, mercadotecnia, marketing etc., para acoplarse a una sociedad tecnológica y así ofrecer mejores servicios con más beneficios. Por lo tanto, ahora los esfuerzos de las empresas también se enfocan a la ciberseguridad. Pero ¿qué es lo que las empresas tienen que proteger? Principalmente lo que deben proteger es uno de sus activos más importantes: la información, que es esencial para la funcionalidad de la empresa. Sin importar la forma de almacenamiento de la información es fundamental tener una protección adecuada y, conocer las vulnerabilidades y riesgos que pueden afectar a la confidencialidad, disponibilidad, autenticidad e integridad de dicha información.

La seguridad informática de una empresa no es tema fácil, pues requiere analizar cada activo detenidamente, para encontrar la manera más adecuada de eliminar o mitigar las vulnerabilidades y riesgos a los que se ve enfrentado. Para el análisis existen normas, estándares y directrices que permiten implementar mecanismos que logren una mayor seguridad. Es un trabajo arduo pero que se puede lograr mediante la implementación de un Sistema de Gestión de la Seguridad Informática, y que para organizarlo es necesario desarrollar un Plan Director de Seguridad.

El Plan Director de Seguridad es la parte de la seguridad de la información que consiste en el análisis de una situación inicial de una empresa para definir un conjunto de proyectos para reducir los riesgos a niveles aceptables. El Pan Director incluye prioridades, responsables, recursos disponibles para ejecutar los proyectos de seguridad y buenas prácticas que deben cumplir todas las personas involucradas directamente con la empresa. Son 6 las fases que se necesita para elaborar y poner en marcha un Plan Director de Seguridad: conocer la situación actual, conocer la estrategia de la organización, definir proyectos e iniciativas, clasificación y priorización, aprobación por la dirección, e implantación. (INCIBE, n.d., p. 3)

En este trabajo se desarrollará el Plan Director de Seguridad para APSA siguiendo normas, directrices y metodologías aceptadas en España, y que son las recomendadas por los institutos relacionados con la ciberseguridad. Para esto, la norma seleccionada es la familia ISO27000 y la metodología es MAGERIT. También hay que considerar ciertos aspectos legales para el manejo de Datos que están dentro del Reglamento General de Protección de Datos, puesto que APSA es una asociación que maneja datos médicos de niños y adultos con distintas capacidades.

1.1. Objetivos

- Realizar un Inventario de Activos de APSA con sus respectivas dependencias
- Establecer las amenazas que afectan a los activos
- Determinar el impacto y el riesgo si las amenazas se materializan
- Caracterizar las salvaguardas y estudiar el impacto que producen sobre el riesgo
- Crear planes de seguridad para los activos de APSA
- Definir acciones para la implantación y concienciación en materia de un Sistema de Gestión de la Seguridad de la Información

2. Estado del Arte

En este capítulo se describe las definiciones necesarias para poner en contexto este trabajo. Se habla brevemente de los Sistemas de Gestión de Seguridad de la Información, el Plan Director de Seguridad, la familia de normas ISO 27000 y la metodología MAGERIT.

2.1. Sistemas de Gestión de Seguridad Informática

Un sistema de Gestión de Seguridad Informática (SGSI) consiste en un conjunto de procesos destinados a organizar y actuar sobre todos los elementos que componen la seguridad de una organización. Un SGSI se usa para establecer, implementar, monitorizar y mejorar la seguridad de la información de una organización para alcanzar sus objetivos comerciales. (International Organization for Standardization (ISO), 2018, pp. 11-12)

La Norma ISO/IEC 27000 (2018, p. 13) recalca que la importancia de un SGSI parte de la necesidad de proteger la información y sus procesos relacionados, los sistemas y las redes que están expuestas a distintos riesgos. Los riesgos pueden ser internos o externos, ya sean físicos como incendios, robo, fraude, etc., o de software como códigos maliciosos, ataques de denegación de servicios, virus, etc.

La adopción de un SGSI tiene que ser una decisión estratégica integrada de manera proporcional y actualizada de acuerdo con las necesidades, intereses y requisitos de seguridad de todas las partes interesadas de una organización. Además, requiere el compromiso de todas las áreas que integran una organización, pues el diseño de un SGSI no solo consiste en soluciones de seguridad técnicas, muchas veces se requiere combinar con soluciones administrativas. Si al final se consigue tener un SGSI coherente, el prestigio de la organización aumenta, pues demuestra a sus usuarios, clientes y todos los interesados, que poseen la capacidad de gestionar riesgos y brindar seguridad a la información. (International Organization for Standardization (ISO), 2018, pp. 13-14)

Existe variada documentación que ayuda a las organizaciones a aplicar un SGSI pero dentro del territorio español la norma recomendada es la familia ISO/IEC 27000 publicada como UNE-ISO/IEC 27000 en su versión más actualizada de febrero del 2019 disponible en la página web de AENOR (Organismo de Normalización de España). Su uso no es obligatorio pero para entendimiento y estandarización muchas organizaciones lo usan.

2.1.1. Familia de normas ISO/IEC 27000

La familia de normas ISO/IEC 27000 está compuesta por una serie de normas para brindar guías metódicas orientadas para desarrollar, implementar y operar un SGSI y no dejar puntos débiles de seguridad en el sistema de una organización. Para el presente trabajo se usó como guía las siguientes normas pertenecientes a la familia de normas ISO/IEC 27000.

- Norma ISO/IEC 27000 Sistemas de Gestión de la Información – Visión de conjunto y vocabulario: visión general de un SGSI y definición de términos relacionados.
- Norma ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información – Requisitos: específica los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI.
- Norma ISO/IEC 27002 Código de Practica para los controles de seguridad de la información: proporciona una lista de objetivos de control comúnmente aceptados, así como, las mejores prácticas de seguridad para utilizarse como guía de aplicación en la selección e implementación de un SGSI.

2.1.2. Implementación de un SGSI

Para su implementación requiere la participación de todos quienes conforman una organización y su diseño depende específicamente de las necesidades y objetivos de la empresa. La norma ISO/IEC 27000 (2018, p. 12) dicta los siguientes principios fundamentales para una implementación exitosa de un SGSI:

- La conciencia de la necesidad de seguridad de la información
- La asignación de responsabilidades en seguridad de la información
- La incorporación del compromiso de la Dirección y los intereses de las partes interesadas
- La mejora de los valores sociales
- Apreciaciones de riesgos para determinar los controles adecuados para alcanzar niveles aceptables de riesgo
- La seguridad incorporada como un elemento esencial de los sistemas y redes de información
- La prevención y detección activas de incidentes de seguridad de la información
- El garantizar una aproximación exhaustiva a la gestión de la seguridad de la información
- La evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

2.2. Plan Director de Seguridad

El Plan Director de Seguridad (PDS) define y prioriza un conjunto de proyectos de seguridad de la información para reducir los riesgos de una organización a niveles aceptables. Un Plan director de Seguridad tiene objetivos, alcance, obligaciones y buenas prácticas de seguridad, que tienen que cumplir todos quienes estén relacionados con la organización. (INCIBE, n.d., p. 3)

2.2.1. Implantación de un Plan Director de Seguridad

El documento de INCIBE Plan Director de seguridad de la Colección: protege a tu empresa (INCIBE, n.d., p. 4), establece que los proyectos que componen un PDS varían en función de los siguientes factores:

- El tamaño de la organización
- El nivel de madurez en tecnología
- El sector al que pertenece la empresa
- El contexto legal que regula las actividades de la organización
- La naturaleza de la información que maneja
- El alcance del PDS, entre otros.

2.2.2. Fases de un Plan Director de Seguridad

A pesar de que existen factores que determinan un PDS, de manera general se puede definir el ciclo de la Figura 1:

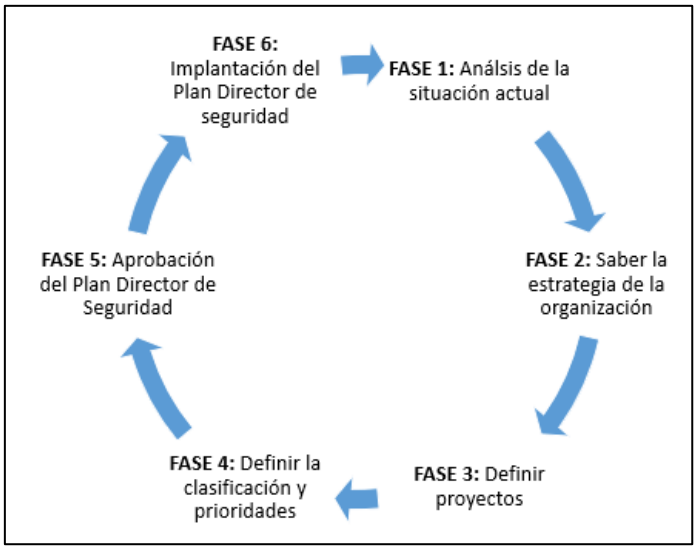

Figura 1. Etapas de un Plan Director de Seguridad.
(Fuente propia)

A continuación, se describen las fases de un Plan Director de Seguridad según el documento de INCIBE Plan Director de Seguridad, Colección: protege tu empresa (INCIBE, n.d., pp. 5-19):

FASE 1 – Análisis de la situación actual

Esta es una fase compleja porque hay que conocer la situación actual, fiable y completa de la organización en materia de ciberseguridad. En el análisis se consideran aspectos técnicos, organizativos, regulatorios, entre otros y, requiere la participación de todas las áreas de la organización.

Antes del análisis inicial, se deben realizar las siguientes actividades:

- Establecer y delimitar el alcance del Plan Director de Seguridad: puede ser un departamento, sistemas, activos, procesos más críticos, etc.
- Responsables de la gestión de los activos: es esencial definir las responsabilidades asociadas a perfiles específicos sobre los activos de información como equipos informáticos, dispositivos móviles, aplicaciones, instalaciones, servicios e información. Los perfiles de responsabilidad pueden ser: Responsable de Seguridad, Responsable de Información y Responsables de ámbitos (lógico, físico, legal y organizativo).
- Valoración inicial: realizar una valoración preliminar mediante controles técnicos, legales y organizativos para determinar en donde contrarrestar los riesgos de seguridad. Para esta valoración se puede considerar la norma ISO/IEC 27002 que contiene el Código de Buenas Prácticas.
- Análisis de cumplimiento: aunque la mayor parte de controles de ciberseguridad lo realiza el departamento TIC de una organización, es necesario la colaboración de los demás departamentos para que la información recolectada sea la más cercana a la realidad. El análisis debe cubrir todos los ámbitos de ciberseguridad, y en caso de ser necesario se registra todos los problemas y evidencias detectados. Al finalizar se puede correlacionar los resultados con una escala de cumplimiento para valorar la madures en ciberseguridad de la organización.
- Establecer los Objetivos: permite identificar cuáles serán los aspectos críticos del sistema en donde se concentrarán los esfuerzos.

Por otra parte, se requiere hacer un análisis técnico de la seguridad informática para valorar aspectos como: antivirus, firewalls, páginas web, servidores, red y accesos físicos. Es preciso realizar pruebas para identificar deficiencias en la seguridad técnica de la organización, que posteriormente serán evidencia de la eficacia de los controles de seguridad.

Dentro del análisis de la situación actual, se requiere realizar un Análisis de Riesgos a los que está expuesta la organización, para esto se requiere de las siguientes etapas:

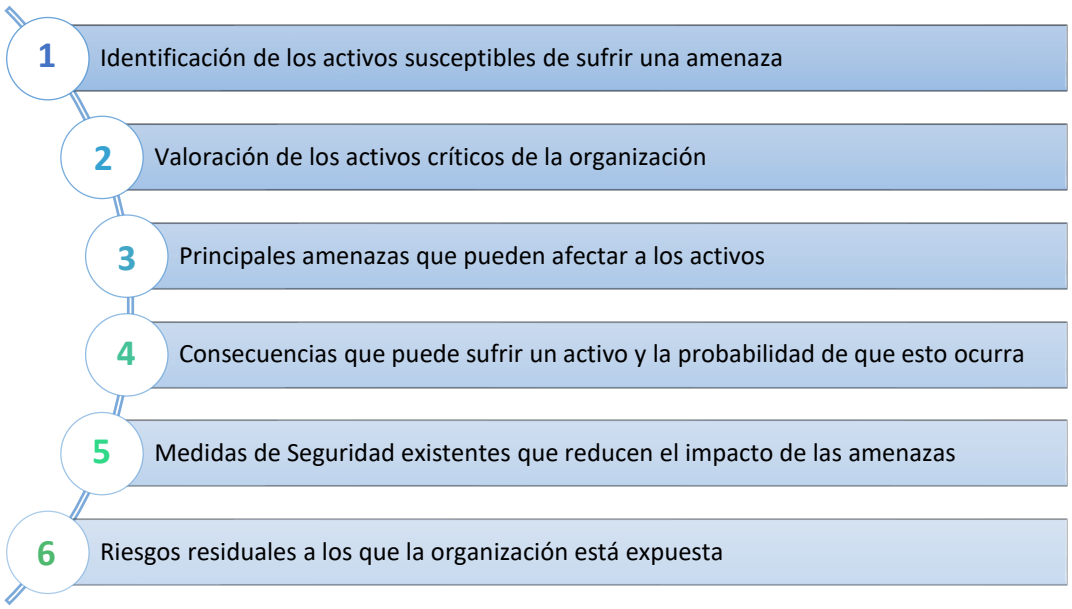

Figura 2. Etapas de un Análisis de Riesgos.
(Fuente propia)

Para el análisis de riesgos existen varias metodologías para el desarrollo de los pasos mostrados la Figura 2, y sus resultados están enfocados a identificar los riesgos que exceden los límites aceptables de una organización.

FASE 2 – Saber la estrategia de la organización

Esta fase considera los proyectos actuales y futuros teniendo en cuenta los planes de crecimiento de la organización, externalización de servicios, inicio de otra actividad, etc. Todos estos factores afectan a la orientación de las medidas y que su implantación sea acorde a las necesidades de la organización.

FASE 3 – Definir proyectos

En esta fase se definen los proyectos necesarios para alcanzar el nivel de seguridad establecido por la organización. Las primeras acciones están dirigidas a mejorar los métodos actuales de trabajo, las segundas acciones estarán relacionadas con los controles técnicos y físicos ausentes o ineficientes y, finalmente las últimas acciones están dirigidas para gestionar los riegos por encima del nivel aceptable de la organización.

FASE 4 – Definir la clasificación y prioridades

Después de identificar los proyectos y acciones que requiere la organización, es conveniente realizar una priorización considerando criterios como el origen y el tipo de acción. Pero también se pueden considerar aspectos como el esfuerzo, coste y plazo que requiere la implementación de un proyecto.

FASE 5 – Aprobación del Plan Director de Seguridad

Esta fase requiere realizar una última revisión al Plan Director de Seguridad especialmente de su alcance, duración y prioridad para que finalmente sea aprobado por la Dirección de la organización. Una vez aprobada, el siguiente paso es socializar a los empleados para que conozcan su importancia y estén dispuestos a colaboración con su implantación.

FASE 6 – Implantación del Plan Director de Seguridad

En este punto las empresas organizan la implementación del PDS y se pueden considerar los siguientes aspectos para el éxito del proyecto:

- Presentación general del proyecto a las personas y departamentos implicados
- Asignar responsabilidades y coordinadores para cada proyecto establecido
- Establecer un método de seguimiento de los proyectos
- Realizar un proceso de retroalimentación con auditoras identificando los riesgos subsanados.

2.3. Metodología MAGERIT

INCIBE como Instituto Nacional de Ciberseguridad de España provee mucha información referente al Plan Director de Seguridad, dentro del cual describe las principales metodologías de análisis de riesgos utilizadas en España y recomendadas por la ENISA (European Union Agency for Network and Information Security (2005-19a):

- MAGERIT v3
- OCTAVE
- CRAMM
- MEHARI
- SP800-30

Para el presente Trabajo Fin de Máster opté por usar la metodología MAGERIT v3, que es una de las más conocidas y empleadas dentro del país. La documentación de MAGERIT (3 libros) está disponible en el Portal de Administración Electrónica de España (PAe).

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) en su versión 3.0 está estructurado por tres libros. El primero denominado Método contiene fundamentos teóricos y guisas prácticas básica para realizar un análisis y gestión de riesgos. El segundo denominado Catálogo de Elementos contiene criterios estándar para definir: clases de activos, dimensiones de valoración, criterios de valoración, amenazas típicas y garantías. El tercero denominado Guía de Técnicas contiene algunas técnicas para realizar un análisis y gestión de riesgos. (European Union Agency for Network and Information Security, 2005-19b)

La metodología MAGERIT siguiendo la normativa ISO 31000 propone un Proceso de Gestión de Riegos para la toma de decisiones dentro de una organización derivado de los riegos que conlleva usar tecnologías de la información. Con este proceso MAGERIT pretende cubrir todo ámbito para no dejar lugar a la improvisación y así cumplir con el objetivo principal que es proteger a la organización teniendo en cuenta las principales dimensiones y subdimensiones de la seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. (Amutio, et al., 2014, p. 7)

2.3.1. Método de análisis de riesgos

El análisis de riesgos que propone MAGERIT (Amutio, et al., 2014, p. 20) contiene varios elementos entrelazados como se ve en la Figura 3 y que están estructurados por los siguientes pasos:

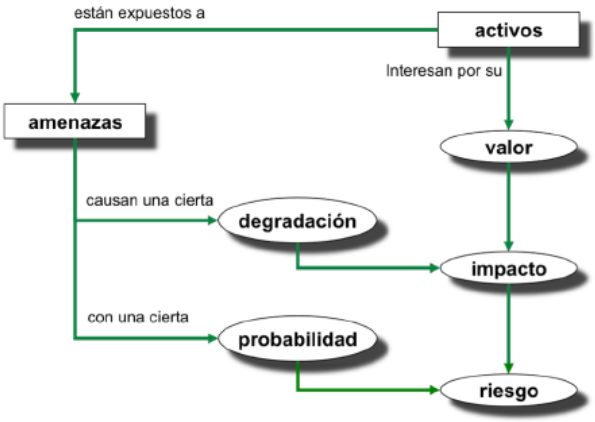

Figura 3. Elementos del análisis de riesgos potenciales.
(Fuente MAGERIT LIBRO I - Método, p. 22)

A continuación se describen todos los pasos del método de análisis de riesgos propuesto por MAGERIT y descritos en su primer libro Método, The Method en su título en inglés (Amutio, et al., 2014).

Paso 1: Determinar los Activos

Un activo es un componente o funcionalidad del sistema de una organización. De todos los activos los esenciales son: la información y los servicios, y de estos se derivan otros grupos de activos detallados en el segundo libro de la Metodología Magerit – Catálogo de Elementos que indica a detalle los grupos y tipos de activos (Amutio Gómez, et al., 2012, pp. 7-13):

- **Datos:** materializan la información.
- **Servicios auxiliares:** servicios necesarios para poder organizar el sistema.
- **Las aplicaciones informáticas (software):** permiten manejar los datos.
- **Los equipos informáticos (hardware):** permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información:** dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar:** complementan el material informático.
- **Las redes de comunicaciones:** permiten intercambiar datos.
- **Las instalaciones:** acogen equipos informáticos y de comunicaciones.
- **Las personas:** explotan u operan todos los elementos anteriormente citados.

Al determinar los activos también se establecen las dependencias entre ellos, creando un árbol de dependencia en donde los activos que están en lo más alto del árbol dependen de los que están en la parte inferior. Aunque muchos activos siempre dependen de otros, el árbol de dependencias cambia según las características de cada organización.

Consecutivamente, a cada activo se le asigna una valoración para determinar cuál es el nivel de protección que se debe aplicar para dicho activo. La valoración también se hace en base al árbol de dependencias pues algunos activos pueden acumular el valor de los activos que se apoyan en ellos.

Conociendo la valoración de cada activo, se determina el impacto que puede provocar un incidente en dicho activo en todas las dimensiones de seguridad. El primer libro de la metodología MAGERIT define 5 dimensiones de seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Para cada activo de debe analizar todas las demisiones y determinar un valor de coste que supone recuperarse de un incidente. El valor de coste puede ser cuantitativo o cualitativo respetando los criterios de homogeneidad y relatividad.

La valoración cualitativa se puede determinar a través de escalas cualitativas asignando un valor a un activo respecto de los demás. La valoración cuantitativa es la suma de valores numéricos que corresponden a una serie de criterios que compara lo que se arriesga con lo que cuesta la solución. Existe un caso especial, la dimensión de la disponibilidad requiere muchas veces de un análisis más profundo para determinar el valor de interrupción de un servicio.

Paso 2: Amenazas

En este paso se determina cuáles son las cosas que pueden ocurrir a un activo y causar daño al activo o al sistema. Las amenazas típicas a las que puede estar expuesto un activo son: de origen natural, del entorno (origen industrial), defectos de las aplicaciones, causadas por personas de forma accidental y causada por personas de forma delibera.

No todas las amenazas afectan a un activo y tampoco una amenaza afecta a todas las dimensiones de seguridad de un activo. Por eso, es necesario tener claro cuál es la amenaza, a que activo y a que dimensión afecta. Para lograr una adecuada valoración de las amenazas se considera el grado de degradación de los activos y probabilidad de materialización la amenaza, como se muestra en la siguiente figura 4:

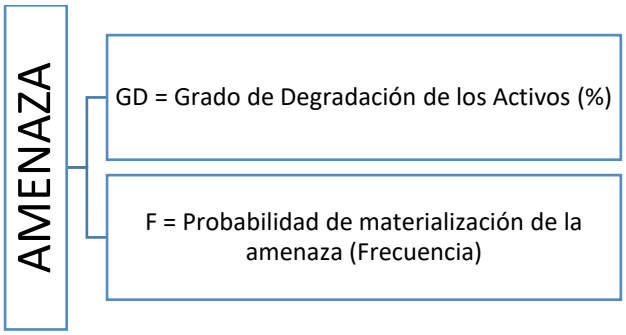

Figura 4. Elementos para la valoración de una amenaza. (Fuente propia)

Paso 2.1: Determinación del impacto potencial

Para determinar el impacto potencial de una amenaza se considera el valor de las dimensiones de un activo y la degradación que causa si una amenaza se materializa. Se calcula así dos impactos. El primero es el impacto acumulado que se determina con su valor acumulado y las amenazas a las que está expuesto; se calcula para cada activo, por cada amenaza y en cada dimensión de valoración. El segundo es el impacto repercutido que se determina con su valor propio y las amenazas que afectan a los activos de los que depende; se calcula para cada activo por cada amenaza y en cada dimensión de valoración.

Paso 2.2: Determinación del riesgo potencial

Considerando el impacto de las amenazas sobre los activos y su probabilidad de ocurrencia, se determina el riesgo. Se distinguen 4 zonas en donde pueden estar ubicados los riesgos: riesgos muy probables y de muy alto impacto, desde situaciones improbables y de impacto medio hasta situaciones muy probables pero de impacto bajo, riesgos improbables y de bajo impacto, y riesgos improbables pero de muy alto impacto.

El riesgo puede ser acumulado o repercutido. El riesgo acumulado se calcula en base al impacto acumulado debido a una amenaza y su probabilidad; cálculos para cada activo, por cada amenaza y en cada dimensión de valoración. El riesgo repercutido se calcula en base al impacto repercutido debido a una amenaza y su probabilidad; cálculos para cada activo, por cada amenaza y en cada dimensión de valoración.

Paso 3: Salvaguardas

Los pasos anteriores se desarrollan considerando que no existe protección y sin considerar las salvaguardas existentes en la organización, para seleccionar las salvaguardas. Para la selección adecuada de las salvaguardas, ningún aspecto desarrollado con los pasos anteriores se descarta pero se debe centrar en aquellos activos esenciales, y en las amenazas con alta ocurrencia y alto impacto. Además, existen salvaguardas que no aplican por ser técnicamente inadecuadas o que no se justifican cuando es desproporcional al riesgo.

Las salvaguardas ofrecen protección a los activos y consigue dos efectos: reducir la probabilidad de las amenazas y limitar su daño. Los tipos de protección son: protección, disuasión, eliminación, minimización del impacto, corrección, recuperación, monitorización, detección, concienciación y administración.

Las salvaguardas se caracterizan por su eficacia frente al riesgo que se evalúa desde dos puntos de vista: técnico (si es idónea, si se emplea siempre) y operación (despliegue, configuración y mantenimientos, procedimientos, formación de usuarios y controles de fallo). El segundo libro Catálogos de Elementos contiene el listado de las salvaguardas propuestas por la metodología Magerit.

Paso 4: Impacto Residual

Después de desplegadas las salvaguardas con su respectivo proceso de gestión, el nivel de degradación del sistema disminuye según la eficacia de las salvaguardas, por lo que, se repiten los cálculos de impacto y el resultado será el imparto residual.

Paso 5: Riesgo Residual

Desplegadas las salvaguardas y su respectivo proceso de gestión, el nivel de degradación del sistema y la probabilidad de las amenazas disminuyen según la eficacia de las salvaguardas, por lo que, se repiten los cálculos de riesgo y el resultado será el riesgo residual.

2.4. Caso de Estudio: APSA

El presente trabajo consiste en un estudio de cómo realizar un Plan Director de Seguridad y su aplicación a un caso real: la asociación APSA.

La asociación APSA es una Organización no gubernamental para el desarrollo (ONGD) creada en 1961 para ayudar en todas las etapas de vida de una persona con diferentes capacidades. Su objetivo principal es acompañar y apoyar a sus usuarios y sus familias, favoreciendo al máximo su autonomía y el desarrollo de su potencial. Dispone de programas de prevención, atención temprana, educación, salud, formación, vivienda, ocio y empleo, orientados a facilitar su inclusión social y laboral. Su misión es “mejorar la calidad de vida de aquellas personas con discapacidad intelectual o riesgo de presentarla, la de su familia y su entorno”. Su visión es “ser una entidad que se enraíza en su pasado y se proyecta hacia su futuro con vocación innovadora y dinámica, prestando atención a las necesidades de sus socios y a las demandas de la sociedad, asumiendo nuevos desafíos y siendo fieles a su misión”. (Asociación APSA, 2019)

APSA está compuesto por varios centros o sedes de actividades y servicios para personas con discapacidad y tres centros especiales de empleo: Avícola Aguamarga, Limencop y Terramar. Mediante estas sedes atiende alrededor de 2000 personas al año en diversas localidades de la provincia de Alicante. Para ello, cuenta con más de 350 trabajadores de los cuales 200 son personas con discapacidad. (González Mataix, 2018, p. 19)

Los servicios que APSA ofrece a sus usuarios dependen de la etapa de vida en la que se encuentren. Sus servicios están divididos para cubrir 4 etapas: Educativa (de 0 a 16 años), Transición a la Vida Adulta (de 16 a 26 años), Vida Adulta (de 26 a 65 años) y Tercera Edad (a partir de 65 años). Dentro de cada etapa ofrece distintos servicios en sus centros para cumplir con su objetivo de mejorar la calidad de vida de sus usuarios. (González Mataix, 2018, p. 19)

Para lograr ofrecer servicios adecuados a sus usuarios, APSA usa muchos recursos económicos, tecnológicos y de personal. Para mejorar todos los procesos que usan estos recursos, es necesario una innovación de las tecnologías de la información (TI) de la asociación. Esta innovación de las TI debe ejecutarse con responsabilidad pues, se pueden abrir nuevas brechas

de seguridad, por lo que siempre debe ir de la mano de la ciberseguridad. La innovación de APSA se empezó hace algunos años y continúa haciéndolo con el objetivo de ofrecer nuevos servicios y mejorar los actuales.

De ahí nace la necesidad de APSA de tener un Plan Director de Seguridad, que le permita conocer cuál es su situación actual en Seguridad Informática de la asociación, cuáles son sus vulnerabilidades y riesgos, y las acciones que hay que mantener, mejorar o implementar para que el impacto de los riesgos sea el mínimo posible. APSA se puede ver beneficiado con este trabajo y proteger sus activos de manera adecuada, por lo que el objetivo principal del presente TFM es Desarrollar un Plan Director de Seguridad para la asociación APSA.

3. Proceso de elaboración del Plan Director de Seguridad

Esta sección describe como se obtuvieron los datos e información para cada uno de los pasos que conforman un Plan Director de Seguridad. Incluye todos los aspectos y consideraciones que se analizaron para realizar valoraciones de riesgos, amenazas e impacto, así como, para decidir las salvaguardas y planes de seguridad.

3.1. Contexto de la Organización

A continuación se describen todos los aspectos generales que se obtuvieron para las actividades de APSA y como esta organizada.

3.1.1. Presentación

En la presentación se realizó una breve descripción de los orígenes de la asociación APSA, visión y misión. También se describió cuáles son los servicios que ofrecen a sus usuarios socios, y una perspectiva general de su estructura, centros, oficinas y sedes. Toda esta información se obtuvo de su página web, mediante entrevistas al personal del departamento TIC, así como del Trabajo previo de fin de Grabo de la Auditoría TI en la Asociación APSA de Paula González.

3.1.2. Estructura

En esta sección se describió la estructura organizacional de APSA. Se detalla cómo está constituida, cuáles son sus áreas y departamentos. Toda esta información se obtuvo del Trabajo previo de fin de Grabo de la Auditoría TI en la Asociación APSA y también mediante entrevistas con personal.

3.1.3. Sedes y servicios

Se realizó una descripción de cómo está constituida la asociación, cuáles son las actividades y servicios que ofrece a sus usuarios. Esta sección es importante pues refleja cuáles son los puntos estratégicos de la asociación y en base a esto, decidir en qué áreas implementar con mayor énfasis las medidas de seguridad. En este sentido, de APSA se recopiló información de sus sedes y centros de trabajo con la distribución de los servicios que allí se frecen de a acuerdo con la etapa de vida de sus usuarios. En APSA a las sedes se les nombra de acuerdo con su ubicación y en el presente trabajo también se las nombra de la misma manera.

3.2. Antecedentes

A continuación se describen todos los aspectos técnicos generales que se obtuvieron para conocer la situación inicial de la Asociación APSA en el área informática.

3.2.1. Aspectos Técnicos

Los aspectos técnicos abordan la información de cómo está constituido APSA en un contexto más técnico. En base a la información obtenida del trabajo de Auditoría de APSA y actualizando dicha información con entrevistas al personal del departamento TIC, este apartado contiene:

- Infraestructura: Se habla de la infraestructura tomando en cuenta servicios y servidores (físicos y en Cloud). Igualmente se recoge información de bases de datos y las aplicaciones que se usan en la asociación.
- Hardware y puestos de trabajo: De manera general se describe el hardware que se usa en la asociación para cumplir con sus actividades diarias, así como, la asignación de los puestos de trabajo en cada una de sus sedes.
- Servicios subcontratados: Como en muchas organizaciones, existen servicios que se subcontratan con empresas externas. APSA subcontrata algunos de los servicios que requiere para el desarrollo de sus actividades diarias y que se detallan en los servicios subcontratados.

3.2.2. Estado inicial de la seguridad informática

Este es uno de los aspectos más importantes dentro del Plan Director de Seguridad, pues es el punto de partida para el análisis de la asociación. Para evaluar la situación actual de la seguridad informática de APSA se usó una herramienta Ofimática en Excel disponible en la página web del Instituto Nacional de Ciberseguridad de España (INCIBE, 2019). La herramienta consiste en un conjunto de preguntas que evalúan la seguridad informática y, abarcan todos los controles que se sugieren evaluar y analizar en base al Anexo A de las normas ISO 27001 del año 2017.

Los criterios de evaluación son 8 y se los identifica con un color dependiendo de la gravedad del estado actual del control. Después estos datos son evaluados en conjunto y se muestra un porcentaje total de los estados actuales de la seguridad informática de APSA (INCIBE, 2019). A continuación se muestra los criterios de evaluación usados y su significado:

- **Desconocido:** No ha sido verificado.
- **Inexistente:** No se lleva a cabo el control de seguridad en los sistemas de información.

- **Inicial:** Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
- **Repetible:** La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
- **Definido:** El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
- **Administrado:** El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.
- **Optimizado:** El control se aplica de acuerdo con un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
- **No aplicable:** A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Los 14 controles que se utilizaron son los objetivos de control y controles de referencia que figuran en los capítulos del 5 al 18 de la Norma ISO/IEC 27002 (Asociación Española de Normalización, 2017, pp. 12-113), y son:

- **Políticas de seguridad de la información:** Directrices de gestión de la seguridad de la información.
- **Organización de la seguridad de la información:** Organización interna, los dispositivos móviles y el teletrabajo.
- **Seguridad relativa a los recursos humanos:** Antes del empleo, durante el empleo y finalización del empleo o cambio en el puesto de trabajo.
- **Gestión de activos:** Responsabilidad sobre los activos, clasificación de la información y manipulación de los soportes.
- **Control de acceso:** Requisitos de negocio para el control de acceso, gestión de acceso de usuario, responsabilidades del usuario, control de acceso a sistemas y aplicaciones
- **Criptografía:** Controles criptográficos.
- **Seguridad física y del entorno:** Áreas seguras y seguridad de los equipos.
- **Seguridad de las operaciones:** Procedimientos y responsabilidades operacionales, protección contra el software malicioso (malware), copias de seguridad, registros y

supervisión, control del software en explotación, gestión de la vulnerabilidad técnica y consideraciones sobre la auditoria de sistemas de información.

- **Seguridad de las comunicaciones:** Gestión de la seguridad de las redes e intercambio de información.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Requisitos de seguridad en los sistemas de información, seguridad en el desarrollo y en los procesos de soporte, y datos de prueba.
- **Relación con proveedores:** Seguridad en las relaciones con proveedores y gestión de la provisión de servicios del proveedor.
- **Gestión de incidentes de seguridad de la información:** Gestión de incidentes de seguridad de la información y mejoras.
- **Aspectos de seguridad de la información para la gestión de la continuidad de negocio:** Continuidad de la seguridad de la información y redundancias.
- **Cumplimiento:** Cumplimiento de los requisitos legales y contractuales y revisiones de la seguridad de la información.

Todas las preguntas usadas para la determinar la situación actual de la seguridad informática en APSA se pueden ver en el ANEXO A.

3.2.3. Políticas de seguridad de la información existentes

Como toda organización que empieza una transformación tecnológica, APSA ha ido implementando ciertas políticas de seguridad informática. La dificultad reside en que la mayoría de las políticas de seguridad que tienen implementadas hasta el momento, no están documentadas. Las políticas fueron adaptadas de acuerdo con las necesidades que surgían con el tiempo. Para esta sección se recogieron algunas de las políticas de seguridad que poseen actualmente y que surgieron al momento de realizar las preguntas del cuestionario de la herramienta usada para la evaluación inicial de la seguridad de APSA. Hay que recalcar que no son todas las políticas de seguridad, pues solo son las que surgieron en las entrevistas a los técnicos. De igual manera, hay algunas políticas que se han ido implementado mientras se desarrolló este TFM y que en esta sección no se redactaron, pero que en otras secciones del documento se las menciona.

3.3. Inventario de activos y amenazas

Para esta sección debido al gran número de datos que se obtuvieron, se creó una herramienta ofimática en Excel llamada Análisis_APSA para facilitar el manejo de los datos y los cálculos del

impacto y riesgos. Al final de cada apartado de la sección 4, se describe cómo y dónde se encuentran los datos dentro del documento ofimático.

3.3.1. Identificación de activos

Como antecedente para esta sección, APSA no posee un registro oficial de todos los activos que posee, especialmente del hardware. APSA ha crecido tecnológicamente y al no poseer un registro organizado, identificar los activos desencadeno en la realización de nuevas tareas para el departamento de TIC. La primera tarea consistió en la elaboración de un inventario completo de todo lo que APSA posee como activos según la clasificación que se propone en este trabajo. La segunda tarea fue etiquetar todo el hardware que ellos poseen. Estas tareas requieren de tiempo y de recursos humanos, pero al no contar con el personal necesario y al poseer muchos activos, estas tareas se retrasaron. Hasta el momento de la finalización de este documento las tareas se continúan realizando, y a pesar del esfuerzo que conllevan, el departamento de TIC se verá muy beneficiado de tener un inventario completo de activos para así tener un mayor control sobre ellos.

Debido a esta dificultad se optó por seleccionar los activos más importantes agrupándolos de forma general. Se evitó detallar aspectos, que aunque propone la metodología Magerit, aún no están claramente definidos dentro de la asociación. La clasificación y agrupación se realizó con la aprobación del personal del departamento de TIC. A continuación, en la Tabla 1 se muestra la ficha modelo para los activos, se describe cada uno de los grupos y cuáles son los activos que pertenecen a cada uno de ellos.

Tabla 1. Plantilla de Activos

<table>
<tr><th colspan="2">[Tipo de Activo ([D], [S], [SW], [HW], [COM], [MEDIA], [AUX], [L], [P])]</th></tr>
<tr><td>Código: Estará formado por las siglas del tipo de activo y un número único por tipo.</td><td>Nombre: Nombre asignado al Activo</td></tr>
<tr><td colspan="2">Descripción: Descripción detallada del activo (características, uso, especificaciones, etc.)</td></tr>
<tr><td colspan="2">Responsable: Personal responsable del Activo</td></tr>
<tr><td colspan="2">Tipo: En el segundo libro de la metodología MAGERIT cada tipo activo se clasifica en subtipos del segundo libro de la Metodología Magerit – Catálogo de elementos.</td></tr>
</table>

Realizado por: Jessica Montero, 2019
Fuente: (Amutio Gómez, et al., 2012, p. 60)

A continuación se detalla la definición de los tipos de activos según la metodología Magerit (Amutio Gómez, et al., 2012, pp. 8-13).

- [D] Datos/Información: los datos son lo más importante de una organización pues permite prestar sus servicios. La información (ficheros o bases de datos) es un activo abstracto que se almacena en equipos y soportes de información o transferido de un lugar a otro por los medios de transmisión de datos. Los activos que pertenecen a este grupo son: ficheros almacenados en ordenadores y servidores, bases de datos, copias de seguridad, datos de configuración, credenciales, código fuente y registros de actividades. Dentro de este grupo de activos hay que recalcar que se considerar como activos los datos dependiendo de su lugar de almacenamiento y los datos informáticos pues, la asociación APSA trabaja con una empresa externa exclusivamente para el cumplimiento del Reglamento de Protección de Datos que actualmente rige en España.
- [S] Servicios: los servicios están creados para satisfacer alguna necesidad de los usuarios. Este grupo contempla los servicios prestados por el sistema y consta de servicios como la página web, correo electrónico, servicio de ftp, intranet documenta, sistemas de incidencias.
- [SW] Software – Aplicaciones Informáticas: denominados programas o aplicaciones, esta sección se refiere a tareas automatizadas para su desempeño en un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. A este grupo pertenecen las aplicaciones internas y externas a nivel de servidores, ordenadores y dispositivos móviles.
- [HW] Equipos Informáticos (Hardware): son todos los medios materiales y físicos destinados para soportar directa o indirectamente los servicios que presta la organización, donde se almacenan los datos, se ejecutan las aplicaciones informáticas, y son responsables del procesado o transmisión de datos. Dentro de este grupo se consideran: servidores físicos, ordenadores (escritorio y portátiles), teléfonos (móviles y de escritorio), impresoras, escáneres y dispositivos electrónicos, switches y routers.
- [COM] Redes de Comunicaciones: esta sección incluye tanto instalaciones dedicadas, como servicios de comunicaciones contratados a terceros. En este grupo están: instalaciones de red, ADSL, redes inalámbricas y redes locales.
- [MEDIA] Soportes de Información: en esta sección se consideran dispositivos físicos que permiten almacenar información de forma permanente o al menos, durante largos periodos de tiempo. Este grupo consta de los activos: discos duros externos, pendrives (USB) y CD/DVD.

- [AUX] Equipamiento Auxiliar: aquí se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos. Generadores eléctricos, fuentes de alimentación, climatización, mobiliarios importantes y cableado para las redes de comunicaciones, son los activos que pertenecen a este grupo.
- [L]Instalaciones: en esta sección se encuentran los lugares donde están los sistemas de información y comunicación, es decir: edificios de las sedes, cuartos en donde se encuentran los principales equipos informáticos y vehículos que sean de uso exclusivo para el traslado del personal del departamento de TIC.
- [P] Personal: este apartado se refiere a las personas relacionadas con los sistemas de información como: operadores y administradores. En APSA son cuatro los empleados que pertenecen al departamento de TIC y que por pedido suyo sus nombres se mantendrán en anonimato, por lo tanto, se los denominó administradores y técnicos. De este grupo se nombra los responsables de los demás activos y, en caso de no existir un responsable definido o los responsables sean varios empleados se usó la abreviatura SR. Además se consideraron dos tipos más de personal, empleados y usuarios generales para evaluar sus riesgos.

Definidos los grupos, se recolecto un total de 75 activos repartidos de la siguiente manera:

- [D] Datos/Información: 13 activos
- [S] Servicios: 9 activos
- [SW] Software – Aplicaciones Informáticas: 18 activos
- [HW] Equipos Informáticos (Hardware): 14 activos
- [COM] Redes de Comunicaciones: 4 activos
- [MEDIA] Soportes de Información: 4 activos
- [AUX] Equipamiento Auxiliar: 6 activos
- [L]Instalaciones: 3 activos
- [P] Personal: 4 activos

En el documento Análisis_APSA, la primera hoja llamada Inventario contiene los grupos de tipos de activos y los activos que los integran. Para separar los grupos, se usó el estándar de colores de la Figura 5 que se usará en todo documento.

Figura 5. Estándar de colores del documento Análisis_APSA.
(Fuente propia)

En la Figura 6 se observa un ejemplo de la estructura de la tabla Inventario, en donde se observa los siguientes encabezados de las columnas: grupo, número, código, nombre, tipos, responsable, descripción y tipo de activo. Las columnas grupo y número se crearon para que la unión de estas forme un código único que identifique a un determinado activo. Las columnas nombre, tipos y descripción se crearon de acuerdo con las especificaciones de la Tabla 1. Por pedido de la asociación se mantiene en anonimato los nombres de los empleados del departamento TIC, por lo que, para la columna responsables pueden ser: administradores, técnicos o SR (sin responsable).

GRUPO	No.	CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
D	1	D1	Datos de configuración	[files][conf][int]	Administradores	Datos usados para la configuración de aplicaciones y servidores
D	2	D2	Código fuente de aplicaciones	[files][source]	Administradores	Código fuente de las aplicaciones que APSA maneja y no pertenece a ningún tercero
D	3	D3	Ficheros almacenados en PC	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en sus respectivos ordenadores
D	4	D4	Ficheros almacenados en servidores en la nube	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en los servidores de la nube mediante el servicio de Intranet Documental. Estos ficheros se pueden compartir con otros profesionales

GRUPO DE ACTIVO
[D] Datos / Información

Figura 6. Ejemplo de la tabla Inventario del documento Análisis_APSA.
(Fuente propia)

3.3.2. Dependencias de Activos

Siguiendo la Tabla 2 donde se identifica las dependencias planteadas por la metodología Magerit se elaboró un Árbol General de Dependencias de Activos.

Tabla 2. Criterios de dependencias de activos

Tipo de activo	Identificación de dependencias por:
[D] Datos / Información	• Equipos que los hospedan • Líneas de comunicación por las que se transfieren • Soportes de información • Personas relacionadas: usuarios
[S] Servicios	• Personas relacionadas: usuarios, operadores y administradores.
[SW] Software – Aplicaciones informáticas	• Personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.
[HW] Equipamiento informático (hardware)	• Personas relacionadas con este equipo: operadores, administradores • Instalaciones que lo acogen
[COM] Redes de comunicaciones	• Personas relacionadas: operadores, administradores • Instalaciones que lo acogen
[MEDIA] Soportes de información	• Personas relacionadas: operadores, administradores • Instalaciones que lo acogen
[AUX] Equipamiento auxiliar	• Personas relacionadas con este equipo: operadores, administradores
[L] Instalaciones	• Personas relacionadas con esta instalación: guardias, encargados de mantenimiento
[P] Personal	• No suelen identificarse dependencias

Realizado por: Jessica Montero, 2019
Fuente: (Amutio Gómez, et al., 2012, pp. 60-69)

El árbol de dependencias de la Figura 7 se realizó con los 9 grupos definidos en la identificación de activos y sirve de guía para definir las dependencias de todos los activos. Para simplificación del gráfico, se usó las abreviaturas de los grupos: [D] Datos/Información, [S] Servicios, [SW] Aplicaciones informáticas (Software), [HW] Equipamiento informático (hardware), [COM] Redes de comunicaciones, [MEDIA] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones y [P] Personal.

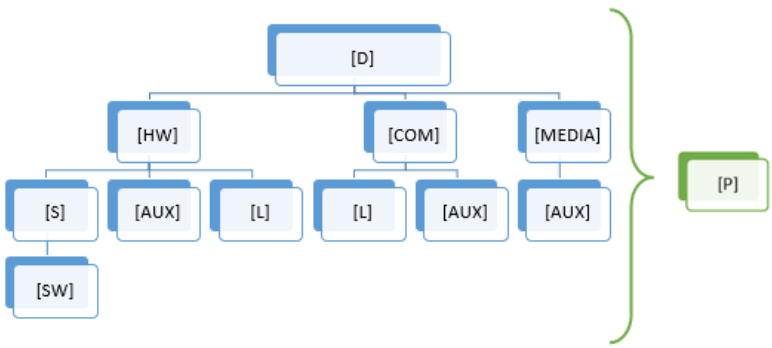

Figura 7. Árbol general de dependencias de activos para APSA.
(Fuente propia)

En la parte superior del árbol se encuentran los Datos/Información y de este se derivan los demás grupos de activos. Además, cada grupo de activo depende del personal, por eso se le colocó abarcando todos los grupos.

Después de definir el Árbol General de Dependencias, se estableció las dependencias de los activos de APSA. La metodología Magerit propone niveles de dependencias según la ubicación del activo dentro del árbol de dependientas, pero para este trabajo, solo se definieron las dependencias de nivel 1: directamente relacionadas. Entonces aunque no este escrito, se asume que un activo A, que depende directamente de un activo B, dependerá indirectamente de todos los activos de los que depende el activo B.

Para el documento Análisis_APSA, se usó el mismo estándar de colores para los tipos de activos de la Figura 5 y se usaron los siguientes encabezados de columnas para la tabla Dependencias: grupo, número, código, nombre y dependencias grado 1. Las columnas grupo, número, código y nombre son iguales que la hoja Inventario. La columna dependencias grado 1 se creó de acuerdo con las especificaciones descritas en esta sección. Un ejemplo de su estructura se puede ver en la siguiente Figura 8:

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
D1	Datos de configuración	Servidores APSA, Servidores locales
D2	Código fuente de aplicaciones	Servidores APSA, Servidores locales
D3	Ficheros almacenados en PC	Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, discos duros externos, pendrives USB
D4	Ficheros almacenados en servidores en la nube	Servidores APSA, Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, redes inalámbricas, redes locales

Figura 8. Ejemplo de la tabla Dependencias del documento Análisis_APSA.
(Fuente propia)

3.3.3. Valoración de Activos

Para la valoración de cada activo se consideraron cinco dimensiones de seguridad aunque no todas las dimensiones aplican a todos los grupos de activos. En las Figuras del 9 al 13 se describen según la metodología Magerit (Amutio Gómez, et al., 2012, pp. 15-16) la definición, razones para una valoración máxima o mínima y a que activo afecta. Todos estos aspectos se usan para evaluar las dimensiones en cada activo:

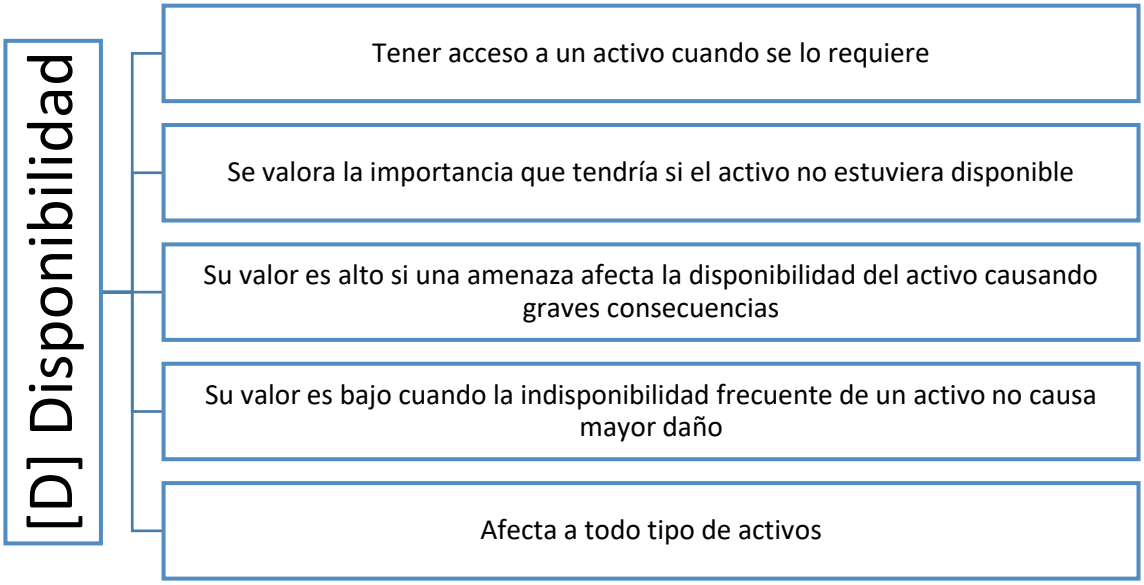

Figura 9. Consideraciones para la valoración de la disponibilidad.
(Fuente propia)

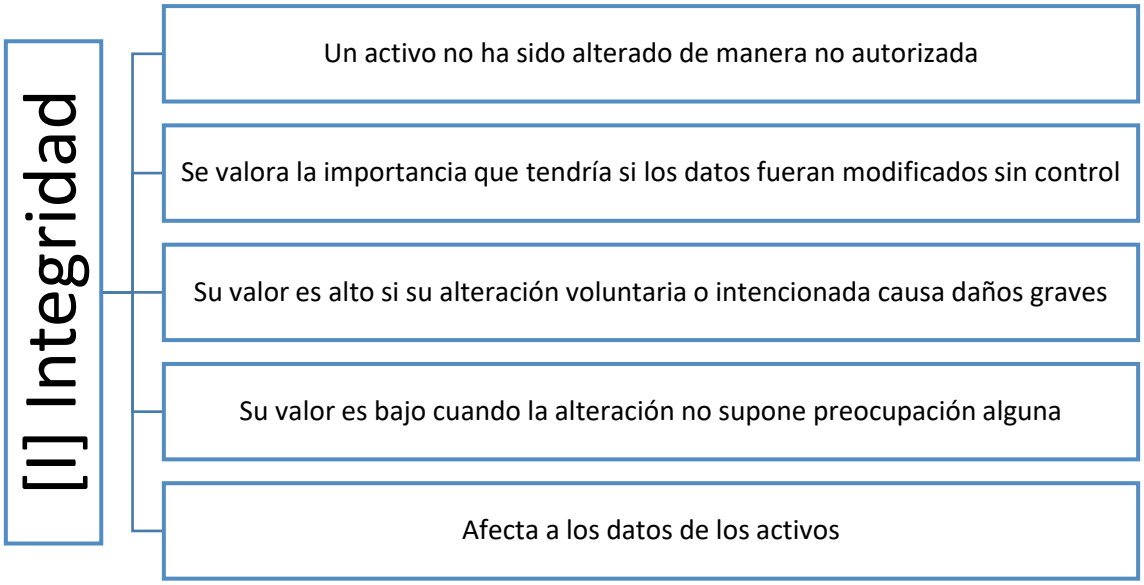

Figura 10. Consideraciones para la valoración de la integridad.
(Fuente propia)

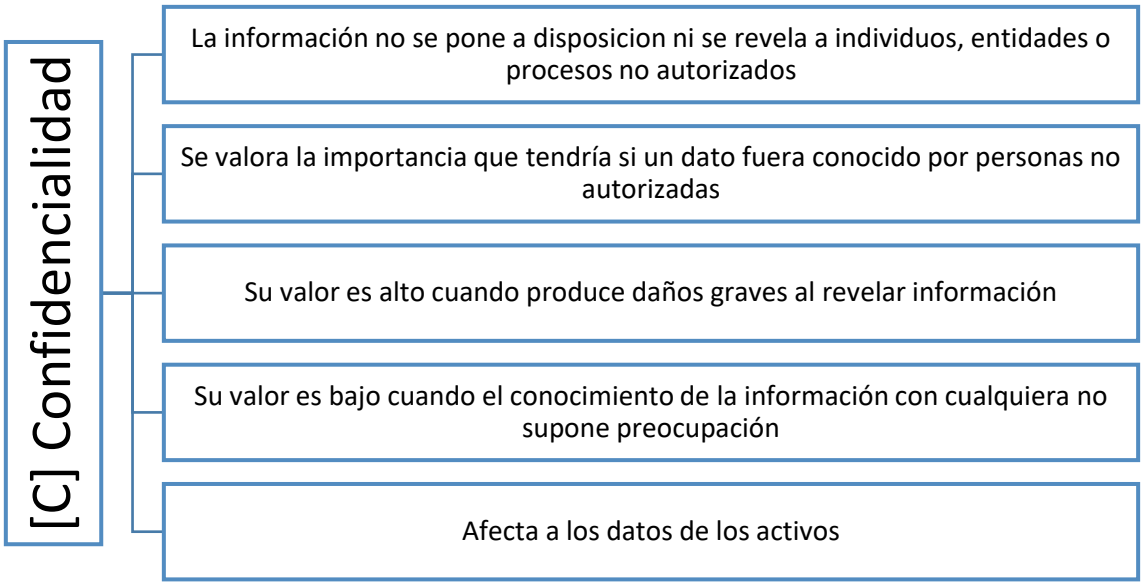

Figura 11. Consideraciones para la valoración de la confidencialidad.
(Fuente propia)

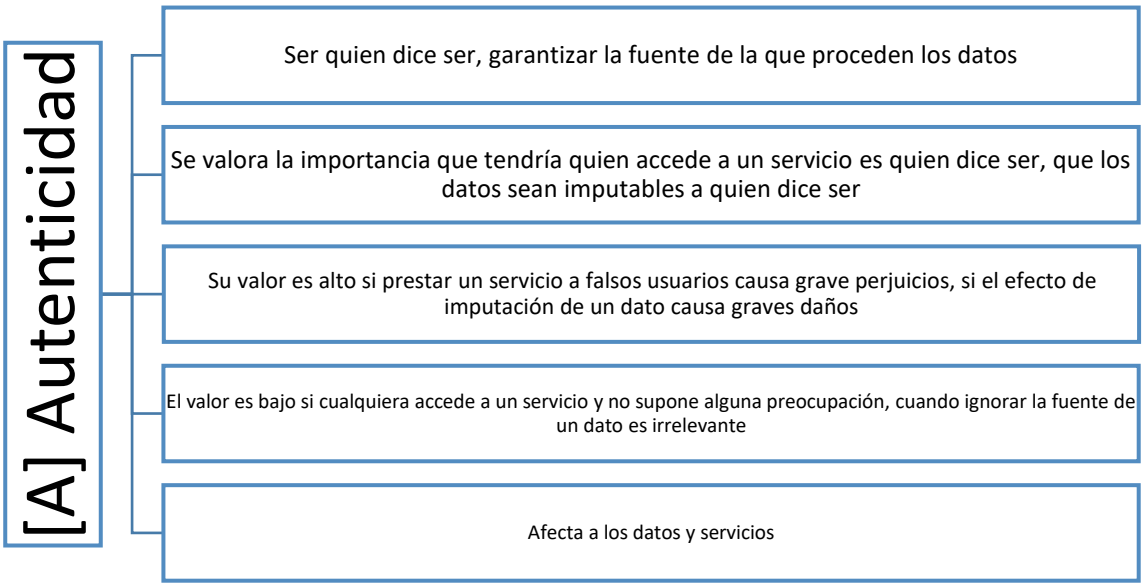

Figura 12. Consideraciones para la valoración de la autenticidad.
(Fuente propia)

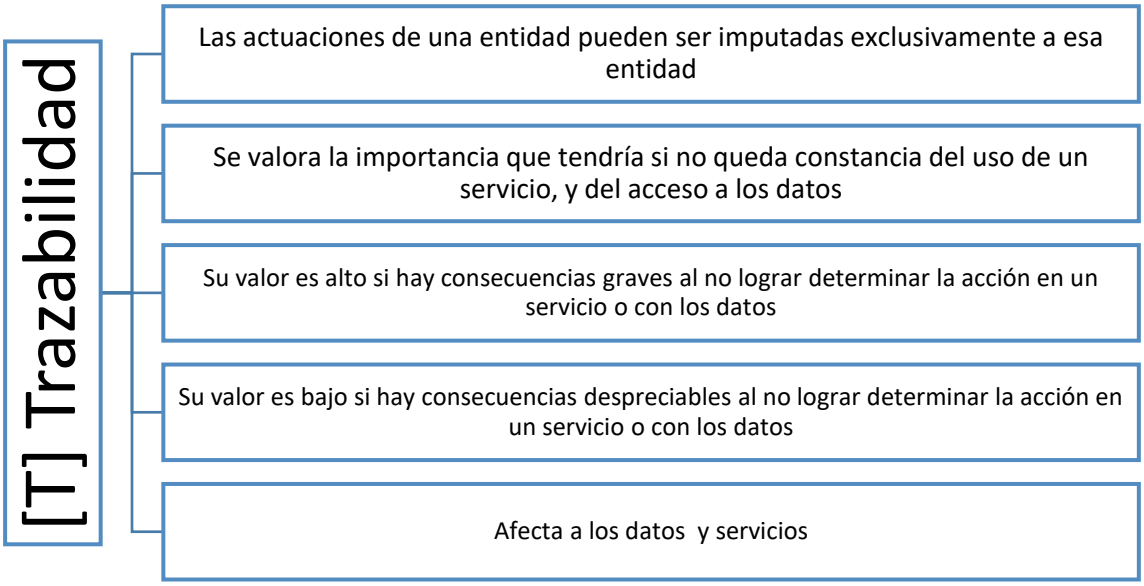

Figura 13. Consideraciones para la valoración de la trazabilidad.
(Fuente propia)

La Tabla 3 muestra la ficha modelo propuesta por la metodología Magerit para la valoración de activos en cada dimensión y que se usó de base para la valoración de activos de APSA.

Tabla 3. Plantilla de valoración de activos

Dimensión	Valor
[D]	
[I]	
[C]	
[A]	
[T]	

Realizado por: Jessica Montero, 2019
Fuente: (Amutio Gómez, et al., 2012, p. 60)

Para la valoración de cada uno de los activos se utilizó la escala de valoración de la Figura 14. La escala varía de 0 a 10, siendo 0 un daño irrelevante hasta 10 en donde el daño es extremadamente grave para la asociación. La imagen tiene colores para una mejor ilustración, siendo los tonos verdes de menor daño y tonos rojos de mayor daño.

10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
8	alto	daño grave
7		
6		
5	medio	daño importante
4		
3		
2	bajo	daño menor
1		
0	despreciable	irrelevante a efectos prácticos

Figura 14. Escala de valoración de activos.
(Fuente propia)

Para el documento Análisis_APSA, se creó una nueva hoja llamada Valoración de Activos que usa el mismo estándar de colores para los tipos de activos de la Figura 5 y los siguientes encabezados de columnas: grupo, número, código, nombre, D (disponibilidad), I (integridad), C (confidencialidad), A (autenticidad) y T (trazabilidad). Las columnas grupo, número, código y nombre son iguales que la hoja Inventario. Las siguientes columnas corresponden a las dimensiones de seguridad que se evaluaron para cada activo. La Figura 15 muestra un ejemplo de la valoración de activos.

CÓDIGO	NOMBRE	D	I	C	A	T
D1	Datos de configuración	8	8	8	9	9
D2	Código fuente de aplicaciones	8	9	8	9	9
D3	Ficheros almacenados en PC	3	7	5	6	7
D4	Ficheros almacenados en servidores en la nube	5	7	7	8	8
D5	Ficheros almacenados en servidores locales	5	7	7	8	8
D6	Bases de datos en servidores locales	8	9	9	9	9
D7	Bases de datos en servidores en la nube	9	9	9	9	9
D8	Copias de seguridad en la nube	9	8	9	9	9

Figura 15. Ejemplo de la Valoración de activos del documento Análisis_APSA.
(Fuente propia)

3.3.4. Determinación de amenazas

La metodología Magerit (Amutio Gómez, et al., 2012, pp. 25-48) clasifica a las amenazas en 4 grupos, integrados por una lista de amenazas con distinto origen que pueden afectar a un activo. Los grupos son:

- [N] de origen natural: son amenazas que ocurren sin intervención humana. Se contemplan todos los desastres naturales.

- [I] de origen industrial: son amenazas que pueden ocurrir derivadas de actividades industriales. Aquí no solo se contempla las amenazas que ocurren accidentalmente, sino también las que ocurren de manera deliberada.
- [E] errores y fallos no intencionados: Errores de personas causados de forma no intencional. Los errores son de origen humano accidental.
- [A] ataques intencionados: amenazas causadas por personas de manera deliberada. Los ataques son premeditados y de origen humano.

Una amenaza cuando se materializa afecta en distinto nivel a las dimensiones de seguridad de un activo, por este motivo se realizó una tabla en el documento Análisis_APSA, en donde se enlista todas las amenazas y a que dimensión afecta según los tipos de activos. Las tablas están realizadas de acuerdo con lo propuesto en la metodología Magerit y sirven de guía para la elaboración de las tablas de cada grupo de activos. Para ver la lista completa de amenazas y a que dimensión de seguridad de los tipos de acticos afecta, ver el Anexo B.

La Figura 16 es una muestra de la tabla completa de cruce de información entre amenazas, dimensiones y grupos de activos.

AMENAZA	TIPO	Datos/Informac ión [D]					Servicios [S]					Software - Aplicaciones [SW]					Equipamiento Informático [HW]					Redes de Comunicacion [COM]					Soportes de Información [MEDIA]					Equipamiento Auxiliar [AUX]					Instalaciones [L]					Personal [P]				
		D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
Daños por agua	N2																X										X					X					X								
Fenómeno climático	N3																X										X					X					X								
Fenómeno sísmico	N4																X										X					X					X								
Fuego	I1																X										X					X					X								
Daños por agua	I2																X										X					X					X								
Contaminación mecánica	I3																X										X					X												
Avería de origen físico/lógico	I4											X					X										X					X												
Corte de suministro eléctrico	I5																X										X					X												
Fallas de climatización	I6																X										X					X												
Fallo servicios de comunicaciones	I7																					X																						
Interrupción de otros servicios y suministros esenciales	I8																															X												
Degradación de los soportes de almacenamiento de la información	I9																										X																		
Emanaciones electromagnéticas	I10																		X										X					X												
Errores de usuarios	E1	X	X	X			X	X	X			X	X	X													X	X	X																
Errores de administración	E2	X	X	X			X	X	X			X	X	X			X	X	X			X	X	X			X	X	X																
Errores de monitorización log	E3		X			X																																							
Errores de configuración	E4		X																																										
Difusión de software dañino	E6											X	X	X																														
Errores de (re)encaminamiento	E7								X					X										X																				
Errores de secuencia	E8							X					X										X																					
Alteración accidental de la información	E10		X					X					X										X					X											X					
Destrucción de información	E11	X					X					X										X					X											X						
Fugas de información	E12			X					X					X										X					X											X				
Vulnerabilidades de los programas	E13											X	X	X																														
Errores de mantenimiento/actualización de programas	E14											X	X																															
Errores de mantenimiento/actualización de equipos	E15																X										X					X												
Caída del sistema por agotamiento de recursos	E16						X										X					X																						
Perdida de equipos	E17																X		X								X		X			X		X										

Figura 16. Muestra de la tabla de amenazas.
(Fuente propia)

La tabla Amenazas se usó como guía para determinar las amenazas que tiene cada uno de los grupos de activos, pero como cada grupo está integrado por varios activos con características diferentes, no se considera todas las amenazas para todos los activos de un grupo. Por otro lado, aunque una amenaza puede afectar a un activo, para la realidad de APSA esa amenaza puede tener una probabilidad de ocurrencia demasiado baja, por lo que no se consideran para el análisis. Es así como, para tener mejores resultados y cercanos a la realidad de la asociación, se realizó una selección de las amenazas por cada activo de cada grupo.

En el documento Análisis_APSA se creó una tabla en una hoja única por cada tipo de activo, en el que se agregan columnas según se desarrolle el análisis. Así, cada tabla consta de las cabeceras de columnas: grupo, número, código, nombre, amenazas, frecuencia, degradación, valor del activo, impacto, riesgo, salvaguardas, efectividad de salvaguardas, efectividad de frecuencia, frecuencia residual, impacto residual y riesgo residual. Las columnas de grupos, número y código son igual que la hoja Inventarios. El contenido de las demás columnas se explica más adelante.

Para un uso didáctico, las amenazas se agrupan dependiendo de su origen y para diferenciarlos se usa una gama de colores que va de claro a obscuro dependiendo del color que identifica el tipo de activo. La Figura 17 corresponde a un ejemplo de la determinación de amenazas. En este caso se trata de un activo del tipo equipamiento auxiliar con el color verde claro y sus amenazas están identificadas con gramas de dicho color.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			
Código	Nombre	Amenaza	
AUX1	Generador eléctrico	Daños Por Agua	Naturales
		Fuego	Industriales
		Daños Por Agua	
		Contaminación Mecánica	
		Degradación por almacenamiento	
		Avería De Origen Físico/ Lógico	
		Errores De Mantenimiento/ Actualización De Equipos	Errores
		Uso No Previsto	Ataques
		Acceso No Autorizado	
		Manipulación De Equipos	

Figura 17. Ejemplo de la determinación de amenazas.
(Fuente propia)

El siguiente paso fue la evaluación de cada amenaza en el caso de materializarse. Para este análisis se determinó:

- La frecuencia de ocurrencia: con cuanta periodicidad sucede determinada amenaza en APSA. Para este cálculo se realizaron las preguntas pertinentes a los administradores del departamento TIC, con quienes se determinó el valor más adecuado para la frecuencia. Para ciertos activos, aunque no han ocurrido algunos errores o ataques, al ser muy conocidos se valoraron con una frecuencia de ocurrencia baja. En la Figura 18, se muestra la escala de valoración para la frecuencia de ocurrencia, que varía desde 0,1 a 1. Para el caso de APSA ciertas amenazas no suceden con regularidad por lo que, la escala de valoración no se puede relacionar con periodos de tiempo determinados como lo sugiere la metodología Magerit.

Muy frecuente	1
frecuente	0,7
normal	0,5
poco frecuente	0,3
muy poco frecuente	0,1

Figura 18. Escala de valoración para la frecuencia de ocurrencia de una amenaza. (Fuente propia)

- El grado o nivel de impacto: Esta valoración es el nivel de degradación de un activo si una amenaza se materializa. La escala de valoración usada es la de la Figura 19. Esta escala tiene 5 niveles de impacto, siendo 5% un impacto muy bajo, 50% impacto medio y 100% el impacto muy alto. La valoración se hace para cada dimensión de seguridad de cada activo. Como lo recomienda la metodología Magerit, dependiendo del activo, algunas de las valoraciones de las amenazas no se realizaron directamente sobre el activo, si no sobre la información que maneja el activo.

Muy alto	100%
Alto	75%
Medio	50%
Bajo	25%
Muy bajo	5%

Figura 19. Escala de valoración del grado de impacto de una amenaza. (Fuente propia)

Las valoraciones anteriores se realizaron sin tener en cuenta las políticas de seguridad que actualmente tiene APSA, porque serán consideradas dentro de las salvaguardas y por tanto en los cálculos del impacto y riesgo residuales.

Para el documento Análisis_APSA los valores de la frecuencia y el grado de impacto se colocan en las columnas frecuencia y degradación respectivamente. La columna degradación se subdivide en 5 columnas que corresponden a las dimensiones de seguridad que afectan a un activo dependiendo de la tabla general de la hoja Amenazas. Para identificarlos se usarán los mismos colores definidos para las amenazas.

En la Figura 20, se observa un ejemplo de un activo y las amenazas que lo afectan con su respectiva frecuencia de ocurrencia y degradación en las 5 dimensiones de seguridad.

DATOS / INFORMACIÓN [D]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	0,3	75%	75%	25%		
		Errores De Configuración	0,3		50%			
		Alteración Accidental De La Información	0,3		50%			
		Destrucción De Información	0,3	100%				
		Fugas De Información	0,1			50%		
		Manipulación De Los Registros De Actividad	0,1		5%			75%
		Manipulación De La Configuración	0,1		100%	100%	100%	
		Abuso De Privilegios De Acceso	0,1	75%	75%	75%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		75%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				

Figura 20. Ejemplo de un activo con sus amenazas, frecuencia y degradación (Fuente propia)

3.4. Impacto y Riesgos

Para esta sección se consideraron todas las fórmulas de cálculo que propone la metodología Magerit para un análisis cuantitativo.

3.4.1. Cálculos para el impacto potencial

Determinada la frecuencia de ocurrencia y la degradación que causa una amenaza, se realizó el cálculo del impacto potencial o impacto repercutido con la fórmula:

$$IP = VA * GD$$

Donde:

IP = Impacto potencial

VA = Valor del activo

GD = Grado de degradación de los activos (%)

Según la fórmula anterior, para el cálculo del impacto potencial se requiere de la valoración de los activos por lo que, en el documento Análisis_APSA se agregó una columna llamada Valor de activo. Dicha columna contiene los mismos valores definidos en la hoja Valoración de Activos del documento.

Con los datos necesarios, en el documento Análisis_APSA se creó la columna Impacto que contiene el valor de los cálculos para el impacto potencial. El resultado del impacto potencial se realizó sin tener en cuenta las políticas de seguridad que tiene APSA, ya que serán consideradas dentro de las salvaguardas y por tanto, en los cálculos del impacto y riesgo residuales. En algunas ocasiones el valor del impacto potencial no existe y se debe a que una amenaza no siempre afecta a todas las dimensiones de seguridad de la asociación. En la Figura 21 se observa un ejemplo de la estructura de la tabla de un activo hasta el cálculo del impacto potencial.

DATOS / INFORMACIÓN [D]			Frecuencia	Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	0,3	75%	75%	25%			8	8	8	9	9	6	6	2		
		Errores De Configuración	0,3		50%				8	8	8	9	9		4			
		Alteración Accidental De La Información	0,3		50%				8	8	8	9	9		4			
		Destrucción De Información	0,3	100%					8	8	8	9	9	8				
		Fugas De Información	0,1			50%			8	8	8	9	9			4		
		Manipulación De Los Registros De Actividad	0,1		5%			75%	8	8	8	9	9		0,4			6,75
		Manipulación De La Configuración	0,1		100%	100%	100%		8	8	8	9	9		8	8	9	
		Abuso De Privilegios De Acceso	0,1	75%	75%	75%			8	8	8	9	9	6	6	6		
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	9		6	8		
		Repudio	0,1		75%			100%	8	8	8	9	9		6			9
		Modificación Deliberada De La Información	0,1		100%				8	8	8	9	9		8			
		Destrucción De Información	0,1	100%					8	8	8	9	9	8				

Figura 21. Ejemplo de un activo calculado el impacto potencial.
(*Fuente propia)*

3.4.2. Cálculos de riesgo potencial

Teniendo el impacto potencial, se procedió al cálculo del riesgo potencial o riesgo repercutido con la fórmula:

$$RP = IP * F$$

Donde:

RP = Riesgo potencial

IP = Impacto potencial

F = Probabilidad de materialización de la amenaza (frecuencia)

En el documento Análisis_APSA, después del impacto potencial se creó una nueva columna llamada Riesgo, la cual contiene los cálculos del riesgo potencial. El resultado del riesgo potencial se realizó sin tener en cuenta las políticas de seguridad que tiene APSA, ya que serán consideradas dentro de las salvaguardas y por tanto, en los cálculos del impacto y riesgo residuales. En algunas ocasiones el valor del riesgo potencial no existe y se debe a que una amenaza no siempre afecta a todas las dimensiones de seguridad de la asociación. En la Figura 22 se observa un ejemplo de la estructura de la tabla de un activo hasta el cálculo del riesgo potencial.

DATOS / INFORMACIÓN [D]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	0,3	75%	75%	25%			8	8	8	9	9	6	6	2			1,8	1,8	0,6		
		Errores De Configuración	0,3		50%				8	8	8	9	9		4					1,2			
		Alteración Accidental De La Información	0,3		50%				8	8	8	9	9		4					1,2			
		Destrucción De Información	0,3	100%					8	8	8	9	9	8					2,4				
		Fugas De Información	0,1			50%			8	8	8	9	9			4					0,4		
		Manipulación De Los Registros De Actividad	0,1		5%			75%	8	8	8	9	9		0,4			6,75		0,04			0,68
		Manipulación De La Configuración	0,1		100%	100%	100%		8	8	8	9	9		8	8	9			0,8	0,8	0,9	
		Abuso De Privilegios De Acceso	0,1	75%	75%	75%			8	8	8	9	9	6	6	6			0,6	0,6	0,6		
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	9		6	8				0,6	0,8		
		Repudio	0,1		75%			100%	8	8	8	9	9		6			9		0,6			0,9
		Modificación Deliberada De La Información	0,1		100%				8	8	8	9	9		8					0,8			
		Destrucción De Información	0,1	100%					8	8	8	9	9	8					0,8				

Figura 22. Ejemplo de un activo calculado el riesgo potencial.
(*Fuente propia)*

3.4.3. Tratamiento del riesgo

Un riesgo puede ser crítico, grave, apreciable o asumible. Todos los riesgos se gestionan con salvaguardas, pero el enfoque de las salvaguardas esta primordialmente en aquellos riesgos críticos y graves. Los valores más altos en los riesgos serán los críticos y los de valores bajos serán los posiblemente asumibles. Por lo cual, se elaboró la escala de clasificación de riesgos de la Figura 23, que según la metodología Magerit se mide en las mismas unidades que el valor de los activos. La escala posee valores entre 0 y 10, y para este trabajo se consideraron a los valores mayores a 4 los graves y que requieren inmediata atención. A pesar de determinar al 4 como valor base, existen activos sensibles para la asociación en los que el valor base debe ser menor. En la sección 3.5.1 Salvaguardas se explica cuáles son los activos que poseen distinto valor base al valor general de 4.

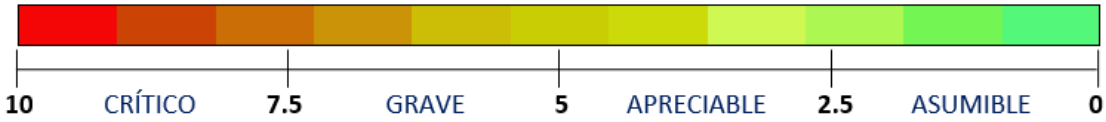

Figura 23. Escala de valoración del grado de impacto de una amenaza.
(Fuente propia)

Para el documento Análisis_APSA, en la columna de riesgos se resaltan con rojo aquellos que se encuentren entre 4 y 10, pues se los considera graves y requieren de salvaguardas. La figura 24 muestra un ejemplo donde se resaltan los valores altos de riesgo.

SERVICIOS [S]			Riesgo				
Código	**Nombre**	**Amenazas**	**D**	**I**	**C**	**A**	**T**
S1	**Página web**	Errores De Usuarios	0,175	0,2	1		
		Errores De Administración	0,7	0,6	0,6		
		Alteración Accidental De La Información		0,6			
		Fugas De Información			0,4		
		Caída Del Sistema Por Agotamiento De Recursos	2,1				
		Suplantación De La Identidad Del Usuario		**4,2**	**4,2**	3,5	
		Abuso De Privilegios De Acceso	1,05	1,8	1,8		
		Uso No Previsto	1,05	1,8	1,8		
		Acceso No Autorizado		**4**	3		
		Repudio		0,4			0,525
		Modificación Deliberada De La Información		0,8			
		Destrucción De Información	0,525				
		Divulgación De Información			2,4		
		Denegación De Servicio	2,1				

Figura 24. Ejemplo de selección de los riesgos graves.
(Fuente propia)

3.5. Impacto y riesgo residuales

Para esta sección se consideraron todas las fórmulas de cálculo que propone la metodología Magerit para un análisis cuantitativo.

3.5.1. Salvaguardas

Para establecer las salvaguardas de los activos se consideró:

- Para seleccionar las salvaguardas de cada grupo de activo, además de usar el listado general de salvaguardas que propone la metodología Magerit, se investigaron otras salvaguardas que se adaptan mejor a las necesidades de APSA.
- En algunos casos, se consideraron como salvaguardas las políticas de seguridad que ya existen en APSA, así como las salvaguardas que se han implementado mientras se desarrollaba este trabajo.
- Las salvaguardas se establecieron de acuerdo con el árbol de dependencias de activos, es decir, al aplicar una salvaguarda a un activo también puede convertirse en salvaguarda para otro activo directamente relacionado en el árbol de dependencias. Esta relación de salvaguardas puede ser desde un activo a sus dependientes o viceversa.
- Las salvaguardas se enfocan más en mitigar aquellos riesgos graves y críticos según la escala de medición de la Figura 23 y las consideraciones definidas en el tratamiento del riesgo.
- En algunos casos el riesgo de los activos es poco y no alcanza valores críticos, pero se definen salvaguardas para mitigar aquellos riesgos altos aunque sean asumibles en la escala de tratamiento del riesgo.
- Para ciertos activos importantes, los riesgos deben ser el mínimo posible y por lo tanto las salvaguardas que se implementan son para mitigarlos a un nivel muy bajo o eliminarlos.
- Algunas salvaguardas seleccionadas son generales y no inciden directamente sobre un activo pero son complementarias, pues ayudan a la seguridad informática global de la asociación.
- En ciertos casos, las salvaguardas que se propone no se detallan a fondo pues corresponden a activos que son gestionados por empresas externas.

Para el documento Análisis_APSA, se creó una columna llamada Salvaguardas. En esta columna se enlistan acciones que se deben tomar para tratar el riesgo, poniendo como prioridad aquellas

que mitigan los valores más altos de riesgo en cada activo. En la Figura 25 se muestra un ejemplo de las salvaguardas para combatir el riesgo de sus amenazas.

DATOS / INFORMACIÓN [D]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
D1	Datos de configuración	Errores De Administración	1,8	1,8	0,6			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos
		Errores De Configuración		1,2				
		Alteración Accidental De La Información		1,2				
		Destrucción De Información	2,4					
		Fugas De Información			0,4			
		Manipulación De Los Registros De Actividad		0,04			0,675	
		Manipulación De La Configuración		0,8	0,8	0,9		
		Abuso De Privilegios De Acceso	0,6	0,6	0,6			
		Acceso No Autorizado		0,6	0,8			
		Repudio		0,6			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,8					

Figura 25. Ejemplo de salvaguardas.
(Fuente propia)

3.5.2. Cálculos de impacto residual

Después de establecer las salvaguardas, el grado de degradación de las amenazas sobre los activos disminuye. Para cada activo la situación es distinta, las salvaguardas que logran ser muy eficaces disminuyen considerablemente el grado de degradación en algunas de las dimensiones de seguridad. Otras salvaguardas aunque ayudan en todas las dimensiones de seguridad, el grado de degradación no tiene una disminución considerable.

Antes del cálculo del impacto residual, se define la eficacia de las salvaguardas sobre los riesgos de un activo. La eficacia se mide en porcentaje con valores de 0% como mínimo y del 100% como máximo. Se procede entonces al cálculo del nuevo impacto denominado impacto residual, con la fórmula:

$$IR = IP * (1 - ES)$$

Donde:

IR = Impacto residual

IP = Impacto potencial

ES = Eficacia de las salvaguardas en una dimensión de seguridad (%)

Para el documento Análisis_APSA se creó dos columnas como se muestra en la Figura 26: la primera columna llamada Efectividad de salvaguardas que se subdivide en 5 columnas que corresponden a las dimensiones de seguridad y, que contienen los valores en porcentaje de la efectividad de las salvaguardas; la segunda columna llamada impacto residual contiene los nuevos valores de impacto calculados con la fórmula anterior.

DATOS / INFORMACIÓN [D]			Salvaguardas	Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas		D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
D1	Datos de configuración	Errores De Administración	• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos	75%	75%	75%			1,5	1,5	0,5		
		Errores De Configuración			75%					1			
		Alteración Accidental De La Información			75%					1			
		Destrucción De Información		75%					2				
		Fugas De Información				75%					1		
		Manipulación De Los Registros De Actividad			25%			50%		0,3			3,375
		Manipulación De La Configuración			75%	100%	75%			2		2,25	
		Abuso De Privilegios De Acceso		75%	75%	100%			1,5	1,5			
		Acceso No Autorizado			75%	100%				1,5			
		Repudio			75%			50%		1,5			4,5
		Modificación Deliberada De La Información			75%					2			
		Destrucción De Información		75%					2				

Figura 26. Ejemplo de la efectividad de las salvaguardas.
(Fuente propia)

3.5.3. Cálculos de riesgo residual

Además de disminuir el grado de degradación de un activo, ciertas salvaguardas también disminuyeron la probabilidad de ocurrencia de la amenaza relacionada. Si las amenazas redujeron la probabilidad, el valor de la frecuencia cambia y si no, el valor de la frecuencia se mantiene.

Antes del cálculo del riesgo residual, se define la eficacia de las salvaguardas sobre la frecuencia de riesgos de un activo. La eficacia se mide en porcentaje con valores de 0% como mínimo y del 100% como máximo. Se procede entonces al cálculo de la frecuencia residual, con la fórmula:

$$FR = F * (1 - EF)$$

Donde

FR= Frecuencia residual

F= Probabilidad de materialización de la amenaza (frecuencia)

EF= Eficacia de la salvaguarda sobre la frecuencia

Definido el valor de la frecuencia residual se procedió a calcular el nuevo riesgo, denominado riesgo residual, con la siguiente fórmula:

$$RR = IR * FR$$

Donde

RR= Riesgo Residual

IR = Impacto Residual

FR = Frecuencia Residual

Calculado el riesgo residual, se logró percibir con mayor claridad la eficacia de las salvaguardas. La mayoría de los valores de los riesgos residuales se encuentran dentro del rango de riesgos asumibles de la escala establecida en la Figura 23.

Para el documento Análisis_APSA se creó tres columnas como se ve en la Figura 27: la primera columna llamada Efectividad de Frecuencia que contiene los valores en porcentaje de la efectividad de las salvaguardas sobre la frecuencia; la segunda columna llamada frecuencia residual contiene el nuevo valor de la frecuencia calculado con la fórmula definida anteriormente; y la tercera columna llamada riesgo residual, contiene los valores calculados con la fórmula correspondiente.

DATOS / INFORMACIÓN [D]			Salvaguardas	Efectividad de Frecuencia	Frecuencia Residual	Riesgo Residual				
Código	Nombre	Amenazas			F´	D'	I'	C'	A'	T'
D1	Datos de configuración	Errores De Administración	• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos	80%	0,06	0,09	0,09	0,03		
		Errores De Configuración		80%	0,06		0,06			
		Alteración Accidental De La Información		90%	0,03		0,03			
		Destrucción De Información		90%	0,03	0,06				
		Fugas De Información		90%	0,01			0,01		
		Manipulación De Los Registros De Actividad		80%	0,02		0,006			0,0675
		Manipulación De La Configuración		90%	0,01		0,02		0,0225	
		Abuso De Privilegios De Acceso		90%	0,01	0,015	0,015			
		Acceso No Autorizado		90%	0,01		0,015			
		Repudio		90%	0,01		0,015			0,045
		Modificación Deliberada De La Información		90%	0,01		0,02			
		Destrucción De Información		90%	0,01	0,02				

Figura 27. Ejemplo del grado de eficacia de la frecuencia de ocurrencia.
(Fuente propia)

3.6. Planes de seguridad

La sintonización de todo el análisis anterior se ve reflejado en los planes de seguridad que se elaboró para la asociación. Para estos planes se considera las salvaguardas de los riesgos más graves detectados mediante el análisis.

3.6.1. Elaboración de los Planes de seguridad

Los planes de seguridad son un compendio de información con una lista de actividades que una organización debe realizar para mejorar la seguridad informática. El documento debe ser muy completo de manera que cumpla con su objetivo principal: combatir las amenazas para reducir o eliminar los riesgos. Un plan de seguridad incluye la siguiente información:

- Identificación del proyecto de seguridad: Se definió un nombre que identifique al plan y brinde una primera idea de lo que se trata.
- Objetivos: Se definió la razón principal y lo que se pretende conseguir al implementar el plan de seguridad.
- Salvaguarda por implementar: Como el plan de seguridad parte de las salvaguardas definidas en el análisis de riesgos, se señaló cuál es la salvaguarda seleccionada.

- Identificar los activos afectados: Se definió cuáles son los activos que se verán involucrados en la implementación del plan de seguridad y así prevenir posibles afectaciones.
- Participantes: Se determinó los responsables de la ejecución del plan de seguridad y los departamentos relacionados.
- Estimación de costes: Aquí se describió el coste económico pero también el costo del trabajo del personal dependiendo de la dificultad de la implementación.
- Relación de subtareas: Se detallaron todas las actividades directas o indirectas que se harán para cumplir un plan de seguridad en su totalidad.
- Estimación de tiempo de ejecución: Dependiendo de los recursos económicos y de personal, se determinó el tiempo estimado de ejecución. Los tiempos para APSA son largos porque su falta de persona técnico.
- Estimación del riesgo residual después de la ejecución: Este riesgo será el riesgo residual calculado en el análisis anterior, pues son el resultado de la implementación de la salvaguarda seleccionada para el plan de seguridad.
- Definir indicadores de eficacia y eficiencia del plan en función de la seguridad que se desea: Se definió como se puede medir la eficacia de las acciones del plan de seguridad.

Con esta estructura, se definió 5 planes de seguridad y una lista de acciones adicionales que debe implementar APSA para mejorar sus políticas de seguridad. Las políticas están destinadas principalmente a mejorar y formalizar procesos existentes en la asociación, pero también a implementar nuevas soluciones.

En el ANEXO C, se observa todo el documento Análisis_APSA con todos los cálculos de impacto, riesgo, salvaguardas y efectividad. La herramienta no contienen esta sección, la creación de planes de seguridad.

4. Plan director de seguridad de APSA

En este capitulo se redacta el documento completo del Plan director de Seguridad de la asociación APSA, sus análisis, resultados y planes de seguridad.

4.1. Contexto de la organización

4.1.1. Presentación

Asociación APSA es una Organización no gubernamental para el desarrollo (ONGD) creada en 1961 que desarrolla actividades para mejorar la calidad de vida de las personas con diferentes capacidades. Para desarrollar dichas actividades posee programas de prevención, atención temprana, educación, salud, formación, vivienda, ocio y empleo, orientados a facilitar su inclusión social y laboral. La sede central de APSA se ubica en la Av. Salamanca en Alicante y además, posee 10 sedes o delegaciones en la provincia.

APSA está compuesto por varios centros de actividades y servicios para personas con discapacidad y tres centros especiales de empleo: Avícola Aguamarga, Limencop y Terramar. Mediante estos centros atiende alrededor de 2000 personas al año en diversas localidades de la provincia de Alicante. Para ello, cuenta con más de 350 trabajadores de los cuales 200 son personas con discapacidad.

4.1.2. Estructura

La estructura de APSA está representado mediante el organigrama de la Figura 28. En el nivel más alto se encuentra la Asamblea General de Socios, después la Junta Rectora y la Junta de Apoyo, debajo está el Gerente, luego la Directora Técnica. De este último se derivan las siguientes áreas: Educativa, Formación, Residencial, C. O. San Juan y Voluntariado, C.CO. Terramar y, Calidad y Ocio, Empleo, Infraestructuras y TIC, y Área de Comunicación y Marketing.

Detrás de las áreas se encuentran las direcciones y coordinaciones de centros y servicios, y finalmente los equipos técnicos.

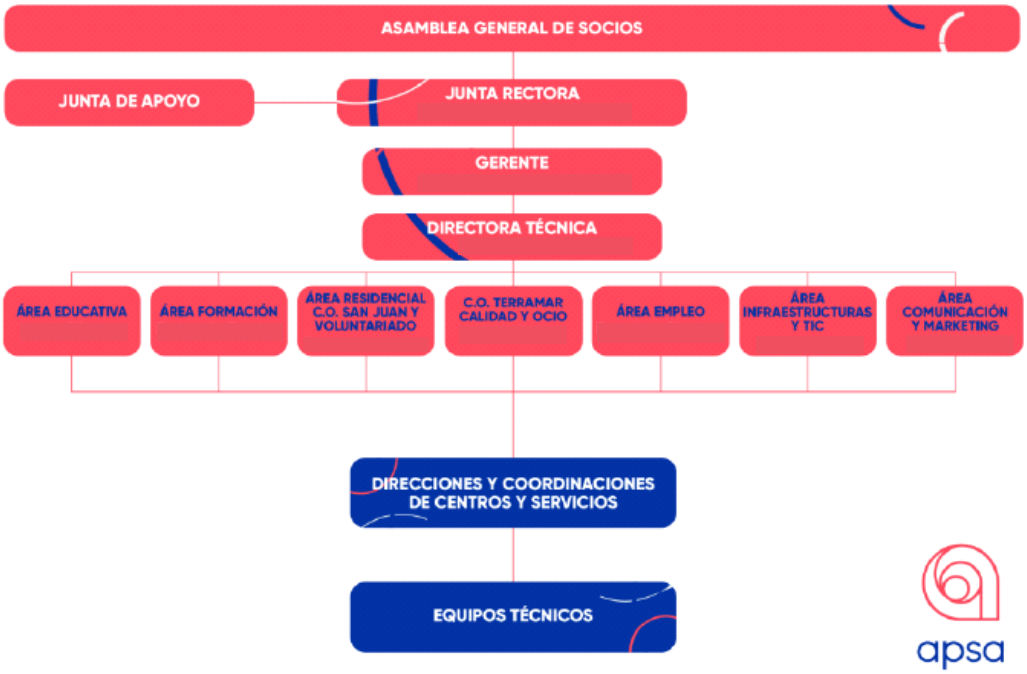

Figura 28. Organigrama de la Asociación APSA.
(Fuente APSA)

4.1.3. Sedes y Servicios

APSA ofrece recursos para satisfacer las necesidades de apoyo de sus socios, a través de todo su ciclo vital. A lo largo de sus más de 50 años de historia, APSA ha desarrollado diversos centros y servicios. Ofrecen servicios en la etapa educativa, la etapa de transición a la vida adulta, etapa de vida adulta y la etapa de tercera edad, como puede observarse en la Figura 29:

De 0 a 16 años	De 16 a 26 años	De 26 a 65 años	A partir de 65 años
ETAPA EDUCATIVA	TRANSICIÓN A LA VIDA ADULTA	VIDA ADULTA	TERCERA EDAD
- Centro de Desarrollo Infantil y Atención Temprana - Centro de Recursos y Apoyo Escolar - Ocio y deporte - Respiro familiar - Apoyo Psicológico - Formación en nuevas tecnologías - Actividades artísticas - Formación a familias - Trabajo social - Unidad Volante de Apoyo a la Dependencia - Servicio de apoyo educativo	- Centro Camí Obert - Ocio y deporte - Respiro familiar - Formación en nuevas tecnologías - Unidad Volante de Apoyo a la Dependencia - Trabajo social - Apoyo Psicológico - Actividades Artísticas - Vivienda	- Centro de Orientación Formación y Asesoramiento Laboral - Centro Ocupacional Terramar - Centros Especiales de Empleo - Ocio y deporte - Respiro familiar - Unidad Volante de Apoyo a la Dependencia - Apoyo Psicológico - Formación a familias - Trabajo social - Actividades Artísticas - Viviendas -Psiquiátrico Penitenciario	-Envejecimiento saludable - Ocio y deporte -Unidad Volante de Apoyo a la Dependencia - Trabajo social - Apoyo Psicológico - Actividades Artísticas

Figura 29. Estructuración de los servicios de APSA según las etapas vitales del individuo.
(Fuente González Mataix, 2018, p.19)

A continuación se detalla cada una de sus sedes, su ubicación y los servicios que ofrece APSA a través de ellas.

- Sede central: se encuentra en Alicante en la Avd. Salamanca y se ocupa del desarrollo infantil y la atención temprana (CDIAT). Esta sede cuenta con 6 plantas con distintos servicios. Distribuidos como muestra la Tabla 4:

Tabla 4. Distribución de la sede central

PLANTA	SERVICIOS Y DEPARTAMENTOS
Sótano y Planta Baja	• Servicio de limpieza • Reprografía del sótano • Mantenimiento • Servicios generales de administración • Servicios generales • Departamento de informática y soporte • Comunicación • Psicóloga de categoría 3 • Fisioterapia y la dirección técnica
Primera Planta	• Dirección del área educativa • Estimulación 3 • Las RSS multimedia área educativa • Psicomotricidad
Segunda Planta	• Estimulación 4, 5 y 6 • Psicóloga de categoría 1
Tercera Planta	• Estimulación 7, 8 y 9 • Dirección de categoría 1
Cuarta Planta	• Estimulación 10 y 11 • Sala Snoezelen • Fisioterapia 2
Quinta Planta	• Dirección de los proyectos de calidad • Trabajo social • Biblioteca
Sexta Planta	• Gerencia • Departamento financiero • Departamento laboral

Realizado por: Jessica Montero, 2019
Fuente: (González Mataix, 2018, pp. 101-102)

- Sede en San Vicente: se ocupa del desarrollo infantil y la atención temprana, además de ser un centro de recursos y apoyo escolar (CRAE). En esta sede está la administración del centro, salas 1, 2, 3 y 4 con la dirección del centro, 5 con fisioterapia, salas del CRAE y Salas de Fisioterapia del CRAE.
- Sede de la Vila Joiosa: es un CDIAT y un CRAE, en donde se encuentran salas y la dirección del centro.
- Sede Alicante, calle Zarandieta: tiene el CRAE con el servicio de ocio y las actividades artísticas y está distribuido como se observa en la Tabla 5:

Tabla 5. Distribución de la sede Alicante calle Zarandieta

PLANTA	SERVICIOS Y DEPARTAMENTOS
Planta Baja	• Salas de la 1 a la 10 • Sala polivalente 1 y 3 • Sala polivalente 2 con fisioterapia • Servicio de ocio • Administración 1 y 2
Primera Planta	• Dirección del CRAE • Despacho 1 • Actividades Artísticas • Dirección de sistemas TIC e infraestructuras

Realizado por: Jessica Montero, 2019
Fuente: (González Mataix, 2018, p. 102)

- Sede Alicante, calle García Morato: se encuentra la actividad artística de Psicoballet con monitores.
- Sede Elche: es un centro de formación permanente CPF o Camí Obert, un CRAE y un área educativa.
- Sede Alicante, calle Catedrático Jaume Mas i Porcel: es un a sede CFP o Camí Obert, donde se encuentra la dirección del área de formación, la dirección del Camí Obert, el departamento de administración y las aulas 1, 2 y 3.
- Sede Alfàs del Pi: es un centro CFP Camí Obert.
- Partida Aguamarga de Alicante: tiene el área de empleo y el centro ocupacional Terramar. En esta distribuida como muestra la Tabla 6:

Tabla 6. Distribución de la sede Partida Aguamarga de Alicante

ÁREA	SERVICIOS Y DEPARTAMENTOS
Empleo	• Dirección del área • Coordinación • Compras • Responsable de reprografía de la UMH • Responsables de reprografía de la UA • Varios conductores y formadores profesionales • Diseñador gráfico
Centro Ocupacional Terramar	• Dirección del centro, administración • Varias psicólogas • Trabajador social • Talleres del 1 al 6 • Casa taller • Ocio y deporte • Jardinería • Cocina • Guarda • Autobuses 1, 2 y 3

Realizado por: Jessica Montero, 2019
Fuente: (González Mataix, 2018, p. 103)

- Sede San Juan: está compuesto por el área residencial y un centro ocupacional; aquí se encuentra la dirección del área residencial, talleres 1, 2, 3 y 4, un trabajador social, una psicóloga del centro, la residencia, la administración, fisioterapia, área de salud, deporte y lavandería.

4.2. Antecedentes

Información necesaria para la evaluación inicial de APSA y su situación actual en el área de seguridad informática.

4.2.1. Aspectos Técnicos

Infraestructura

La asociación APSA utiliza tecnologías de la información como una herramienta administrativa y también es parte de nuevas metodologías para tratamientos de sus usuarios. En cada una de las sedes cuenta con infraestructura tecnológica que permite el desarrollo de todas las actividades que en ellas se realizan. Como se puede ver en la sección de servicios y sedes de APSA, cada sede ofrece servicios definidos que tienen diferentes necesidades y puestos de trabajo que requieren de distintos equipos informáticos que deben ser gestionados.

Para todos los servicios que APSA ofrece a sus empleados, usuarios y socios, cuenta con servidores físicos y servidores en la nube. Los servidores físicos están principalmente orientados al almacenamiento de datos y, estos se encuentran en cada una de las sedes; aunque existen servidores físicos que también ofrecen servicios de aplicaciones. Los servidores que están alojados en la nube están dedicados principalmente para base de datos, aplicaciones web externas, aplicaciones de intranet y almacenamiento de datos. La Figura 30 muestra la arquitectura de red de APSA, a que área están dedicados sus servidores y cuáles son los servicios que en ellos están alojados.

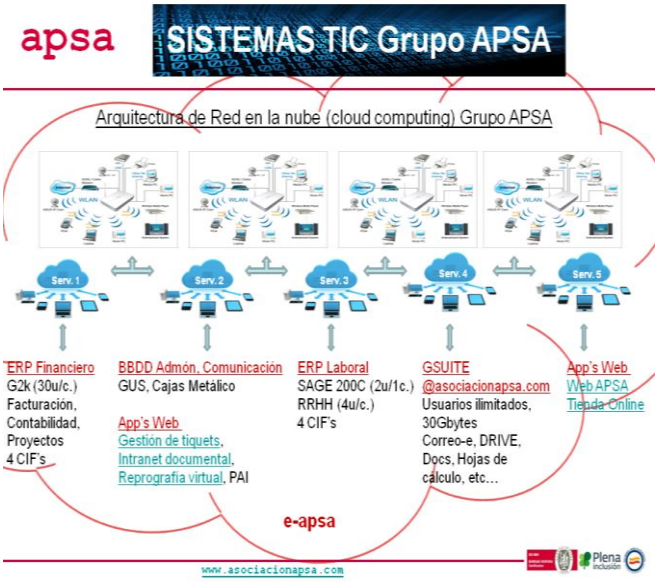

Figura 30. Arquitectura de Red de la Asociación APSA.
(Fuente APSA, 2018)

- En la Tabla 7 y Tabla 8 se detalla los elementos que se encuentran en los servidores de APSA Cloud y Físicos respectivamente.

Tabla 7. Servidores cloud de APSA

SERVIDOR		ELEMENTOS
Servidor 1	ERP Financiero	• Un gestor para empresas G2k • Facturación • Contabilidad • Proyectos • 4 CIF's.
Servidor 2	Base de Datos, Administración y Comunicación	• El Gestor de usuarios socios (GUS) • Registro individual de seguimiento • Cajas metálico • Demandantes de empleo • Formación • Férulas • APP's Web: gestión de tickets, intranet documental, reprografía virtual y el programa de apoyo individual.
Servidor 3	ERP Laboral	• SAGE 200C • RRHH • 4 CIF's
Servidor 4	GSUITE	• GSUITE • @asociacionapsa.com con usuarios ilimitados • Correo-e • DRIVE • Archivos como: documentos, hojas de cálculo, etc.
Servidor 5	APP's Web	• Web APSA

Realizado por: Jessica Montero, 2019
Fuente: (APSA, 2018)

Tabla 8. Servidores físicos de APSA

SERVIDOR	ELEMENTOS
Servidores locales de cada sede	• Ficheros de ofimática • Vídeos • Fotografías, etc.

Realizado por: Jessica Montero, 2019
Fuente: (APSA, 2018)

- Todas las bases de datos están todas en SQL Server Standard Edition y sus tamaños pueden variar entre 2 y 30 GB.
- En la Tabla 9 se detalla la lista de Software (programas o aplicaciones) que hay actualmente en el grupo APSA:

Tabla 9. Aplicaciones de APSA

APLICACIONES	
Corporativas (C/S y Web)	• Gestión Usuarios Socios, GUS, RIS, DEF, ISBN • Gestión Cajas metálico • Gestión Proyectos y Contactos • Gestión empresarial 4 CIF's, ERP, G2k
Comerciales	• ERP SAGE 200C • o ERP RRHH EntiGest
Corporativas Web	• Gestión de tiquets • Intranet documental: mediante carpetas compartidas entre los usuarios de dominios • Reprografía virtual • GSuite (Gmail, drive, docs, Excel, ppt, youtube, etc.) • PAI (en construcción) • E-apsa (en contrucción)

Realizado por: Jessica Montero, 2019
Fuente: (APSA, 2018)

Equipos Informáticos y Puestos de Trabajo

Los principales equipos informáticos que usa APSA para el cumplimiento de todas sus actividades y servicios que ofrece a sus usuarios son:

- 17 servidores: 5 servidores Cloud y 12 servidores en las subredes de las sedes.
- 222 PC's/portátiles, equipos usados para puestos de trabajo y las aulas de informática
- 47 Tablets
- 120 terminales de telefonía móvil
- 29 terminales de telefonía sobremesa
- 5 instalaciones ADLS (fibra óptica)
- 16 puntos de acceso inalámbrico
- 10 proyectores
- 6 pizarras digitales

- 55 impresoras, fotocopiadoras escáner
- 7 impresoras de tickets
- 5 pantallas táctiles

APSA distribuye todos los equipos de la lista anterior en todas sus sedes, para uso de sus empleados y usuarios. La mayoría de los equipos los usan distintas personas, por lo que no tienen un responsable específico, de manera general la responsabilidad recae en los directores de cada sede y en los profesionales del departamento de TIC. En cuanto a los terminales móviles, como son asignados a un solo empleado, están bajo su responsabilidad. En algunos casos los puestos de trabajo están compartidos por varias personas, por lo que es necesario conocer la distribución de los puestos de trabajo. A continuación se detallan los puestos de trabajo que tienen las sedes y que ocupan equipos informáticos:

- Salamanca: 61 puestos de trabajo
- La Vila: 6 puestos de trabajo
- Zarandieta: 25 puestos de trabajo
- Camiobert Alicante: 34 puestos de trabajo
- Camiobert Elche: 25 puestos de trabajo
- San Vicente (CDIAT + CRAE): 10 puestos de trabajo
- Terramar: 30 puestos de trabajo
- Residencia San Juan: 25 puestos de trabajo
- Área de empleo: Repos UA 12 puestos de trabajo
- Repos UMH: 18 puestos de trabajo
- Limencop oficina: 10 puestos de trabajo

Servicios Subcontratados

Al no poseer APSA suficientes recursos tecnológicos y una infraestructura propia, contrata servicios externos a otras empresas como:

- Para el servicio de correo electrónico usan GSuite de Google
- Para el acceso a Internet y telefonía contrata los servicios de la empresa Telefónica, Movistar.
- Para la protección de datos contrata los servicios de la empresa Forlopd
- Usa un almacenamiento externo de servidores y lo hace con 3 servidores en la empresa Strato y uno en la empresa 1&1
- Usa la solución de Sage en programa ERP de nóminas

- Para la gestión de Recursos humanos usa la solución EntiGest de GLMSOFT
- Para crear nuevos servicios virtuales como e-APSA (educación virtual), la organización cuenta con la colaboración de la Universidad de Alicante.

4.2.2. Estado inicial en seguridad informática

Para realizar un análisis de seguridad de todas las áreas de APSA, se utilizó una herramienta del INCIBE que consiste en un documento en Excel. El documento contiene un conjunto de preguntas que evalúan la seguridad informática en todos aspectos. Las preguntas abarcan todos los controles para evaluar y analizar sugeridos en la norma ISO-27001 del año 2017.

Las preguntas que ayudaron en el análisis se encuentran en el ANEXO A de este trabajo y están tomadas de la norma ISO-27001 que generaron la gráfica de la Figura 31 con el siguiente análisis:

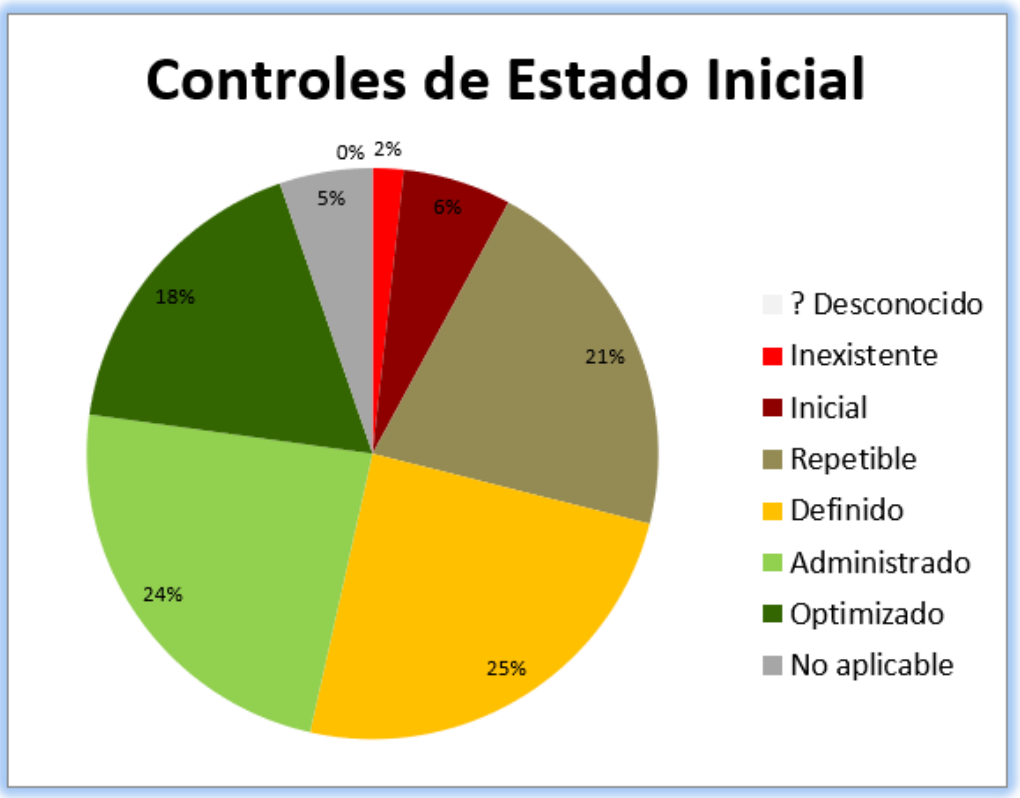

Figura 31. Gráfico de la situación inicial de la seguridad informática en APSA (Fuente APSA, 2018)

- APSA tiene el 18% de sus procesos de seguridad informática optimizados, es decir siguiendo un procedimiento documentado, aprobado, formalizado y con controles habituales. Existen áreas en APSA lo suficientemente maduras en aspectos de seguridad,

ya sea porque lo tienen con empresas externas o porque se han requerido crear políticas para cumplir con normas y proteger su sistema.

- El 24% que constituye cerca de la cuarta parte de la seguridad informática en APSA, lo tienen administrado, es decir se llevan a cabo procedimientos formalizados pero sin controles periódicos. Hay un gran porcentaje de políticas de seguridad que están bien establecidas pero carecen de un proceso de control periódico por falta de personal o tiempo.
- El 25% de la seguridad informática en APSA se encuentra en estado definido, es decir que existe un proceso documentado pero no formalizado. La mayoría de las políticas de seguridad se establecieron según aparecen nuevas necesidades, pero no pasaron por un proceso de formalización.
- El 21% de la seguridad en APSA es repetible, es decir se toman medidas de seguridad pero totalmente informales.
- Aunque con una cantidad baja es importante recalcar que el 6% de la seguridad en APSA es inicial, es decir existen salvaguardas pero dependen de la suerte para medir su eficacia. Esta cifra se refleja por no tener definido políticas de revisión de la seguridad de la información, revisión de auditorías de seguridad y políticas de concientización y capacitación a los empleados.
- Un porcentaje mínimo del 5% de los controles no se aplican a la realidad de APSA por lo que son inaplicables. Esta cantidad se refleja porque no existe desarrollo de aplicaciones dentro de la organización, por lo que no se puede evaluar las etapas de desarrollo y operación.
- Existe el valor mínimo del 2% que se refiere a la seguridad informática inexistente dentro de la asociación. Esto se debe a la poca madurez en materia de ciberseguridad y que por lo tanto no tienen establecidas políticas para escaneo de vulnerabilidades y gestión de evidencias de incidentes.

4.2.3. Políticas de seguridad de la información existentes

La asociación APSA cuenta con políticas de seguridad establecidas por el personal del departamento de TIC, pero que algunas de ellas no están documentadas. Todas las políticas se han creado en base a las necesidades que van apareciendo en la asociación y al criterio del personal de TIC. A continuación, se detallan parte de las políticas de seguridad que se han recolectado. Se recalca que no son todas las políticas de seguridad existentes, además que no están nombradas en orden de importancia.

- Los ordenadores están configurados con dos usuarios: el administrador y usuarios (empleado). Para todas las sedes como los puestos son fijos, se configura el acceso a un único empleado, excepto en la sede principal en donde los puestos de trabajo pueden variar y por lo tanto se configura el acceso para varios empleados.
- Para acceder a todos los ordenadores es necesario ingresar con un usuario y una contraseña. Algunos de ellos tienen salvapantallas que se activa después de un tiempo.
- Un usuario (empleado) normal que tiene acceso a un ordenador, no tiene permisos de administrador por lo tanto no puede instalar ni actualizar ninguna aplicación.
- Al tener contratado los servicios de Google para el correo electrónico, Gsuit obliga a los usuarios a configurar un pin de acceso a los móviles con sistema operativo Andriod, pues los usuarios usan la aplicación de correo en los dispositivos. En los móviles de marca Iphone, el sistema obliga a sus usuarios a tener un pin de acceso.
- Migración de Windows 7 a Windows 10 para no usar un antivirus externo, y en su defecto usar Windows Defender que viene por defecto con el sistema operativo Windows 10.
- Existen manuales de uso de internet, uso de redes sociales, uso de plataformas y aplicaciones que se les entrega a los empleados según su puesto de trabajo.
- Tiene contratado un sistema de Backup con Scrato para los servidores.
- Las copias de seguridad se realizan en la noche y se intenta controlar regularmente. Se realiza copias de seguridad de las imágenes de los servidores como respaldo para levantar el servicio si el servidor principal falla.
- Se ejecuta pruebas de levantamiento de servicio con copias y servidores de respaldo una vez al año.
- A los servidores se tiene acceso solo mediante escritorio remoto y en caso de fallar o presentar problemas con la conexión a un servidor. APSA tiene sistema de respaldo de acceso que consiste en acceder a otro servidor y mediante este acceder al requerido. Es decir tienen comunicación entre servidores.
- Los servidores poseen un sistema de detector de ataques de acceso no autorizado, en el cual, si detecta que desde una IP están haciendo constantes intentos de acceso, bloquea la dirección IP por un tiempos pero si persiste el ataque se puede bloquear de manera permanente.
- Existen lineamientos y ciertas restricciones con los dispositivos móviles como: no conectar a redes públicas (poseen tarifas de datos para uso mínimo) y no usarlo de manera personal si no solo para el trabajo.

- Se realiza un informe anual de actividades y planificación donde se detalla las responsabilidades del departamento de TIC.
- Se pueden crear usuarios y contraseñas temporales en caso de necesidad por actividades especiales en los centros. Después de terminadas las actividades se dan de baja a los usuarios.
- Para incidentes en los servicios que les ofrecen otras empresas, la notificación se realiza a los departamentos técnicos o servicios al cliente y mediante llamada telefónica o correo electrónico.
- Para los ordenadores usados en las Reprografías se configura Windows Defender para que los pendrives solo sean de lectura y que no se ejecute ningún programa. Esto evita la transmisión de virus al ordenador y entre pendrives.
- Las redes Wi-Fi tienen dos tipos de redes configuradas: la primera que permite conectar móviles y portátiles de los empleados, y se conectan a la red de la empresa, la segunda red es libre para que usuarios externos tengan acceso a internet, pero no que tengan accesos a la red interna.
- Para el escaneo de archivos se creó una carpeta “pública” (solo dentro de la red y de acceso para empleados) que permite compartir los escaneos de las impresoras pero, en caso de no hacerlo se debe borrar. Este proceso se les informa a los empleados cuando requieren hacer esta actividad.
- En la sede de Zalamanca manejan información de alto riesgo pues manejan datos, fotos y videos de niños que tienen que estar altamente protegidos.
- Si una persona si requiere el uso de pendrives tiene que notificar al departamento de TIC y firma la recepción del dispositivo USB, pues todos deben ser encriptados con la aplicación Veracript.
- La protección de datos lo maneja la empresa Frorlop, ellos hacen auditorias y se encargan de la aplicación del reglamento 25 de protección de datos y la protección de la información en bases de datos.
- En caso de requerir un cambio de contraseña, este debe ser notificado al departamento de TIC mediante teléfono o correo electrónico. Se cambia inmediatamente la contraseña con una provisional hasta que el empleado ingrese nuevamente al sistema y seleccione una contraseña propia.
- La eliminación de información se realiza manualmente, y solo después de cumplido el periodo de tiempo establecido de 5 años para almacenar datos.

- La gestión de las contraseñas se realiza en todas las aplicaciones, pues no tiene centralizado el sistema de autenticación.
- Una empresa externa se encarga del manejo de la página web y por lo tanto de la seguridad informática pertinente.

4.3. Inventario de activos y amenazas

4.3.1. Identificación de activos

Los activos se clasificaron en 9 tipos: datos/información, servicios, software – aplicaciones informáticas, equipos informáticos (hardware), redes de comunicaciones, soportes de Información, equipamiento auxiliar, instalaciones y personal. Se detecta una gran cantidad de activos, por lo que para el análisis se consideran los esenciales para la asociación.

A continuación, se detallan los activos que componen cada uno de los grupos de tipos de activos de la organización. Para identificar cada grupo se usan las siglas que están antes del nombre del grupo.

NOTA: *En responsables las siglas SR significa Sin Responsable.*

- **[D] Datos /Información**

Los datos son el activo más importante pues permiten a la asociación prestar servicios a sus usuarios. Este grupo de activos se los identificará con tonalidades del color azul claro.

APSA maneja información de la asociación, empleados y usuarios, que pueden ser de carácter público o privado. Los datos de carácter público se muestran a la población en general y, ayuda a que se conozca las actividades de la asociación y los servicios que presta. Los datos de carácter privado son para uso exclusivo de APSA, y de estos se puede destacar los datos: financieros, personales, médicos, educativos, administración, internos e informática. Estos datos también se pueden subclasifican de acuerdo con su nivel de confidencialidad para tener un tratamiento de seguridad distinto, por lo que considerar cada tipo sería un trabajo muy extenso. Por esta razón, se consideran como activos a los datos dependiendo del lugar de su almacenamiento suponiendo que es confidencial y que necesita un mayor grado de seguridad informática. Esta decisión se respalda en el hecho de que la asociación trabaja con una empresa exclusivamente para cumplir con el Reglamento de Protección de Datos que rige en el territorio español.

Los activos que conforman este grupo son: datos de configuración, código fuente de las aplicaciones, ficheros almacenados en PC, ficheros almacenados en servidores en la nube,

ficheros almacenados en servidores locales, bases de datos en servidores locales, bases de datos en servidores en la nube, copias de seguridad en los servidores locales, copias de seguridad en los servidores en la nube, copias de seguridad en discos externos, ficheros de contraseñas, registros de actividades en servidores y ficheros compartidos en las herramientas de Google. En la Figura 32 se muestra la lista de los activos, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
D1	**Datos de configuración**	[files][conf][int]	Administradores	Datos usados para la configuración de aplicaciones y servidores
D2	**Código fuente de aplicaciones**	[files][source]	Administradores	Código fuente de las aplicaciones que APSA maneja y no pertenece a ningún tercero
D3	**Ficheros almacenados en PC**	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en sus respectivos ordenadores
D4	**Ficheros almacenados en servidores en la nube**	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en los servidores de la nube mediante el servicio de Intranet Documental. Estos ficheros se pueden compartir con otros profesionales
D5	**Ficheros almacenados en servidores locales**	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en los servidores que se encuentran en cada una de las sedes mediante el servicio de Intranet Documental. Estos ficheros se pueden compartir con otros profesionales que se encuentran dentro de la misma sede.
D6	**Bases de datos en servidores locales**	[int][auth]	Administradores	Se consideran las bases de datos que están en los servidores locales de cada sede para el acceso al servicio de intranet
D7	**Bases de datos en servidores en la nube**	[int][auth]	Administradores	Se consideran las bases de datos que pertenecen a las aplicaciones que se encuentran almacenadas en los servidores en la nube
D8	**Copias de seguridad en la nube**	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en los servidores en la nube
D9	**Copias de Seguridad en servidores locales**	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en los servidores locales
D10	**Copias de Seguridad en discos externos**	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en discos externos, pendrives o algún otro equipo de almacenamiento
D11	**Ficheros de contraseñas**	[files][password][auth]	Administradores	APSA para el ingreso como administrador tanto para aplicaciones como servidores, cuenta con ficheros de contraseñas compartidos entre administradores
D12	**Registros de actividades en servidores**	[files][int][log]	Administradores	Todos los servidores tienen configurados logs que registran las actividades que en ellos se realiza y son los que pertenecen a este grupo
D13	**Ficheros compartidos Google Drive**	[files][password][int]	Administradores	Se consideran todos los archivos importantes para APSA que se almacenan en Google Drive y que se comparte entre administradores.

Figura 32. Activos del grupo Datos/Información
(Fuente: propia)

- [S] Servicios

Los servicios están creados para satisfacer las necesidades de los empleados y usuarios. Este grupo de activos se los identificará con tonalidades del color verde.

Los activos que conforman este grupo son: página web, correo electrónico, intranet documenta, sistema de tickets de incidencias, educación virtual, servicio de financiero, gestión de usuarios socios, gestión empresarial y gestión de recursos humanos. En la Figura 33 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
S1	**Página web**	[anon][pub][ext][www]	Administradores	Servicio que ofrece APSA a través de su aplicación web
S2	**Correo electrónico**	[int][email][edi]	Administradores	Este es un servicio subcontratado con la Suit de correo electrónico de Gmail para empresas.
S3	**Intranet documental - Servicio FTP**	[int][file][ftp][edi]	Administradores	Este es el servicio que usan los profesionales para compartir sus ficheros
S4	**Sistema de tickets de incidencias**	[int][www]	Administradores	Si ocurre algún tipo de incidencia, todos quienes trabajan en APSA tendrán acceso a un Sistema de tickets de incidencia, mediante el cual se intenta solucionar los problemas con la brevedad posible
S5	**Educación Virtual**	[ext][int][www][edi]	SR	Este es un servicio que se pondrá en marcha en un futuro por lo que se ha considerado para este análisis. La educación Virtual pretende llegar a más usuarios y sus familias. Ahora no dependerá si está cerca de una sede, un usuario puede recibir clases desde su casa.
S6	**Servicio de financiero**	[int]	Administradores	Aquí se involucran los servidores y aplicaciones dedicadas al departamento financiero de APSA
S7	**Gestión de usuarios Socios**	[int][dir]	Administradores	Servicio que se ofrece a todos los usuarios inscritos para los tratamientos que se ofrecen en APSA
S8	**Gestión empresarial**	[int]	Administradores	Ofrece un control empresarial de distintas áreas a través de módulos
S9	**Gestión de recursos humanos, nóminas**	[int][dir]	Administradores	Servicio que se ofrece al departamento de recursos humanos para el tratamiento de nóminas

Figura 33. Activos del grupo Servicios
(Fuente: propia)

- [SW] Software – Aplicaciones Informáticas

Se refiere a tareas automatizadas para el desempeño en un equipo informático. Este grupo de activos se los identificará con tonalidades del color amarillo paja.

Los activos que conforman este grupo son: aplicación de financiero, gestio de usuarios socios, gestión empresarial, gestión de recursos humanos, gestión de bases de datos, página web, intranet, sistema de tickets de incidencias, correo electrónico, e-apsa, aplicaciones de móviles,

sistemas operativos: Ubuntu Server, Windows Server, Windows 7 y Windows10, navegadores web, antivirus y software ofimático. En la Figura 34 y 35 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
SW1	**Aplicación de Financiero**	[prp][app]	Administradores	Aplicación dedicada a tesorería, contabilidad y todo tema relacionado con el sector financiero y económico de APSA
SW2	**GUS Gestión de Usuarios Socios**	[prp][app]	Administradores	Aplicación que usan los profesionales de la salud o interesados, en donde se encuentran todos los usuarios que reciben tratamientos o beneficios dentro de APSA
SW3	**G2K Gestión Empresarial**	[sub][app]	Administradores	Aplicación que permite integrar módulos para la gestión empresarial y que contiene aplicaciones para otros departamentos
SW4	**Sage Gestión de Recursos Humanos (nóminas)**	[sub][app]	Administradores	Sub-aplicación que permite al departamento de recursos humanos manejar las nóminas de los empleados de APSA
SW5	**Gestión de Bases de Datos**	[std][dbms]	Administradores	Aplicaciones que configuran las bases de datos según sean MySQL y SQL Server
SW6	**Aplicación de Página web**	[sub][www][app]	Administradores	Aplicación que contiene la página web de APSA a la que todas las personas tienen acceso, que esta creada y controlada por terceros
SW7	**Aplicación de Intranet**	[prp][app][file][backup]	Administradores	Aplicación que permite guardar y compartir ficheros de interés general entre profesionales
SW8	**Aplicación del Sistema de tickets de incidencias**	[prp][app]	Administradores	Aplicación que ayuda a todos los empleados de APSA notificar si tienen algún tipo de problemas para ser atendidos lo antes posible
SW9	**Aplicación de Correo electrónico Gmail**	[sub][std][email_server]	Administradores	Aplicación contratada con Google mediante la Suit de Gmail que ofrece el servicio de correo electrónico empresarial para APSA
SW10	**E-apsa**	[sub][www][app]	Administradores	Es una aplicación que se encuentra en desarrollo y que aún no ha sido integrada a los servicios de APSA, pero que ha sido considerada pues en poco tiempo lo integraran a su infraestructura
SW11	**Aplicaciones en móviles**	[sub][std]	Administradores	A todos los empleados se les entrega un teléfono móvil o en algunas ocasiones tablets, estos dispositivos tienen aplicaciones como correo electrónico, navegadores web, aplicaciones de chat entre otras que se requiere para el trabajo.
SW12	**Sistema operativo Ubuntu Server**	[sub][std][os]	Administradores	Sistema operativo que se encuentra en uno de los servidores de APSA
SW13	**Sistema Operativo Windows Server**	[sub][std][os]	Administradores	Sistema operativo que se encuentra en el resto de los servidores de APSA
SW14	**Sistema operativo Windows 7**	[sub][std][os]	Administradores	Sistema operativo que usan cerca de la mitad de los ordenadores de APSA, aunque ya se ha empezado la migración a Windows 10, se lo considera porque aún se usa.
SW15	**Sistema operativo Windows 10**	[sub][std][os]	Administradores	Sistema operativo al que están migrado los ordenadores de APSA

Figura 34. Activos del grupo Software – Aplicaciones informáticas (a)
(Fuente: propia)

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
SW16	**Navegadores Web**	[std][browser]	Administradores	Todos los empleados de APSA ingresan a través de navegadores web algunos de las aplicaciones, así también usan para navegar por internet según las necesidades de su trabajo
SW17	**Antivirus**	[sub][std][av]	Administradores	Este está presente en todos los servidores, así como en los ordenadores que operan con Windows 7
SW18	**Software Ofimático**	[std][office]	Administradores	Son herramientas que usan a diario los empleados para cumplir con sus actividades, dentro de estas se consideran documentos, fotografías, imágenes, videos, audios.

Figura 35. Activos del grupo Software – Aplicaciones informáticas (b)
(Fuente: propia)

- [HW] Equipos Informáticos (Hardware)

Medios materiales y físicos destinados para soportar directa o indirectamente los servicios que presta la asociación y donde se almacenan los datos. En la tabla Inventario están caracterizados por una tonalidad del color gris.

Los activos que conforman este grupo son: servidores APSA, servidores locales, ordenadores de escritorio de administradores y empleados, portátiles de administradores, empleados y TIC, móviles/tablets, impresoras de oficina, router, routers inalámbrico, switch, impresoras de repositorios e impresoras de sobremesa. En las Figuras 36 y 37 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
HW1	**Servidores APSA**	[vhost]	Administradores	Se consideran los 4 servidores principales de APSA en donde se encuentran alojados sus principales servicios y aplicaciones
HW2	**Servidores Sedes**	[host]	Administradores	Se consideran a los ordenadores que funcionan como servidores de almacenamiento que existen en cada una de las sedes
HW3	**Ordenadores de escritorio administrativos**	[pc]	Administradores, técnicos	Ordenadores usados por la directiva y parte gerencial de APSA
HW4	**Ordenadores de escritorio empleados**	[pc]	Administradores, técnicos	Ordenadores usados por los empleados de los distintos departamentos que conforman APSA
HW5	**Portátiles de administrativos**	[pc]	Administradores, técnicos	Portátiles usados por la directiva y gerencia de APSA
HW6	**Portátiles de empleados**	[pc]	Administradores, técnicos	Portátiles usados por los empleados de los distintos departamentos que conforman APSA

Figura 36. Activos del grupo equipos informáticos (a)
(Fuente: propia)

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
HW7	**Portátiles TIC**	[pc]	Administradores	Portátiles usados por los empleados del departamento de TIC, estos son de importancia pues es desde allí que se tienen el control de servidores y aplicaciones
HW8	**Móviles/Tablets**	[mobile][pda]	Administradores, técnicos	Dispositivos móviles usados por los empleados de APSA pertenecientes a la organización para comunicación telefónica móvil
HW9	**Impresoras oficinas**	[peripheral] [print][scan]	Administradores, técnicos	Dispositivos de impresión y escaneo que se encuentran en las oficinas de APSA
HW10	**Router**	[mid][network] [router]	Administradores, técnicos	Dispositivos que permiten la conexión de red para entregar el servicio de internet a ordenadores
HW11	**Router inalámbrico**	[network] [modem][wap]	Administradores, técnicos	Dispositivo que permiten la conexión de red para entregar servicio de internet a dispositivos móviles
HW12	**Switch**	[network][switch]	Administradores, técnicos	Dispositivos que permiten la conexión de red para entregar el servicio de internet a ordenadores
HW13	**Impresoras repositorios**	[peripheral] [print][scan]	Administradores, técnicos	Dispositivos de impresión y escaneo que se encuentran en los dos repositorios en los que trabaja APSA
HW14	**Teléfonos de sobremesa**	[ipphone]	Administradores, técnicos	Dispositivos para comunicación telefónica

Figura 37. Activos del grupo equipos informáticos (b)
(Fuente: propia)

- [COM] Redes de Comunicaciones

Instalaciones dedicadas a servicios de comunicaciones, contratados a terceros. En la tabla Inventario están caracterizados por una tonalidad del color naranja. Los activos que conforman este grupo son: redes inalámbricas, redes locales, red telefónica y red de telefonía móvil. En la Figura 38 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
COM1	**Redes inalámbricas**	[wifi][internet]	Administradores, técnicos	Redes de comunicaciones que se realizan a través de routers inalámbricos para brindar conectividad a dispositivos móviles
COM2	**Redes locales**	[LAN][internet]	Administradores, técnicos	Redes de comunicaciones que se realizan a través de routers y switches para dar conectividad a las oficinas y laboratorios de APSA
COM3	**Red telefónica**	[PSTN]	Administradores, técnicos	Red telefónica mediante la cual se ofrece el servicio de comunicación de telefónica entre empleados
COM4	**Red telefonía móvil**	[mobile]	Administradores, técnicos	Red telefónica móvil mediante la cual se ofrece el servicio de comunicación de telefónica móvil entre empleados

Figura 38. Activos del grupo Redes de comunicaciones
(Fuente: propia)

- [MEDIA] Soportes de Información

Dispositivos físicos que permiten almacenar información de forma permanente o al por largos periodos. En la tabla Inventario están caracterizados por una tonalidad del color violeta. Los activos que conforman este grupo son: discos duros externos, pendrives USB, CD/DVD y material impreso. En la Figura 39 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
MEDIA1	**Discos duros externos**	[electrónica] [disk]	Administradores, técnicos	Discos duros usados para realizar copias de seguridad
MEDIA2	**Pendrives USB**	[electronic][usb]	Administradores, técnicos	Dispositivos usados para guardar información que usen los empleados de APSA
MEDIA3	**CD/DVD**	[electronic][cd] [dvd]	Administradores, técnicos	Dispositivos usados para guardar información que usen los empleados de APSA
MEDIA4	**Material impreso**	[non_electronic][printed]	SR	Toda documentación impresa de APSA que sea relevante

Figura 39. Activos del grupo Soportes de información
(Fuente: propia)

- [AUX] Equipamiento Auxiliar

Equipos que sirven de soporte a los sistemas de información. En la tabla Inventario están caracterizados por una tonalidad del color verde claro. Los activos que conforman este grupo son: generador eléctrico, fuentes de alimentación, climatización, cableado UTP, armarios y cajas fuertes. En la Figura 40 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
AUX1	**Generador eléctrico**	[power][gen]	Administradores, técnicos	Generadores eléctricos en caso de fallas eléctricas que permiten proteger momentáneamente los servidores para resguardarlos
AUX2	**Fuentes de alimentación**	[power]	Administradores, técnicos	Fuentes de alimentación usados para distintos elementos informáticos
AUX3	**Climatización**	[ac]	Administradores, técnicos	Dispositivos usados en algunos de los cuartos en los que se encuentran dispositivos informativos relevantes
AUX4	**Cableado UTP**	[cabling][wire]	Administradores, técnicos	Sistema de cableado para establecer las redes y brindar conectividad entre ordenadores y hacia internet
AUX5	**Armarios**	[furniture]	Administradores, técnicos	Armarios en donde se encuentran alojados dispositivos informáticos y dispositivos de red
AUX6	**Cajas fuertes**	[safe]	Administradores	Es aquí en donde se almacenan las cosas más críticas que requieran este tipo de protección

Figura 40. Activos del grupo Equipamiento auxiliar
(Fuente: propia)

- [L]Instalaciones

Lugares donde están los sistemas de información y comunicación. En la tabla Inventario están caracterizados por una tonalidad del color rojo. Los activos que conforman este grupo son: edificios, cuartos servidores y coche. En la Figura 41 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
L1	**Edificios**	[building]	Administradores, técnicos	Se considera a todos los edificios que conforman APSA
L2	**Cuartos servidores**	[local]	Administradores, técnicos	Se consideran los cuartos en donde se encuentran los servidores o dispositivos de red importantes
L3	**Coche**	[car]	SR	Es el medio de transporte en donde se moviliza el personal de TIC a las distintas sedes

Figura 41. Activos del grupo Instalaciones
(Fuente: propia)

- [P] Personal

Personas relacionadas con los sistemas de información. En la tabla Inventario están caracterizados por una tonalidad del color celeste. Los activos que conforman este grupo son: administradores, técnicos, empleados y usuarios. En la Figura 42 se muestra la lista de los activos de este grupo, el tipo, su responsable y una breve descripción.

CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
P1	**Administradores**	[adm][com][sec]	no aplica	Administradores del departamento de TIC y encargados del manejo de casi todo el sistema informático y manejan bases de datos, aplicaciones y servidores, aunque también puede cumplir con otras funciones
P2	**Técnicos**	[dba][sec][des]	no aplica	Encargados de funciones técnicas, mantenimiento infromático y eléctrico
P3	**Empleados**	[ui]	no aplica	Personal que trabaja dentro de la organización como empleado
P4	**Usuarios**	[ue]	no aplica	Son todas las personas y familias que acceden a los servicios o prestan colaboración a la organización

Figura 42. Activos del grupo Personal
(Fuente: propia)

4.3.2. Dependencias de activos

Para definir las dependencias de los activos se utiliza el Árbol de Dependencias General de la Figura 43 basados en las sugerencias de la metodología Magerit. El árbol se realizó con los 9 grupos definidos en la identificación de activos y sirve de guía para definir las dependencias de todos los activos.

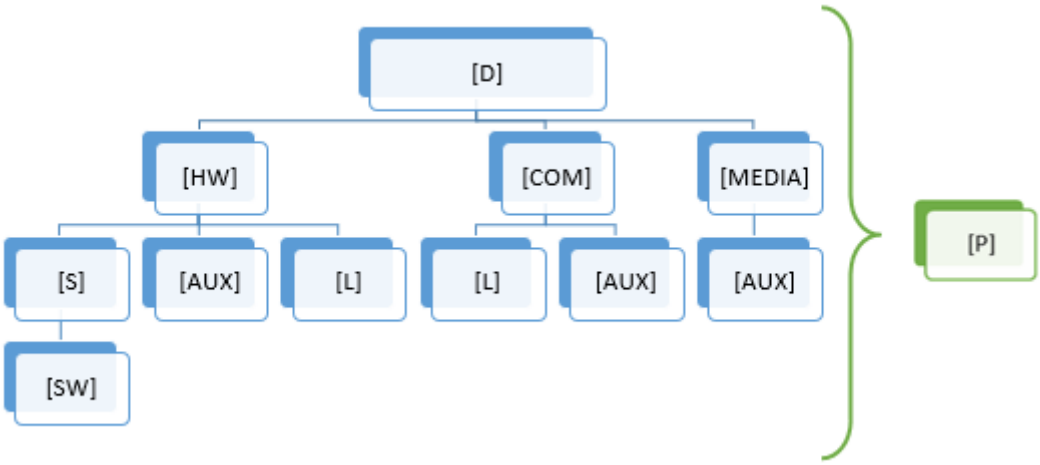

Figura 43. Árbol de dependencias de los activos de APSA.
(Fuente propia)

En la parte superior del árbol se encuentran los Datos/Información y de este se derivan los demás grupos de activos. Además, cada grupo de activo depende del personal, por eso se encuentra abarcando todos los grupos. Las dependencias pueden ser de distintos niveles, pero solo se redactan las dependencias de nivel 1, es decir las directamente relacionadas. Entonces se asume que un activo A, que depende directamente de un activo B, dependerá indirectamente de todos los activos de los que depende el activo B.

A continuación, se detalla la lista de dependencias directas de cada activo, clasificado en su respectivo tipo de activo.

- [D] Datos /Información

Como se observa en las Figuras 44 y 45, los datos dependen directamente de los equipos informáticos, redes de comunicaciones, soportes de información y el personal. Entonces se asume que también dependerá indirectamente de todos los activos que estén debajo de los dependientes directos.

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
D1	Datos de configuración	Servidores APSA, Servidores locales
D2	Código fuente de aplicaciones	Servidores APSA, Servidores locales
D3	Ficheros almacenados en PC	Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, discos duros externos, pendrives USB
D4	Ficheros almacenados en servidores en la nube	Servidores APSA, Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, redes inalámbricas, redes locales

Figura 44. Dependencias del grupo Datos/Información (a)
(Fuente propia)

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
D5	Ficheros almacenados en servidores locales	Servidores locales, Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, redes inalámbricas, redes locales
D6	Bases de datos en servidores locales	Servidores locales, redes inalámbricas, redes locales, , discos duros externos, pendrives USB
D7	Bases de datos en servidores en la nube	Servidores APSA, redes inalámbricas, redes locales
D8	Copias de seguridad en la nube	Servidores APSA, redes inalámbricas, redes locales
D9	Copias de Seguridad en servidores locales	Servidores locales, redes inalámbricas, redes locales
D10	Copias de Seguridad en discos externos	Servidores APSA, Servidores locales, redes inalámbricas, redes locales, , discos duros externos, pendrives USB
D11	Ficheros de contraseñas	Servidores APSA, Servidores locales
D12	Registros de actividades en servidores	Servidores APSA, Servidores locales
D13	Ficheros compartidos Google Drive	Portátiles TIC, redes inalámbricas, redes locales

Figura 45. Dependencias del grupo Datos/Información (b)
(Fuente propia)

- [S] Servicios

Como se observa en la Figura 46, los servicios dependen directamente del Software – Aplicaciones informáticas y del personal. En este caso, no posee dependencias indirectas pues el software no posee dependencias.

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
S1	Página web	Aplicación de Página Web
S2	Correo electrónico	Aplicación de correo electrónico Gmail
S3	Intranet documental - Servicio FTP	Aplicación de intranet
S4	Sistema de tickets de incidencias	Aplicación del sistema de tickets de incidencias
S5	Educación Virtual	E-apsa
S6	Servicio de financiero	Aplicación de Financiero
S7	Gestión de usuarios Socios	GUS Gestión de Usuarios Socios
S8	Gestión empresarial	G2K Gestión empresarial
S9	Gestión de recursos humanos, nóminas	Sage Gestión de Recursos Humanos (nóminas)

Figura 46. Dependencias del grupo Servicios
(Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Como se observa en la Figura 47, los equipos informáticos dependen directamente de los servicios, equipamiento auxiliar, instalaciones y el personal. Entonces se asume que también dependerá indirectamente de todos los activos que estén debajo de los dependientes directos.

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
HW1	Servidores APSA	Página web, Intranet documental - Servicio FTP, Sistema de tickets de incidencias, Servicio de financiero, Gestión de usuarios Socios, Gestión empresarial, Gestión de recursos humanos, nóminas, generador eléctrico, fuentes de alimentación, climatización, cableado UTP, edificios, cuartos de servidores
HW2	Servidores Sedes	Intranet documental - Servicio FTP, generador eléctrico, fuentes de alimentación, climatización, cableado UTP, edificios, cuartos de servidores
HW3	Ordenadores de escritorio administrativos	Fuentes de alimentación, cableado UTP, edificios
HW4	Ordenadores de escritorio empleados	Fuentes de alimentación, cableado UTP, edificios
HW5	Portátiles de administrativos	Fuentes de alimentación, cableado UTP, edificios
HW6	Portátiles de empleados	Fuentes de alimentación, cableado UTP, edificios
HW7	Portátiles TIC	Fuentes de alimentación, cableado UTP, edificios
HW8	Móviles/Tablets	Correo electrónico, conectividad
HW9	Impresoras oficinas	Conectividad, cableado UTP, edificios
HW10	Router	Conectividad, cableado UTP, edificios
HW11	Router inalámbrico	Conectividad, cableado UTP, edificios
HW12	Switch	Conectividad, cableado UTP, edificios
HW13	Impresoras repositorios	Conectividad, cableado UTP
HW14	Teléfonos de sobremesa	Conectividad, cableado UTP, edificios

Figura 47. Dependencias del grupo Equipos informáticos
(Fuente propia)

- [COM] Redes de Comunicaciones

Como se observa en la Figura 48, las redes de comunicaciones dependen directamente del equipamiento auxiliar, instalaciones y del personal. En este caso no posee dependencias indirectas pues ni el equipo auxiliar, ni las instalaciones poseen dependencias.

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
COM1	Redes inalámbricas	Edificios, fuentes de alimentación, armarios, Cableado UTP, router inalámbrico
COM2	Redes locales	Edificios, cuartos servidores, fuentes de alimentación, armarios, Cableado UTP, router, switch
COM3	Red telefónica	Edificios, cableado UTP, router, switch
COM4	Red telefonía móvil	

Figura 48. Dependencias del grupo Redes de comunicaciones
(Fuente propia)

- [MEDIA] Soportes de Información

Como se observa en la Figura 49, los soportes de información dependen directa y únicamente del equipo auxiliar y el personal.

CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
MEDIA1	Discos duros externos	Armarios y mobiliario
MEDIA2	Pendrives USB	Armarios y mobiliario
MEDIA3	CD/DVD	Armarios y mobiliario
MEDIA4	Material impreso	Armarios y mobiliario

Figura 49. Dependencias del grupo Soportes de información
(Fuente propia)

- Sin dependencias: Software – Aplicaciones Informáticas, Equipamiento Auxiliar e Instalaciones, según el árbol general de dependencias, no posee ninguna dependencia directa a excepción del personal.

4.3.3. Valoración de activos

Para la valoración de cada activo se consideran las cinco dimensiones de seguridad: Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T). La valoración sigue la definición y consideraciones descritas en la metodología Magerit.

Para la valoración de cada uno de los activos se utilizó la escala de valoración de la Figura 50. La escala varía de 0 a 10, siendo 0 un daño irrelevante y llegando hasta 10 en donde el daño es extremadamente grave para la asociación. La imagen tiene colores para una mejor ilustración, siendo los tonos verdes de menor daño y tonos rojos de mayor daño.

Figura 50. Escala de valoración de los activos de APSA.
(Fuente propia)

A continuación, se detalla la valoración de los activos de la organización en cada una de las dimensiones de seguridad, y algunas de las consideraciones que se realizaron para la valoración.

- [D] Datos /Información

Los datos son de suma importancia para toda la organización por lo que tiene una valoración alta en casi todos los casos. Los valores de 5 y menores adquieren los datos que en caso de pérdida, el impacto en las dimensiones de seguridad es menor. La Figura 51, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
D1	Datos de configuración	8	8	8	9	9
D2	Código fuente de aplicaciones	8	9	8	9	9
D3	Ficheros almacenados en PC	3	7	5	6	7
D4	Ficheros almacenados en servidores en la nube	5	7	7	8	8
D5	Ficheros almacenados en servidores locales	5	7	7	8	8
D6	Bases de datos en servidores locales	8	9	9	9	9
D7	Bases de datos en servidores en la nube	9	9	9	9	9
D8	Copias de seguridad en la nube	9	8	9	9	9
D9	Copias de Seguridad en servidores locales	8	8	9	9	9
D10	Copias de Seguridad en discos externos	7	8	9	9	9
D11	Ficheros de contraseñas	9	9	9	9	9
D12	Registros de actividades en servidores	8	8	8	9	9
D13	Ficheros compartidos Google Drive	7	8	8	7	7

Figura 51. Valoración de los activos del grupo Datos/Información.
(Fuente propia)

- [S] Servicios

Los servicios al igual que los datos, son esenciales dentro de la asociación, por lo que igualmente se evalúan con valores altos. Los valores de 6 y menores tienen aquellos activos que al no estar en servicio, el impacto en las dimensiones de seguridad de la asociación es menor. La Figura 52, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
S1	Página web	7	8	8	5	7
S2	Correo electrónico	7	8	8	7	8
S3	Intranet documental - Servicio FTP	8	8	8	8	8
S4	Sistema de tickets de incidencias	4	6	6	8	5
S5	Educación Virtual	8	8	7	6	7
S6	Servicio de financiero	8	9	9	9	9
S7	Gestión de usuarios Socios	8	8	8	7	8
S8	Gestión empresarial	7	8	8	7	8
S9	Gestión de recursos humanos, nóminas	7	8	8	8	9

Figura 52. Valoración de los activos del grupo Servicios.
(Fuente propia)

- [SW] Software – Aplicaciones Informáticas

Toman un valor alto cuando los servicios esenciales de la asociación dependen de dichas aplicaciones. Los valores menores están relacionados con aquellos servicios que pueden estar suspendidos por un periodo de tiempo, sin causar impactos considerables. De igual manera, tienen una valoración menor aquellas aplicaciones que no son esenciales o pueden ser sustituidas inmediatamente por otras que cumplen la misma función. La Figura 53, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
SW1	Aplicación de Financiero	9	9	9	9	9
SW2	GUS Gestión de Usuarios Socios	8	8	8	9	9
SW3	G2K Gestión Empresarial	7	8	8	9	9
SW4	Sage Gestión de Recursos Humanos (nóminas)	7	8	8	9	9
SW5	Gestión de Bases de Datos	8	9	9	9	9
SW6	Aplicación de Página web	7	8	8	9	8
SW7	Aplicación de Intranet	8	8	8	9	7
SW8	Aplicación del Sistema de tickets de incidencias	4	6	6	9	5
SW9	Aplicación de Correo electrónico Gmail	7	8	8	9	8
SW10	E-apsa	8	8	7	8	7
SW11	Aplicaciones en móviles	4	8	7	6	5
SW12	Sistema operativo Ubuntu Server	9	9	9	9	9
SW13	Sistema Operativo Windows Server	9	9	9	9	9
SW14	Sistema operativo Windows 7	4	9	5	8	6
SW15	Sistema operativo Windows 10	4	9	5	8	6
SW16	Navegadores Web	4	8	8	8	6
SW17	Antivirus	8	8	5	8	5
SW18	Software Ofimático	3	5	5	4	3

Figura 53. Valoración de los activos del grupo Software.
(Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Los valores altos de estos activos se debe a que son los que almacenan las aplicaciones de servicios esenciales de la asociación. Los valores bajos adquieren los activos que tienen repuesto o se pueden usar otros en reemplazo y no causan impacto a las dimensiones de seguridad de APSA. La Figura 54, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
HW1	Servidores APSA	9	9	9	9	9
HW2	Servidores Sedes	8	8	9	9	9
HW3	Ordenadores de escritorio administrativos	7	8	8	7	8
HW4	Ordenadores de escritorio empleados	3	7	7	7	7
HW5	Portátiles de administrativos	7	8	8	7	8
HW6	Portátiles de empleados	3	7	7	7	7
HW7	Portátiles TIC	8	9	9	9	9
HW8	Móviles/Tablets	4	7	7	8	6
HW9	Impresoras oficinas	3	2	3	3	3
HW10	Router	8	8	8	8	8
HW11	Router inalámbrico	8	8	8	8	8
HW12	Switch	8	8	8	8	8
HW13	Impresoras repositorios	8	5	4	6	5
HW14	Teléfonos de sobremesa	6	5	4	4	4

Figura 54. Valoración de los activos del grupo Equipos informáticos.
(Fuente propia)

- [COM] Redes de Comunicaciones

Todos los activos tienen valores altos pues depende de ellos la comunicación dentro de la asociación para transferir información, por ello se requiere tener una conexión permanente entre todas las sedes. La Figura 55, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
COM1	Redes inalámbricas	7	8	9	9	8
COM2	Redes locales	8	8	9	9	8
COM3	Red telefónica	8	7	8	7	8
COM4	Red telefonía móvil	8	7	8	7	8

Figura 55. Valoración de los activos del grupo Redes de comunicaciones.
(Fuente propia)

- [MEDIA] Soportes de Información

Estos activos tienen una valoración alta considerando que es en estos dispositivos en donde se almacena copias de seguridad o información confidencial de APSA. La divulgación de información confidencial o la pérdida de esta causaría un grave impacto en la asociación. La Figura 56, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
MEDIA1	Discos duros externos	8	9	9	9	9
MEDIA2	Pendrives USB	7	8	9	9	8
MEDIA3	CD/DVD	7	8	9	9	8
MEDIA4	Material impreso	7	8	9	9	9

Figura 56. Valoración de los activos del grupo Soportes de información.
(Fuente propia)

- [AUX] Equipamiento Auxiliar

La mayor parte de estos activos posee valores bajos, pues las actividades de la asociación no dependen de su funcionamiento, o pueden ser reemplazados y no causar graves impactos. Los valores altos de los activos armarios y cajas fuertes se debe a que estos almacenan activos informáticos importantes para APSA. La Figura 57, muestra la valoración de los activos del grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
AUX1	Generador eléctrico	5	5	3	4	4
AUX2	Fuentes de alimentación	5	7	3	4	4
AUX3	Climatización	5	4	3	4	4
AUX4	Cableado UTP	7	8	4	4	4
AUX5	Armarios	8	8	8	8	8
AUX6	Cajas fuertes	8	8	9	9	9

Figura 57. Valoración de los activos del grupo equipamiento auxiliar.
(Fuente propia)

- [L]Instalaciones

Para la evaluación de estos activos se consideró sus funciones y que es lo que almacena. Los cuartos de servidores fueron evaluados con una alta valoración pues estos contienen equipos informáticos importantes y ser vulnerados puede causar graves impactos para la asociación. La Figura 58, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
L1	Edificios	6	7	8	6	5
L2	Cuartos servidores	8	8	8	8	7
L3	Coche	2	5	3	5	2

Figura 58. Valoración de los activos del grupo instalaciones.
(Fuente propia)

- [P] Personal

Estos activos poseen una valoración alta porque de ellos depende el funcionamiento de la asociación. Los valores más altos lo tienen los administradores pues controlan muchos de los servicios de APSA. La Figura 59, muestra la valoración de los activos de este grupo.

CÓDIGO	NOMBRE	D	I	C	A	T
P1	Administradores	8	8	9	9	9
P2	Técnicos	7	8	9	9	8
P3	Empleados	7	8	9	9	8
P4	Usuarios	5	6	9	9	5

Figura 59. Valoración de los activos del grupo Personal.
(Fuente propia)

4.3.4. Determinación de amenazas

Las amenazas según la metodología Magerit se clasifican en 4 grupos: [N] de origen natural, [I] de origen industrial, [E] errores y fallos no intencionados, y [A] ataques intencionados. Estos grupos están integrados por una lista de amenazas que pueden afectar a las dimensiones de seguridad de un activo. El listado completo de las amenazas relacionadas con cada tipo de activo se observa en el Anexo B y se usó para determinar las amenazas de cada activo de la asociación. Al analizar los activos y sus amenazas, se determinó que para la realidad de APSA no se consideran algunas amenazas a pesar de que están dentro de las que afectan al tipo de activo al que corresponda.

Las amenazas se agrupan dependiendo de su origen, por lo que para diferenciarlos se usa una gama de colores de claro a obscuro, según el color que identifique al activo. El color que se usa será el mismo para los próximos cálculos.

Determinación de la Frecuencia de ocurrencia

Determinadas las amenazas de cada activo, se determinó su frecuencia de ocurrencia dentro de la asociación, considerando:

- La frecuencia de ocurrencia: es la periodicidad con la que sucede determinada amenaza en APSA. Para ciertos activos, aunque algunos errores o ataques no han ocurrido, al ser muy conocidos se valoraron con una frecuencia de ocurrencia baja. Para la valoración cuantitativa se usa una escala que varía desde 0,1 a 1 de la Figura 60, donde los valores altos son de mayor frecuencia y los valores bajos son de poca frecuencia.

Figura 60. Escala de valoración para la frecuencia de ocurrencia de una amenaza de APSA. (Fuente propia)

Determinación del nivel de impacto

Determinadas las frecuencias de ocurrencia de las amenazas de cada activo, se determinó el grado o nivel de impacto en la asociación, considerando:

- El grado o nivel de impacto: es el nivel de degradación de un activo si una amenaza se materializa. La escala de valoración usada es la de la Figura 61 y varía desde 5% al 100%. Esta escala tiene 5 niveles de impacto, siendo 5% un impacto muy bajo, 50% un impacto medio y 100% un impacto muy alto. La valoración se hace para cada dimensión de seguridad de cada activo. Algunas de las valoraciones de las amenazas no se realizaron directamente sobre el activo, sino sobre la información que maneja el activo.

Figura 61. Escala de valoración del grado de impacto de una amenaza de APSA.
(Fuente propia)

Las valoraciones corresponden a un análisis sin tener en cuenta las políticas de seguridad que actualmente tiene APSA. A continuación se describe los resultados del análisis de las amenazas con su frecuencia de ocurrencia y nivel de impacto para cada grupo de activo.

- [D] Datos /Información

Para este tipo de activos solo se evalúan dos tipos de amenazas: errores y los ataques (distinguidos por dos tonalidades del color azul claro). Las amenazas que poseen un alto valor de frecuencia son los errores de usuarios y la alteración accidental de la información. El resto de las amenazas poseen una frecuencia de ocurrencia baja. En cuanto a la degradación, los valores son variados pues dependen de la importancia del activo para la asociación. Todos los valores calculados se observan en las Figuras 62 a la 65.

DATOS / INFORMACIÓN [D]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	0,3	75%	75%	25%		
		Errores De Configuración	0,3		50%			
		Alteración Accidental De La Información	0,3		50%			
		Destrucción De Información	0,3	100%				
		Fugas De Información	0,1			50%		
		Manipulación De Los Registros De Actividad	0,1		5%			75%
		Manipulación De La Configuración	0,1		100%	100%	100%	
		Abuso De Privilegios De Acceso	0,1	75%	75%	75%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		75%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				

Figura 62. Frecuencia y degradación de las amenazas del grupo Datos/Información (a)
(Fuente propia)

D2	**Código fuente de aplicaciones**	Errores De Administración	0,3	50%	75%	25%		
		Errores De Configuración	0,3		75%			
		Alteración Accidental De La Información	0,1		100%			
		Manipulación De Los Registros De Actividad	0,1		5%			75%
		Manipulación De La Configuración	0,1		75%	50%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	75%	75%		
		Acceso No Autorizado	0,1		100%	100%		
		Repudio	0,1		75%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
D3	**Ficheros almacenados en PC**	Errores De Usuarios	0,7	75%	75%	50%		
		Errores De Administración	0,3	75%	75%	50%		
		Errores De Configuración	0,3		25%			
		Alteración Accidental De La Información	0,7		75%			
		Destrucción De Información	0,5	100%				
		Fugas De Información	0,1			25%		
		Manipulación De Los Registros De Actividad	0,1		25%			50%
		Manipulación De La Configuración	0,1		50%	50%	25%	
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	75%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%		
		Acceso No Autorizado	0,3		75%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	75%				
D4	**Ficheros almacenados en servidores en la nube**	Errores De Usuarios	0,7	50%	50%	5%		
		Errores De Administración	0,3	75%	75%	50%		
		Errores De Monitorización Log	0,1		50%			75%
		Errores De Configuración	0,3		50%			
		Alteración Accidental De La Información	0,7		75%			
		Destrucción De Información	0,3	75%				
		Manipulación De Los Registros De Actividad	0,1		25%			75%
		Manipulación De La Configuración	0,1		25%	50%	50%	
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	75%	
		Abuso De Privilegios De Acceso	0,1	25%	25%	75%		
		Acceso No Autorizado	0,1		50%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
D5	**Ficheros almacenados en servidores locales**	Errores De Usuarios	0,7	75%	50%	5%		
		Errores De Administración	0,3	75%	75%	50%		
		Errores De Monitorización Log	0,1		50%			75%
		Errores De Configuración	0,3		50%			
		Alteración Accidental De La Información	0,5		75%			
		Destrucción De Información	0,3	75%				
		Manipulación De Los Registros De Actividad	0,1		25%			75%
		Manipulación De La Configuración	0,1		25%	50%	50%	
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	75%	
		Abuso De Privilegios De Acceso	0,1	25%	25%	75%		
		Acceso No Autorizado	0,1		50%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				

Figura 63. Frecuencia y degradación de las amenazas del grupo Datos/Información (b) (Fuente propia)

D6	**Bases de datos en servidores locales**	Errores De Administración	0,3	75%	75%	50%		
		Errores De Monitorización Log	0,1		75%			75%
		Errores De Configuración	0,3		75%			
		Alteración Accidental De La Información	0,5		75%			
		Destrucción De Información	0,1	100%				
		Manipulación De Los Registros De Actividad	0,1		50%			100%
		Manipulación De La Configuración	0,1		50%	75%	50%	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%	
		Abuso De Privilegios De Acceso	0,1	75%	50%	75%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
D7	**Bases de datos en servidores en la nube**	Errores De Administración	0,3	75%	75%	50%		
		Errores De Monitorización Log	0,1		75%			75%
		Errores De Configuración	0,3		75%			
		Alteración Accidental De La Información	0,5		75%			
		Destrucción De Información	0,1	100%				
		Manipulación De Los Registros De Actividad	0,1		50%			100%
		Manipulación De La Configuración	0,1		50%	75%	50%	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%	
		Abuso De Privilegios De Acceso	0,1	75%	50%	75%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
D8	**Copias de seguridad en la nube**	Errores De Administración	0,1	75%	75%	50%		
		Errores De Monitorización Log	0,3		50%			50%
		Errores De Configuración	0,3		100%			
		Alteración Accidental De La Información	0,3		100%			
		Destrucción De Información	0,1	100%				
		Manipulación De Los Registros De Actividad	0,1		25%			75%
		Manipulación De La Configuración	0,1		75%	75%	75%	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
D9	**Copias de Seguridad en servidores locales**	Errores De Administración	0,1	75%	75%	50%		
		Errores De Monitorización Log	0,3		50%			50%
		Errores De Configuración	0,3		100%			
		Alteración Accidental De La Información	0,3		100%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			75%		
		Manipulación De La Configuración	0,1		75%	75%	75%	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		

Figura 64. Frecuencia y degradación de las amenazas del grupo Datos/Información (c) (Fuente propia)

D10	Copias de Seguridad en discos externos	Errores De Administración	0,1	75%	75%	50%		
		Errores De Monitorización Log	0,3		50%			50%
		Errores De Configuración	0,3		100%			
		Alteración Accidental De La Información	0,3		100%			
		Destrucción De Información	0,1	100%				
		Manipulación De Los Registros De Actividad	0,1		25%			75%
		Manipulación De La Configuración	0,1		75%	75%	75%	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
D11	Ficheros de contraseñas	Errores De Administración	0,1	75%	75%	100%		
		Errores De Configuración	0,1		5%			
		Alteración Accidental De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Manipulación De Los Registros De Actividad	0,1		25%			100%
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
D12	Registros de actividades en servidores	Errores De Administración	0,3	75%	50%	50%		
		Errores De Configuración	0,3		75%			
		Destrucción De Información	0,3	75%				
		Manipulación De La Configuración	0,1		75%	50%	75%	
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	50%	
		Abuso De Privilegios De Acceso	0,1	75%	50%	50%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,3		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
D13	Ficheros compartidos Google Drive	Errores De Administración	0,3	75%	50%	50%		
		Errores De Configuración	0,1		25%			
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,3	75%				
		Manipulación De La Configuración	0,1		50%	50%	50%	
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	50%	
		Abuso De Privilegios De Acceso	0,1	50%	50%	50%		
		Acceso No Autorizado	0,1		75%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		

Figura 65. Frecuencia y degradación de las amenazas del grupo Datos/Información (d) (Fuente propia)

- [S] Servicios

Para los servicios se evalúan dos tipos de amenazas: errores y ataques (distinguidos por dos tonalidades del color verde). Las amenazas con un alto valor de frecuencia son: errores de usuarios, suplantación de identidad del usuario, acceso no autorizado, alteración accidental, destrucción y fugas de información. El resto de las amenazas poseen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia del servicio dentro de la asociación. Todos los valores se observan en las Figuras 66 a la 68.

SERVICIOS [S]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
S1	Página web	Errores De Usuarios	0,5	5%	5%	25%		
		Errores De Administración	0,1	100%	75%	75%		
		Alteración Accidental De La Información	0,1		75%			
		Fugas De Información	0,1			50%		
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%				
		Suplantación De La Identidad Del Usuario	0,7		75%	75%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	75%		
		Uso No Previsto	0,3	50%	75%	75%		
		Acceso No Autorizado	0,5		100%	75%		
		Repudio	0,1		50%			75%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	75%				
		Divulgación De Información	0,3			100%		
		Denegación De Servicio	0,3	100%				
S2	Correo electrónico	Errores De Usuarios	0,7	50%	25%	50%		
		Errores De Administración	0,1	75%	25%	75%		
		Alteración Accidental De La Información	0,3		50%			
		Fugas De Información	0,1			75%		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,5		50%	75%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	75%		
		Uso No Previsto	0,3	75%	75%	75%		
		Acceso No Autorizado	0,5		75%	100%		
		Repudio	0,1		50%			75%
		Modificación Deliberada De La Información	0,1		75%			
		Divulgación De Información	0,3			75%		
		Denegación De Servicio	0,1	100%				
S3	Intranet documental - Servicio FTP	Errores De Usuarios	0,7	5%	50%	50%		
		Errores De Administración	0,3	75%	75%	50%		
		Alteración Accidental De La Información	0,5		75%			
		Destrucción De Información	0,5	75%				
		Fugas De Información	0,1			75%		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%		
		Uso No Previsto	0,3	50%	50%	75%		
		Acceso No Autorizado	0,5		50%	100%		
		Repudio	0,3		25%			75%
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			75%		
		Denegación De Servicio	0,3	100%				
S4	Sistema de tickets de incidencias	Errores De Usuarios	0,7	5%	25%	25%		
		Errores De Administración	0,3	75%	50%	25%		
		Alteración Accidental De La Información	0,3		50%			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%	
		Acceso No Autorizado	0,5		75%	75%		
		Repudio	0,1		50%			75%
		Modificación Deliberada De La Información	0,1		50%			
		Divulgación De Información	0,1			50%		
		Denegación De Servicio	0,3	100%				

Figura 66. Frecuencia y degradación de las amenazas del grupo servicios (a)
(Fuente propia)

S5	Educación Virtual	Errores De Usuarios	0,7	5%	25%	50%		
		Errores De Administración	0,3	75%	50%	50%		
		Alteración Accidental De La Información	0,5		75%			
		Destrucción De Información	0,5	100%				
		Fugas De Información	0,5			50%		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,5		25%	75%	50%	
		Abuso De Privilegios De Acceso	0,3	25%	75%	50%		
		Uso No Previsto	0,5	50%	25%	50%		
		Acceso No Autorizado	0,5		75%	75%		
		Repudio	0,1		25%			75%
		Modificación Deliberada De La Información	0,1		75%			
		Divulgación De Información	0,3			50%		
		Denegación De Servicio	0,3	100%				
S6	Servicio de financiero	Errores De Usuarios	0,5	25%	75%	100%		
		Errores De Administración	0,3	75%	50%	75%		
		Alteración Accidental De La Información	0,5		100%			
		Destrucción De Información	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	25%	75%	75%		
		Uso No Previsto	0,3	50%	50%	50%		
		Acceso No Autorizado	0,3		100%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
		Denegación De Servicio	0,3	100%				
S7	Gestión de usuarios Socios	Errores De Usuarios	0,5	25%	75%	50%		
		Errores De Administración	0,3	75%	50%	75%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	50%		
		Uso No Previsto	0,3	50%	25%	75%		
		Acceso No Autorizado	0,5		75%	100%		
		Repudio	0,1		25%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,3			100%		
		Denegación De Servicio	0,3	100%				
S8	Gestión empresarial	Errores De Usuarios	0,5	25%	50%	50%		
		Errores De Administración	0,3	50%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	75%				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	50%		
		Uso No Previsto	0,3	25%	50%	75%		
		Acceso No Autorizado	0,5		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,3			100%		
		Denegación De Servicio	0,3	100%				

Figura 67. Frecuencia y degradación de las amenazas del grupo servicios (b)
(Fuente propia)

S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	0,5	25%	50%	75%		
		Errores De Administración	0,3	50%	50%	75%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	50%	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%		
		Uso No Previsto	0,3	25%	50%	75%		
		Acceso No Autorizado	0,5		75%	100%		
		Repudio	0,1		50%			100%
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,3			100%		
		Denegación De Servicio	0,3	100%				

Figura 68. Frecuencia y degradación de las amenazas del grupo servicios (c)
(Fuente propia)

- [SW] Software – Aplicaciones Informáticas

Para estos activos se evalúan tres tipos de amenazas: de origen industrial, errores y los ataques (distinguidos por tres tonalidades del color amarillo paja). Para la aplicación de correo electrónico – Gmail y los navegadores web no se consideran las amenazas de origen industrial. Las amenazas con un alto valor de frecuencia son: errores de usuarios, uso no previsto y difusión de software dañino. El resto de las amenazas poseen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia de la aplicación dentro de la asociación. Todos los valores calculados se observan en las Figuras 69 a la 73.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
SW1	Aplicación de Financiero	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	25%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	75%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		

Figura 69. Frecuencia y degradación de las amenazas del grupo aplicaciones informáticas (a)
(Fuente propia)

SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	50%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	50%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	50%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	0,1	75%				
		Errores De Administración	0,1	75%	75%	50%		
		Alteración Accidental De La Información	0,3		100%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	100%			
		Suplantación De La Identidad Del Usuario	0,1		100%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	75%	100%	100%		
		Uso No Previsto	0,3	75%	75%	100%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		

Figura 70. Frecuencia y degradación de las amenazas del grupo aplicaciones informáticas (b) (Fuente propia)

SW6	**Aplicación de Página web**	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	25%	25%	25%		
		Errores De Administración	0,1	75%	50%	75%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	75%				
		Fugas De Información	0,1			50%		
		Vulnerabilidades De Los Programas	0,3	75%	75%	75%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,5	50%	50%	100%		
		Difusión De Software Dañino	0,1	50%	50%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			75%		
		Manipulación De Programas	0,1	50%	75%	75%		
SW7	**Aplicación de Intranet**	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	50%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW8	**Aplicación del Sistema de tickets de incidencias**	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	50%	75%	50%		
		Errores De Administración	0,1	75%	50%	50%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	50%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW9	**Aplicación de Correo electrónico Gmail**	Errores De Usuarios	0,5	5%	5%	25%		
		Errores De Administración	0,1	25%	5%	50%		
		Difusión De Software Dañino	0,1	5%	5%	100%		
		Alteración Accidental De La Información	0,3		5%			
		Destrucción De Información	0,1	25%				
		Fugas De Información	0,3			100%		
		Vulnerabilidades De Los Programas	0,3	5%	50%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,1	25%	50%	75%		
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	100%	
		Abuso De Privilegios De Acceso	0,1	5%	75%	75%		
		Uso No Previsto	0,3	50%	75%	100%		
		Difusión De Software Dañino	0,1	5%	50%	100%		
		Acceso No Autorizado	0,1		50%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		

Figura 71. Frecuencia y degradación de las amenazas del grupo aplicaciones informáticas (c) (Fuente propia)

SW10	E-apsa	Fallo De Origen Lógico	0,1	75%				
		Errores De Usuarios	0,5	5%	5%	25%		
		Errores De Administración	0,1	50%	50%	75%		
		Alteración Accidental De La Información	0,3		25%			
		Destrucción De Información	0,3	5%				
		Fugas De Información	0,1			25%		
		Vulnerabilidades De Los Programas	0,3	5%	25%	50%		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%			
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	100%	
		Abuso De Privilegios De Acceso	0,3	5%	25%	75%		
		Uso No Previsto	0,1	25%	5%	50%		
		Difusión De Software Dañino	0,1	5%	25%	50%		
		Acceso No Autorizado	0,1		25%	100%		
		Modificación Deliberada De La Información	0,1		25%			
		Destrucción De Información	0,1	75%				
		Divulgación De Información	0,1			75%		
SW11	Aplicaciones en móviles	Fallo De Origen Lógico	0,1	50%				
		Errores De Usuarios	0,5	5%	25%	50%		
		Errores De Administración	0,1	25%	25%	50%		
		Difusión De Software Dañino	0,3	5%	25%	75%		
		Alteración Accidental De La Información	0,3		25%			
		Destrucción De Información	0,3	25%				
		Fugas De Información	0,3			75%		
		Vulnerabilidades De Los Programas	0,3	25%	25%	75%		
		Errores De Mantenimiento/Actualización De Programas	0,5	50%	25%			
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	100%	
		Abuso De Privilegios De Acceso	0,3	25%	75%	75%		
		Uso No Previsto	0,1	75%	50%	75%		
		Difusión De Software Dañino	0,1	75%	50%	100%		
		Acceso No Autorizado	0,1		25%	100%		
		Modificación Deliberada De La Información	0,1		25%			
		Destrucción De Información	0,1	50%				
		Divulgación De Información	0,1			100%		
SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	0,1	75%				
		Errores De Administración	0,1	100%	75%	100%		
		Alteración Accidental De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Vulnerabilidades De Los Programas	0,1	75%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	75%	75%			
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,1	50%	75%	100%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	0,1	75%				
		Errores De Administración	0,1	100%	75%	100%		
		Alteración Accidental De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Vulnerabilidades De Los Programas	0,1	75%	75%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	75%	75%			
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,1	50%	75%	100%		
		Difusión De Software Dañino	0,1	100%	100%	100%		
		Acceso No Autorizado	0,1		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		

Figura 72. Frecuencia y degradación de las amenazas del grupo aplicaciones informáticas (d) (Fuente propia)

SW14	**Sistema operativo Windows 7**	Fallo De Origen Lógico	0,1	100%				
		Errores De Usuarios	0,5	25%	5%	25%		
		Errores De Administración	0,1	50%	25%	50%		
		Difusión De Software Dañino	0,1	75%	50%	75%		
		Alteración Accidental De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Vulnerabilidades De Los Programas	0,3	25%	25%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%			
		Suplantación De La Identidad Del Usuario	0,3		5%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	5%	5%	75%		
		Uso No Previsto	0,3	25%	25%	100%		
		Difusión De Software Dañino	0,1	75%	75%	100%		
		Acceso No Autorizado	0,3		25%	100%		
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
SW15	**Sistema operativo Windows 10**	Fallo De Origen Lógico	0,1	100%				
		Errores De Usuarios	0,5	25%	5%	25%		
		Errores De Administración	0,1	50%	25%	50%		
		Difusión De Software Dañino	0,1	75%	50%	75%		
		Alteración Accidental De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Vulnerabilidades De Los Programas	0,3	25%	25%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%			
		Suplantación De La Identidad Del Usuario	0,3		5%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	5%	5%	75%		
		Uso No Previsto	0,3	25%	25%	100%		
		Difusión De Software Dañino	0,1	75%	75%	100%		
		Acceso No Autorizado	0,3		25%	100%		
		Modificación Deliberada De La Información	0,1		75%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
SW16	**Navegadores Web**	Errores De Usuarios	0,5	5%	5%	75%		
		Errores De Administración	0,1	25%	5%	75%		
		Fugas De Información	0,1			100%		
		Vulnerabilidades De Los Programas	0,1	25%	50%	100%		
		Errores De Mantenimiento/Actualización De Programas	0,3	5%	50%			
		Abuso De Privilegios De Acceso	0,3	5%	5%	75%		
		Uso No Previsto	0,3	5%	25%	75%		
		Difusión De Software Dañino	0,5	5%	25%	100%		
		Modificación Deliberada De La Información	0,1		25%			
		Destrucción De Información	0,1	25%				
		Divulgación De Información	0,1			25%		
SW17	**Antivirus**	Fallo De Origen Lógico	0,1	75%				
		Errores De Administración	0,1	50%	25%	25%		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	100%			
		Abuso De Privilegios De Acceso	0,1	50%	100%	25%		
		Uso No Previsto	0,1	50%	100%	25%		
		Acceso No Autorizado	0,1		100%	25%		
		Modificación Deliberada De La Información	0,1		100%			
SW18	**Software Ofimático**	Fallo De Origen Lógico	0,3	50%				
		Errores De Usuarios	0,5	50%	5%	25%		
		Errores De Administración	0,1	50%	5%	25%		
		Errores De Mantenimiento/Actualización De Programas	0,3	75%	25%			
		Abuso De Privilegios De Acceso	0,1	25%	25%	25%		
		Uso No Previsto	0,1	50%	25%	25%		

Figura 73. Frecuencia y degradación de las amenazas del grupo aplicaciones informáticas (e) (Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Para este tipo de activos se evalúan tres tipos de amenazas: de origen industrial y los ataques (distinguidos por tres tonalidades del color gris). Las amenazas con un alto valor de frecuencia son: acceso no autorizado, uso no previsto, errores de mantenimiento, avería de origen físico/lógico, abuso de privilegios de acceso, manipulación de equipos y caída del sistema por agotamiento de recursos. El resto de las amenazas poseen una frecuencia de ocurrencia baja.

Los valores de la degradación son variados pues dependen de la importancia del uso del equipo dentro de la asociación. Todos los valores calculados se observan en las Figuras 74 a la 76.

EQUIPOS INFORMÁTICOS [HW]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
HW1	Servidores APSA	Avería De Origen Físico/Lógico	0,3	100%				
		Errores De Administración	0,1	100%	100%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,1	75%	75%	100%		
		Uso No Previsto	0,3	75%	75%	100%		
		Acceso No Autorizado	0,7		75%	100%		
		Denegación De Servicio	0,3	100%				
HW2	Servidores Sedes	Daños Por Agua	0,1	100%				
		Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,3	100%				
		Fallas De Climatización	0,1	25%				
		Errores De Administración	0,1	75%	75%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,3	75%	75%	100%		
		Uso No Previsto	0,3	50%	50%	100%		
		Acceso No Autorizado	0,5		75%	100%		
		Manipulación De Equipos	0,3	75%		75%		
		Denegación De Servicio	0,3	100%				
		Robo	0,1	100%		75%		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	0,1	75%				
		Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,3	100%				
		Errores De Administración	0,1	50%	50%	75%		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%				
		Perdida De Equipos	0,1	100%		100%		
		Abuso De Privilegios De Acceso	0,1	50%	50%	100%		
		Uso No Previsto	0,3	75%	25%	100%		
		Acceso No Autorizado	0,1		25%	100%		
		Manipulación De Equipos	0,3	50%		100%		
		Robo	0,1	100%		100%		
HW4	Ordenadores de escritorio empleados	Daños Por Agua	0,1	75%				
		Avería De Origen Físico/Lógico	0,5	100%				
		Corte De Suministro Eléctrico	0,3	100%				
		Errores De Administración	0,3	50%	50%	75%		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%				
		Perdida De Equipos	0,1	100%		75%		
		Abuso De Privilegios De Acceso	0,5	50%	50%	75%		
		Uso No Previsto	0,5	75%	25%	75%		
		Acceso No Autorizado	0,3		25%	75%		
		Manipulación De Equipos	0,5	50%		75%		
		Robo	0,1	100%		100%		
HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,1	25%				
		Errores De Administración	0,3	50%	25%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%				
		Perdida De Equipos	0,1	100%		100%		
		Abuso De Privilegios De Acceso	0,3	25%	25%	100%		
		Uso No Previsto	0,3	50%	25%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Manipulación De Equipos	0,3	75%		100%		
		Robo	0,1	100%		100%		

Figura 74. Frecuencia y degradación de las amenazas del grupo equipos informáticos (a) (Fuente propia)

HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,1	25%				
		Errores De Administración	0,3	50%	25%	25%		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%				
		Perdida De Equipos	0,1	100%		75%		
		Abuso De Privilegios De Acceso	0,3	25%	25%	75%		
		Uso No Previsto	0,3	50%	25%	75%		
		Acceso No Autorizado	0,3		50%	75%		
		Manipulación De Equipos	0,3	50%		75%		
		Robo	0,1	100%		100%		
HW7	Portátiles TIC	Daños Por Agua	0,1	100%				
		Avería De Origen Físico/Lógico	0,1	100%				
		Corte De Suministro Eléctrico	0,1	75%				
		Errores De Administración	0,1	50%	75%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Manipulación De Equipos	0,1	50%		100%		
HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	0,3	75%				
		Errores De Administración	0,1	25%	25%	50%		
		Errores De Mantenimiento/Actualización De Equipos	0,5	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	50%				
		Perdida De Equipos	0,5	100%		100%		
		Abuso De Privilegios De Acceso	0,3	50%	50%	100%		
		Uso No Previsto	0,5	50%	50%	100%		
		Acceso No Autorizado	0,1		75%	100%		
		Manipulación De Equipos	0,5	75%		100%		
		Robo	0,3	100%		100%		
HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,1	100%				
		Errores De Administración	0,1	50%	50%	5%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	50%				
		Caída Del Sistema Por Agotamiento De Recursos	0,5	75%				
		Perdida De Equipos	0,1	100%		25%		
		Abuso De Privilegios De Acceso	0,3	50%	25%	5%		
		Uso No Previsto	0,3	25%	25%	25%		
		Acceso No Autorizado	0,1		25%	25%		
		Manipulación De Equipos	0,3	50%		25%		
		Robo	0,1	100%		25%		
HW10	Router	Avería De Origen Físico/Lógico	0,1	100%				
		Corte De Suministro Eléctrico	0,1	100%				
		Fallas De Climatización	0,1	50%				
		Errores De Administración	0,1	75%	50%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,1	75%	50%	100%		
		Uso No Previsto	0,1	75%	50%	100%		
		Acceso No Autorizado	0,3		75%	100%		
		Manipulación De Equipos	0,3	75%		100%		
		Denegación De Servicio	0,3	100%				
HW11	Router inalámbrico	Daños Por Agua	0,1	100%				
		Avería De Origen Físico/Lógico	0,1	75%				
		Corte De Suministro Eléctrico	0,1	100%				
		Errores De Administración	0,1	75%	50%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Perdida De Equipos	0,1	100%		50%		
		Abuso De Privilegios De Acceso	0,3	50%	50%	75%		
		Uso No Previsto	0,3	75%	75%	75%		
		Acceso No Autorizado	0,3		75%	100%		
		Manipulación De Equipos	0,3	75%		50%		
		Denegación De Servicio	0,3	100%				
		Robo	0,1	100%		50%		

Figura 75. Frecuencia y degradación de las amenazas del grupo equipos informáticos (b) (Fuente propia)

HW12	Switch	Avería De Origen Físico/Lógico	0,1	100%				
		Corte De Suministro Eléctrico	0,1	100%				
		Fallas De Climatización	0,1	50%				
		Errores De Administración	0,1	75%	50%	100%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,1	75%	50%	100%		
		Uso No Previsto	0,1	75%	50%	100%		
		Acceso No Autorizado	0,3		75%	100%		
		Manipulación De Equipos	0,3	75%		100%		
		Denegación De Servicio	0,3	100%				
HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	0,3	100%				
		Corte De Suministro Eléctrico	0,1	100%				
		Errores De Administración	0,3	75%	25%	50%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%				
		Abuso De Privilegios De Acceso	0,3	50%	50%	25%		
		Uso No Previsto	0,3	75%	50%	25%		
		Acceso No Autorizado	0,1		50%	25%		
		Manipulación De Equipos	0,3	75%		25%		
HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	0,1	100%				
		Corte De Suministro Eléctrico	0,1	100%				
		Errores De Administración	0,1	50%	25%	50%		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Abuso De Privilegios De Acceso	0,3	50%	25%	75%		
		Uso No Previsto	0,3	75%	25%	75%		
		Acceso No Autorizado	0,1		50%	75%		
		Manipulación De Equipos	0,5	75%		75%		
		Robo	0,1	100%		5%		

Figura 76. Frecuencia y degradación de las amenazas del grupo equipos informáticos (c) (Fuente propia)

- [COM] Redes de Comunicaciones

Para las redes de comunicaciones se evalúan tres tipos de amenazas: de origen industrial, errores y los ataques (distinguidos por tres tonalidades del color naranja). Las amenazas con un alto valor de frecuencia son: suplantación de la identidad de usuario, acceso no autorizado, divulgación de la información, denegación de servicio, abuso de privilegios de acceso y uso no previsto. Las demás amenazas poseen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia del servicio que ofrece la red de comunicaciones a la asociación. Todos los valores calculados se observan en las Figuras 77 y 78.

REDES DE COMUNICACIONES [COM]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	0,3	100%				
		Errores De Administración	0,1	75%	25%	75%		
		Alteración Accidental De La Información	0,3		50%			
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%				
		Suplantación De La Identidad Del Usuario	0,7		50%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	50%	75%		
		Uso No Previsto	0,3	50%	25%	75%		
		Acceso No Autorizado	0,5		50%	100%		
		Análisis De Trafico	0,1			100%		
		Interceptación De Información (Escucha)	0,1			100%		
		Modificación Deliberada De La Información	0,3		75%			
		Divulgación De Información	0,5			75%		
		Denegación De Servicio	0,5	100%				

Figura 77. Frecuencia y degradación de las amenazas del grupo redes de comunicaciones (a) (Fuente propia)

COM2	**Redes locales**	Fallo Servicios De Comunicaciones	0,3	100%				
		Errores De Administración	0,1	75%	50%	100%		
		Alteración Accidental De La Información	0,3		50%			
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%				
		Suplantación De La Identidad Del Usuario	0,5		75%	100%	100%	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%		
		Uso No Previsto	0,3	50%	50%	100%		
		Acceso No Autorizado	0,5		50%	100%		
		Análisis De Trafico	0,1			100%		
		Interceptación De Información (Escucha)	0,1			100%		
		Modificación Deliberada De La Información	0,3		75%			
		Divulgación De Información	0,5			75%		
		Denegación De Servicio	0,5	100%				
COM3	**Red telefónica**	Fallo Servicios De Comunicaciones	0,3	100%				
		Errores De Administración	0,1	75%	50%	75%		
		Alteración Accidental De La Información	0,3		50%			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%				
		Abuso De Privilegios De Acceso	0,5	50%	25%	75%		
		Uso No Previsto	0,5	50%	25%	75%		
		Acceso No Autorizado	0,3		25%	100%		
		Análisis De Trafico	0,1			100%		
		Interceptación De Información (Escucha)	0,1			100%		
		Modificación Deliberada De La Información	0,1		50%			
		Divulgación De Información	0,3			75%		
		Denegación De Servicio	0,1	100%				
COM4	**Red telefonía móvil**	Fallo Servicios De Comunicaciones	0,3	100%				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	75%				
		Suplantación De La Identidad Del Usuario	0,1		5%	75%	75%	
		Abuso De Privilegios De Acceso	0,3	5%	5%	50%		
		Uso No Previsto	0,3	5%	5%	75%		
		Acceso No Autorizado	0,3		5%	75%		
		Análisis De Trafico	0,1			100%		
		Interceptación De Información (Escucha)	0,1			100%		
		Divulgación De Información	0,3			100%		

Figura 78. Frecuencia y degradación de las amenazas del grupo redes de comunicaciones (b) (Fuente propia)

- [MEDIA] Soportes de Información: Para este tipo de activos se evalúan todos los tipos de amenazas: de origen natural, de origen industrial, errores y los ataques (distinguidos por cuatro tonalidades de color violeta). Las amenazas con un alto valor de frecuencia son: errores de usuarios, alteración accidental de la información, destrucción de la información, pérdida de soporte, uso no previsto, destrucción, errores de almacenamiento y pérdida. El resto de las amenazas poseen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia del uso del activo dentro de la asociación. Todos los valores calculados se observan en la Figura 79.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	0,3	100%				
		Daños Por Agua	0,3	100%				
		Avería De Origen Físico/Lógico	0,1	75%				
		Degradación De Los Soportes De Almacenamiento De La Información	0,1	75%				
		Errores De Usuarios	0,3	25%	75%	100%		
		Errores De Administración	0,1	25%	75%	100%		
		Alteración Accidental De La Información	0,3		75%			
		Destrucción De Información	0,1	100%				
		Fugas De Información	0,1			100%		
		Errores De Mantenimiento del soporte	0,3	25%				
		Perdida del soporte	0,1	100%		100%		
		Uso No Previsto	0,3	100%	100%	100%		
		Acceso No Autorizado	0,3		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,1			100%		
		Manipulación del soporte	0,3	50%		100%		
		Robo	0,1	100%		100%		
MEDIA2	Pendrives USB	Daños Por Agua	0,1	100%				
		Daños Por Agua	0,3	100%				
		Avería De Origen Físico/Lógico	0,1	75%				
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	75%				
		Errores De Usuarios	0,5	25%	50%	100%		
		Errores De Administración	0,1	25%	50%	100%		
		Alteración Accidental De La Información	0,5		100%			
		Destrucción De Información	0,5	100%				
		Fugas De Información	0,3			100%		
		Errores De Mantenimiento del soporte	0,1	50%				
		Perdida del soporte	0,7	100%		100%		
		Uso No Previsto	0,7	75%	100%	100%		
		Acceso No Autorizado	0,1		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,3			100%		
		Manipulación del soporte	0,1	75%		100%		
		Robo	0,3	100%		100%		
MEDIA3	CD/DVD	Daños Por Agua	0,1	100%				
		Daños Por Agua	0,3	100%				
		Avería De Origen Físico/Lógico	0,1	75%				
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	75%				
		Errores De Usuarios	0,5	25%	50%	100%		
		Errores De Administración	0,1	25%	50%	100%		
		Alteración Accidental De La Información	0,5		100%			
		Destrucción De Información	0,5	100%				
		Fugas De Información	0,3			100%		
		Errores De Mantenimiento del soporte	0,1	50%				
		Perdida del soporte	0,7	100%		100%		
		Uso No Previsto	0,7	75%	100%	100%		
		Acceso No Autorizado	0,1		100%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción De Información	0,1	100%				
		Divulgación De Información	0,3			100%		
		Manipulación del soporte	0,1	75%		100%		
		Robo	0,3	100%		100%		
MEDIA4	Material impreso	Daños Por Agua	0,1	100%				
		Daños Por Agua	0,1	100%				
		Degradación por Almacenamiento	0,3	75%				
		Errores De Usuarios	0,5	50%	75%	75%		
		Errores De Administración	0,1	50%	75%	75%		
		Alteración Accidental De La Información	0,5		50%			
		Destrucción	0,5	100%				
		Fugas De Información	0,1			100%		
		Errores De Almacenamiento	0,5	50%				
		Perdida	0,5	50%		100%		
		Uso No Previsto	0,3	100%	75%	100%		
		Acceso No Autorizado	0,3		75%	100%		
		Modificación Deliberada De La Información	0,1		100%			
		Destrucción	0,1	100%				
		Divulgación	0,1			100%		
		Manipulación	0,1	50%		100%		
		Robo	0,3	50%		100%		

Figura 79. Frecuencia y degradación de las amenazas del grupo soportes de información (a) (Fuente propia)

- [AUX] Equipamiento Auxiliar

Para el equipamiento auxiliar se evaluaron todos los tipos de amenazas: de origen natural, de origen industrial, errores y los ataques (distinguidos por cuatro tonalidades del color verde claro). La única amenaza con un valor alto de frecuencia es la manipulación de equipos. El resto de las amenazas poseen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia del servicio dentro de la asociación. Todos los valores calculados se observan en las Figuras 80 y 81.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Frecuencia	Degradación				
Código	Nombre	Amenaza	F	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	0,3	75%				
		Fuego	0,1	75%				
		Daños Por Agua	0,3	75%				
		Contaminación Mecánica	0,1	50%				
		Degradación por almacenamiento	0,3	50%				
		Avería De Origen Físico/ Lógico	0,3	75%				
		Errores De Mantenimiento/ Actualización De Equipos	0,1	75%				
		Uso No Previsto	0,3	75%	25%	5%		
		Acceso No Autorizado	0,3		25%	5%		
		Manipulación De Equipos	0,3	75%		5%		
AUX2	Fuentes de alimentación	Daños Por Agua	0,3	75%				
		Fuego	0,1	75%				
		Daños Por Agua	0,3	75%				
		Contaminación Mecánica	0,1	50%				
		Degradación por almacenamiento	0,3	50%				
		Avería De Origen Físico/ Lógico	0,3	75%				
		Corte De Suministro Eléctrico	0,3	100%				
		Errores De Mantenimiento/ Actualización De Equipos	0,3	75%				
		Perdida De Equipos	0,1	100%		5%		
		Uso No Previsto	0,3	100%	25%	5%		
		Acceso No Autorizado	0,3		25%	5%		
		Manipulación De Equipos	0,3	75%		5%		
		Robo	0,1	100%		5%		
AUX3	Climatización	Daños Por Agua	0,3	75%				
		Fuego	0,1	75%				
		Daños Por Agua	0,3	75%				
		Contaminación Mecánica	0,1	50%				
		Avería De Origen Físico/Lógico	0,3	75%				
		Corte De Suministro Eléctrico	0,3	100%				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Uso No Previsto	0,3	50%	25%	5%		
		Acceso No Autorizado	0,3		25%	5%		
		Manipulación De Equipos	0,5	50%		5%		
AUX4	Cableado UTP	Daños Por Agua	0,3	75%				
		Fuego	0,1	100%				
		Daños Por Agua	0,3	75%				
		Avería De Origen Físico/Lógico	0,3	75%				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Uso No Previsto	0,3	50%	25%	25%		
		Acceso No Autorizado	0,1		25%	75%		
		Manipulación De Equipos	0,1	50%		75%		

Figura 80. Frecuencia y degradación de las amenazas del grupo equipo auxiliar (a) (Fuente propia)

AUX5	Armarios	Daños Por Agua	0,3	50%				
		Fuego	0,1	75%				
		Daños Por Agua	0,3	50%				
		Degradación por almacenamiento	0,1	25%				
		Avería De Origen Físico/Lógico	0,3	50%				
		Uso No Previsto	0,3	25%	25%	75%		
		Acceso No Autorizado	0,3		25%	75%		
		Manipulación De Equipos	0,5	25%		75%		
AUX6	Cajas fuertes	Daños Por Agua	0,1	25%				
		Fuego	0,1	25%				
		Daños Por Agua	0,1	25%				
		Avería De Origen Físico/Lógico	0,1	75%				
		Corte De Suministro Eléctrico	0,1	75%				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%				
		Perdida De Equipos	0,1	100%		100%		
		Uso No Previsto	0,1	75%	5%	100%		
		Acceso No Autorizado	0,3		5%	100%		
		Manipulación De Equipos	0,5	25%		100%		

Figura 81. Frecuencia y degradación de las amenazas del grupo equipamiento auxiliar (b) (Fuente propia)

- [L]Instalaciones

Para el equipamiento auxiliar se evalúan todos los tipos de amenazas: de origen natural, de origen industrial, errores y los ataques (distinguidos por cuatro tonalidades del color rojo); para el activo coche, se aplica únicamente las amenazas de origen industrial. No existe amenazas con valores altos de frecuencia, todas tienen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia del activo en la asociación. Todos los valores calculados se observan en la Figura 82.

ACTIVOS DE INSTALACIONES [L]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
L1	Edificios	Fuego	0,1	100%				
		Daños Por Agua	0,3	75%				
		Fuego	0,1	75%				
		Daños Por Agua	0,3	50%				
		Fugas De Información	0,3			75%		
		Uso No Previsto	0,1	25%	25%	75%		
		Acceso No Autorizado	0,3		25%	100%		
L2	Cuartos servidores	Fuego	0,1	100%				
		Daños Por Agua	0,1	100%				
		Fuego	0,1	100%				
		Daños Por Agua	0,3	100%				
		Fugas De Información	0,1			100%		
		Uso No Previsto	0,3	75%	75%	75%		
		Acceso No Autorizado	0,3		50%	100%		
L3	Coche	Daños mecánicos	0,1	100%				
		Accidente de tránsito	0,1	100%				

Figura 82. Frecuencia y degradación de las amenazas del grupo instalaciones (Fuente propia)

- [P] Personal

Para el personal se evalúan dos tipos de amenazas: errores y los ataques (distinguidos por dos tonalidades del color celeste). No existe amenazas con valores altos de frecuencia, todas tienen una frecuencia de ocurrencia baja. Los valores de la degradación son variados pues dependen de la importancia de las funciones del personal dentro de la asociación. Todos los valores calculados se observan en la Figura 83.

ACTIVOS DE PERSONAL [P]			Frecuencia	Degradación				
Código	Nombre	Amenazas	F	D	I	C	A	T
P1	Administradores	Fugas De Información	0,1			100%		
		Indisponibilidad Del Personal	0,3	75%				
		Indisponibilidad Del Personal	0,1	75%				
		Extorsión	0,1	25%	75%	100%		
		Ingeniería Social	0,1	25%	75%	100%		
P2	Técnicos	Fugas De Información	0,1			100%		
		Indisponibilidad Del Personal	0,3	50%				
		Indisponibilidad Del Personal	0,1	50%				
		Extorsión	0,1	25%	50%	100%		
		Ingeniería Social	0,1	25%	50%	100%		
P3	Empleados	Fugas De Información	0,1			100%		
		Indisponibilidad Del Personal	0,3	50%				
		Indisponibilidad Del Personal	0,1	50%				
		Extorsión	0,1	25%	50%	100%		
		Ingeniería Social	0,1	25%	50%	100%		
P4	Usuarios	Fugas De Información	0,3			100%		
		Extorsión	0,1	25%	50%	100%		
		Ingeniería Social	0,1	25%	50%	100%		

Figura 83. Frecuencia y degradación de las amenazas del grupo personal
(Fuente propia)

4.4. Impacto y Riesgos

4.4.1. Cálculos de Impacto

Determinada la frecuencia de ocurrencia y la degradación que causa una amenaza, se realiza el cálculo del impacto potencial o impacto repercutido con la fórmula:

$$IP = VA * GD$$

Donde:

IP = Impacto potencial

VA = Valor del activo

GD = Grado de degradación de los activos (%)

Según la fórmula anterior, para el cálculo del impacto potencial se requiere la valoración de los activos determinados anteriormente. Los resultados se pueden ver a continuación:

- [D] Datos /Información

El impacto para este grupo varía entre el valor mínimo de 0,35 y el valor máximo de 9. Para los activos con valoraciones altas, las amenazas producen mucha degradación por lo que, se observa varios valores de impacto de 8 y 9 en todas las dimensiones de seguridad. Además, se encuentran mayormente valores medios entre 4 y 7, ya sea porque el activo tiene un valor bajo o el grado de degradación es bajo. Los pocos valores menores que 4 se producen por valores de activos y degradación bajos. Por otra parte, aunque las amenazas producen degradación en todas las dimensiones de seguridad, en el impacto no se observa valores en aquellas dimensiones en las que no existe degradación. Todos los valores calculados se observan en las Figuras 84 a la 85.

DATOS / INFORMACIÓN [D]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	75%	75%	25%			8	8	8	9	9	6	6	2		
		Errores De Configuración		50%				8	8	8	9	9		4			
		Alteración Accidental De La Información		50%				8	8	8	9	9		4			
		Destrucción De Información	100%					8	8	8	9	9	8				
		Fugas De Información			50%			8	8	8	9	9			4		
		Manipulación De Los Registros De Actividad		5%			75%	8	8	8	9	9		0,4			6,75
		Manipulación De La Configuración		100%	100%	100%		8	8	8	9	9		8	8	9	
		Abuso De Privilegios De Acceso	75%	75%	75%			8	8	8	9	9	6	6	6		
		Acceso No Autorizado		75%	100%			8	8	8	9	9		6	8		
		Repudio		75%			100%	8	8	8	9	9		6			9
		Modificación Deliberada De La Información		100%				8	8	8	9	9		8			
		Destrucción De Información	100%					8	8	8	9	9	8				
D2	Código fuente de aplicaciones	Errores De Administración	50%	75%	25%			8	9	8	9	9	4	6,75	2		
		Errores De Configuración		75%				8	9	8	9	9		6,75			
		Alteración Accidental De La Información		100%				8	9	8	9	9		9			
		Manipulación De Los Registros De Actividad		5%			75%	8	9	8	9	9		0,45			6,75
		Manipulación De La Configuración		75%	50%	50%		8	9	8	9	9		6,75	4	4,5	
		Abuso De Privilegios De Acceso	25%	75%	75%			8	9	8	9	9	2	6,75	6		
		Acceso No Autorizado		100%	100%			8	9	8	9	9		9	8		
		Repudio		75%			100%	8	9	8	9	9		6,75			9
		Modificación Deliberada De La Información		100%				8	9	8	9	9		9			
		Destrucción De Información	100%					8	9	8	9	9	8				
D3	Ficheros almacenados en PC	Errores De Usuarios	75%	75%	50%			3	7	5	6	7	2,25	5,25	2,5		
		Errores De Administración	75%	75%	50%			3	7	5	6	7	2,25	5,25	2,5		
		Errores De Configuración		25%				3	7	5	6	7		1,75			
		Alteración Accidental De La Información		75%				3	7	5	6	7		5,25			
		Destrucción De Información	100%					3	7	5	6	7	3				
		Fugas De Información			25%			3	7	5	6	7			1,25		
		Manipulación De Los Registros De Actividad		25%			50%	3	7	5	6	7		1,75			3,5
		Manipulación De La Configuración		50%	50%	25%		3	7	5	6	7		3,5	2,5	1,5	
		Suplantación De La Identidad Del Usuario		50%	75%	75%		3	7	5	6	7		3,5	3,75	4,5	
		Abuso De Privilegios De Acceso	25%	50%	75%			3	7	5	6	7	0,75	3,5	3,75		
		Acceso No Autorizado		75%	100%			3	7	5	6	7		5,25	5		
		Repudio		25%			100%	3	7	5	6	7		1,75			7
		Modificación Deliberada De La Información		100%				3	7	5	6	7		7			
		Destrucción De Información	75%					3	7	5	6	7	2,25				

Figura 84. Impacto potencial de las amenazas del grupo Datos/Información (a)
(Fuente propia)

D4	Ficheros almacenados en servidores en la nube	Errores De Usuarios	50%	50%	5%			5	7	7	8	8	2,5	3,5	0,35			
		Errores De Administración	75%	75%	50%			5	7	7	8	8	3,75	5,25	3,5			
		Errores De Monitorización Log		50%			75%	5	7	7	8	8		3,5				6
		Errores De Configuración		50%				5	7	7	8	8		3,5				
		Alteración Accidental De La Información		75%				5	7	7	8	8		5,25				
		Destrucción De Información	75%					5	7	7	8	8	3,75					
		Manipulación De Los Registros De Actividad		25%			75%	5	7	7	8	8		1,75				6
		Manipulación De La Configuración		25%	50%	50%		5	7	7	8	8		1,75	3,5	4		
		Suplantación De La Identidad Del Usuario		25%	75%	75%		5	7	7	8	8		1,75	5,25	6		
		Abuso De Privilegios De Acceso	25%	25%	75%			5	7	7	8	8	1,25	1,75	5,25			
		Acceso No Autorizado		50%	100%			5	7	7	8	8		3,5	7			
		Repudio		25%			100%	5	7	7	8	8		1,75				8
		Modificación Deliberada De La Información		100%				5	7	7	8	8		7				
		Destrucción De Información	100%					5	7	7	8	8	5					
D5	Ficheros almacenados en servidores locales	Errores De Usuarios	75%	50%	5%			5	7	7	8	8	3,75	3,5	0,35			
		Errores De Administración	75%	75%	50%			5	7	7	8	8	3,75	5,25	3,5			
		Errores De Monitorización Log		50%			75%	5	7	7	8	8		3,5				6
		Errores De Configuración		50%				5	7	7	8	8		3,5				
		Alteración Accidental De La Información		75%				5	7	7	8	8		5,25				
		Destrucción De Información	75%					5	7	7	8	8	3,75					
		Manipulación De Los Registros De Actividad		25%			75%	5	7	7	8	8		1,75				6
		Manipulación De La Configuración		25%	50%	50%		5	7	7	8	8		1,75	3,5	4		
		Suplantación De La Identidad Del Usuario		25%	75%	75%		5	7	7	8	8		1,75	5,25	6		
		Abuso De Privilegios De Acceso	25%	25%	75%			5	7	7	8	8	1,25	1,75	5,25			
		Acceso No Autorizado		50%	100%			5	7	7	8	8		3,5	7			
		Repudio		25%			100%	5	7	7	8	8		1,75				8
		Modificación Deliberada De La Información		100%				5	7	7	8	8		7				
		Destrucción De Información	100%					5	7	7	8	8	5					
D6	Bases de datos en servidores locales	Errores De Administración	75%	75%	50%			8	9	9	9	9	6	6,75	4,5			
		Errores De Monitorización Log		75%			75%	8	9	9	9	9		6,75				6,75
		Errores De Configuración		75%				8	9	9	9	9		6,75				
		Alteración Accidental De La Información		75%				8	9	9	9	9		6,75				
		Destrucción De Información	100%					8	9	9	9	9	8					
		Manipulación De Los Registros De Actividad		50%			100%	8	9	9	9	9		4,5				9
		Manipulación De La Configuración		50%	75%	50%		8	9	9	9	9		4,5	6,75	4,5		
		Suplantación De La Identidad Del Usuario		50%	100%	75%		8	9	9	9	9		4,5	9	6,75		
		Abuso De Privilegios De Acceso	75%	50%	75%			8	9	9	9	9	6	4,5	6,75			
		Acceso No Autorizado		75%	100%			8	9	9	9	9		6,75	9			
		Repudio		50%			100%	8	9	9	9	9		4,5				9
		Modificación Deliberada De La Información		100%				8	9	9	9	9		9				
		Destrucción De Información	100%					8	9	9	9	9	8					
D7	Bases de datos en servidores en la nube	Errores De Administración	75%	75%	50%			9	9	9	9	9	6,75	6,75	4,5			
		Errores De Monitorización Log		75%			75%	9	9	9	9	9		6,75				6,75
		Errores De Configuración		75%				9	9	9	9	9		6,75				
		Alteración Accidental De La Información		75%				9	9	9	9	9		6,75				
		Destrucción De Información	100%					9	9	9	9	9	9					
		Manipulación De Los Registros De Actividad		50%			100%	9	9	9	9	9		4,5				9
		Manipulación De La Configuración		50%	75%	50%		9	9	9	9	9		4,5	6,75	4,5		
		Suplantación De La Identidad Del Usuario		50%	100%	75%		9	9	9	9	9		4,5	9	6,75		
		Abuso De Privilegios De Acceso	75%	50%	75%			9	9	9	9	9	6,75	4,5	6,75			
		Acceso No Autorizado		75%	100%			9	9	9	9	9		6,75	9			
		Repudio		50%			100%	9	9	9	9	9		4,5				9
		Modificación Deliberada De La Información		100%				9	9	9	9	9		9				
		Destrucción De Información	100%					9	9	9	9	9	9					
D8	Copias de seguridad en la nube	Errores De Administración	75%	75%	50%			9	8	9	9	9	6,75	6	4,5			
		Errores De Monitorización Log		50%			50%	9	8	9	9	9		4				4,5
		Errores De Configuración		100%				9	8	9	9	9		8				
		Alteración Accidental De La Información		100%				9	8	9	9	9		8				
		Destrucción De Información	100%					9	8	9	9	9	9					
		Manipulación De Los Registros De Actividad		25%			75%	9	8	9	9	9		2				6,75
		Manipulación De La Configuración		75%	75%	75%		9	8	9	9	9		6	6,75	6,75		
		Suplantación De La Identidad Del Usuario		50%	100%	75%		9	8	9	9	9		4	9	6,75		
		Abuso De Privilegios De Acceso	50%	75%	100%			9	8	9	9	9	4,5	6	9			
		Acceso No Autorizado		75%	100%			9	8	9	9	9		6	9			
		Repudio		50%			100%	9	8	9	9	9		4				9
		Modificación Deliberada De La Información		100%				9	8	9	9	9		8				
		Destrucción De Información	100%					9	8	9	9	9	9					
		Divulgación De Información			100%			9	8	9	9	9			9			
D9	Copias de Seguridad en servidores locales	Errores De Administración	75%	75%	50%			8	8	9	9	9	6	6	4,5			
		Errores De Monitorización Log		50%			50%	8	8	9	9	9		4				4,5
		Errores De Configuración		100%				8	8	9	9	9		8				
		Alteración Accidental De La Información		100%				8	8	9	9	9		8				
		Destrucción De Información	100%					8	8	9	9	9	8					
		Fugas De Información			75%			8	8	9	9	9			6,75			
		Manipulación De La Configuración		75%	75%	75%		8	8	9	9	9		6	6,75	6,75		
		Suplantación De La Identidad Del Usuario		50%	100%	75%		8	8	9	9	9		4	9	6,75		
		Abuso De Privilegios De Acceso	50%	75%	100%			8	8	9	9	9	4	6	9			
		Acceso No Autorizado		75%	100%			8	8	9	9	9		6	9			
		Repudio		50%			100%	8	8	9	9	9		4				9
		Modificación Deliberada De La Información		100%				8	8	9	9	9		8				
		Destrucción De Información	100%					8	8	9	9	9	8					
		Divulgación De Información			100%			8	8	9	9	9			9			

Figura 85. Impacto potencial de las amenazas del grupo Datos/Información (b)
(Fuente propia)

D10	Copias de Seguridad en discos externos	Errores De Administración	75%	75%	50%			7	8	9	9	9	5,25	6	4,5		
		Errores De Monitorización Log		50%			50%	7	8	9	9	9		4			4,5
		Errores De Configuración		100%				7	8	9	9	9		8			
		Alteración Accidental De La Información		100%				7	8	9	9	9		8			
		Destrucción De Información	100%					7	8	9	9	9	7				
		Manipulación De Los Registros De Actividad		25%			75%	7	8	9	9	9		2			6,75
		Manipulación De La Configuración		75%	75%	75%		7	8	9	9	9		6	6,75	6,75	
		Suplantación De La Identidad Del Usuario		50%	100%	75%		7	8	9	9	9		4	9	6,75	
		Abuso De Privilegios De Acceso	50%	75%	100%			7	8	9	9	9	3,5	6	9		
		Acceso No Autorizado		75%	100%			7	8	9	9	9		6	9		
		Repudio		50%			100%	7	8	9	9	9		4			9
		Modificación Deliberada De La Información		100%				7	8	9	9	9		8			
		Destrucción De Información	100%					7	8	9	9	9	7				
		Divulgación De Información			100%			7	8	9	9	9			9		
D11	Ficheros de contraseñas	Errores De Administración	75%	75%	100%			9	9	9	9	9	6,75	6,75	9		
		Errores De Configuración		5%				9	9	9	9	9		0,45			
		Alteración Accidental De La Información		75%				9	9	9	9	9		6,75			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Manipulación De Los Registros De Actividad		25%			100%	9	9	9	9	9		2,25			9
		Suplantación De La Identidad Del Usuario		50%	100%	50%		9	9	9	9	9		4,5	9	4,5	
		Abuso De Privilegios De Acceso	25%	50%	75%			9	9	9	9	9	2,25	4,5	6,75		
		Acceso No Autorizado		75%	100%			9	9	9	9	9		6,75	9		
		Repudio		25%			100%	9	9	9	9	9		2,25			9
		Modificación Deliberada De La Información		100%				9	9	9	9	9		9			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Divulgación De Información			100%			9	9	9	9	9			9		
D12	Registros de actividades en servidores	Errores De Administración	75%	50%	50%			8	8	8	9	9	6	4	4		
		Errores De Configuración		75%				8	8	8	9	9		6			
		Destrucción De Información	75%					8	8	8	9	9	6				
		Manipulación De La Configuración		75%	50%	75%		8	8	8	9	9		6	4	6,75	
		Suplantación De La Identidad Del Usuario		75%	100%	50%		8	8	8	9	9		6	8	4,5	
		Abuso De Privilegios De Acceso	75%	50%	50%			8	8	8	9	9	6	4	4		
		Acceso No Autorizado		75%	100%			8	8	8	9	9		6	8		
		Repudio		50%			100%	8	8	8	9	9		4			9
		Modificación Deliberada De La Información		100%				8	8	8	9	9		8			
		Destrucción De Información	100%					8	8	8	9	9	8				
D13	Ficheros compartidos Google Drive	Errores De Administración	75%	50%	50%			7	8	8	7	7	5,25	4	4		
		Errores De Configuración		25%				7	8	8	7	7		2			
		Alteración Accidental De La Información		75%				7	8	8	7	7		6			
		Destrucción De Información	75%					7	8	8	7	7	5,25				
		Manipulación De La Configuración		50%	50%	50%		7	8	8	7	7		4	4	3,5	
		Suplantación De La Identidad Del Usuario		75%	100%	50%		7	8	8	7	7		6	8	3,5	
		Abuso De Privilegios De Acceso	50%	50%	50%			7	8	8	7	7	3,5	4	4		
		Acceso No Autorizado		75%	100%			7	8	8	7	7		6	8		
		Repudio		25%			100%	7	8	8	7	7		2			7
		Modificación Deliberada De La Información		100%				7	8	8	7	7		8			
		Destrucción De Información	100%					7	8	8	7	7	7				
		Divulgación De Información			100%			7	8	8	7	7			8		

Figura 86. Impacto potencial de las amenazas del grupo Datos/Información (c)
(Fuente propia)

- [S] Servicios

El impacto en los Servicios varía entre el valor mínimo de 0,2 y el valor máximo de 9. Los activos con el impacto más alto son el servicio financiero y la gestión de recursos humanos, pues poseen una valoración alta y las amenazas podrían producir una degradación grave. Un impacto con valoración de 8 se produce en todos los activos, al igual que los valores medios entre 4 y 7 causados por una valoración o degradación baja. Los valores menores que 4 en su mayoría son el resultado de una degradación baja para el activo. Por otro lado, aunque las amenazas producen degradación en todas las dimensiones de seguridad, la ausencia de valores en el impacto es porque no existe degradación. No obstante, las dimensiones de autenticidad y trazabilidad solo generan un impacto en las amenazas de suplantación de identidad del usuario y repudio. Todos los valores calculados se observan en las Figuras 87 a la 88.

SERVICIOS [S]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
S1	Página web	Errores De Usuarios	5%	5%	25%			7	8	8	5	7	0,35	0,4	2		
		Errores De Administración	100%	75%	75%			7	8	8	5	7	7	6	6		
		Alteración Accidental De La Información		75%				7	8	8	5	7		6			
		Fugas De Información			50%			7	8	8	5	7			4		
		Caída Del Sistema Por Agotamiento De Recursos	100%					7	8	8	5	7	7				
		Suplantación De La Identidad Del Usuario		75%	75%	100%		7	8	8	5	7		6	6	5	
		Abuso De Privilegios De Acceso	50%	75%	75%			7	8	8	5	7	3,5	6	6		
		Uso No Previsto	50%	75%	75%			7	8	8	5	7	3,5	6	6		
		Acceso No Autorizado		100%	75%			7	8	8	5	7		8	6		
		Repudio		50%			75%	7	8	8	5	7		4			5,25
		Modificación Deliberada De La Información		100%				7	8	8	5	7		8			
		Destrucción De Información	75%					7	8	8	5	7	5,25				
		Divulgación De Información			100%			7	8	8	5	7			8		
		Denegación De Servicio	100%					7	8	8	5	7	7				
S2	Correo electrónico	Errores De Usuarios	50%	25%	50%			7	8	8	7	8	3,5	2	4		
		Errores De Administración	75%	25%	75%			7	8	8	7	8	5,25	2	6		
		Alteración Accidental De La Información		50%				7	8	8	7	8		4			
		Fugas De Información			75%			7	8	8	7	8			6		
		Caída Del Sistema Por Agotamiento De Recursos	100%					7	8	8	7	8	7				
		Suplantación De La Identidad Del Usuario		50%	75%	75%		7	8	8	7	8		4	6	5,25	
		Abuso De Privilegios De Acceso	50%	75%	75%			7	8	8	7	8	3,5	6	6		
		Uso No Previsto	75%	75%	75%			7	8	8	7	8	5,25	6	6		
		Acceso No Autorizado		75%	100%			7	8	8	7	8		6	8		
		Repudio		50%			75%	7	8	8	7	8		4			6
		Modificación Deliberada De La Información		75%				7	8	8	7	8		6			
		Divulgación De Información			75%			7	8	8	7	8			6		
		Denegación De Servicio	100%					7	8	8	7	8	7				
S3	Intranet documental - Servicio FTP	Errores De Usuarios	5%	50%	50%			8	8	8	8	8	0,4	4	4		
		Errores De Administración	75%	75%	50%			8	8	8	8	8	6	6	4		
		Alteración Accidental De La Información		75%				8	8	8	8	8		6			
		Destrucción De Información	75%					8	8	8	8	8	6				
		Fugas De Información			75%			8	8	8	8	8			6		
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	8	8	8	8				
		Suplantación De La Identidad Del Usuario		50%	75%	50%		8	8	8	8	8		4	6	4	
		Abuso De Privilegios De Acceso	25%	50%	75%			8	8	8	8	8	2	4	6		
		Uso No Previsto	50%	50%	75%			8	8	8	8	8	4	4	6		
		Acceso No Autorizado		50%	100%			8	8	8	8	8		4	8		
		Repudio		25%			75%	8	8	8	8	8		2			6
		Modificación Deliberada De La Información		75%				8	8	8	8	8		6			
		Destrucción De Información	100%					8	8	8	8	8	8				
		Divulgación De Información			75%			8	8	8	8	8			6		
		Denegación De Servicio	100%					8	8	8	8	8	8				
S4	Sistema de tickets de incidencias	Errores De Usuarios	5%	25%	25%			4	6	6	8	5	0,2	1,5	1,5		
		Errores De Administración	75%	50%	25%			4	6	6	8	5	3	3	1,5		
		Alteración Accidental De La Información		50%				4	6	6	8	5		3			
		Caída Del Sistema Por Agotamiento De Recursos	100%					4	6	6	8	5	4				
		Suplantación De La Identidad Del Usuario		50%	75%	50%		4	6	6	8	5		3	4,5	4	
		Acceso No Autorizado		75%	75%			4	6	6	8	5		4,5	4,5		
		Repudio		50%			75%	4	6	6	8	5		3			3,75
		Modificación Deliberada De La Información		50%				4	6	6	8	5		3			
		Divulgación De Información			50%			4	6	6	8	5			3		
		Denegación De Servicio	100%					4	6	6	8	5	4				
S5	Educación Virtual	Errores De Usuarios	5%	25%	50%			8	8	7	6	7	0,4	2	3,5		
		Errores De Administración	75%	50%	50%			8	8	7	6	7	6	4	3,5		
		Alteración Accidental De La Información		75%				8	8	7	6	7		6			
		Destrucción De Información	100%					8	8	7	6	7	8				
		Fugas De Información			50%			8	8	7	6	7			3,5		
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	7	6	7	8				
		Suplantación De La Identidad Del Usuario		25%	75%	50%		8	8	7	6	7		2	5,25	3	
		Abuso De Privilegios De Acceso	25%	75%	50%			8	8	7	6	7	2	6	3,5		
		Uso No Previsto	50%	25%	50%			8	8	7	6	7	4	2	3,5		
		Acceso No Autorizado		75%	75%			8	8	7	6	7		6	5,25		
		Repudio		25%			75%	8	8	7	6	7		2			5,25
		Modificación Deliberada De La Información		75%				8	8	7	6	7		6			
		Divulgación De Información			50%			8	8	7	6	7			3,5		
		Denegación De Servicio	100%					8	8	7	6	7	8				
S6	Servicio de financiero	Errores De Usuarios	25%	75%	100%			8	9	9	9	9	2	6,75	9		
		Errores De Administración	75%	50%	75%			8	9	9	9	9	6	4,5	6,75		
		Alteración Accidental De La Información		100%				8	9	9	9	9		9			
		Destrucción De Información	75%					8	9	9	9	9	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	9	9	9	9	8				
		Suplantación De La Identidad Del Usuario		75%	100%	75%		8	9	9	9	9		6,75	9	6,75	
		Abuso De Privilegios De Acceso	25%	75%	75%			8	9	9	9	9	2	6,75	6,75		
		Uso No Previsto	50%	50%	50%			8	9	9	9	9	4	4,5	4,5		
		Acceso No Autorizado		100%	100%			8	9	9	9	9		9	9		
		Repudio		50%			100%	8	9	9	9	9		4,5			9
		Modificación Deliberada De La Información		100%				8	9	9	9	9		9			
		Destrucción De Información	100%					8	9	9	9	9	8				
		Divulgación De Información			100%			8	9	9	9	9			9		
		Denegación De Servicio	100%					8	9	9	9	9	8				

Figura 87. Impacto potencial de las amenazas del grupo Servicios (a)
(Fuente propia)

S7	Gestión de usuarios Socios	Errores De Usuarios	25%	75%	50%			8	8	8	7	8	2	6	4		
		Errores De Administración	75%	50%	75%			8	8	8	7	8	6	4	6		
		Alteración Accidental De La Información		75%				8	8	8	7	8		6			
		Destrucción De Información	75%					8	8	8	7	8	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	8	7	8	8				
		Suplantación De La Identidad Del Usuario		75%	100%	50%		8	8	8	7	8		6	8	3,5	
		Abuso De Privilegios De Acceso	25%	50%	50%			8	8	8	7	8	2	4	4		
		Uso No Previsto	50%	25%	75%			8	8	8	7	8	4	2	6		
		Acceso No Autorizado		75%	100%			8	8	8	7	8		6	8		
		Repudio		25%			100%	8	8	8	7	8		2			8
		Modificación Deliberada De La Información		100%				8	8	8	7	8		8			
		Destrucción De Información	100%					8	8	8	7	8	8				
		Divulgación De Información			100%			8	8	8	7	8			8		
		Denegación De Servicio	100%					8	8	8	7	8	8				
S8	Gestión empresarial	Errores De Usuarios	25%	50%	50%			7	8	8	7	8	1,75	4	4		
		Errores De Administración	50%	50%	50%			7	8	8	7	8	3,5	4	4		
		Alteración Accidental De La Información		75%				7	8	8	7	8		6			
		Destrucción De Información	75%					7	8	8	7	8	5,25				
		Caída Del Sistema Por Agotamiento De Recursos	75%					7	8	8	7	8	5,25				
		Suplantación De La Identidad Del Usuario		50%	75%	50%		7	8	8	7	8		4	6	3,5	
		Abuso De Privilegios De Acceso	25%	50%	50%			7	8	8	7	8	1,75	4	4		
		Uso No Previsto	25%	50%	75%			7	8	8	7	8	1,75	4	6		
		Acceso No Autorizado		75%	100%			7	8	8	7	8		6	8		
		Repudio		50%			100%	7	8	8	7	8		4			8
		Modificación Deliberada De La Información		75%				7	8	8	7	8		6			
		Destrucción De Información	100%					7	8	8	7	8	7				
		Divulgación De Información			100%			7	8	8	7	8			8		
		Denegación De Servicio	100%					7	8	8	7	8	7				
S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	25%	50%	75%			7	8	8	8	9	1,75	4	6		
		Errores De Administración	50%	50%	75%			7	8	8	8	9	3,5	4	6		
		Alteración Accidental De La Información		75%				7	8	8	8	9		6			
		Destrucción De Información	75%					7	8	8	8	9	5,25				
		Caída Del Sistema Por Agotamiento De Recursos	100%					7	8	8	8	9	7				
		Suplantación De La Identidad Del Usuario		75%	100%	50%		7	8	8	8	9		6	8	4	
		Abuso De Privilegios De Acceso	25%	50%	75%			7	8	8	8	9	1,75	4	6		
		Uso No Previsto	25%	50%	75%			7	8	8	8	9	1,75	4	6		
		Acceso No Autorizado		75%	100%			7	8	8	8	9		6	8		
		Repudio		50%			100%	7	8	8	8	9		4			9
		Modificación Deliberada De La Información		100%				7	8	8	8	9		8			
		Destrucción De Información	100%					7	8	8	8	9	7				
		Divulgación De Información			100%			7	8	8	8	9			8		
		Denegación De Servicio	100%					7	8	8	8	9	7				

Figura 88. Impacto potencial de las amenazas del grupo Servicios (b)
(Fuente propia)

- [SW] Software – Aplicaciones Informáticas

El impacto en este grupo de activos varía entre el valor mínimo de 0,2 y el valor máximo de 9. Los activos relevantes con el impacto más alto son: la aplicación de financiero, gestión de bases de datos y los sistemas operativos de servidores. El valor de impacto 8 se puede observar en casi todos los activos, al igual que los valores medios entre 4 y 7 causados por una valoración o degradación baja. Los valores menores que 4 en su mayoría son el resultado de una degradación baja para el activo, siendo el software ofimático el activo que tiene el menor impacto de entre todos los activos de este grupo. Por otro lado, las aplicaciones informáticas al no tener degradación en la dimensión de trazabilidad, no tiene valor de impacto en dicha dimensión. Para la dimensión de autenticidad solo la amenaza de suplantación de la identidad del usuario causa degradación y por lo tanto genera un impacto. Todos los valores calculados se observan en las Figuras 89 a la 91.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
SW1	Aplicación de Financiero	Fallo De Origen Lógico	75%					9	9	9	9	9	6,75				
		Errores De Usuarios	25%	75%	50%			9	9	9	9	9	2,25	6,75	4,5		
		Errores De Administración	75%	50%	50%			9	9	9	9	9	6,75	4,5	4,5		
		Alteración Accidental De La Información		75%				9	9	9	9	9		6,75			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Fugas De Información			100%			9	9	9	9	9			9		
		Vulnerabilidades De Los Programas	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Errores De Mantenimiento/Actualización De Programas	50%	75%				9	9	9	9	9	4,5	6,75			
		Suplantación De La Identidad Del Usuario		75%	100%	75%		9	9	9	9	9		6,75	9	6,75	
		Abuso De Privilegios De Acceso	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Uso No Previsto	75%	50%	50%			9	9	9	9	9	6,75	4,5	4,5		
		Difusión De Software Dañino	100%	100%	100%			9	9	9	9	9	9	9	9		
		Acceso No Autorizado		75%	100%			9	9	9	9	9		6,75	9		
		Modificación Deliberada De La Información		100%				9	9	9	9	9		9			
		Destrucción De Información	50%					9	9	9	9	9	4,5				
		Divulgación De Información			100%			9	9	9	9	9			9		
SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	75%					8	8	8	9	9	6				
		Errores De Usuarios	50%	75%	50%			8	8	8	9	9	4	6	4		
		Errores De Administración	75%	50%	50%			8	8	8	9	9	6	4	4		
		Alteración Accidental De La Información		75%				8	8	8	9	9		6			
		Destrucción De Información	100%					8	8	8	9	9	8				
		Fugas De Información			100%			8	8	8	9	9			8		
		Vulnerabilidades De Los Programas	50%	75%	100%			8	8	8	9	9	4	6	8		
		Errores De Mantenimiento/Actualización De Programas	50%	75%				8	8	8	9	9	4	6			
		Suplantación De La Identidad Del Usuario		75%	100%	75%		8	8	8	9	9		6	8	6,75	
		Abuso De Privilegios De Acceso	50%	75%	100%			8	8	8	9	9	4	6	8		
		Uso No Previsto	50%	50%	50%			8	8	8	9	9	4	4	4		
		Difusión De Software Dañino	100%	100%	100%			8	8	8	9	9	8	8	8		
		Acceso No Autorizado		75%	100%			8	8	8	9	9		6	8		
		Modificación Deliberada De La Información		100%				8	8	8	9	9		8			
		Destrucción De Información	50%					8	8	8	9	9	4				
		Divulgación De Información			100%			8	8	8	9	9			8		
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	75%					7	8	8	9	9	5,25				
		Errores De Usuarios	50%	75%	50%			7	8	8	9	9	3,5	6	4		
		Errores De Administración	75%	50%	50%			7	8	8	9	9	5,25	4	4		
		Alteración Accidental De La Información		75%				7	8	8	9	9		6			
		Destrucción De Información	100%					7	8	8	9	9	7				
		Fugas De Información			100%			7	8	8	9	9			8		
		Vulnerabilidades De Los Programas	50%	75%	100%			7	8	8	9	9	3,5	6	8		
		Errores De Mantenimiento/Actualización De Programas	50%	75%				7	8	8	9	9	3,5	6			
		Suplantación De La Identidad Del Usuario		75%	100%	75%		7	8	8	9	9		6	8	6,75	
		Abuso De Privilegios De Acceso	50%	75%	100%			7	8	8	9	9	3,5	6	8		
		Uso No Previsto	50%	50%	50%			7	8	8	9	9	3,5	4	4		
		Difusión De Software Dañino	100%	100%	100%			7	8	8	9	9	7	8	8		
		Acceso No Autorizado		75%	100%			7	8	8	9	9		6	8		
		Modificación Deliberada De La Información		100%				7	8	8	9	9		8			
		Destrucción De Información	50%					7	8	8	9	9	3,5				
		Divulgación De Información			100%			7	8	8	9	9			8		
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	75%					7	8	8	9	9	5,25				
		Errores De Usuarios	50%	75%	50%			7	8	8	9	9	3,5	6	4		
		Errores De Administración	75%	50%	50%			7	8	8	9	9	5,25	4	4		
		Alteración Accidental De La Información		75%				7	8	8	9	9		6			
		Destrucción De Información	100%					7	8	8	9	9	7				
		Fugas De Información			100%			7	8	8	9	9			8		
		Vulnerabilidades De Los Programas	50%	75%	100%			7	8	8	9	9	3,5	6	8		
		Errores De Mantenimiento/Actualización De Programas	50%	75%				7	8	8	9	9	3,5	6			
		Suplantación De La Identidad Del Usuario		75%	100%	75%		7	8	8	9	9		6	8	6,75	
		Abuso De Privilegios De Acceso	50%	75%	100%			7	8	8	9	9	3,5	6	8		
		Uso No Previsto	50%	50%	50%			7	8	8	9	9	3,5	4	4		
		Difusión De Software Dañino	100%	100%	100%			7	8	8	9	9	7	8	8		
		Acceso No Autorizado		75%	100%			7	8	8	9	9		6	8		
		Modificación Deliberada De La Información		100%				7	8	8	9	9		8			
		Destrucción De Información	50%					7	8	8	9	9	3,5				
		Divulgación De Información			100%			7	8	8	9	9			8		
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	75%					8	9	9	9	9	6				
		Errores De Administración	75%	75%	50%			8	9	9	9	9	6	6,75	4,5		
		Alteración Accidental De La Información		100%				8	9	9	9	9		9			
		Destrucción De Información	100%					8	9	9	9	9	8				
		Fugas De Información			100%			8	9	9	9	9			9		
		Vulnerabilidades De Los Programas	50%	75%	100%			8	9	9	9	9	4	6,75	9		
		Errores De Mantenimiento/Actualización De Programas	50%	100%				8	9	9	9	9	4	9			
		Suplantación De La Identidad Del Usuario		100%	100%	100%		8	9	9	9	9		9	9	9	
		Abuso De Privilegios De Acceso	75%	100%	100%			8	9	9	9	9	6	9	9		
		Uso No Previsto	75%	75%	100%			8	9	9	9	9	6	6,75	9		
		Difusión De Software Dañino	100%	100%	100%			8	9	9	9	9	8	9	9		
		Acceso No Autorizado		100%	100%			8	9	9	9	9		9	9		
		Modificación Deliberada De La Información		100%				8	9	9	9	9		9			
		Destrucción De Información	100%					8	9	9	9	9	8				
		Divulgación De Información			100%			8	9	9	9	9			9		

Figura 89. Impacto potencial de las amenazas del grupo Aplicaciones informáticas (a) (Fuente propia)

SW6	Aplicación de Página web	Fallo De Origen Lógico	75%					7	8	8	9	8	5,25						
		Errores De Usuarios	25%	25%	25%			7	8	8	9	8	1,75	2	2				
		Errores De Administración	75%	50%	75%			7	8	8	9	8	5,25	4	6				
		Alteración Accidental De La Información		75%				7	8	8	9	8		6					
		Destrucción De Información	75%					7	8	8	9	8	5,25						
		Fugas De Información			50%			7	8	8	9	8			4				
		Vulnerabilidades De Los Programas	75%	75%	75%			7	8	8	9	8	5,25	6	6				
		Errores De Mantenimiento/Actualización De Programas	50%	75%				7	8	8	9	8	3,5	6					
		Suplantación De La Identidad Del Usuario		50%	100%	100%		7	8	8	9	8		4	8	9			
		Abuso De Privilegios De Acceso	50%	75%	100%			7	8	8	9	8	3,5	6	8				
		Uso No Previsto	50%	50%	100%			7	8	8	9	8	3,5	4	8				
		Difusión De Software Dañino	50%	50%	100%			7	8	8	9	8	3,5	4	8				
		Acceso No Autorizado		75%	100%			7	8	8	9	8		6	8				
		Modificación Deliberada De La Información		75%				7	8	8	9	8		6					
		Destrucción De Información	50%					7	8	8	9	8	3,5						
		Divulgación De Información			75%			7	8	8	9	8			6				
		Manipulación De Programas	50%	75%	75%			7	8	8	9	8	3,5	6	6				
SW7	Aplicación de Intranet	Fallo De Origen Lógico	75%					8	8	8	9	7	6						
		Errores De Usuarios	50%	75%	50%			8	8	8	9	7	4	6	4				
		Errores De Administración	75%	50%	50%			8	8	8	9	7	6	4	4				
		Alteración Accidental De La Información		75%				8	8	8	9	7		6					
		Destrucción De Información	100%					8	8	8	9	7	8						
		Fugas De Información			100%			8	8	8	9	7			8				
		Vulnerabilidades De Los Programas	50%	75%	100%			8	8	8	9	7	4	6	8				
		Errores De Mantenimiento/Actualización De Programas	50%	75%				8	8	8	9	7	4	6					
		Suplantación De La Identidad Del Usuario		75%	100%	75%		8	8	8	9	7		6	8	6,75			
		Abuso De Privilegios De Acceso	50%	75%	100%			8	8	8	9	7	4	6	8				
		Uso No Previsto	50%	50%	50%			8	8	8	9	7	4	4	4				
		Difusión De Software Dañino	100%	100%	100%			8	8	8	9	7	8	8	8				
		Acceso No Autorizado		75%	100%			8	8	8	9	7		6	8				
		Modificación Deliberada De La Información		75%				8	8	8	9	7		6					
		Destrucción De Información	50%					8	8	8	9	7	4						
		Divulgación De Información			100%			8	8	8	9	7			8				
SW8	Aplicación del Sistema de tickets de incidencias	Fallo De Origen Lógico	75%					4	6	6	9	5	3						
		Errores De Usuarios	50%	75%	50%			4	6	6	9	5	2	4,5	3				
		Errores De Administración	75%	50%	50%			4	6	6	9	5	3	3	3				
		Alteración Accidental De La Información		75%				4	6	6	9	5		4,5					
		Destrucción De Información	100%					4	6	6	9	5	4						
		Fugas De Información			100%			4	6	6	9	5			6				
		Vulnerabilidades De Los Programas	50%	75%	100%			4	6	6	9	5	2	4,5	6				
		Errores De Mantenimiento/Actualización De Programas	50%	75%				4	6	6	9	5	2	4,5					
		Suplantación De La Identidad Del Usuario		75%	100%	75%		4	6	6	9	5		4,5	6	6,75			
		Abuso De Privilegios De Acceso	50%	75%	100%			4	6	6	9	5	2	4,5	6				
		Uso No Previsto	50%	50%	50%			4	6	6	9	5	2	3	3				
		Difusión De Software Dañino	100%	100%	100%			4	6	6	9	5	4	6	6				
		Acceso No Autorizado		75%	100%			4	6	6	9	5		4,5	6				
		Modificación Deliberada De La Información		100%				4	6	6	9	5		6					
		Destrucción De Información	50%					4	6	6	9	5	2						
		Divulgación De Información			100%			4	6	6	9	5			6				
SW9	Aplicación de Correo electrónico Gmail	Errores De Usuarios	5%	5%	25%			7	8	8	9	8	0,35	0,4	2				
		Errores De Administración	25%	5%	50%			7	8	8	9	8	1,75	0,4	4				
		Difusión De Software Dañino	5%	5%	100%			7	8	8	9	8	0,35	0,4	8				
		Alteración Accidental De La Información		5%				7	8	8	9	8		0,4					
		Destrucción De Información	25%					7	8	8	9	8	1,75						
		Fugas De Información			100%			7	8	8	9	8			8				
		Vulnerabilidades De Los Programas	5%	50%	100%			7	8	8	9	8	0,35	4	8				
		Errores De Mantenimiento/Actualización De Programas	25%	50%	75%			7	8	8	9	8	1,75	4	6				
		Suplantación De La Identidad Del Usuario		50%	100%	100%		7	8	8	9	8		4	8	9			
		Abuso De Privilegios De Acceso	5%	75%	75%			7	8	8	9	8	0,35	6	6				
		Uso No Previsto	50%	75%	100%			7	8	8	9	8	3,5	6	8				
		Difusión De Software Dañino	5%	50%	100%			7	8	8	9	8	0,35	4	8				
		Acceso No Autorizado		50%	100%			7	8	8	9	8		4	8				
		Modificación Deliberada De La Información		100%				7	8	8	9	8		8					
		Destrucción De Información	100%					7	8	8	9	8	7						
		Divulgación De Información			100%			7	8	8	9	8			8				
SW10	E-apsa	Fallo De Origen Lógico	75%					8	8	7	8	7	6						
		Errores De Usuarios	5%	5%	25%			8	8	7	8	7	0,4	0,4	1,75				
		Errores De Administración	50%	50%	75%			8	8	7	8	7	4	4	5,25				
		Alteración Accidental De La Información		25%				8	8	7	8	7		2					
		Destrucción De Información	5%					8	8	7	8	7	0,4						
		Fugas De Información			25%			8	8	7	8	7			1,75				
		Vulnerabilidades De Los Programas	5%	25%	50%			8	8	7	8	7	0,4	2	3,5				
		Errores De Mantenimiento/Actualización De Programas	25%	25%				8	8	7	8	7	2	2					
		Suplantación De La Identidad Del Usuario		25%	75%	100%		8	8	7	8	7		2	5,25	8			
		Abuso De Privilegios De Acceso	5%	25%	75%			8	8	7	8	7	0,4	2	5,25				
		Uso No Previsto	25%	5%	50%			8	8	7	8	7	2	0,4	3,5				
		Difusión De Software Dañino	5%	25%	50%			8	8	7	8	7	0,4	2	3,5				
		Acceso No Autorizado		25%	100%			8	8	7	8	7		2	7				
		Modificación Deliberada De La Información		25%				8	8	7	8	7		2					
		Destrucción De Información	75%					8	8	7	8	7	6						
		Divulgación De Información			75%			8	8	7	8	7			5,25				
SW11	Aplicaciones en móviles	Fallo De Origen Lógico	50%					4	8	7	6	5	2						
		Errores De Usuarios	5%	25%	50%			4	8	7	6	5	0,2	2	3,5				
		Errores De Administración	25%	25%	50%			4	8	7	6	5	1	2	3,5				
		Difusión De Software Dañino	5%	25%	75%			4	8	7	6	5	0,2	2	5,25				
		Alteración Accidental De La Información		25%				4	8	7	6	5		2					
		Destrucción De Información	25%					4	8	7	6	5	1						
		Fugas De Información			75%			4	8	7	6	5			5,25				
		Vulnerabilidades De Los Programas	25%	25%	75%			4	8	7	6	5	1	2	5,25				
		Errores De Mantenimiento/Actualización De Programas	50%	25%				4	8	7	6	5	2	2					
		Suplantación De La Identidad Del Usuario		25%	75%	100%		4	8	7	6	5		2	5,25	6			
		Abuso De Privilegios De Acceso	25%	75%	75%			4	8	7	6	5	1	6	5,25				
		Uso No Previsto	75%	50%	75%			4	8	7	6	5	3	4	5,25				
		Difusión De Software Dañino	75%	50%	100%			4	8	7	6	5	3	4	7				
		Acceso No Autorizado		25%	100%			4	8	7	6	5		2	7				
		Modificación Deliberada De La Información		25%				4	8	7	6	5		2					
		Destrucción De Información	50%					4	8	7	6	5	2						
		Divulgación De Información			100%			4	8	7	6	5			7				

Figura 90. Impacto potencial de las amenazas del grupo Aplicaciones informáticas (b) (Fuente propia)

SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	75%					9	9	9	9	9	6,75				
		Errores De Administración	100%	75%	100%			9	9	9	9	9	9	6,75	9		
		Alteración Accidental De La Información		75%				9	9	9	9	9		6,75			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Vulnerabilidades De Los Programas	75%	75%	100%			9	9	9	9	9	6,75	6,75	9		
		Errores De Mantenimiento/Actualización De Programas	75%	75%				9	9	9	9	9	6,75	6,75			
		Suplantación De La Identidad Del Usuario		75%	100%	100%		9	9	9	9	9		6,75	9	9	
		Abuso De Privilegios De Acceso	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Uso No Previsto	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Difusión De Software Dañino	100%	100%	100%			9	9	9	9	9	9	9	9		
		Acceso No Autorizado		100%	100%			9	9	9	9	9		9	9		
		Modificación Deliberada De La Información		100%				9	9	9	9	9		9			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Divulgación De Información			100%			9	9	9	9	9			9		
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	75%					9	9	9	9	9	6,75				
		Errores De Administración	100%	75%	100%			9	9	9	9	9	9	6,75	9		
		Alteración Accidental De La Información		75%				9	9	9	9	9		6,75			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Vulnerabilidades De Los Programas	75%	75%	100%			9	9	9	9	9	6,75	6,75	9		
		Errores De Mantenimiento/Actualización De Programas	75%	75%				9	9	9	9	9	6,75	6,75			
		Suplantación De La Identidad Del Usuario		75%	100%	100%		9	9	9	9	9		6,75	9	9	
		Abuso De Privilegios De Acceso	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Uso No Previsto	50%	75%	100%			9	9	9	9	9	4,5	6,75	9		
		Difusión De Software Dañino	100%	100%	100%			9	9	9	9	9	9	9	9		
		Acceso No Autorizado		100%	100%			9	9	9	9	9		9	9		
		Modificación Deliberada De La Información		100%				9	9	9	9	9		9			
		Destrucción De Información	100%					9	9	9	9	9	9				
		Divulgación De Información			100%			9	9	9	9	9			9		
SW14	Sistema operativo Windows 7	Fallo De Origen Lógico	100%					4	9	5	8	6	4				
		Errores De Usuarios	25%	5%	25%			4	9	5	8	6	1	0,45	1,25		
		Errores De Administración	50%	25%	50%			4	9	5	8	6	2	2,25	2,5		
		Difusión De Software Dañino	75%	50%	75%			4	9	5	8	6	3	4,5	3,75		
		Alteración Accidental De La Información		75%				4	9	5	8	6		6,75			
		Destrucción De Información	100%					4	9	5	8	6	4				
		Vulnerabilidades De Los Programas	25%	25%	100%			4	9	5	8	6	1	2,25	5		
		Errores De Mantenimiento/Actualización De Programas	25%	25%				4	9	5	8	6	1	2,25			
		Suplantación De La Identidad Del Usuario		5%	100%	100%		4	9	5	8	6		0,45	5	8	
		Abuso De Privilegios De Acceso	5%	5%	75%			4	9	5	8	6	0,2	0,45	3,75		
		Uso No Previsto	25%	25%	100%			4	9	5	8	6	1	2,25	5		
		Difusión De Software Dañino	75%	75%	100%			4	9	5	8	6	3	6,75	5		
		Acceso No Autorizado		25%	100%			4	9	5	8	6		2,25	5		
		Modificación Deliberada De La Información		75%				4	9	5	8	6		6,75			
		Destrucción De Información	100%					4	9	5	8	6	4				
		Divulgación De Información			100%			4	9	5	8	6			5		
SW15	Sistema operativo Windows 10	Fallo De Origen Lógico	100%					4	9	5	8	6	4				
		Errores De Usuarios	25%	5%	25%			4	9	5	8	6	1	0,45	1,25		
		Errores De Administración	50%	25%	50%			4	9	5	8	6	2	2,25	2,5		
		Difusión De Software Dañino	75%	50%	75%			4	9	5	8	6	3	4,5	3,75		
		Alteración Accidental De La Información		75%				4	9	5	8	6		6,75			
		Destrucción De Información	100%					4	9	5	8	6	4				
		Vulnerabilidades De Los Programas	25%	25%	100%			4	9	5	8	6	1	2,25	5		
		Errores De Mantenimiento/Actualización De Programas	25%	25%				4	9	5	8	6	1	2,25			
		Suplantación De La Identidad Del Usuario		5%	100%	100%		4	9	5	8	6		0,45	5	8	
		Abuso De Privilegios De Acceso	5%	5%	75%			4	9	5	8	6	0,2	0,45	3,75		
		Uso No Previsto	25%	25%	100%			4	9	5	8	6	1	2,25	5		
		Difusión De Software Dañino	75%	75%	100%			4	9	5	8	6	3	6,75	5		
		Acceso No Autorizado		25%	100%			4	9	5	8	6		2,25	5		
		Modificación Deliberada De La Información		75%				4	9	5	8	6		6,75			
		Destrucción De Información	100%					4	9	5	8	6	4				
		Divulgación De Información			100%			4	9	5	8	6			5		
SW16	Navegadores Web	Errores De Usuarios	5%	5%	75%			4	8	8	8	6	0,2	0,4	6		
		Errores De Administración	25%	5%	75%			4	8	8	8	6	1	0,4	6		
		Fugas De Información			100%			4	8	8	8	6			8		
		Vulnerabilidades De Los Programas	25%	50%	100%			4	8	8	8	6	1	4	8		
		Errores De Mantenimiento/Actualización De Programas	5%	50%				4	8	8	8	6	0,2	4			
		Abuso De Privilegios De Acceso	5%	5%	75%			4	8	8	8	6	0,2	0,4	6		
		Uso No Previsto	5%	25%	75%			4	8	8	8	6	0,2	2	6		
		Difusión De Software Dañino	5%	25%	100%			4	8	8	8	6	0,2	2	8		
		Modificación Deliberada De La Información		25%				4	8	8	8	6		2			
		Destrucción De Información	25%					4	8	8	8	6	1				
		Divulgación De Información			25%			4	8	8	8	6			2		
SW17	Antivirus	Fallo De Origen Lógico	75%					8	8	5	8	5	6				
		Errores De Administración	50%	25%	25%			8	8	5	8	5	4	2	1,25		
		Errores De Mantenimiento/Actualización De Programas	25%	100%				8	8	5	8	5	2	8			
		Abuso De Privilegios De Acceso	50%	100%	25%			8	8	5	8	5	4	8	1,25		
		Uso No Previsto	50%	100%	25%			8	8	5	8	5	4	8	1,25		
		Acceso No Autorizado		100%	25%			8	8	5	8	5		8	1,25		
		Modificación Deliberada De La Información		100%				8	8	5	8	5		8			
SW18	Software Ofimático	Fallo De Origen Lógico	50%					3	5	5	4	3	1,5				
		Errores De Usuarios	50%	5%	25%			3	5	5	4	3	1,5	0,25	1,25		
		Errores De Administración	50%	5%	25%			3	5	5	4	3	1,5	0,25	1,25		
		Errores De Mantenimiento/Actualización De Programas	75%	25%				3	5	5	4	3	2,25	1,25			
		Abuso De Privilegios De Acceso	25%	25%	25%			3	5	5	4	3	0,75	1,25	1,25		
		Uso No Previsto	50%	25%	25%			3	5	5	4	3	1,5	1,25	1,25		

Figura 91. Impacto potencial de las amenazas del grupo Aplicaciones informáticas (c) (Fuente propia)

- [HW] Equipos Informáticos (Hardware)

El impacto en los equipos informáticos varía entre el valor mínimo de 0,15 y el valor máximo de 9. Los activos con el mayor impacto son los servidores y los portátiles del departamento TIC,

ordenadores usados por la administración y hardware de comunicaciones como los routers y switches. Los valores medios entre 4 y 7 causados por una valoración o degradación baja se presentan en todos los activos. Los valores menores que 4 en su mayoría son el resultado de una degradación baja para el activo, siendo los activos que usan los empleados (ordenadores, impresoras y teléfonos de sobremesa) los de menor impacto. Para este grupo no existen valores de impacto en las dimensiones de autenticidad y trazabilidad. Todos los valores calculados se observan en las Figuras 92 y 93.

EQUIPOS INFORMÁTICOS [HW]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
HW1	Servidores APSA	Avería De Origen Físico/Lógico	100%					9	9	9	9	9	9				
		Errores De Administración	100%	100%	100%			9	9	9	9	9	9	9	9		
		Errores De Mantenimiento/Actualización De Equipos	75%					9	9	9	9	9	6,75				
		Caída Del Sistema Por Agotamiento De Recursos	100%					9	9	9	9	9	9				
		Abuso De Privilegios De Acceso	75%	75%	100%			9	9	9	9	9	6,75	6,75	9		
		Uso No Previsto	75%	75%	100%			9	9	9	9	9	6,75	6,75	9		
		Acceso No Autorizado		75%	100%			9	9	9	9	9		6,75	9		
		Denegación De Servicio	100%					9	9	9	9	9	9				
HW2	Servidores Sedes	Daños Por Agua	100%					8	8	9	9	9	8				
		Avería De Origen Físico/Lógico	100%					8	8	9	9	9	8				
		Corte De Suministro Eléctrico	100%					8	8	9	9	9	8				
		Fallas De Climatización	25%					8	8	9	9	9	2				
		Errores De Administración	75%	75%	100%			8	8	9	9	9	6	6	9		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	8	9	9	9	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	9	9	9	8				
		Abuso De Privilegios De Acceso	75%	75%	100%			8	8	9	9	9	6	6	9		
		Uso No Previsto	50%	50%	100%			8	8	9	9	9	4	4	9		
		Acceso No Autorizado		75%	100%			8	8	9	9	9		6	9		
		Manipulación De Equipos	75%		75%			8	8	9	9	9	6		6,75		
		Denegación De Servicio	100%					8	8	9	9	9	8				
		Robo	100%		75%			8	8	9	9	9	8		6,75		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	75%					7	8	8	7	8	5,25				
		Avería De Origen Físico/Lógico	100%					7	8	8	7	8	7				
		Corte De Suministro Eléctrico	100%					7	8	8	7	8	7				
		Errores De Administración	50%	50%	75%			7	8	8	7	8	3,5	4	6		
		Errores De Mantenimiento/Actualización De Equipos	50%					7	8	8	7	8	3,5				
		Caída Del Sistema Por Agotamiento De Recursos	75%					7	8	8	7	8	5,25				
		Perdida De Equipos	100%		100%			7	8	8	7	8	7		8		
		Abuso De Privilegios De Acceso	50%	50%	100%			7	8	8	7	8	3,5	4	8		
		Uso No Previsto	75%	25%	100%			7	8	8	7	8	5,25	2	8		
		Acceso No Autorizado		25%	100%			7	8	8	7	8		2	8		
		Manipulación De Equipos	50%		100%			7	8	8	7	8	3,5		8		
		Robo	100%		100%			7	8	8	7	8	7		8		
HW4	Ordenadores de escritorio empleados	Daños Por Agua	75%					3	7	7	7	7	2,25				
		Avería De Origen Físico/Lógico	100%					3	7	7	7	7	3				
		Corte De Suministro Eléctrico	100%					3	7	7	7	7	3				
		Errores De Administración	50%	50%	75%			3	7	7	7	7	1,5	3,5	5,25		
		Errores De Mantenimiento/Actualización De Equipos	50%					3	7	7	7	7	1,5				
		Caída Del Sistema Por Agotamiento De Recursos	75%					3	7	7	7	7	2,25				
		Perdida De Equipos	100%		75%			3	7	7	7	7	3		5,25		
		Abuso De Privilegios De Acceso	50%	50%	75%			3	7	7	7	7	1,5	3,5	5,25		
		Uso No Previsto	75%	25%	75%			3	7	7	7	7	2,25	1,75	5,25		
		Acceso No Autorizado		25%	75%			3	7	7	7	7		1,75	5,25		
		Manipulación De Equipos	50%		75%			3	7	7	7	7	1,5		5,25		
		Robo	100%		100%			3	7	7	7	7	3		7		
HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	100%					7	8	8	7	8	7				
		Corte De Suministro Eléctrico	25%					7	8	8	7	8	1,75				
		Errores De Administración	50%	25%	100%			7	8	8	7	8	3,5	2	8		
		Errores De Mantenimiento/Actualización De Equipos	50%					7	8	8	7	8	3,5				
		Caída Del Sistema Por Agotamiento De Recursos	75%					7	8	8	7	8	5,25				
		Perdida De Equipos	100%		100%			7	8	8	7	8	7		8		
		Abuso De Privilegios De Acceso	25%	25%	100%			7	8	8	7	8	1,75	2	8		
		Uso No Previsto	50%	25%	100%			7	8	8	7	8	3,5	2	8		
		Acceso No Autorizado		75%	100%			7	8	8	7	8		6	8		
		Manipulación De Equipos	75%		100%			7	8	8	7	8	5,25		8		
		Robo	100%		100%			7	8	8	7	8	7		8		
HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	100%					3	7	7	7	7	3				
		Corte De Suministro Eléctrico	25%					3	7	7	7	7	0,75				
		Errores De Administración	50%	25%	25%			3	7	7	7	7	1,5	1,75	1,75		
		Errores De Mantenimiento/Actualización De Equipos	50%					3	7	7	7	7	1,5				
		Caída Del Sistema Por Agotamiento De Recursos	75%					3	7	7	7	7	2,25				
		Perdida De Equipos	100%		75%			3	7	7	7	7	3		5,25		
		Abuso De Privilegios De Acceso	25%	25%	75%			3	7	7	7	7	0,75	1,75	5,25		
		Uso No Previsto	50%	25%	75%			3	7	7	7	7	1,5	1,75	5,25		
		Acceso No Autorizado		50%	75%			3	7	7	7	7		3,5	5,25		
		Manipulación De Equipos	50%		75%			3	7	7	7	7	1,5		5,25		
		Robo	100%		100%			3	7	7	7	7	3		7		

Figura 92. Impacto potencial de las amenazas del grupo Equipos informáticos (a) (Fuente propia)

HW7	Portátiles TIC	Daños Por Agua	100%					8	9	9	9	9	8				
		Avería De Origen Físico/Lógico	100%					8	9	9	9	9	8				
		Corte De Suministro Eléctrico	75%					8	9	9	9	9	6				
		Errores De Administración	50%	75%	100%			8	9	9	9	9	4	6,75	9		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	9	9	9	9	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	9	9	9	9	8				
		Abuso De Privilegios De Acceso	50%	75%	100%			8	9	9	9	9	4	6,75	9		
		Acceso No Autorizado		75%	100%			8	9	9	9	9		6,75	9		
		Manipulación De Equipos	50%		100%			8	9	9	9	9	4		9		
HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	75%					4	7	7	8	6	3				
		Errores De Administración	25%	25%	50%			4	7	7	8	6	1	1,75	3,5		
		Errores De Mantenimiento/Actualización De Equipos	75%					4	7	7	8	6	3				
		Caída Del Sistema Por Agotamiento De Recursos	50%					4	7	7	8	6	2				
		Perdida De Equipos	100%		100%			4	7	7	8	6	4		7		
		Abuso De Privilegios De Acceso	50%	50%	100%			4	7	7	8	6	2	3,5	7		
		Uso No Previsto	50%	50%	100%			4	7	7	8	6	2	3,5	7		
		Acceso No Autorizado		75%	100%			4	7	7	8	6		5,25	7		
		Manipulación De Equipos	75%		100%			4	7	7	8	6	3		7		
		Robo	100%		100%			4	7	7	8	6	4		7		
HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	100%					3	2	3	3	3	3				
		Corte De Suministro Eléctrico	100%					3	2	3	3	3	3				
		Errores De Administración	50%	50%	5%			3	2	3	3	3	1,5	1	0,15		
		Errores De Mantenimiento/Actualización De Equipos	50%					3	2	3	3	3	1,5				
		Caída Del Sistema Por Agotamiento De Recursos	75%					3	2	3	3	3	2,25				
		Perdida De Equipos	100%		25%			3	2	3	3	3	3		0,75		
		Abuso De Privilegios De Acceso	50%	25%	5%			3	2	3	3	3	1,5	0,5	0,15		
		Uso No Previsto	25%	25%	25%			3	2	3	3	3	0,75	0,5	0,75		
		Acceso No Autorizado		25%	25%			3	2	3	3	3		0,5	0,75		
		Manipulación De Equipos	50%		25%			3	2	3	3	3	1,5		0,75		
		Robo	100%		25%			3	2	3	3	3	3		0,75		
HW10	Router	Avería De Origen Físico/Lógico	100%					8	8	8	8	8	8				
		Corte De Suministro Eléctrico	100%					8	8	8	8	8	8				
		Fallas De Climatización	50%					8	8	8	8	8	4				
		Errores De Administración	75%	50%	100%			8	8	8	8	8	6	4	8		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	8	8	8	8	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	8	8	8	8				
		Abuso De Privilegios De Acceso	75%	50%	100%			8	8	8	8	8	6	4	8		
		Uso No Previsto	75%	50%	100%			8	8	8	8	8	6	4	8		
		Acceso No Autorizado		75%	100%			8	8	8	8	8		6	8		
		Manipulación De Equipos	75%		100%			8	8	8	8	8	6		8		
		Denegación De Servicio	100%					8	8	8	8	8	8				
HW11	Router inalámbrico	Daños Por Agua	100%					8	8	8	8	8	8				
		Avería De Origen Físico/Lógico	75%					8	8	8	8	8	6				
		Corte De Suministro Eléctrico	100%					8	8	8	8	8	8				
		Errores De Administración	75%	50%	100%			8	8	8	8	8	6	4	8		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	8	8	8	8	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	8	8	8	8				
		Perdida De Equipos	100%		50%			8	8	8	8	8	8		4		
		Abuso De Privilegios De Acceso	50%	50%	75%			8	8	8	8	8	4	4	6		
		Uso No Previsto	75%	75%	75%			8	8	8	8	8	6	6	6		
		Acceso No Autorizado		75%	100%			8	8	8	8	8		6	8		
		Manipulación De Equipos	75%		50%			8	8	8	8	8	6		4		
		Denegación De Servicio	100%					8	8	8	8	8	8				
		Robo	100%		50%			8	8	8	8	8	8		4		
HW12	Switch	Avería De Origen Físico/Lógico	100%					8	8	8	8	8	8				
		Corte De Suministro Eléctrico	100%					8	8	8	8	8	8				
		Fallas De Climatización	50%					8	8	8	8	8	4				
		Errores De Administración	75%	50%	100%			8	8	8	8	8	6	4	8		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	8	8	8	8	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	8	8	8	8				
		Abuso De Privilegios De Acceso	75%	50%	100%			8	8	8	8	8	6	4	8		
		Uso No Previsto	75%	50%	100%			8	8	8	8	8	6	4	8		
		Acceso No Autorizado		75%	100%			8	8	8	8	8		6	8		
		Manipulación De Equipos	75%		100%			8	8	8	8	8	6		8		
		Denegación De Servicio	100%					8	8	8	8	8	8				
HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	100%					8	5	4	6	5	8				
		Corte De Suministro Eléctrico	100%					8	5	4	6	5	8				
		Errores De Administración	75%	25%	50%			8	5	4	6	5	6	1,25	2		
		Errores De Mantenimiento/Actualización De Equipos	75%					8	5	4	6	5	6				
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	5	4	6	5	8				
		Abuso De Privilegios De Acceso	50%	50%	25%			8	5	4	6	5	4	2,5	1		
		Uso No Previsto	75%	50%	25%			8	5	4	6	5	6	2,5	1		
		Acceso No Autorizado		50%	25%			8	5	4	6	5		2,5	1		
		Manipulación De Equipos	75%		25%			8	5	4	6	5	6		1		
HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	100%					6	5	4	4	4	6				
		Corte De Suministro Eléctrico	100%					6	5	4	4	4	6				
		Errores De Administración	50%	25%	50%			6	5	4	4	4	3	1,25	2		
		Errores De Mantenimiento/Actualización De Equipos	75%					6	5	4	4	4	4,5				
		Abuso De Privilegios De Acceso	50%	25%	75%			6	5	4	4	4	3	1,25	3		
		Uso No Previsto	75%	25%	75%			6	5	4	4	4	4,5	1,25	3		
		Acceso No Autorizado		50%	75%			6	5	4	4	4		2,5	3		
		Manipulación De Equipos	75%		75%			6	5	4	4	4	4,5		3		
		Robo	100%		5%			6	5	4	4	4	6		0,2		

Figura 93. Impacto potencial de las amenazas del grupo Equipos informáticos (b) (Fuente propia)

- [COM] Redes de Comunicaciones

El impacto en los equipos informáticos varía entre el valor mínimo de 0,35 y el valor máximo de 9. Los activos redes locales y redes inalámbricas presentan el valor más alto de impacto, aunque las redes de telefonía fija y móvil también presentan valores altos de impacto de 7 y 8. Los valores medios entre 4 y 7 causados por una valoración o degradación baja se presentan en todos los activos. Los valores menores que 4 en su mayoría son el resultado de una degradación baja para el activo, siendo los ataques: abuso de privilegios de acceso, uso no previsto, acceso no autorizado y suplantación de identidad del usuario, las amenazas que provocan menos impacto en la dimensión de integridad. Para las redes de comunicaciones, el impacto en la dimensión de seguridad de autenticidad solo existe por la suplantación de identidad del usuario. Para este grupo de activos no existe valores de impacto en la dimensión de trazabilidad. Todos los valores calculados se observan en la Figura 94.

REDES DE COMUNICACIONES [COM]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	100%					7	8	9	9	8	7				
		Errores De Administración	75%	25%	75%			7	8	9	9	8	5,25	2	6,75		
		Alteración Accidental De La Información		50%				7	8	9	9	8		4			
		Caída Del Sistema Por Agotamiento De Recursos	100%					7	8	9	9	8	7				
		Suplantación De La Identidad Del Usuario		50%	100%	100%		7	8	9	9	8		4	9	9	
		Abuso De Privilegios De Acceso	50%	50%	75%			7	8	9	9	8	3,5	4	6,75		
		Uso No Previsto	50%	25%	75%			7	8	9	9	8	3,5	2	6,75		
		Acceso No Autorizado		50%	100%			7	8	9	9	8		4	9		
		Análisis De Trafico			100%			7	8	9	9	8			9		
		Interceptación De Información (Escucha)			100%			7	8	9	9	8			9		
		Modificación Deliberada De La Información		75%				7	8	9	9	8		6			
		Divulgación De Información			75%			7	8	9	9	8			6,75		
		Denegación De Servicio	100%					7	8	9	9	8	7				
COM2	Redes locales	Fallo Servicios De Comunicaciones	100%					8	8	9	9	8	8				
		Errores De Administración	75%	50%	100%			8	8	9	9	8	6	4	9		
		Alteración Accidental De La Información		50%				8	8	9	9	8		4			
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	8	9	9	8	8				
		Suplantación De La Identidad Del Usuario		75%	100%	100%		8	8	9	9	8		6	9	9	
		Abuso De Privilegios De Acceso	50%	75%	100%			8	8	9	9	8	4	6	9		
		Uso No Previsto	50%	50%	100%			8	8	9	9	8	4	4	9		
		Acceso No Autorizado		50%	100%			8	8	9	9	8		4	9		
		Análisis De Trafico			100%			8	8	9	9	8			9		
		Interceptación De Información (Escucha)			100%			8	8	9	9	8			9		
		Modificación Deliberada De La Información		75%				8	8	9	9	8		6			
		Divulgación De Información			75%			8	8	9	9	8			6,75		
		Denegación De Servicio	100%					8	8	9	9	8	8				
COM3	Red telefónica	Fallo Servicios De Comunicaciones	100%					8	7	8	7	8	8				
		Errores De Administración	75%	50%	75%			8	7	8	7	8	6	3,5	6		
		Alteración Accidental De La Información		50%				8	7	8	7	8		3,5			
		Caída Del Sistema Por Agotamiento De Recursos	100%					8	7	8	7	8	8				
		Abuso De Privilegios De Acceso	50%	25%	75%			8	7	8	7	8	4	1,75	6		
		Uso No Previsto	50%	25%	75%			8	7	8	7	8	4	1,75	6		
		Acceso No Autorizado		25%	100%			8	7	8	7	8		1,75	8		
		Análisis De Trafico			100%			8	7	8	7	8			8		
		Interceptación De Información (Escucha)			100%			8	7	8	7	8			8		
		Modificación Deliberada De La Información		50%				8	7	8	7	8		3,5			
		Divulgación De Información			75%			8	7	8	7	8			6		
		Denegación De Servicio	100%					8	7	8	7	8	8				
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	100%					8	7	8	7	8	8				
		Caída Del Sistema Por Agotamiento De Recursos	75%					8	7	8	7	8	6				
		Suplantación De La Identidad Del Usuario		5%	75%	75%		8	7	8	7	8		0,35	6	5,25	
		Abuso De Privilegios De Acceso	5%	5%	50%			8	7	8	7	8	0,4	0,35	4		
		Uso No Previsto	5%	5%	75%			8	7	8	7	8	0,4	0,35	6		
		Acceso No Autorizado		5%	75%			8	7	8	7	8		0,35	6		
		Análisis De Trafico			100%			8	7	8	7	8			8		
		Interceptación De Información (Escucha)			100%			8	7	8	7	8			8		
		Divulgación De Información			100%			8	7	8	7	8			8		

Figura 94. Impacto potencial de las amenazas del grupo Redes de comunicaciones (Fuente propia)

- [MEDIA] Soportes de Información

El impacto en este grupo varía entre el valor mínimo de 1,75 y el valor máximo de 9. Todos los activos presentan un impacto alto en las dimensiones: integridad y confidencialidad. Los valores medios entre 4 y 7 causados por una valoración o degradación baja se presentan en todos los activos. Pocos activos poseen valores menores a 4 causado por una degradación baja, y se presenta por las amenazas de errores de usuarios, administradores y mantenimiento. Para los soportes de información no existen valores de impacto en las dimensiones de autenticidad y trazabilidad. Todos los valores calculados se observan en la Figura 95.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	100%					8	9	9	9	9	8				
		Daños Por Agua	100%					8	9	9	9	9	8				
		Avería De Origen Físico/Lógico	75%					8	9	9	9	9	6				
		Degradación De Los Soportes De Almacenamiento De La Información	75%					8	9	9	9	9	6				
		Errores De Usuarios	25%	75%	100%			8	9	9	9	9	2	6,75	9		
		Errores De Administración	25%	75%	100%			8	9	9	9	9	2	6,75	9		
		Alteración Accidental De La Información		75%				8	9	9	9	9		6,75			
		Destrucción De Información	100%					8	9	9	9	9	8				
		Fugas De Información			100%			8	9	9	9	9			9		
		Errores De Mantenimiento del soporte	25%					8	9	9	9	9	2				
		Perdida del soporte	100%		100%			8	9	9	9	9	8		9		
		Uso No Previsto	100%	100%	100%			8	9	9	9	9	8	9	9		
		Acceso No Autorizado		100%	100%			8	9	9	9	9		9	9		
		Modificación Deliberada De La Información		100%				8	9	9	9	9		9			
		Destrucción De Información	100%					8	9	9	9	9	8				
		Divulgación De Información			100%			8	9	9	9	9			9		
		Manipulación del soporte	50%		100%			8	9	9	9	9	4		9		
		Robo	100%		100%			8	9	9	9	9	8		9		
MEDIA2	Pendrives USB	Daños Por Agua	100%					7	8	9	9	8	7				
		Daños Por Agua	100%					7	8	9	9	8	7				
		Avería De Origen Físico/Lógico	75%					7	8	9	9	8	5,25				
		Degradación De Los Soportes De Almacenamiento De La Información	75%					7	8	9	9	8	5,25				
		Errores De Usuarios	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Errores De Administración	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Alteración Accidental De La Información		100%				7	8	9	9	8		8			
		Destrucción De Información	100%					7	8	9	9	8	7				
		Fugas De Información			100%			7	8	9	9	8			9		
		Errores De Mantenimiento del soporte	50%					7	8	9	9	8	3,5				
		Perdida del soporte	100%		100%			7	8	9	9	8	7		9		
		Uso No Previsto	75%	100%	100%			7	8	9	9	8	5,25	8	9		
		Acceso No Autorizado		100%	100%			7	8	9	9	8		8	9		
		Modificación Deliberada De La Información		100%				7	8	9	9	8		8			
		Destrucción De Información	100%					7	8	9	9	8	7				
		Divulgación De Información			100%			7	8	9	9	8			9		
		Manipulación del soporte	75%		100%			7	8	9	9	8	5,25		9		
		Robo	100%		100%			7	8	9	9	8	7		9		
MEDIA3	CD/DVD	Daños Por Agua	100%					7	8	9	9	8	7				
		Daños Por Agua	100%					7	8	9	9	8	7				
		Avería De Origen Físico/Lógico	75%					7	8	9	9	8	5,25				
		Degradación De Los Soportes De Almacenamiento De La Información	75%					7	8	9	9	8	5,25				
		Errores De Usuarios	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Errores De Administración	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Alteración Accidental De La Información		100%				7	8	9	9	8		8			
		Destrucción De Información	100%					7	8	9	9	8	7				
		Fugas De Información			100%			7	8	9	9	8			9		
		Errores De Mantenimiento del soporte	50%					7	8	9	9	8	3,5				
		Perdida del soporte	100%		100%			7	8	9	9	8	7		9		
		Uso No Previsto	75%	100%	100%			7	8	9	9	8	5,25	8	9		
		Acceso No Autorizado		100%	100%			7	8	9	9	8		8	9		
		Modificación Deliberada De La Información		100%				7	8	9	9	8		8			
		Destrucción De Información	100%					7	8	9	9	8	7				
		Divulgación De Información			100%			7	8	9	9	8			9		
		Manipulación del soporte	75%		100%			7	8	9	9	8	5,25		9		
		Robo	100%		100%			7	8	9	9	8	7		9		
MEDIA4	Material impreso	Daños Por Agua	100%					7	8	9	9	9	7				
		Daños Por Agua	100%					7	8	9	9	9	7				
		Degradación por Almacenamiento	75%					7	8	9	9	9	5,25				
		Errores De Usuarios	50%	75%	75%			7	8	9	9	9	3,5	6	6,75		
		Errores De Administración	50%	75%	75%			7	8	9	9	9	3,5	6	6,75		
		Alteración Accidental De La Información		50%				7	8	9	9	9		4			
		Destrucción	100%					7	8	9	9	9	7				
		Fugas De Información			100%			7	8	9	9	9			9		
		Errores De Almacenamiento	50%					7	8	9	9	9	3,5				
		Perdida	50%		100%			7	8	9	9	9	3,5		9		
		Uso No Previsto	100%	75%	100%			7	8	9	9	9	7	6	9		
		Acceso No Autorizado		75%	100%			7	8	9	9	9		6	9		
		Modificación Deliberada De La Información		100%				7	8	9	9	9		8			
		Destrucción	100%					7	8	9	9	9	7				
		Divulgación			100%			7	8	9	9	9			9		
		Manipulación	50%		100%			7	8	9	9	9	3,5		9		
		Robo	50%		100%			7	8	9	9	9	3,5		9		

Figura 95. Impacto potencial de las amenazas del grupo Equipamiento auxiliar (Fuente propia)

- [AUX] Equipamiento Auxiliar

En este grupo de activos, el impacto varía entre el valor mínimo de 0,15 y el valor máximo de 9. El valor máximo de 9 se observa solo en la dimensión de confidencialidad de las cajas fuertes. Los demás valores son medios y no sobrepasan un valor de impacto de 6 excepto, el impacto de 8 causado por la pérdida de quipos en el activo: cajas fuertes. El menor valor de impacto se presenta en la dimensión de confidencialidad en los activos: generador eléctrico, fuentes de alimentación y climatización. El equipamiento auxiliar no presenta valores de impacto en autenticidad y trazabilidad debido a que no existe degradación en dichas dimensiones. Todos los valores calculados se observan en la Figura 96.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	75%					5	5	3	4	4	3,75				
		Fuego	75%					5	5	3	4	4	3,75				
		Daños Por Agua	75%					5	5	3	4	4	3,75				
		Contaminación Mecánica	50%					5	5	3	4	4	2,5				
		Degradación por almacenamiento	50%					5	5	3	4	4	2,5				
		Avería De Origen Físico/ Lógico	75%					5	5	3	4	4	3,75				
		Errores De Mantenimiento/ Actualización De Equipos	75%					5	5	3	4	4	3,75				
		Uso No Previsto	75%	25%	5%			5	5	3	4	4	3,75	1,25	0,15		
		Acceso No Autorizado		25%	5%			5	5	3	4	4		1,25	0,15		
		Manipulación De Equipos	75%		5%			5	5	3	4	4	3,75		0,15		
AUX2	Fuentes de alimentación	Daños Por Agua	75%					5	7	3	4	4	3,75				
		Fuego	75%					5	7	3	4	4	3,75				
		Daños Por Agua	75%					5	7	3	4	4	3,75				
		Contaminación Mecánica	50%					5	7	3	4	4	2,5				
		Degradación por almacenamiento	50%					5	7	3	4	4	2,5				
		Avería De Origen Físico/ Lógico	75%					5	7	3	4	4	3,75				
		Corte De Suministro Eléctrico	100%					5	7	3	4	4	5				
		Errores De Mantenimiento/ Actualización De Equipos	75%					5	7	3	4	4	3,75				
		Perdida De Equipos	100%		5%			5	7	3	4	4	5		0,15		
		Uso No Previsto	100%	25%	5%			5	7	3	4	4	5	1,75	0,15		
		Acceso No Autorizado		25%	5%			5	7	3	4	4		1,75	0,15		
		Manipulación De Equipos	75%		5%			5	7	3	4	4	3,75		0,15		
		Robo	100%		5%			5	7	3	4	4	5		0,15		
AUX3	Climatización	Daños Por Agua	75%					5	4	3	4	4	3,75				
		Fuego	75%					5	4	3	4	4	3,75				
		Daños Por Agua	75%					5	4	3	4	4	3,75				
		Contaminación Mecánica	50%					5	4	3	4	4	2,5				
		Avería De Origen Físico/Lógico	75%					5	4	3	4	4	3,75				
		Corte De Suministro Eléctrico	100%					5	4	3	4	4	5				
		Errores De Mantenimiento/Actualización De Equipos	75%					5	4	3	4	4	3,75				
		Uso No Previsto	50%	25%	5%			5	4	3	4	4	2,5	1	0,15		
		Acceso No Autorizado		25%	5%			5	4	3	4	4		1	0,15		
		Manipulación De Equipos	50%		5%			5	4	3	4	4	2,5		0,15		
AUX4	Cableado UTP	Daños Por Agua	75%					7	8	4	4	4	5,25				
		Fuego	100%					7	8	4	4	4	7				
		Daños Por Agua	75%					7	8	4	4	4	5,25				
		Avería De Origen Físico/Lógico	75%					7	8	4	4	4	5,25				
		Errores De Mantenimiento/Actualización De Equipos	75%					7	8	4	4	4	5,25				
		Uso No Previsto	50%	25%	25%			7	8	4	4	4	3,5	2	1		
		Acceso No Autorizado		25%	75%			7	8	4	4	4		2	3		
		Manipulación De Equipos	50%		75%			7	8	4	4	4	3,5		3		
AUX5	Armarios	Daños Por Agua	50%					8	8	8	8	8	4				
		Fuego	75%					8	8	8	8	8	6				
		Daños Por Agua	50%					8	8	8	8	8	4				
		Degradación por almacenamiento	25%					8	8	8	8	8	2				
		Avería De Origen Físico/Lógico	50%					8	8	8	8	8	4				
		Uso No Previsto	25%	25%	75%			8	8	8	8	8	2	2	6		
		Acceso No Autorizado		25%	75%			8	8	8	8	8		2	6		
		Manipulación De Equipos	25%		75%			8	8	8	8	8	2		6		
AUX6	Cajas fuertes	Daños Por Agua	25%					8	8	9	9	9	2				
		Fuego	25%					8	8	9	9	9	2				
		Daños Por Agua	25%					8	8	9	9	9	2				
		Avería De Origen Físico/Lógico	75%					8	8	9	9	9	6				
		Corte De Suministro Eléctrico	75%					8	8	9	9	9	6				
		Errores De Mantenimiento/Actualización De Equipos	75%					8	8	9	9	9	6				
		Perdida De Equipos	100%		100%			8	8	9	9	9	8		9		
		Uso No Previsto	75%	5%	100%			8	8	9	9	9	6	0,4	9		
		Acceso No Autorizado		5%	100%			8	8	9	9	9		0,4	9		
		Manipulación De Equipos	25%		100%			8	8	9	9	9	2		9		

Figura 96. Impacto potencial de las amenazas del grupo Equipamiento auxiliar (Fuente propia)

- [L]Instalaciones

El impacto en este grupo varía entre el valor mínimo de 1,5 y el valor máximo de 8. En las dimensiones de disponibilidad y confidencialidad de los activos edificios y cuartos de servidores, se presenta el valor máximo de impacto. Los valores menores que 4 en su mayoría son el resultado de una degradación baja para el activo, siendo las amenazas de uso no previsto y acceso no autorizado del activo edificio, las que causan menor impacto. Para los activos de las Instalaciones no existen valores de impacto en las dimensiones de autenticidad y trazabilidad, además que el activo coche solo se calculó en el impacto en la dimensión de seguridad de disponibilidad. Todos los valores calculados se observan en la Figuras 97.

ACTIVOS DE INSTALACIONES [L]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
L1	Edificios	Fuego	100%					6	7	8	6	5	6				
		Daños Por Agua	75%					6	7	8	6	5	4,5				
		Fuego	75%					6	7	8	6	5	4,5				
		Daños Por Agua	50%					6	7	8	6	5	3				
		Fugas De Información			75%			6	7	8	6	5			6		
		Uso No Previsto	25%	25%	75%			6	7	8	6	5	1,5	1,75	6		
		Acceso No Autorizado		25%	100%			6	7	8	6	5		1,75	8		
L2	Cuartos servidores	Fuego	100%					8	8	8	8	7	8				
		Daños Por Agua	100%					8	8	8	8	7	8				
		Fuego	100%					8	8	8	8	7	8				
		Daños Por Agua	100%					8	8	8	8	7	8				
		Fugas De Información			100%			8	8	8	8	7			8		
		Uso No Previsto	75%	75%	75%			8	8	8	8	7	6	6	6		
		Acceso No Autorizado		50%	100%			8	8	8	8	7		4	8		
L3	Coche	Daños mecánicos	100%					2	5	3	5	2	2				
		Accidente de tránsito	100%					2	5	3	5	2	2				

Figura 97. Impacto potencial de las amenazas del grupo Instalaciones
(Fuente propia)

- [P] Personal

El impacto en el grupo de activos Personal varía entre el valor mínimo de 1,25 y el valor máximo de 9. En todos los activos se presenta el valor máximo de impacto en la dimensión de seguridad de confidencialidad. Los valores medios entre 3 y 6 causados por una valoración o degradación baja se presentan en todos los activos, excepto en el activo usuarios. Los valores de impacto menores que 4 en su mayoría son el resultado de una degradación baja para el activo y se presenta en la dimensión de disponibilidad. Para este grupo de activos no existen valores de impacto en las dimensiones de autenticidad y trazabilidad. Todos los valores calculados se observan en la Figura 98.

ACTIVOS DE PERSONAL [P]			Degradación					Valor del Activo					Impacto				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
P1	Administradores	Fugas De Información			100%			8	8	9	9	9			9		
		Indisponibilidad Del Personal	75%					8	8	9	9	9	6				
		Indisponibilidad Del Personal	75%					8	8	9	9	9	6				
		Extorsión	25%	75%	100%			8	8	9	9	9	2	6	9		
		Ingeniería Social	25%	75%	100%			8	8	9	9	9	2	6	9		
P2	Técnicos	Fugas De Información			100%			7	8	9	9	8			9		
		Indisponibilidad Del Personal	50%					7	8	9	9	8	3,5				
		Indisponibilidad Del Personal	50%					7	8	9	9	8	3,5				
		Extorsión	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Ingeniería Social	25%	50%	100%			7	8	9	9	8	1,75	4	9		
P3	Empleados	Fugas De Información			100%			7	8	9	9	8			9		
		Indisponibilidad Del Personal	50%					7	8	9	9	8	3,5				
		Indisponibilidad Del Personal	50%					7	8	9	9	8	3,5				
		Extorsión	25%	50%	100%			7	8	9	9	8	1,75	4	9		
		Ingeniería Social	25%	50%	100%			7	8	9	9	8	1,75	4	9		
P4	Usuarios	Fugas De Información			100%			5	6	9	9	5			9		
		Extorsión	25%	50%	100%			5	6	9	9	5	1,25	3	9		
		Ingeniería Social	25%	50%	100%			5	6	9	9	5	1,25	3	9		

Figura 98. Impacto potencial de las amenazas del grupo Personal
(Fuente propia)

4.4.2. Cálculos de Riesgo

Obtenido el impacto potencial, se procede al cálculo del riesgo potencial o riesgo repercutido con la fórmula:

$$RP = IP * F$$

Donde:

RP = Riesgo Potencial

IP = Impacto Potencial

F = Probabilidad de Materialización de la amenaza (frecuencia)

Según la fórmula anterior, para el cálculo del riesgo potencial se requiere de la frecuencia de ocurrencia determinada anteriormente. El resultado y análisis del riesgo potencial se pueden ver en las imágenes que se presentan a continuación:

- [D] Datos /Información

El riesgo potencial varía entre el valor mínimo de 0,04 y el valor máximo de 3,68. En este grupo no se observan valores altos de riesgo, debido a que las amenazas no tienen alta la frecuencia de ocurrencia, lo que disminuye los riesgos considerablemente. El riesgo en todos los activos es muy variante, pero se puede observar que los valores menores de riesgo se encuentran en la dimensión de Integridad. El mayor riesgo se presenta por la vulnerabilidad de alteración accidental de la información que afecta a los ficheros almacenados en PC y en servidores en la

nube, y bases de datos en servidores locales y en la nube. Todos los valores calculados se observan en las Figuras 99 a la 101.

DATOS / INFORMACIÓN [D]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
D1	Datos de configuración	Errores De Administración	0,3	6	6	2			1,8	1,8	0,6		
		Errores De Configuración	0,3		4					1,2			
		Alteración Accidental De La Información	0,3		4					1,2			
		Destrucción De Información	0,3	8					2,4				
		Fugas De Información	0,1			4					0,4		
		Manipulación De Los Registros De Actividad	0,1		0,4			6,75		0,04			0,675
		Manipulación De La Configuración	0,1		8	8	9			0,8	0,8	0,9	
		Abuso De Privilegios De Acceso	0,1	6	6	6			0,6	0,6	0,6		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Repudio	0,1		6			9		0,6			0,9
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	8					0,8				
D2	Código fuente de aplicaciones	Errores De Administración	0,3	4	6,75	2			1,2	2,025	0,6		
		Errores De Configuración	0,3		6,75					2,025			
		Alteración Accidental De La Información	0,1		9					0,9			
		Manipulación De Los Registros De Actividad	0,1		0,45			6,75		0,045			0,675
		Manipulación De La Configuración	0,1		6,75	4	4,5			0,675	0,4	0,45	
		Abuso De Privilegios De Acceso	0,1	2	6,75	6			0,2	0,675	0,6		
		Acceso No Autorizado	0,1		9	8				0,9	0,8		
		Repudio	0,1		6,75			9		0,675			0,9
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	8					0,8				
D3	Ficheros almacenados en PC	Errores De Usuarios	0,7	2,25	5,25	2,5			1,575	3,675	1,75		
		Errores De Administración	0,3	2,25	5,25	2,5			0,675	1,575	0,75		
		Errores De Configuración	0,3		1,75					0,525			
		Alteración Accidental De La Información	0,7		5,25					3,675			
		Destrucción De Información	0,5	3					1,5				
		Fugas De Información	0,1			1,25					0,125		
		Manipulación De Los Registros De Actividad	0,1		1,75			3,5		0,175			0,35
		Manipulación De La Configuración	0,1		3,5	2,5	1,5			0,35	0,25	0,15	
		Suplantación De La Identidad Del Usuario	0,3		3,5	3,75	4,5			1,05	1,125	1,35	
		Abuso De Privilegios De Acceso	0,1	0,75	3,5	3,75			0,075	0,35	0,375		
		Acceso No Autorizado	0,3		5,25	5				1,575	1,5		
		Repudio	0,1		1,75			7		0,175			0,7
		Modificación Deliberada De La Información	0,1		7					0,7			
		Destrucción De Información	0,1	2,25					0,225				
D4	Ficheros almacenados en servidores en la nube	Errores De Usuarios	0,7	2,5	3,5	0,35			1,75	2,45	0,245		
		Errores De Administración	0,3	3,75	5,25	3,5			1,125	1,575	1,05		
		Errores De Monitorización Log	0,1		3,5			6		0,35			0,6
		Errores De Configuración	0,3		3,5					1,05			
		Alteración Accidental De La Información	0,7		5,25					3,675			
		Destrucción De Información	0,3	3,75					1,125				
		Manipulación De Los Registros De Actividad	0,1		1,75			6		0,175			0,6
		Manipulación De La Configuración	0,1		1,75	3,5	4			0,175	0,35	0,4	
		Suplantación De La Identidad Del Usuario	0,3		1,75	5,25	6			0,525	1,575	1,8	
		Abuso De Privilegios De Acceso	0,1	1,25	1,75	5,25			0,125	0,175	0,525		
		Acceso No Autorizado	0,1		3,5	7				0,35	0,7		
		Repudio	0,1		1,75			8		0,175			0,8
		Modificación Deliberada De La Información	0,1		7					0,7			
		Destrucción De Información	0,1	5					0,5				
D5	Ficheros almacenados en servidores locales	Errores De Usuarios	0,7	3,75	3,5	0,35			2,625	2,45	0,245		
		Errores De Administración	0,3	3,75	5,25	3,5			1,125	1,575	1,05		
		Errores De Monitorización Log	0,1		3,5			6		0,35			0,6
		Errores De Configuración	0,3		3,5					1,05			
		Alteración Accidental De La Información	0,5		5,25					2,625			
		Destrucción De Información	0,3	3,75					1,125				
		Manipulación De Los Registros De Actividad	0,1		1,75			6		0,175			0,6
		Manipulación De La Configuración	0,1		1,75	3,5	4			0,175	0,35	0,4	
		Suplantación De La Identidad Del Usuario	0,3		1,75	5,25	6			0,525	1,575	1,8	
		Abuso De Privilegios De Acceso	0,1	1,25	1,75	5,25			0,125	0,175	0,525		
		Acceso No Autorizado	0,1		3,5	7				0,35	0,7		
		Repudio	0,1		1,75			8		0,175			0,8
		Modificación Deliberada De La Información	0,1		7					0,7			
		Destrucción De Información	0,1	5					0,5				

Figura 99. Riesgo potencial de las amenazas del grupo Datos/Información (a)
(Fuente propia)

D6	Bases de datos en servidores locales	Errores De Administración	0,3	6	6,75	4,5			1,8	2,025	1,35		
		Errores De Monitorización Log	0,1		6,75			6,75		0,675			0,675
		Errores De Configuración	0,3		6,75					2,025			
		Alteración Accidental De La Información	0,5		6,75					3,375			
		Destrucción De Información	0,1	8					0,8				
		Manipulación De Los Registros De Actividad	0,1		4,5			9		0,45			0,9
		Manipulación De La Configuración	0,1		4,5	6,75	4,5			0,45	0,675	0,45	
		Suplantación De La Identidad Del Usuario	0,1		4,5	9	6,75			0,45	0,9	0,675	
		Abuso De Privilegios De Acceso	0,1	6	4,5	6,75			0,6	0,45	0,675		
		Acceso No Autorizado	0,1		6,75	9				0,675	0,9		
		Repudio	0,1		4,5			9		0,45			0,9
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	8					0,8				
D7	Bases de datos en servidores en la nube	Errores De Administración	0,3	6,75	6,75	4,5			2,025	2,025	1,35		
		Errores De Monitorización Log	0,1		6,75			6,75		0,675			0,675
		Errores De Configuración	0,3		6,75					2,025			
		Alteración Accidental De La Información	0,5		6,75					3,375			
		Destrucción De Información	0,1	9					0,9				
		Manipulación De Los Registros De Actividad	0,1		4,5			9		0,45			0,9
		Manipulación De La Configuración	0,1		4,5	6,75	4,5			0,45	0,675	0,45	
		Suplantación De La Identidad Del Usuario	0,1		4,5	9	6,75			0,45	0,9	0,675	
		Abuso De Privilegios De Acceso	0,1	6,75	4,5	6,75			0,675	0,45	0,675		
		Acceso No Autorizado	0,1		6,75	9				0,675	0,9		
		Repudio	0,1		4,5			9		0,45			0,9
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	9					0,9				
D8	Copias de seguridad en la nube	Errores De Administración	0,1	6,75	6	4,5			0,675	0,6	0,45		
		Errores De Monitorización Log	0,3		4			4,5		1,2			1,35
		Errores De Configuración	0,3		8					2,4			
		Alteración Accidental De La Información	0,3		8					2,4			
		Destrucción De Información	0,1	9					0,9				
		Manipulación De Los Registros De Actividad	0,1		2			6,75		0,2			0,675
		Manipulación De La Configuración	0,1		6	6,75	6,75			0,6	0,675	0,675	
		Suplantación De La Identidad Del Usuario	0,1		4	9	6,75			0,4	0,9	0,675	
		Abuso De Privilegios De Acceso	0,1	4,5	6	9			0,45	0,6	0,9		
		Acceso No Autorizado	0,1		6	9				0,6	0,9		
		Repudio	0,1		4			9		0,4			0,9
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	9					0,9				
		Divulgación De Información	0,1			9					0,9		
D9	Copias de Seguridad en servidores locales	Errores De Administración	0,1	6	6	4,5			0,6	0,6	0,45		
		Errores De Monitorización Log	0,3		4			4,5		1,2			1,35
		Errores De Configuración	0,3		8					2,4			
		Alteración Accidental De La Información	0,3		8					2,4			
		Destrucción De Información	0,1	8					0,8				
		Fugas De Información	0,1			6,75					0,675		
		Manipulación De La Configuración	0,1		6	6,75	6,75			0,6	0,675	0,675	
		Suplantación De La Identidad Del Usuario	0,1		4	9	6,75			0,4	0,9	0,675	
		Abuso De Privilegios De Acceso	0,1	4	6	9			0,4	0,6	0,9		
		Acceso No Autorizado	0,1		6	9				0,6	0,9		
		Repudio	0,1		4			9		0,4			0,9
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,1			9					0,9		
D10	Copias de Seguridad en discos externos	Errores De Administración	0,1	5,25	6	4,5			0,525	0,6	0,45		
		Errores De Monitorización Log	0,3		4			4,5		1,2			1,35
		Errores De Configuración	0,3		8					2,4			
		Alteración Accidental De La Información	0,3		8					2,4			
		Destrucción De Información	0,1	7					0,7				
		Manipulación De Los Registros De Actividad	0,1		2			6,75		0,2			0,675
		Manipulación De La Configuración	0,1		6	6,75	6,75			0,6	0,675	0,675	
		Suplantación De La Identidad Del Usuario	0,1		4	9	6,75			0,4	0,9	0,675	
		Abuso De Privilegios De Acceso	0,1	3,5	6	9			0,35	0,6	0,9		
		Acceso No Autorizado	0,1		6	9				0,6	0,9		
		Repudio	0,1		4			9		0,4			0,9
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	7					0,7				
		Divulgación De Información	0,1			9					0,9		
D11	Ficheros de contraseñas	Errores De Administración	0,1	6,75	6,75	9			0,675	0,675	0,9		
		Errores De Configuración	0,1		0,45					0,045			
		Alteración Accidental De La Información	0,1		6,75					0,675			
		Destrucción De Información	0,1	9					0,9				
		Manipulación De Los Registros De Actividad	0,1		2,25			9		0,225			0,9
		Suplantación De La Identidad Del Usuario	0,1		4,5	9	4,5			0,45	0,9	0,45	
		Abuso De Privilegios De Acceso	0,1	2,25	4,5	6,75			0,225	0,45	0,675		
		Acceso No Autorizado	0,1		6,75	9				0,675	0,9		
		Repudio	0,1		2,25			9		0,225			0,9
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	9					0,9				
		Divulgación De Información	0,1			9					0,9		

Figura 100. Riesgo potencial de las amenazas del grupo Datos/Información (b)
(Fuente propia)

D12	Registros de actividades en servidores	Errores De Administración	0,3	6	4	4			1,8	1,2	1,2		
		Errores De Configuración	0,3		6					1,8			
		Destrucción De Información	0,3	6					1,8				
		Manipulación De La Configuración	0,1		6	4	6,75			0,6	0,4	0,675	
		Suplantación De La Identidad Del Usuario	0,1		6	8	4,5			0,6	0,8	0,45	
		Abuso De Privilegios De Acceso	0,1	6	4	4			0,6	0,4	0,4		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Repudio	0,3		4			9		1,2			2,7
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	8					0,8				
D13	Ficheros compartidos Google Drive	Errores De Administración	0,3	5,25	4	4			1,575	1,2	1,2		
		Errores De Configuración	0,1		2					0,2			
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,3	5,25					1,575				
		Manipulación De La Configuración	0,1		4	4	3,5			0,4	0,4	0,35	
		Suplantación De La Identidad Del Usuario	0,1		6	8	3,5			0,6	0,8	0,35	
		Abuso De Privilegios De Acceso	0,1	3,5	4	4			0,35	0,4	0,4		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Repudio	0,1		2			7		0,2			0,7
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	7					0,7				
		Divulgación De Información	0,1			8					0,8		

Figura 101. Riesgo potencial de las amenazas del grupo Datos/Información (c)
(Fuente propia)

- [S] Servicios

El riesgo potencial en este grupo varía entre el valor mínimo de 0,175 y el valor máximo de 4,5. La mayoría de los valores de riesgo son menores exceptuando los riesgos causados mayormente por el acceso no autorizado, además de la suplantación de la identidad del usuario, destrucción de información, errores de usuarios y alteración accidental de la información. En general la mayoría de los valores bajos se presentan porque la frecuencia de ocurrencia es menor. El valor mínimo se encuentra en el servicio de página web a causa de los errores de usuarios en la dimensión de disponibilidad. Los valores calculados se observan en las Figuras 102 a la 104.

SERVICIOS [S]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
S1	Página web	Errores De Usuarios	0,5	0,35	0,4	2			0,175	0,2	1		
		Errores De Administración	0,1	7	6	6			0,7	0,6	0,6		
		Alteración Accidental De La Información	0,1		6					0,6			
		Fugas De Información	0,1			4					0,4		
		Caída Del Sistema Por Agotamiento De Recursos	0,3	7					2,1				
		Suplantación De La Identidad Del Usuario	0,7		6	6	5			4,2	4,2	3,5	
		Abuso De Privilegios De Acceso	0,3	3,5	6	6			1,05	1,8	1,8		
		Uso No Previsto	0,3	3,5	6	6			1,05	1,8	1,8		
		Acceso No Autorizado	0,5		8	6				4	3		
		Repudio	0,1		4			5,25		0,4			0,525
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	5,25					0,525				
		Divulgación De Información	0,3			8					2,4		
		Denegación De Servicio	0,3	7					2,1				
S2	Correo electrónico	Errores De Usuarios	0,7	3,5	2	4			2,45	1,4	2,8		
		Errores De Administración	0,1	5,25	2	6			0,525	0,2	0,6		
		Alteración Accidental De La Información	0,3		4					1,2			
		Fugas De Información	0,1			6					0,6		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	7					0,7				
		Suplantación De La Identidad Del Usuario	0,5		4	6	5,25			2	3	2,625	
		Abuso De Privilegios De Acceso	0,3	3,5	6	6			1,05	1,8	1,8		
		Uso No Previsto	0,3	5,25	6	6			1,575	1,8	1,8		
		Acceso No Autorizado	0,5		6	8				3	4		
		Repudio	0,1		4			6		0,4			0,6
		Modificación Deliberada De La Información	0,1		6					0,6			
		Divulgación De Información	0,3			6					1,8		
		Denegación De Servicio	0,1	7					0,7				

Figura 102. Riesgo potencial de las amenazas del grupo Servicios (a)
(Fuente propia)

S3	Intranet documental - Servicio FTP	Errores De Usuarios	0,7	0,4	4	4			0,28	2,8	2,8		
		Errores De Administración	0,3	6	6	4			1,8	1,8	1,2		
		Alteración Accidental De La Información	0,5		6					3			
		Destrucción De Información	0,5	6					3				
		Fugas De Información	0,1			6					0,6		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Suplantación De La Identidad Del Usuario	0,3		4	6	4			1,2	1,8	1,2	
		Abuso De Privilegios De Acceso	0,1	2	4	6			0,2	0,4	0,6		
		Uso No Previsto	0,3	4	4	6			1,2	1,2	1,8		
		Acceso No Autorizado	0,5		4	8				2	4		
		Repudio	0,3		2			6		0,6			1,8
		Modificación Deliberada De La Información	0,1		6					0,6			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,1			6					0,6		
		Denegación De Servicio	0,3	8					2,4				
S4	Sistema de tickets de incidencias	Errores De Usuarios	0,7	0,2	1,5	1,5			0,14	1,05	1,05		
		Errores De Administración	0,3	3	3	1,5			0,9	0,9	0,45		
		Alteración Accidental De La Información	0,3		3					0,9			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	4					0,4				
		Suplantación De La Identidad Del Usuario	0,3		3	4,5	4			0,9	1,35	1,2	
		Acceso No Autorizado	0,5		4,5	4,5				2,25	2,25		
		Repudio	0,1		3			3,75		0,3			0,375
		Modificación Deliberada De La Información	0,1		3					0,3			
		Divulgación De Información	0,1			3					0,3		
		Denegación De Servicio	0,3	4					1,2				
S5	Educación Virtual	Errores De Usuarios	0,7	0,4	2	3,5			0,28	1,4	2,45		
		Errores De Administración	0,3	6	4	3,5			1,8	1,2	1,05		
		Alteración Accidental De La Información	0,5		6					3			
		Destrucción De Información	0,5	8					4				
		Fugas De Información	0,5			3,5					1,75		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Suplantación De La Identidad Del Usuario	0,5		2	5,25	3			1	2,625	1,5	
		Abuso De Privilegios De Acceso	0,3	2	6	3,5			0,6	1,8	1,05		
		Uso No Previsto	0,5	4	2	3,5			2	1	1,75		
		Acceso No Autorizado	0,5		6	5,25				3	2,625		
		Repudio	0,1		2			5,25		0,2			0,525
		Modificación Deliberada De La Información	0,1		6					0,6			
		Divulgación De Información	0,3			3,5					1,05		
		Denegación De Servicio	0,3	8					2,4				
S6	Servicio de financiero	Errores De Usuarios	0,5	2	6,75	9			1	3,375	4,5		
		Errores De Administración	0,3	6	4,5	6,75			1,8	1,35	2,025		
		Alteración Accidental De La Información	0,5		9					4,5			
		Destrucción De Información	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	8					2,4				
		Suplantación De La Identidad Del Usuario	0,3		6,75	9	6,75			2,025	2,7	2,025	
		Abuso De Privilegios De Acceso	0,3	2	6,75	6,75			0,6	2,025	2,025		
		Uso No Previsto	0,3	4	4,5	4,5			1,2	1,35	1,35		
		Acceso No Autorizado	0,3		9	9				2,7	2,7		
		Repudio	0,1		4,5			9		0,45			0,9
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,1			9					0,9		
		Denegación De Servicio	0,3	8					2,4				
S7	Gestión de usuarios Socios	Errores De Usuarios	0,5	2	6	4			1	3	2		
		Errores De Administración	0,3	6	4	6			1,8	1,2	1,8		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	6					0,6				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Suplantación De La Identidad Del Usuario	0,3		6	8	3,5			1,8	2,4	1,05	
		Abuso De Privilegios De Acceso	0,1	2	4	4			0,2	0,4	0,4		
		Uso No Previsto	0,3	4	2	6			1,2	0,6	1,8		
		Acceso No Autorizado	0,5		6	8				3	4		
		Repudio	0,1		2			8		0,2			0,8
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,3			8					2,4		
		Denegación De Servicio	0,3	8					2,4				

Figura 103. Riesgo potencial de las amenazas del grupo Servicios (b)
(Fuente propia)

S8	Gestión empresarial	Errores De Usuarios	0,5	1,75	4	4			0,875	2	2		
		Errores De Administración	0,3	3,5	4	4			1,05	1,2	1,2		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	5,25					0,525				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	5,25					0,525				
		Suplantación De La Identidad Del Usuario	0,3		4	6	3,5			1,2	1,8	1,05	
		Abuso De Privilegios De Acceso	0,1	1,75	4	4			0,175	0,4	0,4		
		Uso No Previsto	0,3	1,75	4	6			0,525	1,2	1,8		
		Acceso No Autorizado	0,5		6	8				3	4		
		Repudio	0,1		4			8		0,4			0,8
		Modificación Deliberada De La Información	0,1		6					0,6			
		Destrucción De Información	0,1	7					0,7				
		Divulgación De Información	0,3			8					2,4		
		Denegación De Servicio	0,3	7					2,1				
S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	0,5	1,75	4	6			0,875	2	3		
		Errores De Administración	0,3	3,5	4	6			1,05	1,2	1,8		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	5,25					0,525				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	7					0,7				
		Suplantación De La Identidad Del Usuario	0,3		6	8	4			1,8	2,4	1,2	
		Abuso De Privilegios De Acceso	0,1	1,75	4	6			0,175	0,4	0,6		
		Uso No Previsto	0,3	1,75	4	6			0,525	1,2	1,8		
		Acceso No Autorizado	0,5		6	8				3	4		
		Repudio	0,1		4			9		0,4			0,9
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	7					0,7				
		Divulgación De Información	0,3			8					2,4		
		Denegación De Servicio	0,3	7					2,1				

Figura 104. Riesgo potencial de las amenazas del grupo Servicios (c)
(Fuente propia)

- [SW] Software – Aplicaciones Informáticas

El riesgo potencial de estos activos varía entre el valor mínimo de 0,03 y el valor máximo de 4. En las aplicaciones informáticas no se observa valores altos de riesgo, debido a que las amenazas no tienen alta la frecuencia de ocurrencia. El valor máximo de riesgo se presenta en los activos aplicación de Página web y Navegador web producido por las amenazas de uso no previsto y difusión de software dañino respectivamente. Los valores menores a 0,1 se han producido en las dimensiones de integridad y disponibilidad en los activos: aplicación de correo electrónico Gmail, E-apsa, sistemas operativos Windows 7 y 10, navegadores web y software ofimático. Todos los valores calculados se observan en las Figuras de la 105 a la 108.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
SW1	Aplicación de Financiero	Fallo De Origen Lógico	0,1	6,75					0,675				
		Errores De Usuarios	0,5	2,25	6,75	4,5			1,125	3,375	2,25		
		Errores De Administración	0,1	6,75	4,5	4,5			0,675	0,45	0,45		
		Alteración Accidental De La Información	0,3		6,75					2,025			
		Destrucción De Información	0,1	9					0,9				
		Fugas De Información	0,1			9					0,9		
		Vulnerabilidades De Los Programas	0,3	4,5	6,75	9			1,35	2,025	2,7		
		Errores De Mantenimiento/Actualización De Programas	0,3	4,5	6,75				1,35	2,025			
		Suplantación De La Identidad Del Usuario	0,1		6,75	9	6,75			0,675	0,9	0,675	
		Abuso De Privilegios De Acceso	0,3	4,5	6,75	9			1,35	2,025	2,7		
		Uso No Previsto	0,3	6,75	4,5	4,5			2,025	1,35	1,35		
		Difusión De Software Dañino	0,1	9	9	9			0,9	0,9	0,9		
		Acceso No Autorizado	0,1		6,75	9				0,675	0,9		
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	4,5					0,45				
		Divulgación De Información	0,1			9					0,9		

Figura 105. Riesgo potencial de las amenazas del grupo Aplicaciones informáticas (a)
(Fuente propia)

SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	0,1	6					0,6				
		Errores De Usuarios	0,5	4	6	4			2	3	2		
		Errores De Administración	0,1	6	4	4			0,6	0,4	0,4		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	8					0,8				
		Fugas De Información	0,1			8					0,8		
		Vulnerabilidades De Los Programas	0,3	4	6	8			1,2	1,8	2,4		
		Errores De Mantenimiento/Actualización De Programas	0,3	4	6				1,2	1,8			
		Suplantación De La Identidad Del Usuario	0,1		6	8	6,75			0,6	0,8	0,675	
		Abuso De Privilegios De Acceso	0,3	4	6	8			1,2	1,8	2,4		
		Uso No Previsto	0,3	4	4	4			1,2	1,2	1,2		
		Difusión De Software Dañino	0,1	8	8	8			0,8	0,8	0,8		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	4					0,4				
		Divulgación De Información	0,1			8					0,8		
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	0,1	5,25					0,525				
		Errores De Usuarios	0,5	3,5	6	4			1,75	3	2		
		Errores De Administración	0,1	5,25	4	4			0,525	0,4	0,4		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	7					0,7				
		Fugas De Información	0,1			8					0,8		
		Vulnerabilidades De Los Programas	0,3	3,5	6	8			1,05	1,8	2,4		
		Errores De Mantenimiento/Actualización De Programas	0,3	3,5	6				1,05	1,8			
		Suplantación De La Identidad Del Usuario	0,1		6	8	6,75			0,6	0,8	0,675	
		Abuso De Privilegios De Acceso	0,3	3,5	6	8			1,05	1,8	2,4		
		Uso No Previsto	0,3	3,5	4	4			1,05	1,2	1,2		
		Difusión De Software Dañino	0,1	7	8	8			0,7	0,8	0,8		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	3,5					0,35				
		Divulgación De Información	0,1			8					0,8		
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	0,1	5,25					0,525				
		Errores De Usuarios	0,5	3,5	6	4			1,75	3	2		
		Errores De Administración	0,1	5,25	4	4			0,525	0,4	0,4		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	7					0,7				
		Fugas De Información	0,1			8					0,8		
		Vulnerabilidades De Los Programas	0,3	3,5	6	8			1,05	1,8	2,4		
		Errores De Mantenimiento/Actualización De Programas	0,3	3,5	6				1,05	1,8			
		Suplantación De La Identidad Del Usuario	0,1		6	8	6,75			0,6	0,8	0,675	
		Abuso De Privilegios De Acceso	0,3	3,5	6	8			1,05	1,8	2,4		
		Uso No Previsto	0,3	3,5	4	4			1,05	1,2	1,2		
		Difusión De Software Dañino	0,1	7	8	8			0,7	0,8	0,8		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Modificación Deliberada De La Información	0,1		8					0,8			
		Destrucción De Información	0,1	3,5					0,35				
		Divulgación De Información	0,1			8					0,8		
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	0,1	6					0,6				
		Errores De Administración	0,1	6	6,75	4,5			0,6	0,675	0,45		
		Alteración Accidental De La Información	0,3		9					2,7			
		Destrucción De Información	0,1	8					0,8				
		Fugas De Información	0,1			9					0,9		
		Vulnerabilidades De Los Programas	0,3	4	6,75	9			1,2	2,025	2,7		
		Errores De Mantenimiento/Actualización De Programas	0,3	4	9				1,2	2,7			
		Suplantación De La Identidad Del Usuario	0,1		9	9	9			0,9	0,9	0,9	
		Abuso De Privilegios De Acceso	0,3	6	9	9			1,8	2,7	2,7		
		Uso No Previsto	0,3	6	6,75	9			1,8	2,025	2,7		
		Difusión De Software Dañino	0,1	8	9	9			0,8	0,9	0,9		
		Acceso No Autorizado	0,1		9	9				0,9	0,9		
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,1			9					0,9		
SW6	Aplicación de Página web	Fallo De Origen Lógico	0,1	5,25					0,525				
		Errores De Usuarios	0,5	1,75	2	2			0,875	1	1		
		Errores De Administración	0,1	5,25	4	6			0,525	0,4	0,6		
		Alteración Accidental De La Información	0,3		6					1,8			
		Destrucción De Información	0,1	5,25					0,525				
		Fugas De Información	0,1			4					0,4		
		Vulnerabilidades De Los Programas	0,3	5,25	6	6			1,575	1,8	1,8		
		Errores De Mantenimiento/Actualización De Programas	0,3	3,5	6				1,05	1,8			
		Suplantación De La Identidad Del Usuario	0,1		4	8	9			0,4	0,8	0,9	
		Abuso De Privilegios De Acceso	0,3	3,5	6	8			1,05	1,8	2,4		
		Uso No Previsto	0,5	3,5	4	8			1,75	2	4		
		Difusión De Software Dañino	0,1	3,5	4	8			0,35	0,4	0,8		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Modificación Deliberada De La Información	0,1		6					0,6			
		Destrucción De Información	0,1	3,5					0,35				
		Divulgación De Información	0,1			6					0,6		
		Manipulación De Programas	0,1	3,5	6	6			0,35	0,6	0,6		

Figura 106. Riesgo potencial de las amenazas del grupo Aplicaciones informáticas (b)
(Fuente propia)

SW7	Aplicación de Intranet	Fallo De Origen Lógico	0,1	6					0,6					
		Errores De Usuarios	0,5	4	6	4			2	3	2			
		Errores De Administración	0,1	6	4	4			0,6	0,4	0,4			
		Alteración Accidental De La Información	0,3		6					1,8				
		Destrucción De Información	0,1	8					0,8					
		Fugas De Información	0,1			8					0,8			
		Vulnerabilidades De Los Programas	0,3	4	6	8			1,2	1,8	2,4			
		Errores De Mantenimiento/Actualización De Programas	0,3	4	6				1,2	1,8				
		Suplantación De La Identidad Del Usuario	0,1		6	8	6,75			0,6	0,8	0,675		
		Abuso De Privilegios De Acceso	0,3	4	6	8			1,2	1,8	2,4			
		Uso No Previsto	0,3	4	4	4			1,2	1,2	1,2			
		Difusión De Software Dañino	0,1	8	8	8			0,8	0,8	0,8			
		Acceso No Autorizado	0,1		6	8				0,6	0,8			
		Modificación Deliberada De La Información	0,1		6					0,6				
		Destrucción De Información	0,1	4					0,4					
		Divulgación De Información	0,1			8					0,8			
SW8	Aplicación del Sistema de tickets de incidencias	Fallo De Origen Lógico	0,1	3					0,3					
		Errores De Usuarios	0,5	2	4,5	3			1	2,25	1,5			
		Errores De Administración	0,1	3	3	3			0,3	0,3	0,3			
		Alteración Accidental De La Información	0,3		4,5					1,35				
		Destrucción De Información	0,1	4					0,4					
		Fugas De Información	0,1			6					0,6			
		Vulnerabilidades De Los Programas	0,3	2	4,5	6			0,6	1,35	1,8			
		Errores De Mantenimiento/Actualización De Programas	0,3	2	4,5				0,6	1,35				
		Suplantación De La Identidad Del Usuario	0,1		4,5	6	6,75			0,45	0,6	0,675		
		Abuso De Privilegios De Acceso	0,3	2	4,5	6			0,6	1,35	1,8			
		Uso No Previsto	0,3	2	3	3			0,6	0,9	0,9			
		Difusión De Software Dañino	0,1	4	6	6			0,4	0,6	0,6			
		Acceso No Autorizado	0,1		4,5	6				0,45	0,6			
		Modificación Deliberada De La Información	0,1		6					0,6				
		Destrucción De Información	0,1	2					0,2					
		Divulgación De Información	0,1			6					0,6			
SW9	Aplicación de Correo electrónico Gmail	Errores De Usuarios	0,5	0,35	0,4	2			0,175	0,2	1			
		Errores De Administración	0,1	1,75	0,4	4			0,175	0,04	0,4			
		Difusión De Software Dañino	0,1	0,35	0,4	8			0,035	0,04	0,8			
		Alteración Accidental De La Información	0,3		0,4					0,12				
		Destrucción De Información	0,1	1,75					0,175					
		Fugas De Información	0,3			8					2,4			
		Vulnerabilidades De Los Programas	0,3	0,35	4	8			0,105	1,2	2,4			
		Errores De Mantenimiento/Actualización De Programas	0,1	1,75	4	6			0,175	0,4	0,6			
		Suplantación De La Identidad Del Usuario	0,1		4	8	9			0,4	0,8	0,9		
		Abuso De Privilegios De Acceso	0,1	0,35	6	6			0,035	0,6	0,6			
		Uso No Previsto	0,3	3,5	6	8			1,05	1,8	2,4			
		Difusión De Software Dañino	0,1	0,35	4	8			0,035	0,4	0,8			
		Acceso No Autorizado	0,1		4	8				0,4	0,8			
		Modificación Deliberada De La Información	0,1		8					0,8				
		Destrucción De Información	0,1	7					0,7					
		Divulgación De Información	0,1			8					0,8			
SW10	E-apsa	Fallo De Origen Lógico	0,1	6					0,6					
		Errores De Usuarios	0,5	0,4	0,4	1,75			0,2	0,2	0,875			
		Errores De Administración	0,1	4	4	5,25			0,4	0,4	0,525			
		Alteración Accidental De La Información	0,3		2					0,6				
		Destrucción De Información	0,3	0,4					0,12					
		Fugas De Información	0,1			1,75					0,175			
		Vulnerabilidades De Los Programas	0,3	0,4	2	3,5			0,12	0,6	1,05			
		Errores De Mantenimiento/Actualización De Programas	0,3	2	2				0,6	0,6				
		Suplantación De La Identidad Del Usuario	0,3		2	5,25	8			0,6	1,575	2,4		
		Abuso De Privilegios De Acceso	0,3	0,4	2	5,25			0,12	0,6	1,575			
		Uso No Previsto	0,1	2	0,4	3,5			0,2	0,04	0,35			
		Difusión De Software Dañino	0,1	0,4	2	3,5			0,04	0,2	0,35			
		Acceso No Autorizado	0,1		2	7				0,2	0,7			
		Modificación Deliberada De La Información	0,1		2					0,2				
		Destrucción De Información	0,1	6					0,6					
		Divulgación De Información	0,1			5,25					0,525			
SW11	Aplicaciones en móviles	Fallo De Origen Lógico	0,1	2					0,2					
		Errores De Usuarios	0,5	0,2	2	3,5			0,1	1	1,75			
		Errores De Administración	0,1	1	2	3,5			0,1	0,2	0,35			
		Difusión De Software Dañino	0,3	0,2	2	5,25			0,06	0,6	1,575			
		Alteración Accidental De La Información	0,3		2					0,6				
		Destrucción De Información	0,3	1					0,3					
		Fugas De Información	0,3			5,25					1,575			
		Vulnerabilidades De Los Programas	0,3	1	2	5,25			0,3	0,6	1,575			
		Errores De Mantenimiento/Actualización De Programas	0,5	2	2				1	1				
		Suplantación De La Identidad Del Usuario	0,3		2	5,25	6			0,6	1,575	1,8		
		Abuso De Privilegios De Acceso	0,3	1	6	5,25			0,3	1,8	1,575			
		Uso No Previsto	0,1	3	4	5,25			0,3	0,4	0,525			
		Difusión De Software Dañino	0,1	3	4	7			0,3	0,4	0,7			
		Acceso No Autorizado	0,1		2	7				0,2	0,7			
		Modificación Deliberada De La Información	0,1		2					0,2				
		Destrucción De Información	0,1	2					0,2					
		Divulgación De Información	0,1			7					0,7			

Figura 107. Riesgo potencial de las amenazas del grupo Aplicaciones informáticas (c) (Fuente propia)

SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	0,1	6,75					0,675					
		Errores De Administración	0,1	9	6,75	9			0,9	0,675	0,9			
		Alteración Accidental De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	9					0,9					
		Vulnerabilidades De Los Programas	0,1	6,75	6,75	9			0,675	0,675	0,9			
		Errores De Mantenimiento/Actualización De Programas	0,3	6,75	6,75				2,025	2,025				
		Suplantación De La Identidad Del Usuario	0,3		6,75	9	9			2,025	2,7	2,7		
		Abuso De Privilegios De Acceso	0,3	4,5	6,75	9			1,35	2,025	2,7			
		Uso No Previsto	0,1	4,5	6,75	9			0,45	0,675	0,9			
		Difusión De Software Dañino	0,1	9	9	9			0,9	0,9	0,9			
		Acceso No Autorizado	0,1		9	9				0,9	0,9			
		Modificación Deliberada De La Información	0,1		9					0,9				
		Destrucción De Información	0,1	9					0,9					
		Divulgación De Información	0,1			9					0,9			
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	0,1	6,75					0,675					
		Errores De Administración	0,1	9	6,75	9			0,9	0,675	0,9			
		Alteración Accidental De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	9					0,9					
		Vulnerabilidades De Los Programas	0,1	6,75	6,75	9			0,675	0,675	0,9			
		Errores De Mantenimiento/Actualización De Programas	0,3	6,75	6,75				2,025	2,025				
		Suplantación De La Identidad Del Usuario	0,3		6,75	9	9			2,025	2,7	2,7		
		Abuso De Privilegios De Acceso	0,3	4,5	6,75	9			1,35	2,025	2,7			
		Uso No Previsto	0,1	4,5	6,75	9			0,45	0,675	0,9			
		Difusión De Software Dañino	0,1	9	9	9			0,9	0,9	0,9			
		Acceso No Autorizado	0,1		9	9				0,9	0,9			
		Modificación Deliberada De La Información	0,1		9					0,9				
		Destrucción De Información	0,1	9					0,9					
		Divulgación De Información	0,1			9					0,9			
SW14	Sistema operativo Windows 7	Fallo De Origen Lógico	0,1	4					0,4					
		Errores De Usuarios	0,5	1	0,45	1,25			0,5	0,225	0,625			
		Errores De Administración	0,1	2	2,25	2,5			0,2	0,225	0,25			
		Difusión De Software Dañino	0,1	3	4,5	3,75			0,3	0,45	0,375			
		Alteración Accidental De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	4					0,4					
		Vulnerabilidades De Los Programas	0,3	1	2,25	5			0,3	0,675	1,5			
		Errores De Mantenimiento/Actualización De Programas	0,3	1	2,25				0,3	0,675				
		Suplantación De La Identidad Del Usuario	0,3		0,45	5	8			0,135	1,5	2,4		
		Abuso De Privilegios De Acceso	0,3	0,2	0,45	3,75			0,06	0,135	1,125			
		Uso No Previsto	0,3	1	2,25	5			0,3	0,675	1,5			
		Difusión De Software Dañino	0,1	3	6,75	5			0,3	0,675	0,5			
		Acceso No Autorizado	0,3		2,25	5				0,675	1,5			
		Modificación Deliberada De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	4					0,4					
		Divulgación De Información	0,1			5					0,5			
SW15	Sistema operativo Windows 10	Fallo De Origen Lógico	0,1	4					0,4					
		Errores De Usuarios	0,5	1	0,45	1,25			0,5	0,225	0,625			
		Errores De Administración	0,1	2	2,25	2,5			0,2	0,225	0,25			
		Difusión De Software Dañino	0,1	3	4,5	3,75			0,3	0,45	0,375			
		Alteración Accidental De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	4					0,4					
		Vulnerabilidades De Los Programas	0,3	1	2,25	5			0,3	0,675	1,5			
		Errores De Mantenimiento/Actualización De Programas	0,3	1	2,25				0,3	0,675				
		Suplantación De La Identidad Del Usuario	0,3		0,45	5	8			0,135	1,5	2,4		
		Abuso De Privilegios De Acceso	0,3	0,2	0,45	3,75			0,06	0,135	1,125			
		Uso No Previsto	0,3	1	2,25	5			0,3	0,675	1,5			
		Difusión De Software Dañino	0,1	3	6,75	5			0,3	0,675	0,5			
		Acceso No Autorizado	0,3		2,25	5				0,675	1,5			
		Modificación Deliberada De La Información	0,1		6,75					0,675				
		Destrucción De Información	0,1	4					0,4					
		Divulgación De Información	0,1			5					0,5			
SW16	Navegadores Web	Errores De Usuarios	0,5	0,2	0,4	6			0,1	0,2	3			
		Errores De Administración	0,1	1	0,4	6			0,1	0,04	0,6			
		Fugas De Información	0,1			8					0,8			
		Vulnerabilidades De Los Programas	0,1	1	4	8			0,1	0,4	0,8			
		Errores De Mantenimiento/Actualización De Programas	0,3	0,2	4				0,06	1,2				
		Abuso De Privilegios De Acceso	0,3	0,2	0,4	6			0,06	0,12	1,8			
		Uso No Previsto	0,3	0,2	2	6			0,06	0,6	1,8			
		Difusión De Software Dañino	0,5	0,2	2	8			0,1	1	4			
		Modificación Deliberada De La Información	0,1		2					0,2				
		Destrucción De Información	0,1	1					0,1					
		Divulgación De Información	0,1			2					0,2			
SW17	Antivirus	Fallo De Origen Lógico	0,1	6					0,6					
		Errores De Administración	0,1	4	2	1,25			0,4	0,2	0,125			
		Errores De Mantenimiento/Actualización De Programas	0,3	2	8				0,6	2,4				
		Abuso De Privilegios De Acceso	0,1	4	8	1,25			0,4	0,8	0,125			
		Uso No Previsto	0,1	4	8	1,25			0,4	0,8	0,125			
		Acceso No Autorizado	0,1		8	1,25				0,8	0,125			
		Modificación Deliberada De La Información	0,1		8					0,8				
SW18	Software Ofimático	Fallo De Origen Lógico	0,3	1,5					0,45					
		Errores De Usuarios	0,5	1,5	0,25	1,25			0,75	0,125	0,625			
		Errores De Administración	0,1	1,5	0,25	1,25			0,15	0,025	0,125			
		Errores De Mantenimiento/Actualización De Programas	0,3	2,25	1,25				0,675	0,375				
		Abuso De Privilegios De Acceso	0,1	0,75	1,25	1,25			0,075	0,125	0,125			
		Uso No Previsto	0,1	1,5	1,25	1,25			0,15	0,125	0,125			

Figura 108. Riesgo potencial de las amenazas del grupo Aplicaciones informáticas (d) (Fuente propia)

- [HW] Equipos Informáticos (Hardware)

El riesgo potencial en los equipos informáticos varía entre el valor mínimo de 0.02 y el valor máximo de 6,3. En este grupo de activos se observan 3 valores mayores a 4, debido a que las amenazas tienen alta la frecuencia de ocurrencia. Los valores altos de riesgo se observan en las dimensiones de integridad y confidencialidad en los servidores APSA y servidores sedes, debido a las amenazas de acceso no autorizado y uso no previsto respectivamente. El riesgo en todos los activos es muy variante, pero se observa que los valores menores se presentan en los activos teléfonos de sobremesa y especialmente en las impresoras de oficinas en las dimensiones de integridad y confidencialidad. Todos los valores del riesgo calculados se observan en las Figuras 109 a la 111.

EQUIPOS INFORMÁTICOS [HW]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
HW1	Servidores APSA	Avería De Origen Físico/Lógico	0,3	9					2,7				
		Errores De Administración	0,1	9	9	9			0,9	0,9	0,9		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6,75					2,025				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	9					0,9				
		Abuso De Privilegios De Acceso	0,1	6,75	6,75	9			0,675	0,675	0,9		
		Uso No Previsto	0,3	6,75	6,75	9			2,025	2,025	2,7		
		Acceso No Autorizado	0,7		6,75	9				4,725	6,3		
		Denegación De Servicio	0,3	9					2,7				
HW2	Servidores Sedes	Daños Por Agua	0,1	8					0,8				
		Avería De Origen Físico/Lógico	0,3	8					2,4				
		Corte De Suministro Eléctrico	0,3	8					2,4				
		Fallas De Climatización	0,1	2					0,2				
		Errores De Administración	0,1	6	6	9			0,6	0,6	0,9		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Abuso De Privilegios De Acceso	0,3	6	6	9			1,8	1,8	2,7		
		Uso No Previsto	0,3	4	4	9			1,2	1,2	2,7		
		Acceso No Autorizado	0,5		6	9				3	4,5		
		Manipulación De Equipos	0,3	6		6,75			1,8		2,025		
		Denegación De Servicio	0,3	8					2,4				
		Robo	0,1	8		6,75			0,8		0,675		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	0,1	5,25					0,525				
		Avería De Origen Físico/Lógico	0,3	7					2,1				
		Corte De Suministro Eléctrico	0,3	7					2,1				
		Errores De Administración	0,1	3,5	4	6			0,35	0,4	0,6		
		Errores De Mantenimiento/Actualización De Equipos	0,5	3,5					1,75				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	5,25					1,575				
		Perdida De Equipos	0,1	7		8			0,7		0,8		
		Abuso De Privilegios De Acceso	0,1	3,5	4	8			0,35	0,4	0,8		
		Uso No Previsto	0,3	5,25	2	8			1,575	0,6	2,4		
		Acceso No Autorizado	0,1		2	8				0,2	0,8		
		Manipulación De Equipos	0,3	3,5		8			1,05		2,4		
		Robo	0,1	7		8			0,7		0,8		
HW4	Ordenadores de escritorio empleados	Daños Por Agua	0,1	2,25					0,225				
		Avería De Origen Físico/Lógico	0,5	3					1,5				
		Corte De Suministro Eléctrico	0,3	3					0,9				
		Errores De Administración	0,3	1,5	3,5	5,25			0,45	1,05	1,575		
		Errores De Mantenimiento/Actualización De Equipos	0,5	1,5					0,75				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	2,25					0,675				
		Perdida De Equipos	0,1	3		5,25			0,3		0,525		
		Abuso De Privilegios De Acceso	0,5	1,5	3,5	5,25			0,75	1,75	2,625		
		Uso No Previsto	0,5	2,25	1,75	5,25			1,125	0,875	2,625		
		Acceso No Autorizado	0,3		1,75	5,25				0,525	1,575		
		Manipulación De Equipos	0,5	1,5		5,25			0,75		2,625		
		Robo	0,1	3		7			0,3		0,7		

Figura 109. Riesgo potencial de las amenazas del grupo Equipos informáticos (a) (Fuente propia)

HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	0,3	7					2,1				
		Corte De Suministro Eléctrico	0,1	1,75					0,175				
		Errores De Administración	0,3	3,5	2	8			1,05	0,6	2,4		
		Errores De Mantenimiento/Actualización De Equipos	0,5	3,5					1,75				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	5,25					1,575				
		Perdida De Equipos	0,1	7		8			0,7		0,8		
		Abuso De Privilegios De Acceso	0,3	1,75	2	8			0,525	0,6	2,4		
		Uso No Previsto	0,3	3,5	2	8			1,05	0,6	2,4		
		Acceso No Autorizado	0,1		6	8				0,6	0,8		
		Manipulación De Equipos	0,3	5,25		8			1,575		2,4		
		Robo	0,1	7		8			0,7		0,8		
HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	0,3	3					0,9				
		Corte De Suministro Eléctrico	0,1	0,75					0,075				
		Errores De Administración	0,3	1,5	1,75	1,75			0,45	0,525	0,525		
		Errores De Mantenimiento/Actualización De Equipos	0,5	1,5					0,75				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	2,25					0,675				
		Perdida De Equipos	0,1	3		5,25			0,3		0,525		
		Abuso De Privilegios De Acceso	0,3	0,75	1,75	5,25			0,225	0,525	1,575		
		Uso No Previsto	0,3	1,5	1,75	5,25			0,45	0,525	1,575		
		Acceso No Autorizado	0,3		3,5	5,25				1,05	1,575		
		Manipulación De Equipos	0,3	1,5		5,25			0,45		1,575		
		Robo	0,1	3		7			0,3		0,7		
HW7	Portátiles TIC	Daños Por Agua	0,1	8					0,8				
		Avería De Origen Físico/Lógico	0,1	8					0,8				
		Corte De Suministro Eléctrico	0,1	6					0,6				
		Errores De Administración	0,1	4	6,75	9			0,4	0,675	0,9		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Abuso De Privilegios De Acceso	0,1	4	6,75	9			0,4	0,675	0,9		
		Acceso No Autorizado	0,1		6,75	9				0,675	0,9		
		Manipulación De Equipos	0,1	4		9			0,4		0,9		
HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	0,3	3					0,9				
		Errores De Administración	0,1	1	1,75	3,5			0,1	0,175	0,35		
		Errores De Mantenimiento/Actualización De Equipos	0,5	3					1,5				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	2					0,6				
		Perdida De Equipos	0,5	4		7			2		3,5		
		Abuso De Privilegios De Acceso	0,3	2	3,5	7			0,6	1,05	2,1		
		Uso No Previsto	0,5	2	3,5	7			1	1,75	3,5		
		Acceso No Autorizado	0,1		5,25	7				0,525	0,7		
		Manipulación De Equipos	0,5	3		7			1,5		3,5		
		Robo	0,3	4		7			1,2		2,1		
HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	0,3	3					0,9				
		Corte De Suministro Eléctrico	0,1	3					0,3				
		Errores De Administración	0,1	1,5	1	0,15			0,15	0,1	0,015		
		Errores De Mantenimiento/Actualización De Equipos	0,3	1,5					0,45				
		Caída Del Sistema Por Agotamiento De Recursos	0,5	2,25					1,125				
		Perdida De Equipos	0,1	3		0,75			0,3		0,075		
		Abuso De Privilegios De Acceso	0,3	1,5	0,5	0,15			0,45	0,15	0,045		
		Uso No Previsto	0,3	0,75	0,5	0,75			0,225	0,15	0,225		
		Acceso No Autorizado	0,1		0,5	0,75				0,05	0,075		
		Manipulación De Equipos	0,3	1,5		0,75			0,45		0,225		
		Robo	0,1	3		0,75			0,3		0,075		
HW10	Router	Avería De Origen Físico/Lógico	0,1	8					0,8				
		Corte De Suministro Eléctrico	0,1	8					0,8				
		Fallas De Climatización	0,1	4					0,4				
		Errores De Administración	0,1	6	4	8			0,6	0,4	0,8		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Abuso De Privilegios De Acceso	0,1	6	4	8			0,6	0,4	0,8		
		Uso No Previsto	0,1	6	4	8			0,6	0,4	0,8		
		Acceso No Autorizado	0,3		6	8				1,8	2,4		
		Manipulación De Equipos	0,3	6		8			1,8		2,4		
		Denegación De Servicio	0,3	8					2,4				
HW11	Router inalámbrico	Daños Por Agua	0,1	8					0,8				
		Avería De Origen Físico/Lógico	0,1	6					0,6				
		Corte De Suministro Eléctrico	0,1	8					0,8				
		Errores De Administración	0,1	6	4	8			0,6	0,4	0,8		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Perdida De Equipos	0,1	8		4			0,8		0,4		
		Abuso De Privilegios De Acceso	0,3	4	4	6			1,2	1,2	1,8		
		Uso No Previsto	0,3	6	6	6			1,8	1,8	1,8		
		Acceso No Autorizado	0,3		6	8				1,8	2,4		
		Manipulación De Equipos	0,3	6		4			1,8		1,2		
		Denegación De Servicio	0,3	8					2,4				
		Robo	0,1	8		4			0,8		0,4		

Figura 110. Riesgo potencial de las amenazas del grupo Equipos informáticos (b)
(Fuente propia)

HW12	Switch	Avería De Origen Físico/Lógico	0,1	8					0,8				
		Corte De Suministro Eléctrico	0,1	8					0,8				
		Fallas De Climatización	0,1	4					0,4				
		Errores De Administración	0,1	6	4	8			0,6	0,4	0,8		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Abuso De Privilegios De Acceso	0,1	6	4	8			0,6	0,4	0,8		
		Uso No Previsto	0,1	6	4	8			0,6	0,4	0,8		
		Acceso No Autorizado	0,3		6	8				1,8	2,4		
		Manipulación De Equipos	0,3	6		8			1,8		2,4		
		Denegación De Servicio	0,3	8					2,4				
HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	0,3	8					2,4				
		Corte De Suministro Eléctrico	0,1	8					0,8				
		Errores De Administración	0,3	6	1,25	2			1,8	0,375	0,6		
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	8					2,4				
		Abuso De Privilegios De Acceso	0,3	4	2,5	1			1,2	0,75	0,3		
		Uso No Previsto	0,3	6	2,5	1			1,8	0,75	0,3		
		Acceso No Autorizado	0,1		2,5	1				0,25	0,1		
		Manipulación De Equipos	0,3	6		1			1,8		0,3		
HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	0,1	6					0,6				
		Corte De Suministro Eléctrico	0,1	6					0,6				
		Errores De Administración	0,1	3	1,25	2			0,3	0,125	0,2		
		Errores De Mantenimiento/Actualización De Equipos	0,3	4,5					1,35				
		Abuso De Privilegios De Acceso	0,3	3	1,25	3			0,9	0,375	0,9		
		Uso No Previsto	0,3	4,5	1,25	3			1,35	0,375	0,9		
		Acceso No Autorizado	0,1		2,5	3				0,25	0,3		
		Manipulación De Equipos	0,5	4,5		3			2,25		1,5		
		Robo	0,1	6		0,2			0,6		0,02		

Figura 111. Riesgo potencial de las amenazas del grupo Equipos informáticos (c)
(Fuente propia)

- [COM] Redes de Comunicaciones

El riesgo potencial en este grupo varía entre el valor mínimo de 0,04 y el valor máximo de 6,3. En este grupo de activos los valores más altos de riesgo se observan en las redes inalámbricas y locales en las dimensiones de confidencialidad y autenticidad, causadas por la suplantación de la identidad del usuario y el uso no previsto. El riesgo en todos los activos es muy variante, pero se puede observar que los valores menores de riesgo están en la red telefónica móvil y la red telefónica. Todos los valores calculados se observan en las Figuras 112 y 113.

REDES DE COMUNICACIONES [COM]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	0,3	7					2,1				
		Errores De Administración	0,1	5,25	2	6,75			0,525	0,2	0,675		
		Alteración Accidental De La Información	0,3		4					1,2			
		Caída Del Sistema Por Agotamiento De Recursos	0,3	7					2,1				
		Suplantación De La Identidad Del Usuario	0,7		4	9	9			2,8	6,3	6,3	
		Abuso De Privilegios De Acceso	0,3	3,5	4	6,75			1,05	1,2	2,025		
		Uso No Previsto	0,3	3,5	2	6,75			1,05	0,6	2,025		
		Acceso No Autorizado	0,5		4	9				2	4,5		
		Análisis De Trafico	0,1			9					0,9		
		Interceptación De Información (Escucha)	0,1			9					0,9		
		Modificación Deliberada De La Información	0,3		6					1,8			
		Divulgación De Información	0,5			6,75					3,375		
		Denegación De Servicio	0,5	7					3,5				
COM2	Redes locales	Fallo Servicios De Comunicaciones	0,3	8					2,4				
		Errores De Administración	0,1	6	4	9			0,6	0,4	0,9		
		Alteración Accidental De La Información	0,3		4					1,2			
		Caída Del Sistema Por Agotamiento De Recursos	0,3	8					2,4				
		Suplantación De La Identidad Del Usuario	0,5		6	9	9			3	4,5	4,5	
		Abuso De Privilegios De Acceso	0,3	4	6	9			1,2	1,8	2,7		
		Uso No Previsto	0,3	4	4	9			1,2	1,2	2,7		
		Acceso No Autorizado	0,5		4	9				2	4,5		
		Análisis De Trafico	0,1			9					0,9		
		Interceptación De Información (Escucha)	0,1			9					0,9		
		Modificación Deliberada De La Información	0,3		6					1,8			
		Divulgación De Información	0,5			6,75					3,375		
		Denegación De Servicio	0,5	8					4				

Figura 112. Riesgo potencial de las amenazas del grupo Redes de comunicaciones (a)
(Fuente propia)

COM3	Red telefónica	Fallo Servicios De Comunicaciones	0,3	8					2,4				
		Errores De Administración	0,1	6	3,5	6			0,6	0,35	0,6		
		Alteración Accidental De La Información	0,3		3,5					1,05			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	8					0,8				
		Abuso De Privilegios De Acceso	0,5	4	1,75	6			2	0,875	3		
		Uso No Previsto	0,5	4	1,75	6			2	0,875	3		
		Acceso No Autorizado	0,3		1,75	8				0,525	2,4		
		Análisis De Trafico	0,1			8					0,8		
		Interceptación De Información (Escucha)	0,1			8					0,8		
		Modificación Deliberada De La Información	0,1		3,5					0,35			
		Divulgación De Información	0,3			6					1,8		
		Denegación De Servicio	0,1	8					0,8				
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	0,3	8					2,4				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	6					0,6				
		Suplantación De La Identidad Del Usuario	0,1		0,35	6	5,25			0,035	0,6	0,525	
		Abuso De Privilegios De Acceso	0,3	0,4	0,35	4			0,12	0,105	1,2		
		Uso No Previsto	0,3	0,4	0,35	6			0,12	0,105	1,8		
		Acceso No Autorizado	0,3		0,35	6				0,105	1,8		
		Análisis De Trafico	0,1			8					0,8		
		Interceptación De Información (Escucha)	0,1			8					0,8		
		Divulgación De Información	0,3			8					2,4		

Figura 113. Riesgo potencial de las amenazas del grupo Redes de comunicaciones (b)
(Fuente propia)

- [MEDIA] Soportes de Información

Para este grupo de activos, el riesgo potencial varía entre el valor mínimo de 0,18 y el valor máximo de 6,3. Los soportes de información presentan los valores más altos de riesgo de entre todos los grupos de activos. Los valores altos se presentan en los activos: pendrives USB, CD/DVD y material impreso a causa de las amenazas: errores de usuarios, alteración accidental de la información, pérdida de soporte y uso no previsto. El riesgo en todos los activos es muy variante, pero se puede observar que los valores menores de riesgo se encuentran en la dimensión de disponibilidad en CD/DVD a causa de errores de administración. Todos los valores calculados se observan en las Figuras 114 y 115.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	0,3	8					2,4				
		Daños Por Agua	0,3	8					2,4				
		Avería De Origen Físico/Lógico	0,1	6					0,6				
		Degradación De Los Soportes De Almacenamiento De La Información	0,1	6					0,6				
		Errores De Usuarios	0,3	2	6,75	9			0,6	2,025	2,7		
		Errores De Administración	0,1	2	6,75	9			0,2	0,675	0,9		
		Alteración Accidental De La Información	0,3		6,75					2,025			
		Destrucción De Información	0,1	8					0,8				
		Fugas De Información	0,1			9					0,9		
		Errores De Mantenimiento del soporte	0,3	2					0,6				
		Perdida del soporte	0,1	8		9			0,8		0,9		
		Uso No Previsto	0,3	8	9	9			2,4	2,7	2,7		
		Acceso No Autorizado	0,3		9	9				2,7	2,7		
		Modificación Deliberada De La Información	0,1		9					0,9			
		Destrucción De Información	0,1	8					0,8				
		Divulgación De Información	0,1			9					0,9		
		Manipulación del soporte	0,3	4		9			1,2		2,7		
		Robo	0,1	8		9			0,8		0,9		

Figura 114. Riesgo potencial de las amenazas del grupo Soportes de información (a)
(Fuente propia)

MEDIA2	Pendrives USB	Daños Por Agua	0,1	7					0,7					
		Daños Por Agua	0,3	7					2,1					
		Avería De Origen Físico/Lógico	0,1	5,25					0,525					
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	5,25					1,575					
		Errores De Usuarios	0,5	1,75	4	9			0,875	2	4,5			
		Errores De Administración	0,1	1,75	4	9			0,175	0,4	0,9			
		Alteración Accidental De La Información	0,5		8					4				
		Destrucción De Información	0,5	7					3,5					
		Fugas De Información	0,3			9					2,7			
		Errores De Mantenimiento del soporte	0,1	3,5					0,35					
		Perdida del soporte	0,7	7		9			4,9		6,3			
		Uso No Previsto	0,7	5,25	8	9			3,675	5,6	6,3			
		Acceso No Autorizado	0,1		8	9				0,8	0,9			
		Modificación Deliberada De La Información	0,1		8					0,8				
		Destrucción De Información	0,1	7					0,7					
		Divulgación De Información	0,3			9					2,7			
		Manipulación del soporte	0,1	5,25		9			0,525		0,9			
		Robo	0,3	7		9			2,1		2,7			
MEDIA3	CD/DVD	Daños Por Agua	0,1	7					0,7					
		Daños Por Agua	0,3	7					2,1					
		Avería De Origen Físico/Lógico	0,1	5,25					0,525					
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	5,25					1,575					
		Errores De Usuarios	0,5	1,75	4	9			0,875	2	4,5			
		Errores De Administración	0,1	1,75	4	9			0,175	0,4	0,9			
		Alteración Accidental De La Información	0,5		8					4				
		Destrucción De Información	0,5	7					3,5					
		Fugas De Información	0,3			9					2,7			
		Errores De Mantenimiento del soporte	0,1	3,5					0,35					
		Perdida del soporte	0,7	7		9			4,9		6,3			
		Uso No Previsto	0,7	5,25	8	9			3,675	5,6	6,3			
		Acceso No Autorizado	0,1		8	9				0,8	0,9			
		Modificación Deliberada De La Información	0,1		8					0,8				
		Destrucción De Información	0,1	7					0,7					
		Divulgación De Información	0,3			9					2,7			
		Manipulación del soporte	0,1	5,25		9			0,525		0,9			
		Robo	0,3	7		9			2,1		2,7			
MEDIA4	Material impreso	Daños Por Agua	0,1	7					0,7					
		Daños Por Agua	0,1	7					0,7					
		Degradación por Almacenamiento	0,3	5,25					1,575					
		Errores De Usuarios	0,5	3,5	6	6,75			1,75	3	3,375			
		Errores De Administración	0,1	3,5	6	6,75			0,35	0,6	0,675			
		Alteración Accidental De La Información	0,5		4					2				
		Destrucción	0,5	7					3,5					
		Fugas De Información	0,1			9					0,9			
		Errores De Almacenamiento	0,5	3,5					1,75					
		Perdida	0,5	3,5		9			1,75		4,5			
		Uso No Previsto	0,3	7	6	9			2,1	1,8	2,7			
		Acceso No Autorizado	0,3		6	9				1,8	2,7			
		Modificación Deliberada De La Información	0,1		8					0,8				
		Destrucción	0,1	7					0,7					
		Divulgación	0,1			9					0,9			
		Manipulación	0,1	3,5		9			0,35		0,9			
		Robo	0,3	3,5		9			1,05		2,7			

Figura 115. Riesgo potencial de las amenazas del grupo Soportes de información (b) (Fuente propia)

- [AUX] Equipamiento Auxiliar

El riesgo potencial del equipamiento auxiliar varía entre el valor mínimo de 0,02 y el valor máximo de 4,5. En este grupo de activos no se observa valores altos de riesgo, excepto en la dimensión de confidencialidad del activo cajas fuertes causadas por la amenaza de manipulación de equipos. Los valores de riesgo en este tipo de activos con considerablemente menores debido a que el impacto potencial de las amenazas es bajo. Todos los valores calculados se observan en la Figura 116.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenaza	F	D	I	C	A	T	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	0,3	3,75					1,125				
		Fuego	0,1	3,75					0,375				
		Daños Por Agua	0,3	3,75					1,125				
		Contaminación Mecánica	0,1	2,5					0,25				
		Degradación por almacenamiento	0,3	2,5					0,75				
		Avería De Origen Físico/ Lógico	0,3	3,75					1,125				
		Errores De Mantenimiento/ Actualización De Equipos	0,1	3,75					0,375				
		Uso No Previsto	0,3	3,75	1,25	0,15			1,125	0,375	0,045		
		Acceso No Autorizado	0,3		1,25	0,15				0,375	0,045		
		Manipulación De Equipos	0,3	3,75		0,15			1,125		0,045		
AUX2	Fuentes de alimentación	Daños Por Agua	0,3	3,75					1,125				
		Fuego	0,1	3,75					0,375				
		Daños Por Agua	0,3	3,75					1,125				
		Contaminación Mecánica	0,1	2,5					0,25				
		Degradación por almacenamiento	0,3	2,5					0,75				
		Avería De Origen Físico/ Lógico	0,3	3,75					1,125				
		Corte De Suministro Eléctrico	0,3	5					1,5				
		Errores De Mantenimiento/ Actualización De Equipos	0,3	3,75					1,125				
		Perdida De Equipos	0,1	5		0,15			0,5		0,015		
		Uso No Previsto	0,3	5	1,75	0,15			1,5	0,525	0,045		
		Acceso No Autorizado	0,3		1,75	0,15				0,525	0,045		
		Manipulación De Equipos	0,3	3,75		0,15			1,125		0,045		
		Robo	0,1	5		0,15			0,5		0,015		
AUX3	Climatización	Daños Por Agua	0,3	3,75					1,125				
		Fuego	0,1	3,75					0,375				
		Daños Por Agua	0,3	3,75					1,125				
		Contaminación Mecánica	0,1	2,5					0,25				
		Avería De Origen Físico/Lógico	0,3	3,75					1,125				
		Corte De Suministro Eléctrico	0,3	5					1,5				
		Errores De Mantenimiento/Actualización De Equipos	0,3	3,75					1,125				
		Uso No Previsto	0,3	2,5	1	0,15			0,75	0,3	0,045		
		Acceso No Autorizado	0,3		1	0,15				0,3	0,045		
		Manipulación De Equipos	0,5	2,5		0,15			1,25		0,075		
AUX4	Cableado UTP	Daños Por Agua	0,3	5,25					1,575				
		Fuego	0,1	7					0,7				
		Daños Por Agua	0,3	5,25					1,575				
		Avería De Origen Físico/Lógico	0,3	5,25					1,575				
		Errores De Mantenimiento/Actualización De Equipos	0,3	5,25					1,575				
		Uso No Previsto	0,3	3,5	2	1			1,05	0,6	0,3		
		Acceso No Autorizado	0,1		2	3				0,2	0,3		
		Manipulación De Equipos	0,1	3,5		3			0,35		0,3		
AUX5	Armarios	Daños Por Agua	0,3	4					1,2				
		Fuego	0,1	6					0,6				
		Daños Por Agua	0,3	4					1,2				
		Degradación por almacenamiento	0,1	2					0,2				
		Avería De Origen Físico/Lógico	0,3	4					1,2				
		Uso No Previsto	0,3	2	2	6			0,6	0,6	1,8		
		Acceso No Autorizado	0,3		2	6				0,6	1,8		
		Manipulación De Equipos	0,5	2		6			1		3		
AUX6	Cajas fuertes	Daños Por Agua	0,1	2					0,2				
		Fuego	0,1	2					0,2				
		Daños Por Agua	0,1	2					0,2				
		Avería De Origen Físico/Lógico	0,1	6					0,6				
		Corte De Suministro Eléctrico	0,1	6					0,6				
		Errores De Mantenimiento/Actualización De Equipos	0,3	6					1,8				
		Perdida De Equipos	0,1	8		9			0,8		0,9		
		Uso No Previsto	0,1	6	0,4	9			0,6	0,04	0,9		
		Acceso No Autorizado	0,3		0,4	9				0,12	2,7		
		Manipulación De Equipos	0,5	2		9			1		4,5		

Figura 116. Riesgo potencial de las amenazas del grupo Equipamiento auxiliar (Fuente propia)

- [L]Instalaciones

El riesgo potencial en este grupo de activos varía entre el valor mínimo de 0,15 y el valor máximo de 2,4. En este grupo de activos no se observa valores altos de riesgo. Los valores más altos se presentan en la confidencialidad de edificios y cuartos de servidores a causa del acceso no autorizado, y la disponibilidad de los cuartos de servidores causados por daños por agua. El riesgo en este tipo de activos es considerablemente menor debido a que la frecuencia de ocurrencia es baja. El riesgo más bajo se observa en la disponibilidad a causa del uso no previsto en edificios. Todos los valores calculados se observan en la Figura 117.

ACTIVOS DE INSTALACIONES [L]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
L1	Edificios	Fuego	0,1	6					0,6				
		Daños Por Agua	0,3	4,5					1,35				
		Fuego	0,1	4,5					0,45				
		Daños Por Agua	0,3	3					0,9				
		Fugas De Información	0,3			6					1,8		
		Uso No Previsto	0,1	1,5	1,75	6			0,15	0,175	0,6		
		Acceso No Autorizado	0,3		1,75	8				0,525	2,4		
L2	Cuartos servidores	Fuego	0,1	8					0,8				
		Daños Por Agua	0,1	8					0,8				
		Fuego	0,1	8					0,8				
		Daños Por Agua	0,3	8					2,4				
		Fugas De Información	0,1			8					0,8		
		Uso No Previsto	0,3	6	6	6			1,8	1,8	1,8		
		Acceso No Autorizado	0,3		4	8				1,2	2,4		
L3	Coche	Daños mecánicos	0,1	2					0,2				
		Accidente de tránsito	0,1	2					0,2				

Figura 117. Riesgo potencial de las amenazas del grupo Instalaciones
(Fuente propia)

- [P] Personal

El riesgo potencial varía entre el valor mínimo de 0,125 y el valor máximo de 2,7. El riesgo en este tipo de activos es considerablemente menor debido a que la frecuencia de ocurrencia es baja. El mayor riesgo se produce por fugas de información de los usuarios que afectan a la confidencialidad. El menor riesgo se produce en la dimensión de integridad en todos los activos de este grupo. Todos los valores calculados se observan en la Figura 118.

ACTIVOS DE PERSONAL [P]			Frecuencia	Impacto					Riesgo				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T
P1	Administradores	Fugas De Información	0,1			9					0,9		
		Indisponibilidad Del Personal	0,3	6					1,8				
		Indisponibilidad Del Personal	0,1	6					0,6				
		Extorsión	0,1	2	6	9			0,2	0,6	0,9		
		Ingeniería Social	0,1	2	6	9			0,2	0,6	0,9		
P2	Técnicos	Fugas De Información	0,1			9					0,9		
		Indisponibilidad Del Personal	0,3	3,5					1,05				
		Indisponibilidad Del Personal	0,1	3,5					0,35				
		Extorsión	0,1	1,75	4	9			0,175	0,4	0,9		
		Ingeniería Social	0,1	1,75	4	9			0,175	0,4	0,9		
P3	Empleados	Fugas De Información	0,1			9					0,9		
		Indisponibilidad Del Personal	0,3	3,5					1,05				
		Indisponibilidad Del Personal	0,1	3,5					0,35				
		Extorsión	0,1	1,75	4	9			0,175	0,4	0,9		
		Ingeniería Social	0,1	1,75	4	9			0,175	0,4	0,9		
P4	Usuarios	Fugas De Información	0,3			9					2,7		
		Extorsión	0,1	1,25	3	9			0,125	0,3	0,9		
		Ingeniería Social	0,1	1,25	3	9			0,125	0,3	0,9		

Figura 118. Riesgo potencial de las amenazas del grupo Personal
(Fuente propia)

4.5. Impacto y Riesgo Residuales

4.5.1. Salvaguardas

Tratamiento del riesgo

Definidos los valores de riesgo de cada activo se procede al tratamiento de los resultados. Un riesgo puede ser crítico, grave, apreciable o asumible. Todos los riesgos se gestionan con salvaguardas, pero el enfoque de las salvaguardas está destinado primordialmente a aquellos riesgos críticos y graves. Los valores más altos en los riesgos serán los críticos y los de valores bajos serán los posiblemente asumibles. Por lo cual, se elaboró la escala de clasificación de riesgos de la Figura 119, medida en las mismas unidades que el valor de los activos. La escala posee valores entre 0 y 10, considerando a los valores mayores a 4 los graves y los que requieren inmediata atención. A pesar de determinar al 4 como valor base, existen activos sensibles para la organización en los que el valor base debe ser menor.

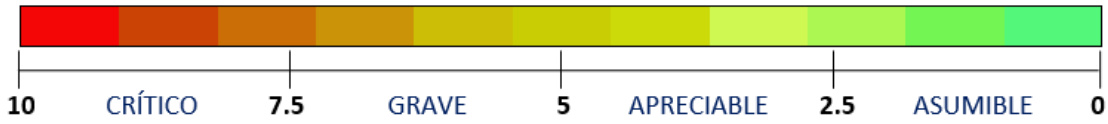

Figura 119. Escala de valoración del grado de impacto de una amenaza de APSA (Fuente propia)

Salvaguardas

Conociendo los niveles mínimos de riesgo aceptados para cada activo según la escala de valoración predefinida, se procede a establecer una lista de salvaguardas que procuran eliminar, mitigar o disminuir los riesgos en cada activo. A continuación, se observa el análisis del tratamiento del riesgo y la lista de salvaguardas definidas para todos los activos.

- [D] Datos /Información

Tratamiento del riesgo general de los Datos/Información: Si bien se definió que los valores de riesgo mayores a 4 son graves, para este grupo de activos esa condición va a cambiar. Al considerar a este grupo como el activo más importante de la asociación, se considera que los niveles de riesgo tienen que ser los mínimos posibles, por lo que las salvaguardas irán orientadas a mitigar los riesgos más altos y que no sobrepasen un riesgo del 0,1. En ciertas ocasiones las salvaguardas no cumplirán con esta condición, pero serán riesgos que se puedan asumir pues las amenazas no tienen efecto relevante para el activo y la asociación. Además, al tener relación

directa de dependencias con otros activos, los datos heredan las salvaguardas de dichos activos logrando mayor seguridad. Estas salvaguardas heredadas solo se describen de manera general pues están desarrolladas en su correspondiente activo.

A continuación se definen las salvaguardas de todos los activos del grupo Datos/Información y cuáles son los riesgos sobre los que actúan.

Salvaguardas D1, D2: 1) La seguridad de los equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los grupos de activos hardware (servidores, ordenadores o portátiles) y soportes de información (discos duros, pendrives, CD/DVD). 2) La seguridad de las aplicaciones que manejan los datos, hereda las salvaguardas definidas para el grupo de activos servicios y software. 3) Al ser datos de configuración y el código fuente de aplicaciones del software esencial de la asociación, es importante tener un respaldo mediante copias de seguridad verificadas y actualizadas periódicamente. 4) Para complementar la salvaguarda anterior, tanto el fichero original como las copias de seguridad requieren cifrado para brindar protección ante la manipulación y acceso no autorizado. 5) La última salvaguarda es un complemento de todas las anteriores. El registro de actualizaciones se usa para comprobar las modificaciones y acceso a los datos. Además, el registro puede contener instrucciones del correcto uso de los datos y debe estar protegido y legalizado.

Los errores de administración y configuración, y repudio y son mitigados por la 1ª, 2ª y 5ª salvaguarda. Para el resto de las amenazas, actúan todas las salvaguardas en especial la 3ª, 4ª y 5ª. La Figura 120 muestra las salvaguardas establecidas para los riesgos de los activos D1 y D2.

DATOS / INFORMACIÓN [D]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
D1	Datos de configuración	Errores De Administración	1,8	1,8	0,6			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos
		Errores De Configuración		1,2				
		Alteración Accidental De La Información		1,2				
		Destrucción De Información	2,4					
		Fugas De Información			0,4			
		Manipulación De Los Registros De Actividad		0,04			0,675	
		Manipulación De La Configuración		0,8	0,8	0,9		
		Abuso De Privilegios De Acceso	0,6	0,6	0,6			
		Acceso No Autorizado		0,6	0,8			
		Repudio		0,6			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,8					
D2	Código fuente de aplicaciones	Errores De Administración	1,2	2,025	0,6			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos
		Errores De Configuración		2,025				
		Alteración Accidental De La Información		0,9				
		Manipulación De Los Registros De Actividad		0,045			0,675	
		Manipulación De La Configuración		0,675	0,4	0,45		
		Abuso De Privilegios De Acceso	0,2	0,675	0,6			
		Acceso No Autorizado		0,9	0,8			
		Repudio		0,675			0,9	
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,8					

Figura 120. Salvaguardas de los activos D1 y D2
(Fuente propia)

Salvaguardas D3, D4, D5: 1) La seguridad de equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los grupos de activos hardware (servidores y ordenadores). 2) La seguridad de las aplicaciones que manejan los datos, hereda las salvaguardas definidas para el grupo de activos servicios y software que usan este tipo de ficheros. 3) El contenido de los ficheros puede ser confidencial, por lo que se requiere realizar copias de seguridad. 4) Para complementar la salvaguarda anterior, tanto el fichero original como las copias de seguridad se deben cifrar para brindar protección principalmente ante la manipulación y acceso no autorizado. 5) Se debe crear un manual de usuarios aprobado y legalizado para los usuarios, con los procedimientos para: almacenar, reconocer su grado de confidencialidad, realizar copias de seguridad y cifrar. 6) Es necesario realizar una depuración de ficheros para evitar que los dispositivos que los almacenan se queden sin recursos. Para el proceso de depuración se definirán normas para la eliminación de ficheros por fechas de caducidad, uso y contenido.

Los errores de administración, repudio y errores de configuración están mitigados por la 1ª, 2ª, 3ª y 6ª salvaguarda. Para el resto de las amenazas, actúan todas las salvaguardas especialmente la 3ª, 4ª, 5ª y 6ª. Las Figuras 121 y 122 muestran las salvaguardas establecidas para los riesgos de los activos D3, D4 y D5.

D3	**Ficheros almacenados en PC**	Errores De Usuarios	1,575	3,675	1,75			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad archivos confidenciales • Cifrado de la información • Manual de Usuarios • Depuración
		Errores De Administración	0,675	1,575	0,75			
		Errores De Configuración		0,525				
		Alteración Accidental De La Información		3,675				
		Destrucción De Información	1,5					
		Fugas De Información			0,125			
		Manipulación De Los Registros De Actividad		0,175			0,35	
		Manipulación De La Configuración		0,35	0,25	0,15		
		Suplantación De La Identidad Del Usuario		1,05	1,125	1,35		
		Abuso De Privilegios De Acceso	0,075	0,35	0,375			
		Acceso No Autorizado		1,575	1,5			
		Repudio		0,175			0,7	
		Modificación Deliberada De La Información		0,7				
		Destrucción De Información	0,225					
D4	**Ficheros almacenados en servidores en la nube**	Errores De Usuarios	1,75	2,45	0,245			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Usuarios • Depuración
		Errores De Administración	1,125	1,575	1,05			
		Errores De Monitorización Log		0,35			0,6	
		Errores De Configuración		1,05				
		Alteración Accidental De La Información		3,675				
		Destrucción De Información	1,125					
		Manipulación De Los Registros De Actividad		0,175			0,6	
		Manipulación De La Configuración		0,175	0,35	0,4		
		Suplantación De La Identidad Del Usuario		0,525	1,575	1,8		
		Abuso De Privilegios De Acceso	0,125	0,175	0,525			
		Acceso No Autorizado		0,35	0,7			
		Repudio		0,175			0,8	
		Modificación Deliberada De La Información		0,7				
		Destrucción De Información	0,5					

Figura 121. Salvaguardas de los activos D3 y D4
(Fuente propia)

D5	Ficheros almacenados en servidores locales	Errores De Usuarios	2,625	2,45	0,245			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Usuarios • Depuración
		Errores De Administración	1,125	1,575	1,05			
		Errores De Monitorización Log		0,35			0,6	
		Errores De Configuración		1,05				
		Alteración Accidental De La Información		2,625				
		Destrucción De Información	1,125					
		Manipulación De Los Registros De Actividad		0,175			0,6	
		Manipulación De La Configuración		0,175	0,35	0,4		
		Suplantación De La Identidad Del Usuario		0,525	1,575	1,8		
		Abuso De Privilegios De Acceso	0,125	0,175	0,525			
		Acceso No Autorizado		0,35	0,7			
		Repudio		0,175			0,8	
		Modificación Deliberada De La Información		0,7				
		Destrucción De Información	0,5					

Figura 122. Salvaguardas del activo D5
(Fuente propia)

Salvaguardas D6, D7: 1) La seguridad de equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los grupos de activos hardware y soportes de información. 2) La seguridad de las aplicaciones que manejan los datos, hereda las salvaguardas definidas para el grupo de activos servicios y software que usan las bases de datos. 3) Las bases de datos son esenciales para la asociación, por ello es importante tener un respaldo mediante copias de seguridad verificadas y actualizadas periódicamente. 4) Para complementar la salvaguarda anterior, todas las bases de datos y sus copias deben estar cifradas para dar protección principalmente ante la manipulación y acceso no autorizado. 5) Se debe crear un manual de administración aprobado y legalizado para: el manejo, modificación, actualización, copias de seguridad y cifrado. 6) Periódicamente hay que realizar un proceso de depuración para buscar errores dentro de las bases de datos y que no contengan información innecesaria. 7) La manipulación de las bases de datos es crítico, por lo que cualquier acción debe constar en el registro de incidencias y actualizaciones. 8) Las bases de datos se usan en distintas aplicaciones informáticas, por eso se debe tener un control periódico de los recursos para hacer las bases de datos eficientes. 9) La configuración de logs es una salvaguarda heredada de las aplicaciones que usan las bases de datos.

El repudio, la suplantación de identidad del usuario y los errores de administración, monitorización de logs y configuración están mitigados por la 1ª, 2ª, 5ª, 7ª y 9ª salvaguarda. Para el resto de las amenazas, actúan todas las salvaguardas especialmente la 3ª, 4ª, 5ª, 6ª y 8ª. La Figura 123 muestra las salvaguardas establecidas para los riesgos de los activos D6 y D7.

D6	Bases de datos en servidores locales	Errores De Administración	1,8	2,025	1,35			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Administración • Depuración • Registro de incidencias y actualizaciones • Control de recursos • Configuración de Logs
		Errores De Monitorización Log		0,675			0,675	
		Errores De Configuración		2,025				
		Alteración Accidental De La Información		3,375				
		Destrucción De Información	0,8					
		Manipulación De Los Registros De Actividad		0,45			0,9	
		Manipulación De La Configuración		0,45	0,675	0,45		
		Suplantación De La Identidad Del Usuario		0,45	0,9	0,675		
		Abuso De Privilegios De Acceso	0,6	0,45	0,675			
		Acceso No Autorizado		0,675	0,9			
		Repudio		0,45			0,9	
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,8					
D7	Bases de datos en servidores en la nube	Errores De Administración	2,025	2,025	1,35			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Administración • Depuración • Registro de incidencias y actualizaciones • Control de recursos • Configuración de Logs
		Errores De Monitorización Log		0,675			0,675	
		Errores De Configuración		2,025				
		Alteración Accidental De La Información		3,375				
		Destrucción De Información	0,9					
		Manipulación De Los Registros De Actividad		0,45			0,9	
		Manipulación De La Configuración		0,45	0,675	0,45		
		Suplantación De La Identidad Del Usuario		0,45	0,9	0,675		
		Abuso De Privilegios De Acceso	0,675	0,45	0,675			
		Acceso No Autorizado		0,675	0,9			
		Repudio		0,45			0,9	
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,9					

Figura 123. Salvaguardas de los activos D6 y D7
(Fuente propia)

Salvaguardas D8, D9, D10: 1) La seguridad de equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los activos hardware (servidores) y soportes de información. 2) La seguridad de las aplicaciones que manejan los datos, hereda las salvaguardas definidas para los activos servicios y software relacionadas con las copias de seguridad. 3) Dependiendo del contenido de las copias de seguridad se debe cifrar para su protección. 4) Se requiere establecer un proceso de depuración de las copias de seguridad controlando: el tiempo de almacenamiento, número de copias de seguridad y actualización. 5) Se debe crear un manual de administración aprobado y legalizado para realizar, cifrar, eliminar y actualizar las copias de seguridad. 6) Todas las copias de seguridad se debe registrar para tener un control sobre todo cuando se actualice una copia. 7) Juntamente con la depuración, es necesario un control de recursos para evitar la saturación de los dispositivos que almacenan las copias de seguridad. 8) Se recomienda realizar una comprobación de las copias de seguridad verificando si se realizaron completas y que en caso de requerirlas estas funcionen igual a los ficheros originales.

El repudio, la suplantación de identidad del usuario y los errores de administración, monitorización de logs y configuración están mitigados por la 1ª, 2ª, 4ª, 5ª y 8ª salvaguarda. Para el resto de las amenazas, actúan todas las salvaguardas especialmente la 3ª, 6ª y 7ª. La Figura 124 muestra las salvaguardas establecidas para los riesgos de los activos D8, D9 y D10.

D8	Copias de seguridad en la nube	Errores De Administración	0,675	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Configuración de Logs • Comprobación de efectividad de las copias de seguridad
		Errores De Monitorización Log		1,2			1,35	
		Errores De Configuración		2,4				
		Alteración Accidental De La Información		2,4				
		Destrucción De Información	0,9					
		Manipulación De Los Registros De Actividad		0,2			0,675	
		Manipulación De La Configuración		0,6	0,675	0,675		
		Suplantación De La Identidad Del Usuario		0,4	0,9	0,675		
		Abuso De Privilegios De Acceso	0,45	0,6	0,9			
		Acceso No Autorizado		0,6	0,9			
		Repudio		0,4			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,9					
		Divulgación De Información			0,9			
D9	Copias de Seguridad en servidores locales	Errores De Administración	0,6	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Configuración de Logs • Comprobación de efectividad de las copias de seguridad
		Errores De Monitorización Log		1,2			1,35	
		Errores De Configuración		2,4				
		Alteración Accidental De La Información		2,4				
		Destrucción De Información	0,8					
		Fugas De Información			0,675			
		Manipulación De La Configuración		0,6	0,675	0,675		
		Suplantación De La Identidad Del Usuario		0,4	0,9	0,675		
		Abuso De Privilegios De Acceso	0,4	0,6	0,9			
		Acceso No Autorizado		0,6	0,9			
		Repudio		0,4			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,8					
		Divulgación De Información			0,9			
D10	Copias de Seguridad en discos externos	Errores De Administración	0,525	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Comprobación de efectividad de las copias de seguridad
		Errores De Monitorización Log		1,2			1,35	
		Errores De Configuración		2,4				
		Alteración Accidental De La Información		2,4				
		Destrucción De Información	0,7					
		Manipulación De Los Registros De Actividad		0,2			0,675	
		Manipulación De La Configuración		0,6	0,675	0,675		
		Suplantación De La Identidad Del Usuario		0,4	0,9	0,675		
		Abuso De Privilegios De Acceso	0,35	0,6	0,9			
		Acceso No Autorizado		0,6	0,9			
		Repudio		0,4			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			0,9			

Figura 124. Salvaguardas de los activos D8, D9 y D10
(Fuente propia)

Salvaguardas D11, D13: 1) La seguridad de equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los grupos de activos hardware y soportes de información. 2) La seguridad de las aplicaciones que manejan o almacenan los datos, hereda las salvaguardas definidas para los grupos de activos servicios y software relacionados con estos ficheros. 3) Tanto los ficheros de contraseñas como los ficheros confidenciales compartidos requieren ser cifrados al igual que sus copias de seguridad. 4) Se debe establecer un proceso de depuración para que los ficheros de contraseñas y los ficheros compartidos contengan información actualizada de la asociación. 5) Al ser archivos confidenciales se requiere un control de acceso estricto a través de procesos de doble autenticación. 6) Los ficheros de contraseñas y los ficheros compartidos deben ser respaldados con copias de seguridad cifradas y proteger su acceso.

El repudio, la suplantación de identidad del usuario y los errores de administración, y configuración están mitigados por la 1ª, 2ª, 4ª y 5ª salvaguarda. Para el resto de las amenazas,

actúan todas las salvaguardas especialmente la 3ª, 4ª y 6ª. La Figura 125 muestra las salvaguardas establecidas para los riesgos de los activos D11 y D13.

D11	**Ficheros de contraseñas**	Errores De Administración	0,675	0,675	0,9			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Control de acceso • Copias de seguridad
		Errores De Configuración		0,045				
		Alteración Accidental De La Información		0,675				
		Destrucción De Información	0,9					
		Manipulación De Los Registros De Actividad		0,225			0,9	
		Suplantación De La Identidad Del Usuario		0,45	0,9	0,45		
		Abuso De Privilegios De Acceso	0,225	0,45	0,675			
		Acceso No Autorizado		0,675	0,9			
		Repudio		0,225			0,9	
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,9					
		Divulgación De Información			0,9			
D13	**Ficheros compartidos Google Drive**	Errores De Administración	1,575	1,2	1,2			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Depuración • Actualización permanente control de accesos • Cifrado de información confidencial
		Errores De Configuración		0,2				
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	1,575					
		Manipulación De La Configuración		0,4	0,4	0,35		
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,35		
		Abuso De Privilegios De Acceso	0,35	0,4	0,4			
		Acceso No Autorizado		0,6	0,8			
		Repudio		0,2			0,7	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			0,8			

Figura 125. Salvaguardas de los activos D11 y D13
(Fuente propia)

Salvaguardas D12: 1) La seguridad de equipos/dispositivos que los alojan, hereda las salvaguardas definidas para los grupos de activos hardware (servidores). 2) Hereda las salvaguardas para la seguridad de las aplicaciones que controlan los registros de actividades de los servidores. 3) Por ser los servidores parte importante de la asociación, cualquier evento relevante sobre ellos se debe notificar inmediatamente a los administradores informáticos, por lo que es conveniente convertirlo en un sistema activo que notifique a través de alarmas o correos electrónicos todas las incidencias. 4) Los logs deben almacenarse por algún tiempo, por lo que se recomienda un uso controlado de los recursos de memoria para tener siempre espacio de almacenamiento.

Todas las salvaguardas ayudan a enfrentar todas las amenazas pero la 3ª salvaguarda es la más importante. La Figura 126 muestra las salvaguardas establecidas para los riesgos del activo D12.

D12	**Registros de actividades en servidores**	Errores De Administración	1,8	1,2	1,2			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Convertirlo en sistema activo • Depuración
		Errores De Configuración		1,8				
		Destrucción De Información	1,8					
		Manipulación De La Configuración		0,6	0,4	0,675		
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,45		
		Abuso De Privilegios De Acceso	0,6	0,4	0,4			
		Acceso No Autorizado		0,6	0,8			
		Repudio		1,2			2,7	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,8					

Figura 126. Salvaguardas del activo D12
(Fuente propia)

- [S] Servicios

Tratamiento del riesgo general de los Servicios: Si bien se estableció que los valores de riesgo mayores a 4 son graves, para este grupo de activos esa condición va a cambiar. Al considerar que de estos servicios depende el funcionamiento de la asociación, se considera que los niveles de riesgo tienen que ser los mínimos posibles, por lo que las salvaguardas irán orientadas a mitigar los riesgos más altos y que no sobrepasen un riesgo del 0,5. Al tener relación directa de dependencias con otros activos, los servicios heredan las salvaguardas de dichos activos logrando mayor seguridad. Estas salvaguardas heredadas solo se describen de manera general pues están desarrolladas en su correspondiente activo. A continuación, se definen las salvaguardas para este grupo y cuáles son los riesgos sobre los que actúan.

Salvaguardas S1: 1) Este servicio hereda directamente la seguridad de la aplicación de la Página web. 2) Establecer un proceso formalizado y periódico de cambios y mejoras para brindar mejores y actualizados servicios a los usuarios externos de la asociación. 3) Por ser un servicio que está expuesto al exterior, debe tener un proceso de registros de incidencias para tomar las medidas de seguridad correspondientes. 4) Una empresa externa a APSA maneja la aplicación de la página web, que repercute directamente sobre este servicio, por lo que es necesario pedir informes periódicos de las medidas de seguridad que se implementan. A esto se le puede añadir que los informes cada cierto tiempo sean presenciales. 5) Esta aplicación estará almacenada en un servidor que por seguridad debe estar configurado logs de incidencias, y así complementar las acciones de la 3ª salvaguarda.

Los riesgos graves son la suplantación de identidad del usuario y acceso no autorizado que se mitigan con la 1ª, 2ª y 3ª salvaguarda. Para el resto de las amenazas se establecieron todas las salvaguardas listadas anteriormente. Aun así, la mayor parte de la seguridad depende de la aplicación web. La Figura 127 muestra las salvaguardas para los riesgos del activo S1.

SERVICIOS [S]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
S1	Página web	Errores De Usuarios	0,175	0,2	1			• Seguridad en la aplicación • Gestión de cambios y mejoras • Registros de incidencias • Pedir informes de actividades • Logs de incidencias
		Errores De Administración	0,7	0,6	0,6			
		Alteración Accidental De La Información		0,6				
		Fugas De Información			0,4			
		Caída Del Sistema Por Agotamiento De Recursos	2,1					
		Suplantación De La Identidad Del Usuario		4,2	4,2	3,5		
		Abuso De Privilegios De Acceso	1,05	1,8	1,8			
		Uso No Previsto	1,05	1,8	1,8			
		Acceso No Autorizado		4	3			
		Repudio		0,4			0,525	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,525					
		Divulgación De Información			2,4			
		Denegación De Servicio	2,1					

Figura 127. Salvaguardas del activo S1
(Fuente propia)

Salvaguardas S2, S3, S4, S5, S6: 1) La seguridad que heredan estos activos corresponde a las aplicaciones de correo electrónico, intranet documental, sistema de tickets de Incidencias, educación virtual y servicio financiero. 2) Estos servicios pueden ser víctimas de errores y amenazas que se deben exponer en un registro de incidencias, para realizar un análisis posterior y mejorar las medidas de seguridad. 3) Este grupo de activos, son gestionados por los administradores TIC y usados por los empleados de la asociación, por lo que es necesario crear manuales para evitar errores y usarse como referencia para los nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 4) Las salvaguardas que heredan estas aplicaciones corresponden a la configuración Logs de incidencias. 5) Habitualmente, los servicios deben pasar por un proceso de gestión de mejoras para actualizar y mejorar su funcionalidad considerando la seguridad informática.

En este grupo de activos los riesgos graves son a causa del acceso no autorizado, destrucción de información, errores de usuarios y alteración accidental de la información, y se mitigan con la seguridad de las aplicaciones de los servicios. Para los errores de usuarios y administración, repudio y, para detectar amenazas se crearon las demás salvaguardas. Las Figuras 128 y 129 muestran las salvaguardas para los riesgos de los activos S2, S3, S4, S5 y S6.

S2	**Correo electrónico**	Errores De Usuarios	2,45	1,4	2,8			• Seguridad de la aplicación de correo electrónico • Resgistro de incidencias • Analisis de informes de ataques • Manual de Administración • Manual de Buenas prácticas para Usuario • Logs de incidencias
		Errores De Administración	0,525	0,2	0,6			
		Alteración Accidental De La Información		1,2				
		Fugas De Información			0,6			
		Caída Del Sistema Por Agotamiento De Recursos	0,7					
		Suplantación De La Identidad Del Usuario		2	3	2,625		
		Abuso De Privilegios De Acceso	1,05	1,8	1,8			
		Uso No Previsto	1,575	1,8	1,8			
		Acceso No Autorizado		3	4			
		Repudio		0,4			0,6	
		Modificación Deliberada De La Información		0,6				
		Divulgación De Información			1,8			
		Denegación De Servicio	0,7					
S3	**Intranet documental - Servicio FTP**	Errores De Usuarios	0,28	2,8	2,8			• Seguridad de la aplicación de Intranet • Resgistro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,8	1,8	1,2			
		Alteración Accidental De La Información		3				
		Destrucción De Información	3					
		Fugas De Información			0,6			
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Suplantación De La Identidad Del Usuario		1,2	1,8	1,2		
		Abuso De Privilegios De Acceso	0,2	0,4	0,6			
		Uso No Previsto	1,2	1,2	1,8			
		Acceso No Autorizado		2	4			
		Repudio		0,6			1,8	
		Modificación Deliberada De La Información		0,6				
		Destrucción De Información	0,8					
		Divulgación De Información			0,6			
		Denegación De Servicio	2,4					

Figura 128. Salvaguardas de los activos S2 Y S3
(Fuente propia)

S4	Sistema de tickets de incidencias	Errores De Usuarios	0,14	1,05	1,05			• Seguridad de la aplicación de sistema de tockets de incidencias • Resgistro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	0,9	0,9	0,45			
		Alteración Accidental De La Información		0,9				
		Caída Del Sistema Por Agotamiento De Recursos	0,4					
		Suplantación De La Identidad Del Usuario		0,9	1,35	1,2		
		Acceso No Autorizado		2,25	2,25			
		Repudio		0,3			0,375	
		Modificación Deliberada De La Información		0,3				
		Divulgación De Información			0,3			
		Denegación De Servicio	1,2					
S5	Educación Virtual	Errores De Usuarios	0,28	1,4	2,45			• Seguridad de la aplicación E-apsa • Registro de incidencias • Manual de Administración • Manual de Usuarios • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,8	1,2	1,05			
		Alteración Accidental De La Información		3				
		Destrucción De Información	4					
		Fugas De Información			1,75			
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Suplantación De La Identidad Del Usuario		1	2,625	1,5		
		Abuso De Privilegios De Acceso	0,6	1,8	1,05			
		Uso No Previsto	2	1	1,75			
		Acceso No Autorizado		3	2,625			
		Repudio		0,2			0,525	
		Modificación Deliberada De La Información		0,6				
		Divulgación De Información			1,05			
		Denegación De Servicio	2,4					
S6	Servicio de financiero	Errores De Usuarios	1	3,375	4,5			• Seguridad de la aplicación financiero • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,8	1,35	2,025			
		Alteración Accidental De La Información		4,5				
		Destrucción De Información	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	2,4					
		Suplantación De La Identidad Del Usuario		2,025	2,7	2,025		
		Abuso De Privilegios De Acceso	0,6	2,025	2,025			
		Uso No Previsto	1,2	1,35	1,35			
		Acceso No Autorizado		2,7	2,7			
		Repudio		0,45			0,9	
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,8					
		Divulgación De Información			0,9			
		Denegación De Servicio	2,4					

Figura 129. Salvaguardas de los activos S4, S5 y S6.
(Fuente propia)

Salvaguardas S7, S8, S9: 1) La seguridad que heredan estos activos corresponde a las aplicaciones de Gestión de usuarios-socios, gestión empresarial y gestión de recursos humanos. 2) Este tipo de activos manejan bases de datos de empleados y usuarios que requieren de una adecuada gestión, por lo que se deben establecer pautas para tener las bases de datos actualizadas y depuradas. 3) Estos servicios pueden ser víctimas de errores y amenazas que se deben exponer en un registro de incidencias, para realizar un análisis posterior y mejorar las medidas de seguridad. 4) Este grupo de activos, son gestionados por los administradores TIC y usados por los empleados de la asociación, por lo que es necesario establecer manuales para evitar errores y que sirva como referencia para nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 5) Habitualmente, estos servicios deben pasar por un proceso de gestión de mejoras para actualizar y mejorar su funcionalidad considerando la seguridad informática. 6) Las salvaguardas que también heredan estas aplicaciones corresponden a la configuración Logs de incidencias.

En este grupo de activos el riesgo grave es causado por el acceso no autorizado y se mitiga con la seguridad de las correspondientes aplicaciones de los servicios. Para el resto de las amenazas se crearon las demás salvaguardas. La Figura 130 muestra las salvaguardas para los riesgos de los activos S7, S8 y S9.

S7	Gestión de usuarios Socios	Errores De Usuarios	1	3	2			• Seguridad de la aplicación GUS • Gestión de Usuarios Socios • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,8	1,2	1,8			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,6					
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Suplantación De La Identidad Del Usuario		1,8	2,4	1,05		
		Abuso De Privilegios De Acceso	0,2	0,4	0,4			
		Uso No Previsto	1,2	0,6	1,8			
		Acceso No Autorizado		3	4			
		Repudio		0,2			0,8	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,8					
		Divulgación De Información			2,4			
		Denegación De Servicio	2,4					
S8	Gestión empresarial	Errores De Usuarios	0,875	2	2			• Seguridad de la aplicación G2K • Gestión empresarial • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,05	1,2	1,2			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,525					
		Caída Del Sistema Por Agotamiento De Recursos	0,525					
		Suplantación De La Identidad Del Usuario		1,2	1,8	1,05		
		Abuso De Privilegios De Acceso	0,175	0,4	0,4			
		Uso No Previsto	0,525	1,2	1,8			
		Acceso No Autorizado		3	4			
		Repudio		0,4			0,8	
		Modificación Deliberada De La Información		0,6				
		Destrucción De Información	0,7					
		Divulgación De Información			2,4			
		Denegación De Servicio	2,1					
S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	0,875	2	3			• Seguridad de la aplicación Sage • Gestión de Recursos Humanos • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias
		Errores De Administración	1,05	1,2	1,8			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,525					
		Caída Del Sistema Por Agotamiento De Recursos	0,7					
		Suplantación De La Identidad Del Usuario		1,8	2,4	1,2		
		Abuso De Privilegios De Acceso	0,175	0,4	0,6			
		Uso No Previsto	0,525	1,2	1,8			
		Acceso No Autorizado		3	4			
		Repudio		0,4			0,9	
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			2,4			
		Denegación De Servicio	2,1					

Figura 130. Salvaguardas de los activos S7, S8 y S9.
(Fuente propia)

- [SW] Software – Aplicaciones Informáticas

Tratamiento del riesgo general de las Aplicaciones informáticas: Si bien se determinó que los valores de riesgo mayores a 4 son graves, para este grupo de activos esa condición va a cambiar. Considerando que de estas aplicaciones depende el funcionamiento de la asociación, se considera que los niveles de riesgo tienen que ser los mínimos posibles, por lo que las salvaguardas irán orientadas a mitigar los riesgos más graves y que no sobrepasen un riesgo de 1. Al tener relación directa de dependencias con otros activos, las aplicaciones heredan las salvaguardas de dichos activos logrando mayor seguridad. Estas salvaguardas heredadas solo se

describen de manera general pues están desarrolladas en su correspondiente activo. A continuación se definen las salvaguardas de todos los activos del grupo Software y cuáles son los riesgos sobre los que actúan.

Salvaguardas SW1, SW2, SW3, SW4, SW5, SW6, SW7, SW8, SW10: 1) Las copias de seguridad que se deben realizar son: de las configuraciones, el código fuente (para aplicaciones propias) y bases de datos. Esto ayudará a reestablecer una aplicación en caso de tener un incidente. 2) Actualmente, existe mucha información de los riesgos de seguridad en aplicaciones, por lo que se recomienda configurar medidas de protección para los ataques más comunes. Organizaciones de ciberseguridad como el OWASP anualmente brindan una lista de los riesgos más comunes de seguridad. Adicionalmente, se pueden suscribir a foros oficiales de seguridad informática para compartir experiencia con otras empresas y mejorar el nivel de seguridad que ya tiene la asociación. 3) Los datos de configuración, ficheros confidenciales y bases de datos se deben cifrar para protegerlos del acceso no autorizado y las fugas de información. 4) Periódicamente hay que realizar un análisis de vulnerabilidades de las aplicaciones. Se recomienda que una empresa externa realice el análisis y tomar acciones de acuerdo con los resultados. 5) Como complemento de las anteriores salvaguardas, la actualización habitual de la aplicación brinda mejor servicio y mejora el nivel de seguridad. 6) Todas las aplicaciones deben estar en servidores con una configuración de logs, en donde los eventos de mayor relevancia deben ser notificados a los administradores para tomar acciones inmediatas. 7) Este grupo de activos, son gestionados por los administradores TIC y usados por los empleados de la asociación, por lo que se debe establecer manuales para evitar errores y que quede como referente para nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 8) Finalmente, se debe tener un registro de configuración e incidencias que quede como referente para la toma de futuras acciones y sirva de retroalimentación para la seguridad en las aplicaciones.

De las anteriores salvaguardas, las más importantes son 1ª, 2dª 3ª y 4ª pues mitigan el riesgo de las amenazas definidas como ataques. Las demás salvaguardas están destinadas a mitigar los riesgos producidos por los errores y amenazas de origen industrial. El mayor riesgo se encuentra en la aplicación de página Web causada por el uso no previsto, por ello se definió la 2ª salvaguarda para una revisión de ese tipo de ataques. Además, como la aplicación lo administra otra empresa, se debe pedir informes y análisis de seguridad para verificar que existan medidas contra esta vulnerabilidad. Las Figuras 131 y 132 muestran las salvaguardas para los riesgos de los activos SW1, SW2, SW3, SW4, SW5, SW6, SW7, SW8 y SW10.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
SW1	Aplicación de Financiero	Fallo De Origen Lógico	0,675					• Copias de seguridad • Revisión de la configuración de seguridad • Cifrado de información • Análisis de vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	1,125	3,375	2,25			
		Errores De Administración	0,675	0,45	0,45			
		Alteración Accidental De La Información		2,025				
		Destrucción De Información	0,9					
		Fugas De Información			0,9			
		Vulnerabilidades De Los Programas	1,35	2,025	2,7			
		Errores De Mantenimiento/Actualización De Programas	1,35	2,025				
		Suplantación De La Identidad Del Usuario		0,675	0,9	0,675		
		Abuso De Privilegios De Acceso	1,35	2,025	2,7			
		Uso No Previsto	2,025	1,35	1,35			
		Difusión De Software Dañino	0,9	0,9	0,9			
		Acceso No Autorizado		0,675	0,9			
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,45					
		Divulgación De Información			0,9			
SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	0,6					• Copias de seguridad • Revisión de la configuración de seguridad • Cifrado de información • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	2	3	2			
		Errores De Administración	0,6	0,4	0,4			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,8					
		Fugas De Información			0,8			
		Vulnerabilidades De Los Programas	1,2	1,8	2,4			
		Errores De Mantenimiento/Actualización De Programas	1,2	1,8				
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,675		
		Abuso De Privilegios De Acceso	1,2	1,8	2,4			
		Uso No Previsto	1,2	1,2	1,2			
		Difusión De Software Dañino	0,8	0,8	0,8			
		Acceso No Autorizado		0,6	0,8			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,4					
		Divulgación De Información			0,8			
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	0,525					• Copias de seguridad • Revisión de la configuración de seguridad • Cifrado de información • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	1,75	3	2			
		Errores De Administración	0,525	0,4	0,4			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,7					
		Fugas De Información			0,8			
		Vulnerabilidades De Los Programas	1,05	1,8	2,4			
		Errores De Mantenimiento/Actualización De Programas	1,05	1,8				
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,675		
		Abuso De Privilegios De Acceso	1,05	1,8	2,4			
		Uso No Previsto	1,05	1,2	1,2			
		Difusión De Software Dañino	0,7	0,8	0,8			
		Acceso No Autorizado		0,6	0,8			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,35					
		Divulgación De Información			0,8			
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	0,525					• Copias de seguridad • Revisión de la configuración de seguridad • Cifrado de información • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	1,75	3	2			
		Errores De Administración	0,525	0,4	0,4			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,7					
		Fugas De Información			0,8			
		Vulnerabilidades De Los Programas	1,05	1,8	2,4			
		Errores De Mantenimiento/Actualización De Programas	1,05	1,8				
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,675		
		Abuso De Privilegios De Acceso	1,05	1,8	2,4			
		Uso No Previsto	1,05	1,2	1,2			
		Difusión De Software Dañino	0,7	0,8	0,8			
		Acceso No Autorizado		0,6	0,8			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,35					
		Divulgación De Información			0,8			
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	0,6					• Copias de seguridad • Cifrado de Información • Revisión de la configuración de seguridad • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Administración	0,6	0,675	0,45			
		Alteración Accidental De La Información		2,7				
		Destrucción De Información	0,8					
		Fugas De Información			0,9			
		Vulnerabilidades De Los Programas	1,2	2,025	2,7			
		Errores De Mantenimiento/Actualización De Programas	1,2	2,7				
		Suplantación De La Identidad Del Usuario		0,9	0,9	0,9		
		Abuso De Privilegios De Acceso	1,8	2,7	2,7			
		Uso No Previsto	1,8	2,025	2,7			
		Difusión De Software Dañino	0,8	0,9	0,9			
		Acceso No Autorizado		0,9	0,9			
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,8					
		Divulgación De Información			0,9			

Figura 131. Salvaguardas de los activos SW1, SW2, SW3, SW4 y SW5.
(Fuente propia)

SW6	Aplicación de Página web	Fallo De Origen Lógico	0,525					• Copias de seguridad • Revisión de la configuración de seguridad • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Registro de configuración e Incidencias
		Errores De Usuarios	0,875	1	1			
		Errores De Administración	0,525	0,4	0,6			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,525					
		Fugas De Información			0,4			
		Vulnerabilidades De Los Programas	1,575	1,8	1,8			
		Errores De Mantenimiento/Actualización De Programas	1,05	1,8				
		Suplantación De La Identidad Del Usuario		0,4	0,8	0,9		
		Abuso De Privilegios De Acceso	1,05	1,8	2,4			
		Uso No Previsto	1,75	2	4			
		Difusión De Software Dañino	0,35	0,4	0,8			
		Acceso No Autorizado		0,6	0,8			
		Modificación Deliberada De La Información		0,6				
		Destrucción De Información	0,35					
		Divulgación De Información			0,6			
		Manipulación De Programas	0,35	0,6	0,6			
SW7	Aplicación de Intranet	Fallo De Origen Lógico	0,6					• Copias de seguridad • Revisión de la configuración de seguridad • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	2	3	2			
		Errores De Administración	0,6	0,4	0,4			
		Alteración Accidental De La Información		1,8				
		Destrucción De Información	0,8					
		Fugas De Información			0,8			
		Vulnerabilidades De Los Programas	1,2	1,8	2,4			
		Errores De Mantenimiento/Actualización De Programas	1,2	1,8				
		Suplantación De La Identidad Del Usuario		0,6	0,8	0,675		
		Abuso De Privilegios De Acceso	1,2	1,8	2,4			
		Uso No Previsto	1,2	1,2	1,2			
		Difusión De Software Dañino	0,8	0,8	0,8			
		Acceso No Autorizado		0,6	0,8			
		Modificación Deliberada De La Información		0,6				
		Destrucción De Información	0,4					
		Divulgación De Información			0,8			
SW8	Aplicación del Sistema de tickets de incidencias	Fallo De Origen Lógico	0,3					• Copias de seguridad • Revisión de la configuración de seguridad • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	1	2,25	1,5			
		Errores De Administración	0,3	0,3	0,3			
		Alteración Accidental De La Información		1,35				
		Destrucción De Información	0,4					
		Fugas De Información			0,6			
		Vulnerabilidades De Los Programas	0,6	1,35	1,8			
		Errores De Mantenimiento/Actualización De Programas	0,6	1,35				
		Suplantación De La Identidad Del Usuario		0,45	0,6	0,675		
		Abuso De Privilegios De Acceso	0,6	1,35	1,8			
		Uso No Previsto	0,6	0,9	0,9			
		Difusión De Software Dañino	0,4	0,6	0,6			
		Acceso No Autorizado		0,45	0,6			
		Modificación Deliberada De La Información		0,6				
		Destrucción De Información	0,2					
		Divulgación De Información			0,6			
SW10	E-apsa	Fallo De Origen Lógico	0,6					• Copias de seguridad • Revisión de la configuración de seguridad • Análisis de Vulnerabilidades • Actualizaciones • Configuración y revisión de logs • Manual de Administración • Manual de Usuarios • Registro de configuración e Incidencias
		Errores De Usuarios	0,2	0,2	0,875			
		Errores De Administración	0,4	0,4	0,525			
		Alteración Accidental De La Información		0,6				
		Destrucción De Información	0,12					
		Fugas De Información			0,175			
		Vulnerabilidades De Los Programas	0,12	0,6	1,05			
		Errores De Mantenimiento/Actualización De Programas	0,6	0,6				
		Suplantación De La Identidad Del Usuario		0,6	1,575	2,4		
		Abuso De Privilegios De Acceso	0,12	0,6	1,575			
		Uso No Previsto	0,2	0,04	0,35			
		Difusión De Software Dañino	0,04	0,2	0,35			
		Acceso No Autorizado		0,2	0,7			
		Modificación Deliberada De La Información		0,2				
		Destrucción De Información	0,6					
		Divulgación De Información			0,525			

Figura 132. Salvaguardas de los activos SW6, SW7, SW8 y SW10.
(Fuente propia)

Salvaguardas SW9: 1) Esta aplicación es subcontratada a Google, por lo que la administración TIC solo gestiona la configuración que incluye el cifrado de correos electrónicos. El cifrado se realiza a todos los correos con el objetivo de proteger la información que contienen. 2) Las reglas de filtros también pueden ser configuradas por la administración, para lo cual se puede realizar listas blancas y negras de correos electrónicos. 3) Esta aplicación en ordenadores y móviles se deben actualizar, sobre todo cuando las actualizaciones corrigen problemas de seguridad. 4) La

gestión de este activo es responsabilidad de los administradores TIC, pero todos los empleados de la asociación usan la aplicación. Por ello es necesario establecer manuales para evitar errores, un mal uso y que sirva de referente para los nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 5) Finalmente, se debe tener un registro de los cambios de configuración e incidencias para tomar acciones y realizar una retroalimentación de la seguridad de la aplicación.

Para esta aplicación no existen salvaguardas contra los ataques debido a que es una aplicación externa, pero las salvaguardas se concentran en mejorar la configuración y uso de la aplicación de correo electrónico. La Figura 133 muestra las salvaguardas para los riesgos del activo SW9.

SW9	**Aplicación de Correo electrónico Gmail**	Errores De Usuarios	0,175	0,2	1			• Cifrado de correo electrónicos • Reglas de Filtro de correos maliciosos • Actualización • Manual de Administración • Manual de Buenas prácticas para Usuario • Registro de Cambios e incidencias
		Errores De Administración	0,175	0,04	0,4			
		Difusión De Software Dañino	0,035	0,04	0,8			
		Alteración Accidental De La Información		0,12				
		Destrucción De Información	0,175					
		Fugas De Información			2,4			
		Vulnerabilidades De Los Programas	0,105	1,2	2,4			
		Errores De Mantenimiento/Actualización De Programas	0,175	0,4	0,6			
		Suplantación De La Identidad Del Usuario		0,4	0,8	0,9		
		Abuso De Privilegios De Acceso	0,035	0,6	0,6			
		Uso No Previsto	1,05	1,8	2,4			
		Difusión De Software Dañino	0,035	0,4	0,8			
		Acceso No Autorizado		0,4	0,8			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			0,8			

Figura 133. Salvaguardas del activo SW9.
(Fuente propia)

Salvaguardas SW11: 1) Uno de los principales problemas de los móviles es la confidencialidad, pero se puede solucionar con la configuración de una carpeta segura que viene por defecto en los móviles, en los que se puede proteger a las aplicaciones. 2) Si la información de las aplicaciones es confidencial, se precisa encriptarlos para protegerlos del acceso no autorizado. 3) Las aplicaciones de un móvil, especialmente el sistema operativo, se deben actualizar porque puede corregir errores y problemas de seguridad. 4) Para la protección de ataques, virus, troyanos, etc., se debe instalar un antivirus en aquellos dispositivos que no los tengan por defecto. 7) Como complemento de la salvaguarda anterior, hay que realizar un análisis periódico con el antivirus para eliminar posibles amenazas. 8) Crear un manual de usuarios y buenas prácticas para el uso y mantenimiento de las aplicaciones de los móviles.

Las salvaguardas definidas dependen mucho de los empleados que usen los móviles, por lo que es un punto importante la entrega del manual de usuarios y buenas prácticas, que incluyan firmas de responsabilidad para asegurar su cumplimiento. La Figura 134 muestra las salvaguardas para los riesgos del activo SW11.

SW11	Aplicaciones en móviles	Fallo De Origen Lógico	0,2					• Configuración de carpeta Segura • Cifrado de Información • Actualización del Sistema Operativo y Aplicaciones • Instalación/Actualización Antivirus • Análisis de Virus • Manual de buenas practicas y de Usuarios
		Errores De Usuarios	0,1	1	1,75			
		Errores De Administración	0,1	0,2	0,35			
		Difusión De Software Dañino	0,06	0,6	1,575			
		Alteración Accidental De La Información		0,6				
		Destrucción De Información	0,3					
		Fugas De Información			1,575			
		Vulnerabilidades De Los Programas	0,3	0,6	1,575			
		Errores De Mantenimiento/Actualización De Programas	1	1				
		Suplantación De La Identidad Del Usuario		0,6	1,575	1,8		
		Abuso De Privilegios De Acceso	0,3	1,8	1,575			
		Uso No Previsto	0,3	0,4	0,525			
		Difusión De Software Dañino	0,3	0,4	0,7			
		Acceso No Autorizado		0,2	0,7			
		Modificación Deliberada De La Información		0,2				
		Destrucción De Información	0,2					
		Divulgación De Información			0,7			

Figura 134. Salvaguardas del activo SW11.
(Fuente propia)

Salvaguardas SW12, SW13: 1) El sistema operativo de un servidor es esencial, por lo que la configuración de Políticas de seguridad es necesario. La configuración debe incluir, cifrado, configuración de acceso, procesos de verificación, configuración de logs, firewalls, depuración, y medidas de seguridad que dependen del servicio que alojen. Para estas configuraciones se debe consultar documentación oficial de proveedores y, organizaciones y foros de ciberseguridad. 2) Como complemento de la salvaguarda anterior, existen ficheros críticos y confidenciales del sistema operativo, por lo que se debe cifrar y proteger el acceso. 3) Para acceder a los servidores, se deben definir perfiles de seguridad, los cuales permiten delimitar las acciones dentro del servidor. 4) Las actualizaciones deben ser controladas y realizadas solo cuando sea necesario, analizando si mejora o no el nivel de seguridad. 5) El antivirus que se use debe estar en su versión más actualizada. Se puede actualizar lista de virus o vulnerabilidades que protejan al sistema operativo. 6) Un servidor no funciona sin el sistema operativo, así que se requiere realizar un respaldo de su configuración para levantar un servidor de respaldo. 7) Como complemento de la salvaguarda anterior, se debe hacer copias de seguridad de todo aquello que este configurado en el sistema operativo. 8) Todos los cambios o incidencias se deben registrar para tomar acciones o que sirva como retroalimentación de seguridad. 9) Realizar una configuración de logs de eventos, para que las alertas sean notificadas a los administradores para conocer todo lo que en el servidor se hace.

De las anteriores salvaguardas, las más importantes son la 1ª y la 5ª, pues con una buena configuración de seguridad, se puede evitan la mayoría de las amenazas que afectan a este activo. La Figura 135 muestra las salvaguardas para los riesgos de los activos SW12 y SW13.

SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	0,675					• Configuración de Políticas de seguridad Local • Cifrado de Información • Perfiles de Usuarios • Actualización del Sistema Operativo • Actualización Antivirus • Respaldos de configuración • Copias de seguridad • Registro de cambios e incidentes • Configuración de logs de incidencias
		Errores De Administración	0,9	0,675	0,9			
		Alteración Accidental De La Información		0,675				
		Destrucción De Información	0,9					
		Vulnerabilidades De Los Programas	0,675	0,675	0,9			
		Errores De Mantenimiento/Actualización De Programas	2,025	2,025				
		Suplantación De La Identidad Del Usuario		2,025	2,7	2,7		
		Abuso De Privilegios De Acceso	1,35	2,025	2,7			
		Uso No Previsto	0,45	0,675	0,9			
		Difusión De Software Dañino	0,9	0,9	0,9			
		Acceso No Autorizado		0,9	0,9			
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,9					
		Divulgación De Información			0,9			
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	0,675					• Configuración de Políticas de seguridad Local • Cifrado de Información • Perfiles de Usuarios • Actualización del Sistema Operativo • Actualización Antivirus • Respaldos de configuración • Copias de seguridad • Registro de cambios e incidentes • Configuración de logs de incidencias
		Errores De Administración	0,9	0,675	0,9			
		Alteración Accidental De La Información		0,675				
		Destrucción De Información	0,9					
		Vulnerabilidades De Los Programas	0,675	0,675	0,9			
		Errores De Mantenimiento/Actualización De Programas	2,025	2,025				
		Suplantación De La Identidad Del Usuario		2,025	2,7	2,7		
		Abuso De Privilegios De Acceso	1,35	2,025	2,7			
		Uso No Previsto	0,45	0,675	0,9			
		Difusión De Software Dañino	0,9	0,9	0,9			
		Acceso No Autorizado		0,9	0,9			
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,9					
		Divulgación De Información			0,9			

Figura 135. Salvaguardas de los activos SW12 y SW13.
(Fuente propia)

Salvaguardas SW14, SW15: 1) Para controlar el sistema operativo de ordenadores de empleados, se debe definir perfiles de usuarios con control de acceso y delimitados por el tipo de actividad que en ellos pueden realizar. Se recomienda 3 perfiles: administrativo, empleado e invitado. 2) Aunque este software solo lo usan los ordenadores, también se debe realizar una adecuada configuración de seguridad con las opciones que ofrece el sistema como firewall, proxy, antivirus, perfiles, restauración del sistema, entre otros. 3) Las actualizaciones del software son importantes porque contienen mejoras y parches de seguridad para nuevas vulnerabilidades. Además nuevas opciones de protección, privacidad y seguridad. 4) Todas las actualizaciones, configuraciones e incidencias deben estar registradas para controlar los cambios y realizar retroalimentaciones para futuras configuraciones de seguridad. 5) Para brindar seguridad a las aplicaciones y documentos, se recomienda la configuración de una carpeta segura y así evitar accesos no autorizados. 7) Como complemento de la salvaguarda anterior, todos aquellos ficheros con nivel de confidencialidad hay que cifrarlos. 8) La configuración de seguridad para estos activos está controlada por los administradores TIC. Asimismo, todos los empleados usan estas aplicaciones, por lo que es necesario establecer manuales para las dos partes y así evitar errores y que quede como referente para nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 9) En lo posible deben estar activos todos los registros de logs, para analizar las actividades que se han realizado en el sistema operativo y sus aplicaciones. 10) La seguridad de un sistema operativo se puede complementar con la seguridad que ofrecen otros

aplicativos como firewalls y antivirus. 11) Los ficheros críticos del sistema operativo, se puede respaldar para disponer de ellos en caso de algún incidente.

Los riesgos graves pueden ser mitigados con: configuración de seguridad adecuada, actualización, copias de seguridad y cifrado de la información. Sus acciones son complementadas con el resto de las salvaguardas. La Figura 136 muestra las salvaguardas para los riesgos de los activos SW14 y SW15.

SW14	Sistema operativo Windows 7	Fallo De Origen Lógico	0,4				
		Errores De Usuarios	0,5	0,225	0,625		
		Errores De Administración	0,2	0,225	0,25		
		Difusión De Software Dañino	0,3	0,45	0,375		
		Alteración Accidental De La Información		0,675			
		Destrucción De Información	0,4				
		Vulnerabilidades De Los Programas	0,3	0,675	1,5		
		Errores De Mantenimiento/Actualización De Programas	0,3	0,675			
		Suplantación De La Identidad Del Usuario		0,135	1,5	2,4	
		Abuso De Privilegios De Acceso	0,06	0,135	1,125		
		Uso No Previsto	0,3	0,675	1,5		
		Difusión De Software Dañino	0,3	0,675	0,5		
		Acceso No Autorizado		0,675	1,5		
		Modificación Deliberada De La Información		0,675			
		Destrucción De Información	0,4				
		Divulgación De Información			0,5		
SW15	Sistema operativo Windows 10	Fallo De Origen Lógico	0,4				
		Errores De Usuarios	0,5	0,225	0,625		
		Errores De Administración	0,2	0,225	0,25		
		Difusión De Software Dañino	0,3	0,45	0,375		
		Alteración Accidental De La Información		0,675			
		Destrucción De Información	0,4				
		Vulnerabilidades De Los Programas	0,3	0,675	1,5		
		Errores De Mantenimiento/Actualización De Programas	0,3	0,675			
		Suplantación De La Identidad Del Usuario		0,135	1,5	2,4	
		Abuso De Privilegios De Acceso	0,06	0,135	1,125		
		Uso No Previsto	0,3	0,675	1,5		
		Difusión De Software Dañino	0,3	0,675	0,5		
		Acceso No Autorizado		0,675	1,5		
		Modificación Deliberada De La Información		0,675			
		Destrucción De Información	0,4				
		Divulgación De Información			0,5		

• Perfiles de usuarios
• Configuración de seguridad
• Actualizaciones de Software
• Registro de cambio e incidencias
• Configuración de la Carpeta Segura
• Cifrado de Información
• Manual de buenas prácticas
• Configuración de logs de incidencias
• Seguridad con otras aplicaciones
• Copias de seguridad

• Perfiles de usuarios
• Configuración de seguridad
• Actualizaciones de Software
• Registro de cambio e incidencias
• Configuración de la Carpeta Segura
• Cifrado de Información
• Manual de buenas prácticas
• Configuración de logs de incidencias
• Seguridad con otras aplicaciones copias de seguridad

Figura 136. Salvaguardas de los activos SW14 y SW15.
(Fuente propia)

Salvaguardas SW16: 1) La configuración de seguridad de este activo está gestionado por los administradores TIC, pero la aplicación la usan todos los empleados, por lo que es necesario establecer manuales para evitar errores y que sirva como referencia para los nuevos empleados. Los manuales deben estar formalizados y cumplir con un proceso de revisión y actualización periódica. 2) Todos los navegadores web poseen opciones de seguridad y privacidad para configurar de acuerdo con las políticas de la asociación. 3) Los navegadores web pueden ser la ventana para ataques de seguridad, por lo que mantener actualizada la aplicación ofrece mayor seguridad y mejores servicios a los usuarios. 4) Todas las actualizaciones, configuraciones e incidencias deben estar registradas para controlar los cambios en la aplicación y realizar retroalimentaciones para futuras configuraciones de seguridad.

Todas las salvaguardas están orientadas para mitigar el mayor riesgo que tiene este activo a causa de la difusión de software dañino, pero lo más importante es mantener actualizada la

aplicación con una configuración adecuada de privacidad. La Figura 137 muestra las salvaguardas para los riesgos del activo SW16.

SW16	**Navegadores Web**	Errores De Usuarios	0,1	0,2	3			• Manual de administración • Manual de buenas prácticas de usuarios • Configuración de seguridad • Actualización del software • Registro de cambio e incidencias
		Errores De Administración	0,1	0,04	0,6			
		Fugas De Información			0,8			
		Vulnerabilidades De Los Programas	0,1	0,4	0,8			
		Errores De Mantenimiento/Actualización De Programas	0,06	1,2				
		Abuso De Privilegios De Acceso	0,06	0,12	1,8			
		Uso No Previsto	0,06	0,6	1,8			
		Difusión De Software Dañino	0,1	1	4			
		Modificación Deliberada De La Información		0,2				
		Destrucción De Información	0,1					
		Divulgación De Información			0,2			

Figura 137. Salvaguardas de los activos SW16.
(Fuente propia)

Salvaguardas SW17: 1) Los únicos que deben tener acceso a la configuración de un antivirus son los administradores, a pesar de esto hay que establecer un manual para cuando se requiera volver a configurarlo. 2) La actualización de este software es importante, pues mejoran procesos y actualizan listas de búsqueda de virus, bases de datos de gusanos, troyanos y virus. 3) Tanto su actualización como su uso debe ser periódico, por lo que se puede crear un programa de actualización y ejecución de un análisis de virus en los dispositivos que este instalado. 4) Todas las actualizaciones y configuraciones deben estar registradas para controlar los cambios en la aplicación.

De las anteriores salvaguardas, lo más importante es mantener actualizada la aplicación pues ofrece protección a otras aplicaciones, servicios y dispositivos. La Figura 138 muestra las salvaguardas para los riesgos del activo SW17.

SW17	**Antivirus**	Fallo De Origen Lógico	0,6					• Manual de administración • Actualización de software • Análisis con el software • Registro de cambio e incidencias
		Errores De Administración	0,4	0,2	0,125			
		Errores De Mantenimiento/Actualización De Programas	0,6	2,4				
		Abuso De Privilegios De Acceso	0,4	0,8	0,125			
		Uso No Previsto	0,4	0,8	0,125			
		Acceso No Autorizado		0,8	0,125			
		Modificación Deliberada De La Información		0,8				

Figura 138. Salvaguardas de los activos SW138.
(Fuente propia)

Salvaguardas SW18: 1) Aunque se trate de una aplicación de uso común, es necesario establecer un manual de usuarios especialmente para configuración de protección de acceso o modificación del contenido. 2) Las actualizaciones son necesarias para las correcciones de errores o mejoras de opciones de seguridad. 3) Finalmente, se debe tener un registro de cambios y actualizaciones realizados en todos los ordenadores que contengan la aplicación.

El riesgo en este activo es muy bajo y puede ser asumido por la asociación, pero se pueden establecer salvaguardas que ayuden al uso correcto del software ofimático. La Figura 139 muestra las salvaguardas para los riesgos del activo SW18.

SW18	**Software Ofimático**	Fallo De Origen Lógico	0,45					• Manual de usuarios • Actualización de software • Registros de Cambio
		Errores De Usuarios	0,75	0,125	0,625			
		Errores De Administración	0,15	0,025	0,125			
		Errores De Mantenimiento/Actualización De Programas	0,675	0,375				
		Abuso De Privilegios De Acceso	0,075	0,125	0,125			
		Uso No Previsto	0,15	0,125	0,125			

Figura 139. Salvaguardas del activo SW18.
(Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Tratamiento del riesgo general de los Equipos Informáticos: El nivel mínimo de riesgo para estos activos será de 4, definido previamente en el tratamiento general de riesgo. Esta condición se cumple para los equipos informáticos excepto servidores (APSA y locales) y equipos de redes de comunicaciones (routers y switches), en donde el nivel mínimo de riesgo aceptado será 1. La condición se establece considerando que estos activos son esenciales para el funcionamiento de la asociación, por lo que su seguridad es fundamental. Definidas las condiciones, se procura definir salvaguardas que logren disminuir los riesgos hasta el nivel requerido. En algunos casos las salvaguardas heredadas solo se describen de manera general pues están desarrolladas en su correspondiente activo.

A continuación se definen las salvaguardas de todos los activos del grupo Equipos informáticos y cuáles son los riesgos sobre los que actúan.

Salvaguardas HW1: 1) La configuración lógica de la seguridad de los servidores se realiza en el sistema operativo. 2) Como complemento de la salvaguarda anterior, todos los servicios y aplicaciones adicionales deben asegurarse. 3) Una de las partes más importantes de un servidor es su capacidad de almacenamiento. Esta característica puede influir en el rendimiento del dispositivo, por lo que se debe crear un proceso de revisión de recursos. Adicionalmente, se debe realizar una revisión de la capacidad de procesamiento y memoria. 4) Es esencial realizar copias de seguridad de la configuración, en caso de necesitar levantar un servidor. 5) Parte de la configuración de seguridad requiere establecer mecanismos de accesos eficientes. 6) Para la configuración, cambios e incidentes, se requiere tener un manual de administración formalizado para brindar ayuda a los empleados del departamento TIC. 7) Como se mencionó, un aspecto importante de un servidor es el espacio de almacenamiento, por ello se debe realizar una depuración periódica, eliminando todos los ficheros que no se requieren. 8) De igual manera, parte de la configuración de seguridad es tener un sistema de logs de incidencias para mitigar

los riesgos en la dimensión de trazabilidad. 9) Por ser estos dispositivos la base de la asociación, se debe tener servidores de respaldo para levantar los servicios cuando el servidor principal no está disponible. 10) El cifrado de la información confidencial es importante, especialmente para ficheros de configuración, claves y contraseñas.

El riesgo grave en los equipos informáticos se produce por el acceso no autorizado. La seguridad física no depende de la asociación, pues el servicio está contratado en una empresa externa. Entonces se creó salvaguardas para el acceso lógico, que dependen también de los servicios y aplicaciones que almacenan los servidores. La Figura 140 muestra las salvaguardas para los riesgos del activo HW1.

EQUIPOS INFORMÁTICOS [HW]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
HW1	Servidores APSA	Avería De Origen Físico/Lógico	2,7					• Configuración de seguridad
		Errores De Administración	0,9	0,9	0,9			• Seguridad en servicios alojados
		Errores De Mantenimiento/Actualización De Equipos	2,025					• Revisión de recursos
		Caída Del Sistema Por Agotamiento De Recursos	0,9					• Copias de segruidad de configuración
		Abuso De Privilegios De Acceso	0,675	0,675	0,9			• Registro de accesos
		Uso No Previsto	2,025	2,025	2,7			• Manuales de Administración
		Acceso No Autorizado		4,725	6,3			• Depuración
		Denegación De Servicio	2,7					• Logs de incidencias • Servidores de Respaldo • Cifrado de Información

Figura 140. Salvaguardas del activo HW1.
(Fuente propia)

Salvaguardas HW2: Las salvaguardas para estos servidores son las mismas establecidas para los servidores APSA, pero en adicional se definieron las siguientes salvaguardas: 1) La seguridad física depende de la asociación, por eso se debe proteger las instalaciones e instalar videovigilancia. 2) Los servidores tienen que estar siempre en funcionamiento, por lo que ante cortes de suministros eléctricos se puede usar equipos auxiliares que mantengan su funcionamiento. 3) Realizar mantenimientos periódicos y así evitar averías lógicas o físicas.

El acceso no autorizado causa el mayor riesgo, por eso se definieron salvaguardas para controlar de acceso físico y lógico. La Figura 141 muestra las salvaguardas para los riesgos del activo HW2.

HW2	Servidores Sedes	Daños Por Agua	0,8					• Configuración de seguridad
		Avería De Origen Físico/Lógico	2,4					• Seguridad en servicios alojados
		Corte De Suministro Eléctrico	2,4					• Revisión de recursos
		Fallas De Climatización	0,2					• Copias de segruidad de configuración
		Errores De Administración	0,6	0,6	0,9			• Manuales de Administración
		Errores De Mantenimiento/Actualización De Equipos	1,8					• Depuración
		Caída Del Sistema Por Agotamiento De Recursos	0,8					• Seguridad física
		Abuso De Privilegios De Acceso	1,8	1,8	2,7			• Registro de accesos lógicos y físicos
		Uso No Previsto	1,2	1,2	2,7			• Asegurar suministro eléctrico
		Acceso No Autorizado		3	4,5			• Registro de cambios e incidencias
		Manipulación De Equipos	1,8		2,025			• Protección física
		Denegación De Servicio	2,4					• Logs de incidencias
		Robo	0,8		0,675			• Mantenimiento • Servidores de Respaldo • Ubicaciones adecuadas • Cifrado de Información

Figura 141. Salvaguardas del activo HW2.
(Fuente propia)

Salvaguardas HW3, HW4, HW5, HW6: 1) La protección lógica del equipo, depende de la seguridad del sistema operativo que tenga. 2) Los recursos de estos equipos son importantes por lo tanto requieren una revisión periódica de: la capacidad de almacenamiento, procesamiento, memoria, imagen y sonido. 3) Para evitar un colapso en el almacenamiento, se debe realizar una depuración eliminando todos los ficheros innecesarios o que han terminado su tiempo de vida; y ordenar los ficheros según las necesidades de los profesionales. 4) Realizar copias de seguridad especialmente de los ficheros de configuración y archivos importantes. 5) Para evitar los errores de administradores, empleados y usuarios, se deben crean manuales de administración y buenas prácticas. 6) Los accesos lógicos deben estar restringidos de acuerdo con la configuración de perfiles de los sistemas operativos. 7) El mantenimiento debe ser periódico, pues puede ayudar a prevenir o detectar problemas en los equipos. 8) Al realizar mantenimiento, actualización, cambios o incidencias es importante registrar para crear un historial de acciones. 9) Tanto los ordenadores de escritorio como los portátiles deben tener una ubicación adecuada, protegida de daños físicos y del acceso no autorizado. 10) Toda información confidencial debe estar encriptada.

Los riesgos de estos dispositivos no son altos, pero se definieron salvaguardas para mejorar su protección. Las Figuras 142 y 143 muestran las salvaguardas para los riesgos de los activos HW3, HW4, HW5, HW6.

HW3	**Ordenadores de escritorio administrativos**	Daños Por Agua	0,525					• Seguridad en sistemas operativos • Revisión de recursos • Depuración • Copias de seguridad • Manuales de Administración • Registro de accesos lógicos • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Ubicaciones adecuadas • Cifrado de información • Protección física
		Avería De Origen Físico/Lógico	2,1					
		Corte De Suministro Eléctrico	2,1					
		Errores De Administración	0,35	0,4	0,6			
		Errores De Mantenimiento/Actualización De Equipos	1,75					
		Caída Del Sistema Por Agotamiento De Recursos	1,575					
		Perdida De Equipos	0,7		0,8			
		Abuso De Privilegios De Acceso	0,35	0,4	0,8			
		Uso No Previsto	1,575	0,6	2,4			
		Acceso No Autorizado		0,2	0,8			
		Manipulación De Equipos	1,05		2,4			
		Robo	0,7		0,8			
HW4	**Ordenadores de escritorio empleados**	Daños Por Agua	0,225					• Seguridad en sistemas operativos • Revisión de recursos • Depuración • Copias de seguridad • Manuales de Adnimistración • Registro de accesos lógicos • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Ubicaciones adecuadas • Cifrado de Infromación • Protección física
		Avería De Origen Físico/Lógico	1,5					
		Corte De Suministro Eléctrico	0,9					
		Errores De Administración	0,45	1,05	1,575			
		Errores De Mantenimiento/Actualización De Equipos	0,75					
		Caída Del Sistema Por Agotamiento De Recursos	0,675					
		Perdida De Equipos	0,3		0,525			
		Abuso De Privilegios De Acceso	0,75	1,75	2,625			
		Uso No Previsto	1,125	0,875	2,625			
		Acceso No Autorizado		0,525	1,575			
		Manipulación De Equipos	0,75		2,625			
		Robo	0,3		0,7			
HW5	**Portátiles de administrativos**	Avería De Origen Físico/Lógico	2,1					• Seguridad en sistemas operativos • Revisión de recursos • Depuración • Copias de seguridad • Manuales de Adnimistración • Registro de accesos lógicos • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Cifrado de Información
		Corte De Suministro Eléctrico	0,175					
		Errores De Administración	1,05	0,6	2,4			
		Errores De Mantenimiento/Actualización De Equipos	1,75					
		Caída Del Sistema Por Agotamiento De Recursos	1,575					
		Perdida De Equipos	0,7		0,8			
		Abuso De Privilegios De Acceso	0,525	0,6	2,4			
		Uso No Previsto	1,05	0,6	2,4			
		Acceso No Autorizado		0,6	0,8			
		Manipulación De Equipos	1,575		2,4			
		Robo	0,7		0,8			

Figura 142. Salvaguardas de los activos HW3, HW4 y HW5.
(Fuente propia)

HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	0,9					• Seguridad en sistemas operativos • Revisión de recursos • Depuración • Copias de segruidad • Manuales de Adnimistración • Registro de accesos lógicos • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Cifrado de Infromación
		Corte De Suministro Eléctrico	0,075					
		Errores De Administración	0,45	0,525	0,525			
		Errores De Mantenimiento/Actualización De Equipos	0,75					
		Caída Del Sistema Por Agotamiento De Recursos	0,675					
		Perdida De Equipos	0,3		0,525			
		Abuso De Privilegios De Acceso	0,225	0,525	1,575			
		Uso No Previsto	0,45	0,525	1,575			
		Acceso No Autorizado		1,05	1,575			
		Manipulación De Equipos	0,45		1,575			
		Robo	0,3		0,7			

Figura 143. Salvaguardas del activo HW6.
(Fuente propia)

Salvaguardas HW7: Las salvaguardas para este activo son las mismas establecidas para los ordenadores y portátiles, pero adicionalmente se crearon las siguientes salvaguardas: 1) Son equipos importantes para la administración de todo el sistema informático, por lo que su funcionalidad no se debería ver afectada por un corte de suministro eléctrico. Entonces se requiere usar soporte auxiliar para asegurar la continuidad de los portátiles. 2) Definir métodos seguros de acceso lógico y físico.

Los riesgos de este activo aumentan por el tipo de software e información que almacena. Su protección de acceso y la continuidad de su funcionamiento son las salvaguardas más relevantes. La Figura 144 muestra las salvaguardas para los riesgos del activo HW7.

HW7	Portátiles TIC	Daños Por Agua	0,8					• Seguridad en sistemas operativos • Revisión de recursos • Depuración Copias de segruidad • Manuales de Adnimistración • Registro de accesos lógicos • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Seguridad Física • Ubicaciones adecuadas • Cifrado de Información • Asegurar suministro electrico
		Avería De Origen Físico/Lógico	0,8					
		Corte De Suministro Eléctrico	0,6					
		Errores De Administración	0,4	0,675	0,9			
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Abuso De Privilegios De Acceso	0,4	0,675	0,9			
		Acceso No Autorizado		0,675	0,9			
		Manipulación De Equipos	0,4		0,9			

Figura 144. Salvaguardas del activo HW7.
(Fuente propia)

Salvaguardas HW8: 1) La protección lógica de estos dispositivos depende de la seguridad de las aplicaciones alojadas. 2) Existen varias características físicas importantes de este activo, pero se recomienda especialmente la revisión de los recursos de almacenamiento. Se puede realizar una depuración periódica para eliminar ficheros innecesarios. 3) Para configurarlos y usarlos se recomienda definir manuales de administración y buenas prácticas para evitar los errores definidos en las amenazas. 4) El mantenimiento debe ser habitual para ayudar en la disponibilidad del dispositivo. 5) Toda información confidencial se debe cifrar con aplicaciones propias del dispositivo o aplicaciones externas. 6) El registro de entrega, cambios, mantenimiento e incidencias se debe realizar para controlar los dispositivos.

Los riesgos de estos activos no son altos, pero se establecieron salvaguardas orientadas a buenas prácticas tanto administrativas como para usuarios. La Figura 145 muestra las salvaguardas para los riesgos del activo HW8.

HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	0,9					• Seguridad en aplicaciones alojadas • Revisión de recursos • Manual de buenas prácticas, con depuración • Mantenimiento • Cifrado de Información • Registro de cambios e incidencias
		Errores De Administración	0,1	0,175	0,35			
		Errores De Mantenimiento/Actualización De Equipos	1,5					
		Caída Del Sistema Por Agotamiento De Recursos	0,6					
		Perdida De Equipos	2		3,5			
		Abuso De Privilegios De Acceso	0,6	1,05	2,1			
		Uso No Previsto	1	1,75	3,5			
		Acceso No Autorizado		0,525	0,7			
		Manipulación De Equipos	1,5		3,5			
		Robo	1,2		2,1			

Figura 145. Salvaguardas del activo HW8.
(Fuente propia)

Salvaguardas HW9, HW13: 1) Para el funcionamiento de las impresoras, la disponibilidad de recursos como tinta y papel es esencial, por lo tanto se requiere una revisión periódica de recursos. 2) La depuración de memoria es importante, para que no mantenga guardados ficheros innecesarios. 3) Para su uso y configuración se deben crear manuales de administración y buenas prácticas. 4) El mantenimiento debe ser periódico para prevenir errores o fallas. 5) Es preciso crear registros de entregas, cambios e incidencias para tener un control de estos activos. 6) Las impresoras deben estar disponibles para todos los empleados, pero no exponerlos a personas no autorizadas. 7) Para mejorar la disponibilidad, los empleados pueden acceder a más de uno de estos dispositivos. 8) Para el caso de las impresoras que se encuentran en repositorios, se debe asegurar el acceso físico.

Los riesgos de estos activos no son altos, pero se establecieron salvaguardas orientadas a buenas prácticas tanto administrativas como para usuarios. La Figura 146 muestra las salvaguardas para los riesgos de los activos HW9 y HW13.

HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	0,9					• Revisión de recursos • Depuración • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Ubicaciones adecuadas • Duplicación
		Corte De Suministro Eléctrico	0,3					
		Errores De Administración	0,15	0,1	0,015			
		Errores De Mantenimiento/Actualización De Equipos	0,45					
		Caída Del Sistema Por Agotamiento De Recursos	1,125					
		Perdida De Equipos	0,3		0,075			
		Abuso De Privilegios De Acceso	0,45	0,15	0,045			
		Uso No Previsto	0,225	0,15	0,225			
		Acceso No Autorizado		0,05	0,075			
		Manipulación De Equipos	0,45		0,225			
		Robo	0,3		0,075			
HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	2,4					• Revisión de recursos • Depuración • Manuales de Administración • Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Ubicaciones adecuadas • Seguridad física
		Corte De Suministro Eléctrico	0,8					
		Errores De Administración	1,8	0,375	0,6			
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	2,4					
		Abuso De Privilegios De Acceso	1,2	0,75	0,3			
		Uso No Previsto	1,8	0,75	0,3			
		Acceso No Autorizado		0,25	0,1			
		Manipulación De Equipos	1,8		0,3			

Figura 146. Salvaguardas de los activos HW9 y HW13.
(Fuente propia)

Salvaguardas HW10, HW11, HW12: 1) La protección lógica para estos activos de comunicaciones depende de su software de configuración. Se debe realizar una máxima configuración de seguridad. 2) Hay que establecer perfiles de acceso para configuración lógica y física. 3) Las salvaguardas que heredan estos activos pertenecen a las redes de comunicaciones. 4) Realizar un mantenimiento periódico previene errores y fallas. El mantenimiento debe incluir una revisión de recursos. 5) Periódicamente se debe realizar una depuración de la configuración con listas blancas y negras. 6) Para controlar los dispositivos se deben crear manuales de administración formalizados. 7) Anualmente se puede realizar mantenimiento para prevenir errores y fallas. 8) Para tener un control de estos activos se debe crear un registro de cambios e incidencias. 9) Para evitar la manipulación no autorizada de los dispositivos hay que establecer métodos de protección física. 10) Para complementar la salvaguarda anterior, para asegurar la confidencialidad y autenticidad de los activos se debe establecer ubicaciones seguras.

Los riesgos en estos activos se mitigan principalmente con la configuración de seguridad del software que llevan, para ello se establecieron la mitad de las salvaguardas. La otra mitad de las salvaguardas están destinadas para la seguridad física. La Figura 147 muestra las salvaguardas para los riesgos de los activos HW10, HW11 y HW12.

HW10	**Router**	Avería De Origen Físico/Lógico	0,8					• Máxima configuracióon de seguridad • Aplicación de perfiles • Seguridad de redes • Revisión de recursos • Depuración • Manual de administración • Mantenimiento • Registro de cambios e incidencias • Protección física • Ubicaciones adecuadas
		Corte De Suministro Eléctrico	0,8					
		Fallas De Climatización	0,4					
		Errores De Administración	0,6	0,4	0,8			
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Abuso De Privilegios De Acceso	0,6	0,4	0,8			
		Uso No Previsto	0,6	0,4	0,8			
		Acceso No Autorizado		1,8	2,4			
		Manipulación De Equipos	1,8		2,4			
		Denegación De Servicio	2,4					
HW11	**Router inalámbrico**	Daños Por Agua	0,8					• Máxima configuracióon de seguridad • Aplicación de perfiles • Seguridad de redes inálambricas • Revisión de recursos • Depuración • Manual de administración • Mantenimiento • Registro de cambios e incidencias • Protección física • Ubicaciones adecuadas
		Avería De Origen Físico/Lógico	0,6					
		Corte De Suministro Eléctrico	0,8					
		Errores De Administración	0,6	0,4	0,8			
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Perdida De Equipos	0,8		0,4			
		Abuso De Privilegios De Acceso	1,2	1,2	1,8			
		Uso No Previsto	1,8	1,8	1,8			
		Acceso No Autorizado		1,8	2,4			
		Manipulación De Equipos	1,8		1,2			
		Denegación De Servicio	2,4					
		Robo	0,8		0,4			
HW12	**Switch**	Avería De Origen Físico/Lógico	0,8					• Máxima configuracióon de seguridad • Aplicación de perfiles • Seguridad de redes • Revisión de recursos • Depuración • Manual de administración • Mantenimiento • Registro de cambios e incidencias • Protección física • Ubicaciones adecuadas
		Corte De Suministro Eléctrico	0,8					
		Fallas De Climatización	0,4					
		Errores De Administración	0,6	0,4	0,8			
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Abuso De Privilegios De Acceso	0,6	0,4	0,8			
		Uso No Previsto	0,6	0,4	0,8			
		Acceso No Autorizado		1,8	2,4			
		Manipulación De Equipos	1,8		2,4			
		Denegación De Servicio	2,4					

Figura 147. Salvaguardas de los activos HW10, HW11 y HW12.
(Fuente propia)

Salvaguardas HW14: 1) Estos activos los usan todos los empleados, por lo que es necesario establecer manuales para evitar errores y que sirva de referencia para los nuevos empleados. 2)

Realizar mantenimiento para prevenir errores y fallas. 3) Para gestionar estos dispositivos se deben crear manuales de administración formalizados. 4) Este activo hereda las salvaguardas de la red telefónica. 5) Para asegurar la confidencialidad de este activo hay que establecer ubicaciones seguras.

Los riesgos bajos de los teléfonos de sobremesa se solventan con las salvaguardas orientadas a las buenas prácticas. Los riesgos altos se mitigan especialmente con las salvaguardas heredadas de la red telefónica. La Figura 148 muestra las salvaguardas para los riesgos del activo HW14.

HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	0,6					• Manual de buenas prácticas • Mantenimiento • Registro de cambios e incidencias • Seguridad Red telefónica • Ubicaciones adecuadas
		Corte De Suministro Eléctrico	0,6					
		Errores De Administración	0,3	0,125	0,2			
		Errores De Mantenimiento/Actualización De Equipos	1,35					
		Abuso De Privilegios De Acceso	0,9	0,375	0,9			
		Uso No Previsto	1,35	0,375	0,9			
		Acceso No Autorizado		0,25	0,3			
		Manipulación De Equipos	2,25		1,5			
		Robo	0,6		0,02			

Figura 148. Salvaguardas del activo HW14.
(Fuente propia)

- [COM] Redes de Comunicaciones:

Tratamiento del riesgo general de las Redes de Comunicaciones: Si bien se definió que los valores de riesgo mayores a 4 son graves, para este grupo de activos esa condición va a cambiar. Al conocer que la seguridad de las redes de comunicaciones es fundamental para la asociación, se considera que el nivel mínimo de riesgo es 1. Entonces, todas las salvaguardas irán orientadas a disminuir los riesgos hasta los niveles aceptados. Además, para las salvaguardas heredadas de la relación con otros activos solo se describen de manera general pues están desarrolladas en su correspondiente activo.

A continuación se definen las salvaguardas de todos los activos del grupo Redes de Comunicaciones y cuáles son los riesgos sobre los que actúan.

Salvaguardas COM1, COM2: 1) Por medio de estos activos los empleados tienen acceso a Internet, por lo que es fundamental establecer un control de acceso tanto a la red como a sus recursos. 2) Para complementar la salvaguarda anterior, hay que definir perfiles de seguridad para delimitar el acceso a la red y sus recursos. Dentro de esta salvaguarda también se considera la configuración de restricciones de navegación por internet, estableciendo listas blancas y configurando firewalls. 3) Estos activos heredan las salvaguardas referentes a la configuración de seguridad de los dispositivos de red. 4) Crear un manual de administración e incidencias para ayudar en futuras configuraciones y acciones de seguridad. 5) Periódicamente hay que realizar un análisis de vulnerabilidades pues son activos que están muy expuestos a ataques. 6) La

seguridad de estos activos depende de los empleados por lo que es necesario proveer manuales de uso y acceso a todo aquel que lo requiera. Esto puede incluir firmas de responsabilidad para asegurar su cumplimiento. 7) Para tener control sobre las redes locales, se debe crear un registro de direccionamiento IP de todos los dispositivos fijos conectados a la red. Adicionalmente, este registro debe actualizarse periódicamente. 8) Para tomar acciones de seguridad, se puede crear un registro de incidentes que sirva de referente.

En estos activos se observa un nivel alto de riesgo causados por la suplantación de la identidad del usuario y el acceso no autorizado. Se crearon entonces salvaguardas como configuración de seguridad y delimitación de perfiles de acceso. La Figura 149 muestra las salvaguardas para los riesgos de los activos COM1 y COM2.

REDES DE COMUNICACIONES [COM]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	2,1					• Controlar acceso • Definir perfiles de seguridad • Configuración de seguriad (dispositivo) • Manuales de administración e incidencias • Analisis de vulnerabilidades • Manuales de uso y acceso usuario • Registro de direccionamiento IP • Registro de Incidentes
		Errores De Administración	0,525	0,2	0,675			
		Alteración Accidental De La Información		1,2				
		Caída Del Sistema Por Agotamiento De Recursos	2,1					
		Suplantación De La Identidad Del Usuario		2,8	6,3	6,3		
		Abuso De Privilegios De Acceso	1,05	1,2	2,025			
		Uso No Previsto	1,05	0,6	2,025			
		Acceso No Autorizado		2	4,5			
		Análisis De Trafico			0,9			
		Interceptación De Información (Escucha)			0,9			
		Modificación Deliberada De La Información		1,8				
		Divulgación De Información			3,375			
		Denegación De Servicio	3,5					
COM2	Redes locales	Fallo Servicios De Comunicaciones	2,4					• Controlar acceso • Definir perfiles de seguridad • Configuración de seguriad (dispositivo) • Manuales de administración e incidencias IDS-IPS • Analisis de vulnerabilidades • Manuales de uso y acceso usuario • Registro de direccionamiento IP • Registro de Incidencias
		Errores De Administración	0,6	0,4	0,9			
		Alteración Accidental De La Información		1,2				
		Caída Del Sistema Por Agotamiento De Recursos	2,4					
		Suplantación De La Identidad Del Usuario		3	4,5	4,5		
		Abuso De Privilegios De Acceso	1,2	1,8	2,7			
		Uso No Previsto	1,2	1,2	2,7			
		Acceso No Autorizado		2	4,5			
		Análisis De Trafico			0,9			
		Interceptación De Información (Escucha)			0,9			
		Modificación Deliberada De La Información		1,8				
		Divulgación De Información			3,375			
		Denegación De Servicio	4					

Figura 149. Salvaguardas de los activos COM1 y COM2.
(Fuente propia)

Salvaguardas COM3, COM4: 1) Estos activos están relacionados con los móviles y teléfonos de sobremesa usados por los empleados, por lo que se deben crear manuales de buenas prácticas. 2) Para los administradores se debe crear manuales de gestión e incidencias para tomar acciones inmediatas en caso de tener problemas de seguridad. 3) La red de telefonía requiere de configuración de seguridad dentro del software y dispositivo. 4) Crear un registro telefónico de los empleados, socios, colaboradores y empresas externas. 5) Para futuras acciones de seguridad y retroalimentación se debe crear un registro de incidencias.

La mayoría de los riesgos son bajos, por lo que las salvaguardas están orientadas a crear buenas prácticas. La seguridad de la red de telefonía depende de la configuración y las redes locales.

Por otra parte la red de telefonía móvil la ofrece una empresa externa, por lo que la seguridad depende exclusivamente de dicha empresa. La Figura 150 muestra las salvaguardas para los riesgos de los activos COM3 y COM4.

COM3	Red telefónica	Fallo Servicios De Comunicaciones	2,4					• Manual de buenas prácticas para usuarios • Manuales de administración e incidencias • Configuraciones de seguridad • Registro telefónico de empleados • Registro de incidencias
		Errores De Administración	0,6	0,35	0,6			
		Alteración Accidental De La Información		1,05				
		Caída Del Sistema Por Agotamiento De Recursos	0,8					
		Abuso De Privilegios De Acceso	2	0,875	3			
		Uso No Previsto	2	0,875	3			
		Acceso No Autorizado		0,525	2,4			
		Análisis De Trafico			0,8			
		Interceptación De Información (Escucha)			0,8			
		Modificación Deliberada De La Información		0,35				
		Divulgación De Información			1,8			
		Denegación De Servicio	0,8					
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	2,4					• Manual de buenas prácticas para usuarios • Manuales de administración e incidencias • Registro telefónico de empleados • Registro de incidencias • Servicio exterior
		Caída Del Sistema Por Agotamiento De Recursos	0,6					
		Suplantación De La Identidad Del Usuario		0,035	0,6	0,525		
		Abuso De Privilegios De Acceso	0,12	0,105	1,2			
		Uso No Previsto	0,12	0,105	1,8			
		Acceso No Autorizado		0,105	1,8			
		Análisis De Trafico			0,8			
		Interceptación De Información (Escucha)			0,8			
		Divulgación De Información			2,4			

Figura 150. Salvaguardas de los activos COM3 y COM4.
(Fuente propia)

- [MEDIA] Soportes de Información

Tratamiento del riesgo general de los Soportes de Información: El nivel mínimo de riesgo para estos activos será 4, definido previamente en el tratamiento general de riesgo. En base a esta condición, se procura definir salvaguardas que logren disminuir los riesgos hasta el nivel requerido. En algunos casos las salvaguardas heredadas de otros activos solo se describen de manera general pues están desarrolladas en su correspondiente activo. A continuación se definen las salvaguardas de todos los activos del grupo Soportes de Información y cuáles son los riesgos sobre los que actúan.

Salvaguardas MEDIA1: 1) La información que se guarda en estos soportes son importantes para la asociación, por lo que requiere protección de acceso físico y lógico, además de encriptar aquellos ficheros confidenciales. 2) Como parte de la seguridad física, se debe asegurar su almacenamiento estableciendo ubicaciones adecuadas. 3) Para tener controlados este tipo de soportes se debe crear un registro de entrega, uso e incidencias. 4) Para todos quienes usen los soportes deben poseer un manual de uso, configuración de seguridad y almacenamiento. Incluyendo la creación de procesos de eliminación de la información y destrucción del soporte.

Los riesgos causados por las amenazas que afectan a estos soportes se mitigan con las salvaguardas de protección de acceso, encriptación y manuales de uso. La Figura 151 muestra las salvaguardas para los riesgos del activo MEDIA1.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
MEDIA1	Discos duros externos	Daños Por Agua	2,4					• Protección criptográfica y de acceso lógico y físico • Establecer ubicaciones adecuadas • Protección de acceso • Registro del dispositivo, uso e incidentes • Manual de uso del dispositivo
		Daños Por Agua	2,4					
		Avería De Origen Físico/Lógico	0,6					
		Degradación De Los Soportes De Almacenamiento De La Información	0,6					
		Errores De Usuarios	0,6	2,025	2,7			
		Errores De Administración	0,2	0,675	0,9			
		Alteración Accidental De La Información		2,025				
		Destrucción De Información	0,8					
		Fugas De Información			0,9			
		Errores De Mantenimiento del soporte	0,6					
		Perdida del soporte	0,8		0,9			
		Uso No Previsto	2,4	2,7	2,7			
		Acceso No Autorizado		2,7	2,7			
		Modificación Deliberada De La Información		0,9				
		Destrucción De Información	0,8					
		Divulgación De Información			0,9			
		Manipulación del soporte	1,2		2,7			
		Robo	0,8		0,9			

Figura 151. Salvaguardas del activo MEDIA 1.
(Fuente propia)

Salvaguardas MEDIA2: 1) Toda la información que se almacene en este tipo de soporte requiere de protección criptográfica y de acceso. 2) Casi todos los empleados usan estos soportes por ello hay que establecer un manual de uso del dispositivo. 3) Se debe registrar las entregas e incidencias para tener un control de estos activos. Estos registros pueden incluir firmas de responsabilidad para evitar un mal uso del soporte. 4) Parte de las buenas prácticas es establecer ubicaciones adecuadas de donde usar y almacenar estos activos. 5) Al ser dispositivos pequeños, existe una tendencia a perderlos, por ello se puede prevenir la pérdida de información haciendo copias de seguridad. 5) Aquellos soportes devueltos requieren de una limpieza de contenido, asegurando que se puede borrar la información y que no se pueda recuperarlos. 6) Establecer procesos formalizados de eliminación de la información y destrucción del soporte.

Para los valores altos de riesgos causados por: los errores de usuarios, alteración accidental de la información, pérdida del soporte y el uso no previsto se estableció las 4 primeras salvaguardas. El resto de las salvaguardas están orientadas a ser buenas prácticas de uso de estos soportes. La Figura 152 muestra las salvaguardas para los riesgos del activo MEDIA2.

MEDIA2	Pendrives USB	Daños Por Agua	0,7					• Protección criptográfica y de acceso lógico y físico • Manual de uso del dispositivo • Registro de la entrega e incidentes • Establecer ubicaciones adecuadas • Copias de seguridad de información crucial • Limpieza de contenidos • Destrucción de soportes
		Daños Por Agua	2,1					
		Avería De Origen Físico/Lógico	0,525					
		Degradación De Los Soportes De Almacenamiento De La Información	1,575					
		Errores De Usuarios	0,875	2	**4,5**			
		Errores De Administración	0,175	0,4	0,9			
		Alteración Accidental De La Información		**4**				
		Destrucción De Información	3,5					
		Fugas De Información			2,7			
		Errores De Mantenimiento del soporte	0,35					
		Perdida del soporte	**4,9**		**6,3**			
		Uso No Previsto	3,675	**5,6**	**6,3**			
		Acceso No Autorizado		0,8	0,9			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			2,7			
		Manipulación del soporte	0,525		0,9			
		Robo	2,1		2,7			

Figura 152. Salvaguardas del activo MEDIA2.
(Fuente propia)

Salvaguardas MEDIA3: 1) Resguardar la documentación que contiene el soporte mediante protección criptográfica y, el acceso lógico y físico. Si es necesario para abrir su contenido se debe establecer una contraseña. De igual manera hay que guardarlos en ubicaciones adecuadas. 2) Para todos los usuarios se debe crear un manual para su uso correcto. 3) La administración debe tener un control de estos soportes, por lo tanto se deben crear registros de entrega, destrucción e incidencias. 4) Estos soportes son muy sensibles, por lo que su almacenamiento debe ser adecuado. 5) Si la información que se almacena es importante se pueden crear copias de seguridad. 6) Por ser soportes de bajo uso y sensibles para el almacenamiento de información, hay que crear un programa de cambio de soporte de almacenamiento y destrucción.

El riesgo que tienen este tipo de soporte es alto, por eso se estableció la salvaguarda de cambio del soporte y si no es posible se establece métodos de protección. La Figura 153 muestra las salvaguardas para los riesgos del activo MEDIA3.

MEDIA3	CD/DVD	Daños Por Agua	0,7					• Protección criptográfica y acceso lógico y físico • Manual de uso del dispositivo • Registro de la entrega e incidentes • Establecer ubicaciones adecuadas • Copias de seguridad de información confidencial • Destrucción de soportes y cambio de almacenamiento de información
		Daños Por Agua	2,1					
		Avería De Origen Físico/Lógico	0,525					
		Degradación De Los Soportes De Almacenamiento De La Información	1,575					
		Errores De Usuarios	0,875	2	4,5			
		Errores De Administración	0,175	0,4	0,9			
		Alteración Accidental De La Información		4				
		Destrucción De Información	3,5					
		Fugas De Información			2,7			
		Errores De Mantenimiento del soporte	0,35					
		Perdida del soporte	4,9		6,3			
		Uso No Previsto	3,675	5,6	6,3			
		Acceso No Autorizado		0,8	0,9			
		Modificación Deliberada De La Información		0,8				
		Destrucción De Información	0,7					
		Divulgación De Información			2,7			
		Manipulación del soporte	0,525		0,9			
		Robo	2,1		2,7			

Figura 153. Salvaguardas del activo MEDIA3.
(Fuente propia)

Salvaguardas MEDIA4: 1) Todo el material impreso debe estar correctamente guardado y no exponerlo ante personas no autorizadas. Aquellos materiales impresos con carácter confidencial deben estar guardados con seguridad física. 2) Para salvaguardar la información confidencial, deben existir manuales que ofrezcan una guía de protección de documentos. 3) Como complemento a la anterior salvaguarda, se pueden crear registros de responsabilidad de los documentos confidenciales. 4) Para poder mejorar su protección de los documentos importantes impresos se pueden digitalizar. 5) Para evitar que se filtre información, cuando ya no se requiere la documentación debe pasar por un proceso formalizado de eliminación.

El nivel de riesgo más alto para el material impreso es la pérdida de la documentación, para ello se establecieron las salvaguardas de protección y sobre todo de digitalización. La Figura 154 muestra las salvaguardas para los riesgos del activo MEDIA4.

MEDIA4	Material impreso	Daños Por Agua	0,7					• Establecer ubicaciones adecuadas • Manual de uso de información confidencial, establecer respondables • Digitalización • Destrucción
		Daños Por Agua	0,7					
		Degradación por Almacenamiento	1,575					
		Errores De Usuarios	1,75	3	3,375			
		Errores De Administración	0,35	0,6	0,675			
		Alteración Accidental De La Información		2				
		Destrucción	3,5					
		Fugas De Información			0,9			
		Errores De Almacenamiento	1,75					
		Perdida	1,75		4,5			
		Uso No Previsto	2,1	1,8	2,7			
		Acceso No Autorizado		1,8	2,7			
		Modificación Deliberada De La Información		0,8				
		Destrucción	0,7					
		Divulgación			0,9			
		Manipulación	0,35		0,9			
		Robo	1,05		2,7			

Figura 154. Salvaguardas del activo MEDIA4.
(Fuente propia)

- [AUX] Equipamiento Auxiliar

Tratamiento del riesgo general del Equipamiento Auxiliar: El nivel mínimo de riesgo para estos activos será 4, definido previamente en el tratamiento general de riesgo. Determinada esta condición se procura definir salvaguardas que logren disminuir los riesgos hasta el nivel requerido. En algunos casos las salvaguardas heredadas de otros activos solo se describen de manera general pues están desarrolladas en su correspondiente activo. A continuación, se definen las salvaguardas de todos los activos del grupo Equipamiento Auxiliar y cuáles son los riesgos sobre los que actúan.

Salvaguardas AUX1, AUX2, AUX3, AUX4: 1) Estos activos son auxiliares del hardware y deben estar siempre disponibles, por ello hay que establecer y señalizar ubicaciones adecuadas. Esta salvaguarda no aplica para el activo AUX4, pues es una red fija en las instalaciones de la asociación. 2) Para todos los activos se debe realizar un mantenimiento periódico por parte del personal técnico para evitar fallas. 3) Todos los cambios, mantenimientos e incidencias deben estar debidamente registrados para tener un control de uso y responsabilidades.

Casi todos los riesgos son menores, pero se han creado salvaguardas básicas para el mantenimiento y control de incidencias. Las Figuras 155 y 156 muestran las salvaguardas para los riesgos de los activos AUX1, AUX2, AUX3, AUX4.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Riesgo					Salvaguardas
Código	Nombre	Amenaza	D	I	C	A	T	
AUX1	Generador eléctrico	Daños Por Agua	1,125					• Establecer y señalizar ubicaciones adecuadas • Mantenimiento periódico, uso exclusivo del personal técnico • Registro de uso, cambios e incidentes
		Fuego	0,375					
		Daños Por Agua	1,125					
		Contaminación Mecánica	0,25					
		Degradación por almacenamiento	0,75					
		Avería De Origen Físico/ Lógico	1,125					
		Errores De Mantenimiento/ Actualización De Equipos	0,375					
		Uso No Previsto	1,125	0,375	0,045			
		Acceso No Autorizado		0,375	0,045			
		Manipulación De Equipos	1,125		0,045			

Figura 155. Salvaguardas del activo AUX1.
(Fuente propia)

AUX2	Fuentes de alimentación	Daños Por Agua	1,125					• Registro del equipo, uso, cambios e incidentes • Establecer ubicaciones adecuadas • Mantenimiento periódico, uso exclusivo del personal técnico
		Fuego	0,375					
		Daños Por Agua	1,125					
		Contaminación Mecánica	0,25					
		Degradación por almacenamiento	0,75					
		Avería De Origen Físico/ Lógico	1,125					
		Corte De Suministro Eléctrico	1,5					
		Errores De Mantenimiento/ Actualización De Equipos	1,125					
		Perdida De Equipos	0,5		0,015			
		Uso No Previsto	1,5	0,525	0,045			
		Acceso No Autorizado		0,525	0,045			
		Manipulación De Equipos	1,125		0,045			
		Robo	0,5		0,015			
AUX3	Climatización	Daños Por Agua	1,125					• Mantenimiento periódico • Establecer ubicaciones adecuadas • Registro de Incidentes
		Fuego	0,375					
		Daños Por Agua	1,125					
		Contaminación Mecánica	0,25					
		Avería De Origen Físico/Lógico	1,125					
		Corte De Suministro Eléctrico	1,5					
		Errores De Mantenimiento/Actualización De Equipos	1,125					
		Uso No Previsto	0,75	0,3	0,045			
		Acceso No Autorizado		0,3	0,045			
		Manipulación De Equipos	1,25		0,075			
AUX4	Cableado UTP	Daños Por Agua	1,575					• Mantenimiento periódico • uso exclusivo del personal técnico • Registro de uso, cambios e incidentes
		Fuego	0,7					
		Daños Por Agua	1,575					
		Avería De Origen Físico/Lógico	1,575					
		Errores De Mantenimiento/Actualización De Equipos	1,575					
		Uso No Previsto	1,05	0,6	0,3			
		Acceso No Autorizado		0,2	0,3			
		Manipulación De Equipos	0,35		0,3			

Figura 156. Salvaguardas de los activos AUX2, AUX3 y AUX4.
(Fuente propia)

Salvaguardas AUX5: 1) Todos los armarios que almacenen equipos informáticos deben tener protección física para evitar acceso no autorizado. 2) Es importante realizar un mantenimiento periódico para evitar dañar los dispositivos que están en su interior. El mantenimiento y manipulación de los armarios lo debe hacer solo el personal técnico. 3) Todo acceso, cambio o incidencia con los armarios debe ser registrado para definir responsabilidades y tomar acciones de seguridad. 4) Las ubicaciones de los armarios deben estar de acuerdo con las necesidades de la asociación y evitando exponer los dispositivos informáticos.

El mayor riesgo es producido por los ataques de uso no previsto y acceso no autorizado por lo que la salvaguarda de protección física es esencial para este activo. La Figura 157 muestra las salvaguardas para los riesgos del activo AUX5.

AUX5	Armarios	Daños Por Agua	1,2					• Protección física • Mantenimiento periodico, uso exclusivo del personal técnico • Resgistro de uso, cambios e incidentes • Establecer ubicaciones adecuadas
		Fuego	0,6					
		Daños Por Agua	1,2					
		Degradación por almacenamiento	0,2					
		Avería De Origen Físico/Lógico	1,2					
		Uso No Previsto	0,6	0,6	1,8			
		Acceso No Autorizado		0,6	1,8			
		Manipulación De Equipos	1		3			

Figura 157. Salvaguardas del activo AUX5.
(Fuente propia)

Salvaguardas AUX6: 1) Este activo es un equipamiento auxiliar confidencial de uso exclusivo de personal autorizado, por lo que se puede formalizar procesos de uso. 2) Parte de la protección

de este equipamiento es controlar quien accede, por lo tanto establecer responsabilidades. 3) Como complemento, deben tener ubicaciones adecuadas para no exponerlo a personas no autorizadas. 4) Para que no sufran de fallos, se deben realizar mantenimientos periódicos. 5) Finalmente, se debe registrar los cambios importantes que se realicen en el equipamiento.

El mayor riesgo tiene la confidencialidad a causa de la manipulación de equipos, por esto se establecieron las dos primeras salvaguardas. La Figura 158 muestra las salvaguardas para los riesgos del activo AUX6.

AUX6	Cajas fuertes	Daños Por Agua	0,2					• Uso exclusivo de personal autorizado, protección de acceso y física • Establecer ubicaciones adecuadas • Mantenimiento periódico • Registro de Incidentes
		Fuego	0,2					
		Daños Por Agua	0,2					
		Avería De Origen Físico/Lógico	0,6					
		Corte De Suministro Eléctrico	0,6					
		Errores De Mantenimiento/Actualización De Equipos	1,8					
		Perdida De Equipos	0,8		0,9			
		Uso No Previsto	0,6	0,04	0,9			
		Acceso No Autorizado		0,12	2,7			
		Manipulación De Equipos	1		4,5			

Figura 158. Salvaguardas del activo AUX6.
(Fuente propia)

- [L]Instalaciones

Tratamiento del riesgo general de las Instalaciones: El nivel mínimo de riesgo para estos activos será 4, definido previamente en el tratamiento general de riesgo. Determinada esta condición se procura definir salvaguardas que logren disminuir los riesgos hasta el nivel requerido. En algunos casos las salvaguardas heredadas de otros activos solo se describen de manera general pues están desarrolladas en su correspondiente activo.

A continuación se definen las salvaguardas de todos los activos del grupo Instalaciones y cuáles son los riesgos sobre los que actúan.

Salvaguardas L1: 1) Todos los edificios de la asociación deben estar con protección física y poseer un registro de las personas y la razón de su acceso. 2) En todos los edificios se deben señalizar los puntos informáticos vulnerables y otros para información de los empleados. 3) Para aquellas personas que vayan a permanecer por un largo periodo de tiempo, se debe entregar manuales de uso de las instalaciones para no vulnerar la confidencialidad de los usuarios y la asociación.

El riesgo más importante es el acceso no autorizado, por lo que la salvaguardas deben ir orientadas a controlar quienes acceden a las instalaciones. La Figura 159 muestra las salvaguardas para los riesgos del activo L1.

ACTIVOS DE INSTALACIONES [L]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
L1	Edificios	Fuego	0,6					• Control de los accesos físicos • Determinación y señalización de puntos vulnerables a daños físicos • Establecer manuales de uso de las instalaciones • Registro de Incidentes
		Daños Por Agua	1,35					
		Fuego	0,45					
		Daños Por Agua	0,9					
		Fugas De Información			1,8			
		Uso No Previsto	0,15	0,175	0,6			
		Acceso No Autorizado		0,525	2,4			

Figura 159. Salvaguardas del activo L1.
(Fuente propia)

Salvaguardas L2: 1) Los cuartos de los servidores necesitan protección física en la puerta y cámaras de seguridad. 2) Se deben establecer quienes acceden a los cuartos y el motivo, para definir responsabilidades en caso de incidentes. 3) Como complemento de la anterior salvaguarda, todo aquel que acceda a los cuartos de servidores debe tener un manual de uso de las instalaciones. 4) Realizar una evaluación física de los cuartos, señalizando los puntos de mayor vulnerabilidad. 5) Se debe llevar un registro de incidentes para definir responsabilidades y tomar acciones.

Los mayores riesgos se pueden evitar realizando una evaluación física de los cuartos y protegerlos del acceso no autorizado. La Figura 160 muestra las salvaguardas para los riesgos del activo L2.

L2	Cuartos servidores	Fuego	0,8					• Protección física • Control de los accesos físicos • Establecer manuales de uso de las instalaciones • Determinación y señalización de puntos vulnerables a daños físicos • Registro de Incidentes
		Daños Por Agua	0,8					
		Fuego	0,8					
		Daños Por Agua	2,4					
		Fugas De Información			0,8			
		Uso No Previsto	1,8	1,8	1,8			
		Acceso No Autorizado		1,2	2,4			

Figura 160. Salvaguardas del activo L2.
(Fuente propia)

Salvaguardas L3: Como se observa en la Figura 161, los riesgos para este activo son menores y por lo tanto son asumibles; razón por la que no se definen salvaguardas.

L3	Coche	Daños mecánicos	0,2					• Riesgos asumibles
		Accidente de tránsito	0,2					

Figura 161. Riesgo asumido del activo L3.
(Fuente propia)

- [P] Personal

Tratamiento del riesgo general del Personal: El nivel mínimo de riesgo para estos activos será 4, definido previamente en el tratamiento general de riesgo. Determinada esta condición se

procura definir salvaguardas que logren disminuir los riesgos hasta el nivel requerido. En algunos casos las salvaguardas heredadas de otros activos se describen de manera general pues están desarrolladas en su correspondiente activo. A continuación, se definen las salvaguardas de todos los activos del grupo Personal y cuáles son los riesgos sobre los que actúan.

Salvaguardas P1: 1) Es esencial que los administradores del departamento TIC reciban una capacitación anual para actualizar sus conocimientos en ciberseguridad e implementarlos en la asociación. 2) Para cubrir la ausencia de uno de los administradores es necesario actualizar manuales o guías para el control de las actividades esenciales de la asociación.

El riesgo más alto ocurre por la indisponibilidad del personal, para lo cual se define la salvaguarda de actualizar manuales y guías. Entonces, si sucede un incidente y uno de los administradores falta se pueden tomar acciones inmediatas sin requerir del empleado faltante. Ayuda además a mantener formalizados todos los procesos dentro del departamento TIC. La Figura 162 muestra las salvaguardas para los riesgos del activo P1.

ACTIVOS DE PERSONAL [P]			Riesgo					Salvaguardas
Código	Nombre	Amenazas	D	I	C	A	T	
P1	Administradores	Fugas De Información			0,9			• Capacitación del personal • Actualizar manuales o guías
		Indisponibilidad Del Personal	1,8					
		Indisponibilidad Del Personal	0,6					
		Extorsión	0,2	0,6	0,9			
		Ingeniería Social	0,2	0,6	0,9			

Figura 162. Salvaguardas del activo P1.
(Fuente propia)

Salvaguardas P2, P3, P4: 1) Los usuarios y empleados deben tener mínimo una capacitación anual de concienciación de la seguridad de la asociación. 2) Mantener actualizado los manuales y guías que usen los usuarios disminuye los errores y sirven de referencia para otros empleados o usuarios. 3) En la capacitación de seguridad informática, también se debe crear conciencia de que la seguridad de la asociación depende de todos.

El riesgo más alto es la indisponibilidad del personal, por lo que en el caso de los empleados y técnicos su ausencia no debe causar problemas en el sistema informático de la asociación. Las Figuras 163 y 164 muestran las salvaguardas para los riesgos de los activos P2, P3 y P4.

P2	Técnicos	Fugas De Información			0,9			• Capacitación del personal • Actualizar manuales o guías • Concientización
		Indisponibilidad Del Personal	1,05					
		Indisponibilidad Del Personal	0,35					
		Extorsión	0,175	0,4	0,9			
		Ingeniería Social	0,175	0,4	0,9			

Figura 163. Salvaguardas del activo P2.
(Fuente propia)

P3	**Empleados**	Fugas De Información			0,9			• Capacitación del personal • Actualizar manuales o guías • Concientización
		Indisponibilidad Del Personal	1,05					
		Indisponibilidad Del Personal	0,35					
		Extorsión	0,175	0,4	0,9			
		Ingeniería Social	0,175	0,4	0,9			
P4	**Usuarios**	Fugas De Información			2,7			• Capacitación del personal • Actualizar manuales o guías • Concientización
		Extorsión	0,125	0,3	0,9			
		Ingeniería Social	0,125	0,3	0,9			

Figura 164. Salvaguardas de los activos P3 y P4.
(Fuente propia)

4.5.2. Cálculos de Impacto Residual

Después de establecer las salvaguardas, el grado de degradación de las amenazas sobre los activos disminuye. Para cada activo la situación es distinta. Las salvaguardas que logran ser muy eficaces disminuyen considerablemente el grado de degradación en algunas de las dimensiones de seguridad. Otras salvaguardas aunque ayudan en todas las dimensiones de seguridad, el grado de degradación no tiene una disminución considerable.

Antes del cálculo del impacto residual, se define la eficacia de las salvaguardas sobre los riesgos de un activo. La eficacia se mide en porcentaje con valores de 0% como mínimo y del 100% como máximo. Se procede entonces al cálculo del nuevo impacto denominado impacto residual, con la fórmula:

$$IR = IP * (1 - ES)$$

Donde:

IR = Impacto residual

IP = Impacto potencial

ES = Eficacia de las salvaguardas en una dimensión de seguridad (%)

Según la fórmula anterior, para el cálculo del impacto residual se requiere del impacto determinado anteriormente. El resultado y análisis del impacto residual se puede ver a continuación.

- [D] Datos /Información

Para este grupo de activos las salvaguardas tienen un porcentaje alto de efectividad del 75% al 100%. Existen unas pocas salvaguardas con efectividad menor del 50% y se hacen más evidentes en la integridad de las copias de seguridad. Los resultados de la efectividad de las salvaguardas

repercuten directamente sobre el impacto residual, causando una disminución considerable en el valor del impacto exceptuando los casos en los que la efectividad es baja. Existen casos en los que las salvaguardas no tienen efectividad sobre una dimensión de seguridad, por lo que su impacto se mantiene y estos casos son: en las copias de seguridad los errores o ataques de destrucción y fugas de información. En otras ocasiones el valor de impacto residual no existe debido a que la efectividad de las salvaguardas es del 100%, y esto se presenta principalmente en la dimensión de confidencialidad. Las Figuras 165 a la 167 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

DATOS / INFORMACIÓN [D]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
D1	Datos de configuración	Errores De Administración	6	6	2			75%	75%	75%			1,5	1,5	0,5		
		Errores De Configuración		4					75%					1			
		Alteración Accidental De La Información		4					75%					1			
		Destrucción De Información	8					75%					2				
		Fugas De Información			4					75%					1		
		Manipulación De Los Registros De Actividad		0,4			6,75		25%			50%		0,3			3,375
		Manipulación De La Configuración		8	8	9			75%	100%	75%			2		2,25	
		Abuso De Privilegios De Acceso	6	6	6			75%	75%	100%			1,5	1,5			
		Acceso No Autorizado		6	8				75%	100%				1,5			
		Repudio		6			9		75%			50%		1,5			4,5
		Modificación Deliberada De La Información		8					75%					2			
		Destrucción De Información	8					75%					2				
D2	Código fuente de aplicaciones	Errores De Administración	4	6,75	2			75%	75%	75%			1	1,688	0,5		
		Errores De Configuración		6,75					75%					1,688			
		Alteración Accidental De La Información		9					75%					2,25			
		Manipulación De Los Registros De Actividad		0,45			6,75		25%			50%		0,338			3,375
		Manipulación De La Configuración		6,75	4	4,5			75%	100%	75%			1,688		1,125	
		Abuso De Privilegios De Acceso	2	6,75	6			75%	75%	100%			0,5	1,688			
		Acceso No Autorizado		9	8				75%	100%				2,25			
		Repudio		6,75			9		75%			50%		1,688			4,5
		Modificación Deliberada De La Información		9					75%					2,25			
		Destrucción De Información	8					75%					2				
D3	Ficheros almacenados en PC	Errores De Usuarios	2,25	5,25	2,5			75%	50%	50%			0,563	2,625	1,25		
		Errores De Administración	2,25	5,25	2,5			75%	75%	50%			0,563	1,313	1,25		
		Errores De Configuración		1,75					75%					0,438			
		Alteración Accidental De La Información		5,25					50%					2,625			
		Destrucción De Información	3					75%					0,75				
		Fugas De Información			1,25					75%					0,313		
		Manipulación De Los Registros De Actividad		1,75			3,5					50%		1,75			1,75
		Manipulación De La Configuración		3,5	2,5	1,5			70%	75%	25%			1,05	0,625	1,125	
		Suplantación De La Identidad Del Usuario		3,5	3,75	4,5			70%	75%	25%			1,05	0,938	3,375	
		Abuso De Privilegios De Acceso	0,75	3,5	3,75			75%	70%	75%			0,188	1,05	0,938		
		Acceso No Autorizado		5,25	5				70%	75%				1,575	1,25		
		Repudio		1,75			7		70%			50%		0,525			3,5
		Modificación Deliberada De La Información		7					70%					2,1			
		Destrucción De Información	2,25					75%					0,563				
D4	Ficheros almacenados en servidores en la nube	Errores De Usuarios	2,5	3,5	0,35			75%	50%	50%			0,625	1,75	0,175		
		Errores De Administración	3,75	5,25	3,5			75%	75%	90%			0,938	1,313	0,35		
		Errores De Monitorización Log		3,5			6		75%			75%		0,875			1,5
		Errores De Configuración		3,5					75%					0,875			
		Alteración Accidental De La Información		5,25					75%					1,313			
		Destrucción De Información	3,75					75%					0,938				
		Manipulación De Los Registros De Actividad		1,75			6		75%			75%		0,438			1,5
		Manipulación De La Configuración		1,75	3,5	4			75%	90%	50%			0,438	0,35	2	
		Suplantación De La Identidad Del Usuario		1,75	5,25	6			75%	90%	50%			0,438	0,525	3	
		Abuso De Privilegios De Acceso	1,25	1,75	5,25			75%	75%	90%			0,313	0,438	0,525		
		Acceso No Autorizado		3,5	7				75%	90%				0,875	0,7		
		Repudio		1,75			8		90%			90%		0,175			0,8
		Modificación Deliberada De La Información		7					75%					1,75			
		Destrucción De Información	5					75%					1,25				
D5	Ficheros almacenados en servidores locales	Errores De Usuarios	3,75	3,5	0,35			75%	50%	50%			0,938	1,75	0,175		
		Errores De Administración	3,75	5,25	3,5			75%	75%	80%			0,938	1,313	0,7		
		Errores De Monitorización Log		3,5			6		75%			75%		0,875			1,5
		Errores De Configuración		3,5					75%					0,875			
		Alteración Accidental De La Información		5,25					75%					1,313			
		Destrucción De Información	3,75					75%					0,938				
		Manipulación De Los Registros De Actividad		1,75			6		75%			75%		0,438			1,5
		Manipulación De La Configuración		1,75	3,5	4			75%	80%	50%			0,438	0,7	2	
		Suplantación De La Identidad Del Usuario		1,75	5,25	6			75%	80%	50%			0,438	1,05	3	
		Abuso De Privilegios De Acceso	1,25	1,75	5,25			75%	75%	80%			0,313	0,438	1,05		
		Acceso No Autorizado		3,5	7				75%	80%				0,875	1,4		
		Repudio		1,75			8		90%			90%		0,175			0,8
		Modificación Deliberada De La Información		7					75%					1,75			
		Destrucción De Información	5					75%					1,25				

Figura 165. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (a) (Fuente propia)

D6	Bases de datos en servidores locales	Errores De Administración	6	6,75	4,5			90%	90%	100%			0,6	0,675				
		Errores De Monitorización Log		6,75			6,75		90%			100%		0,675				
		Errores De Configuración		6,75					90%					0,675				
		Alteración Accidental De La Información		6,75					90%					0,675				
		Destrucción De Información	8					90%					0,8					
		Manipulación De Los Registros De Actividad		4,5			9		90%			100%		0,45				
		Manipulación De La Configuración		4,5	6,75	4,5			90%	100%	80%			0,45		0,9		
		Suplantación De La Identidad Del Usuario		4,5	9	6,75			90%	100%	80%			0,45		1,35		
		Abuso De Privilegios De Acceso	6	4,5	6,75			90%	90%	100%			0,6	0,45				
		Acceso No Autorizado		6,75	9				90%	100%				0,675				
		Repudio		4,5			9		90%			100%		0,45				
		Modificación Deliberada De La Información		9					90%					0,9				
		Destrucción De Información	8					90%					0,8					
D7	Bases de datos en servidores en la nube	Errores De Administración	6,75	6,75	4,5			90%	90%	100%			0,675	0,675				
		Errores De Monitorización Log		6,75			6,75		90%			100%		0,675				
		Errores De Configuración		6,75					90%					0,675				
		Alteración Accidental De La Información		6,75					90%					0,675				
		Destrucción De Información	9					90%					0,9					
		Manipulación De Los Registros De Actividad		4,5			9		90%			100%		0,45				
		Manipulación De La Configuración		4,5	6,75	4,5			90%	100%	80%			0,45		0,9		
		Suplantación De La Identidad Del Usuario		4,5	9	6,75			90%	100%	80%			0,45		1,35		
		Abuso De Privilegios De Acceso	6,75	4,5	6,75			90%	90%	100%			0,675	0,45				
		Acceso No Autorizado		6,75	9				90%	100%				0,675				
		Repudio		4,5			9		90%			100%		0,45				
		Modificación Deliberada De La Información		9					90%					0,9				
		Destrucción De Información	9					90%					0,9					
D8	Copias de seguridad en la nube	Errores De Administración	6,75	6	4,5			80%	90%	90%			1,35	0,6	0,45			
		Errores De Monitorización Log		4			4,5		90%			50%		0,4				2,25
		Errores De Configuración		8					75%					2				
		Alteración Accidental De La Información		8					75%					2				
		Destrucción De Información	9					50%					4,5					
		Manipulación De Los Registros De Actividad		2			6,75		75%			75%		0,5				1,688
		Manipulación De La Configuración		6	6,75	6,75			75%	90%	75%			1,5	0,675	1,688		
		Suplantación De La Identidad Del Usuario		4	9	6,75			75%	90%	75%			1	0,9	1,688		
		Abuso De Privilegios De Acceso	4,5	6	9			75%	75%	90%			1,125	1,5	0,9			
		Acceso No Autorizado		6	9				75%	90%				1,5	0,9			
		Repudio		4			9		75%			75%		1				2,25
		Modificación Deliberada De La Información		8					75%					2				
		Destrucción De Información	9					50%					4,5					
		Divulgación De Información			9					90%					0,9			
D9	Copias de Seguridad en servidores locales	Errores De Administración	6	6	4,5			80%	75%	90%			1,2	1,5	0,45			
		Errores De Monitorización Log		4			4,5		75%			50%		1				2,25
		Errores De Configuración		8					75%					2				
		Alteración Accidental De La Información		8					75%					2				
		Destrucción De Información	8										8					
		Fugas De Información			6,75				25%			75%			6,75			
		Manipulación De La Configuración		6	6,75	6,75			25%	90%	75%			4,5	0,675	1,688		
		Suplantación De La Identidad Del Usuario		4	9	6,75			25%	90%	75%			3	0,9	1,688		
		Abuso De Privilegios De Acceso	4	6	9			50%	25%	90%			2	4,5	0,9			
		Acceso No Autorizado		6	9				25%	90%				4,5	0,9			
		Repudio		4			9		25%			75%		3				2,25
		Modificación Deliberada De La Información		8					25%					6				
		Destrucción De Información	8										8					
		Divulgación De Información			9					90%					0,9			
D10	Copias de Seguridad en discos externos	Errores De Administración	5,25	6	4,5			80%	75%	90%			1,05	1,5	0,45			
		Errores De Monitorización Log		4			4,5		50%			50%		2				2,25
		Errores De Configuración		8					75%					2				
		Alteración Accidental De La Información		8					75%					2				
		Destrucción De Información	7										7					
		Manipulación De Los Registros De Actividad		2			6,75		25%			75%		1,5				1,688
		Manipulación De La Configuración		6	6,75	6,75			25%	90%	75%			4,5	0,675	1,688		
		Suplantación De La Identidad Del Usuario		4	9	6,75			25%	90%	75%			3	0,9	1,688		
		Abuso De Privilegios De Acceso	3,5	6	9			50%	25%	90%			1,75	4,5	0,9			
		Acceso No Autorizado		6	9				25%	90%				4,5	0,9			
		Repudio		4			9		25%			75%		3				2,25
		Modificación Deliberada De La Información		8					25%					6				
		Destrucción De Información	7										7					
		Divulgación De Información			9					90%					0,9			
D11	Ficheros de contraseñas	Errores De Administración	6,75	6,75	9			50%	75%	100%			3,375	1,688				
		Errores De Configuración		0,45					75%					0,113				
		Alteración Accidental De La Información		6,75					75%					1,688				
		Destrucción De Información	9					75%					2,25					
		Manipulación De Los Registros De Actividad		2,25			9		75%			75%		0,563				2,25
		Suplantación De La Identidad Del Usuario		4,5	9	4,5			75%	100%	50%			1,125		2,25		
		Abuso De Privilegios De Acceso	2,25	4,5	6,75			25%	75%	100%			1,688	1,125				
		Acceso No Autorizado		6,75	9				75%	100%				1,688				
		Repudio		2,25			9		75%			75%		0,563				2,25
		Modificación Deliberada De La Información		9					75%					2,25				
		Destrucción De Información	9					75%					2,25					
		Divulgación De Información			9					75%					2,25			

Figura 166. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (b) (Fuente propia)

D12	Registros de actividades en servidores	Errores De Administración	6	4	4			75%	75%	80%			1,5	1	0,8			
		Errores De Configuración		6					75%					1,5				
		Destrucción De Información	6					75%					1,5					
		Manipulación De La Configuración		6	4	6,75			75%	80%	90%			1,5	0,8	0,675		
		Suplantación De La Identidad Del Usuario		6	8	4,5			75%	80%	90%			1,5	1,6	0,45		
		Abuso De Privilegios De Acceso	6	4	4			75%	50%	80%			1,5	2	0,8			
		Acceso No Autorizado		6	8				75%	80%				1,5	1,6			
		Repudio		4			9		75%			75%		1				2,25
		Modificación Deliberada De La Información		8					75%					2				
		Destrucción De Información	8					75%					2					
D13	Ficheros compartidos Google Drive	Errores De Administración	5,25	4	4			75%	90%	90%			1,313	0,4	0,4			
		Errores De Configuración		2					90%					0,2				
		Alteración Accidental De La Información		6					90%					0,6				
		Destrucción De Información	5,25					75%					1,313					
		Manipulación De La Configuración		4	4	3,5			90%	90%	50%			0,4	0,4	1,75		
		Suplantación De La Identidad Del Usuario		6	8	3,5			90%	90%	50%			0,6	0,8	1,75		
		Abuso De Privilegios De Acceso	3,5	4	4			75%	90%	90%			0,875	0,4	0,4			
		Acceso No Autorizado		6	8				90%	90%				0,6	0,8			
		Repudio		2			7		90%			100%		0,2				
		Modificación Deliberada De La Información		8					90%					0,8				
		Destrucción De Información	7					75%					1,75					
		Divulgación De Información			8					90%					0,8			

Figura 167. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (c) (Fuente propia)

- [S] Servicios

Para los servicios la mayoría de las salvaguardas tienen un 50% de efectividad. Los mayores porcentajes de efectividad de las salvaguardas (mayores a 75%) se presentan en las dimensiones de confidencialidad, autenticidad y trazabilidad. La reducción de los valores de impacto es inversamente proporcional a la efectividad de las salvaguardas. Para este grupo de activos no existe una eficacia de salvaguardas del 100%, pero todas tienen eficacia aunque sea un valor pequeño. Las Figuras 168 a la 170 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

SERVICIOS [S]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
S1	Página web	Errores De Usuarios	0,35	0,4	2			75%	50%	80%			0,088	0,2	0,4		
		Errores De Administración	7	6	6			75%	75%	80%			1,75	1,5	1,2		
		Alteración Accidental De La Información		6					75%					1,5			
		Fugas De Información			4					80%					0,8		
		Caída Del Sistema Por Agotamiento De Recursos	7					75%					1,75				
		Suplantación De La Identidad Del Usuario		6	6	5			75%	80%	80%			1,5	1,2	1	
		Abuso De Privilegios De Acceso	3,5	6	6			75%	75%	80%			0,875	1,5	1,2		
		Uso No Previsto	3,5	6	6			75%	75%	80%			0,875	1,5	1,2		
		Acceso No Autorizado		8	6				75%	80%				2	1,2		
		Repudio		4			5,25		75%			90%		1			0,525
		Modificación Deliberada De La Información		8					75%					2			
		Destrucción De Información	5,25					75%					1,313				
		Divulgación De Información			8					80%					1,6		
		Denegación De Servicio	7					50%					3,5				
S2	Correo electrónico	Errores De Usuarios	3,5	2	4			50%	25%	50%			1,75	1,5	2		
		Errores De Administración	5,25	2	6			50%	25%	50%			2,625	1,5	3		
		Alteración Accidental De La Información		4					50%					2			
		Fugas De Información			6					50%					3		
		Caída Del Sistema Por Agotamiento De Recursos	7					50%					3,5				
		Suplantación De La Identidad Del Usuario		4	6	5,25			50%	50%	75%			2	3	1,313	
		Abuso De Privilegios De Acceso	3,5	6	6			50%	75%	50%			1,75	1,5	3		
		Uso No Previsto	5,25	6	6			50%	75%	50%			2,625	1,5	3		
		Acceso No Autorizado		6	8				75%	75%				1,5	2		
		Repudio		4			6		50%			75%		2			1,5
		Modificación Deliberada De La Información		6					75%					1,5			
		Divulgación De Información			6					50%					3		
		Denegación De Servicio	7					50%					3,5				

Figura 168. Efectividad de las salvaguardas e impacto residual del grupo Servicios. (a) (Fuente propia)

S3	Intranet documental - Servicio FTP	Errores De Usuarios	0,4	4	4			25%	25%	75%			0,3	3	1		
		Errores De Administración	6	6	4			25%	25%	75%			4,5	4,5	1		
		Alteración Accidental De La Información		6					50%					3			
		Destrucción De Información	6					50%					3				
		Fugas De Información			6					75%					1,5		
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Suplantación De La Identidad Del Usuario		4	6	4			50%	75%	75%			2	1,5	1	
		Abuso De Privilegios De Acceso	2	4	6			50%	50%	75%			1	2	1,5		
		Uso No Previsto	4	4	6			50%	50%	75%			2	2	1,5		
		Acceso No Autorizado		4	8				50%	75%				2	2		
		Repudio		2			6		25%			75%		1,5			1,5
		Modificación Deliberada De La Información		6					50%					3			
		Destrucción De Información	8					50%					4				
		Divulgación De Información			6					75%					1,5		
		Denegación De Servicio	8					50%					4				
S4	Sistema de tickets de incidencias	Errores De Usuarios	0,2	1,5	1,5			0,25	25%	75%			0,15	1,125	0,375		
		Errores De Administración	3	3	1,5			25%	25%	75%			2,25	2,25	0,375		
		Alteración Accidental De La Información		3					50%					1,5			
		Caída Del Sistema Por Agotamiento De Recursos	4					50%					2				
		Suplantación De La Identidad Del Usuario		3	4,5	4			50%	75%	75%			1,5	1,125	1	
		Acceso No Autorizado		4,5	4,5				50%	75%				2,25	1,125		
		Repudio		3			3,75		25%			75%		2,25			0,938
		Modificación Deliberada De La Información		3					50%					1,5			
		Divulgación De Información			3					75%					0,75		
		Denegación De Servicio	4					50%					2				
S5	Educación Virtual	Errores De Usuarios	0,4	2	3,5			25%	25%	75%			0,3	1,5	0,875		
		Errores De Administración	6	4	3,5			25%	25%	75%			4,5	3	0,875		
		Alteración Accidental De La Información		6					50%					3			
		Destrucción De Información	8					50%					4				
		Fugas De Información			3,5					75%					0,875		
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Suplantación De La Identidad Del Usuario		2	5,25	3			50%	75%	75%			1	1,313	0,75	
		Abuso De Privilegios De Acceso	2	6	3,5			50%	50%	75%			1	3	0,875		
		Uso No Previsto	4	2	3,5			50%	50%	75%			2	1	0,875		
		Acceso No Autorizado		6	5,25				50%	75%				3	1,313		
		Repudio		2			5,25		50%			75%		1			1,313
		Modificación Deliberada De La Información		6					50%					3			
		Divulgación De Información			3,5					75%					0,875		
		Denegación De Servicio	8					50%					4				
S6	Servicio de financiero	Errores De Usuarios	2	6,75	9			25%	25%	75%			1,5	5,063	2,25		
		Errores De Administración	6	4,5	6,75			25%	25%	75%			4,5	3,375	1,688		
		Alteración Accidental De La Información		9					50%					4,5			
		Destrucción De Información	6					50%					3				
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Suplantación De La Identidad Del Usuario		6,75	9	6,75			50%	75%	75%			3,375	2,25	1,688	
		Abuso De Privilegios De Acceso	2	6,75	6,75			50%	50%	75%			1	3,375	1,688		
		Uso No Previsto	4	4,5	4,5			50%	50%	75%			2	2,25	1,125		
		Acceso No Autorizado		9	9				50%	75%				4,5	2,25		
		Repudio		4,5			9		50%			75%		2,25			2,25
		Modificación Deliberada De La Información		9					50%					4,5			
		Destrucción De Información	8					50%					4				
		Divulgación De Información			9					75%					2,25		
		Denegación De Servicio	8					50%					4				
S7	Gestión de usuarios Socios	Errores De Usuarios	2	6	4			25%	25%	75%			1,5	4,5	1		
		Errores De Administración	6	4	6			25%	25%	75%			4,5	3	1,5		
		Alteración Accidental De La Información		6					50%					3			
		Destrucción De Información	6					50%					3				
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Suplantación De La Identidad Del Usuario		6	8	3,5			50%	75%	75%			3	2	0,875	
		Abuso De Privilegios De Acceso	2	4	4			50%	50%	75%			1	2	1		
		Uso No Previsto	4	2	6			50%	50%	75%			2	1	1,5		
		Acceso No Autorizado		6	8				50%	75%				3	2		
		Repudio		2			8		50%			75%		1			2
		Modificación Deliberada De La Información		8					50%					4			
		Destrucción De Información	8					50%					4				
		Divulgación De Información			8					75%					2		
		Denegación De Servicio	8					50%					4				
S8	Gestión empresarial	Errores De Usuarios	1,75	4	4			25%	50%	50%			1,313	2	2		
		Errores De Administración	3,5	4	4			25%	50%	50%			2,625	2	2		
		Alteración Accidental De La Información		6					50%					3			
		Destrucción De Información	5,25					50%					2,625				
		Caída Del Sistema Por Agotamiento De Recursos	5,25					50%					2,625				
		Suplantación De La Identidad Del Usuario		4	6	3,5			50%	50%	50%			2	3	1,75	
		Abuso De Privilegios De Acceso	1,75	4	4			50%	50%	50%			0,875	2	2		
		Uso No Previsto	1,75	4	6			50%	50%	50%			0,875	2	3		
		Acceso No Autorizado		6	8				50%	50%				3	4		
		Repudio		4			8		50%			75%		2			2
		Modificación Deliberada De La Información		6					50%					3			
		Destrucción De Información	7					50%					3,5				
		Divulgación De Información			8					50%					4		
		Denegación De Servicio	7					50%					3,5				

Figura 169. Efectividad de las salvaguardas e impacto residual del grupo Servicios. (b)
(Fuente propia)

S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	1,75	4	6			25%	25%	75%			1,313	3	1,5		
		Errores De Administración	3,5	4	6			25%	25%	75%			2,625	3	1,5		
		Alteración Accidental De La Información		6					50%					3			
		Destrucción De Información	5,25					50%					2,625				
		Caída Del Sistema Por Agotamiento De Recursos	7					50%					3,5				
		Suplantación De La Identidad Del Usuario		6	8	4			50%	75%	75%			3	2	1	
		Abuso De Privilegios De Acceso	1,75	4	6			50%	50%	75%			0,875	2	1,5		
		Uso No Previsto	1,75	4	6			50%	50%	75%			0,875	2	1,5		
		Acceso No Autorizado		6	8				50%	75%				3	2		
		Repudio		4			9		50%			75%		2			2,25
		Modificación Deliberada De La Información		8					50%					4			
		Destrucción De Información	7					50%					3,5				
		Divulgación De Información			8					75%					2		
		Denegación De Servicio	7					50%					3,5				

Figura 170. Efectividad de las salvaguardas e impacto residual del grupo Servicios. (c) (Fuente propia)

- [SW] Software – Aplicaciones Informáticas

Para este grupo de activos casi todas las salvaguardas tienen una efectividad del 50%. La mayor efectividad se observa en las dimensiones de confidencialidad y autenticidad. En los activos: aplicación de correo electrónico, E-apsa, aplicaciones, sistemas operativos Windows, navegadores web y software ofimático, se ve una efectividad del 5%, pues las salvaguardas tienen un efecto mínimo sobre los riesgos. En base a los resultados, se observa que el valor del impacto residual es inversamente proporcional a la efectividad de las salvaguardas, reduciendo el valor original de impacto. En estos activos no se presentan casos en los que las salvaguardas no tienen efectividad sobre una dimensión de seguridad. En ciertos casos el valor de impacto residual no existe debido a que la efectividad de las salvaguardas es del 100%, y esto se presenta en: difusión de software dañino en los navegadores web y, suplantación de identidad de usuario en la gestión de bases de datos y la aplicación de página web. Las Figuras 171 a la 174 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Impacto					Efectividade de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
SW1	Aplicación de Financiero	Fallo De Origen Lógico	6,75					50%					3,375				
		Errores De Usuarios	2,25	6,75	4,5			25%	50%	50%			1,688	3,375	2,25		
		Errores De Administración	6,75	4,5	4,5			50%	25%	50%			3,375	3,375	2,25		
		Alteración Accidental De La Información		6,75					50%					3,375			
		Destrucción De Información	9					75%					2,25				
		Fugas De Información			9					50%					4,5		
		Vulnerabilidades De Los Programas	4,5	6,75	9			25%	50%	50%			3,375	3,375	4,5		
		Errores De Mantenimiento/Actualización De Programas	4,5	6,75				50%	50%				2,25	3,375			
		Suplantación De La Identidad Del Usuario		6,75	9	6,75			50%	75%	75%			3,375	2,25	1,688	
		Abuso De Privilegios De Acceso	4,5	6,75	9			50%	50%	75%			2,25	3,375	2,25		
		Uso No Previsto	6,75	4,5	4,5			50%	25%	75%			3,375	3,375	1,125		
		Difusión De Software Dañino	9	9	9			50%	50%	75%			4,5	4,5	2,25		
		Acceso No Autorizado		6,75	9				50%	75%				3,375	2,25		
		Modificación Deliberada De La Información		9					50%					4,5			
		Destrucción De Información	4,5					50%					2,25				
		Divulgación De Información			9					75%					2,25		

Figura 171. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (a) (Fuente propia)

SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	6					50%					3						
		Errores De Usuarios	4	6	4			25%	50%	50%			3	3	2				
		Errores De Administración	6	4	4			50%	25%	50%			3	3	2				
		Alteración Accidental De La Información		6					50%					3					
		Destrucción De Información	8					75%					2						
		Fugas De Información			8					50%					4				
		Vulnerabilidades De Los Programas	4	6	8			25%	50%	50%			3	3	4				
		Errores De Mantenimiento/Actualización De Programas	4	6				50%	50%				2	3					
		Suplantación De La Identidad Del Usuario		6	8	6,75			50%	75%	75%			3	2	1,688			
		Abuso De Privilegios De Acceso	4	6	8			50%	50%	75%			2	3	2				
		Uso No Previsto	4	4	4			50%	25%	75%			2	3	1				
		Difusión De Software Dañino	8	8	8			50%	50%	75%			4	4	2				
		Acceso No Autorizado		6	8				50%	75%				3	2				
		Modificación Deliberada De La Información		8					50%					4					
		Destrucción De Información	4					50%					2						
		Divulgación De Información			8					75%					2				
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	5,25					50%					2,625						
		Errores De Usuarios	3,5	6	4			25%	50%	50%			2,625	3	2				
		Errores De Administración	5,25	4	4			50%	25%	50%			2,625	3	2				
		Alteración Accidental De La Información		6					50%					3					
		Destrucción De Información	7					75%					1,75						
		Fugas De Información			8					50%					4				
		Vulnerabilidades De Los Programas	3,5	6	8			25%	50%	50%			2,625	3	4				
		Errores De Mantenimiento/Actualización De Programas	3,5	6				50%	50%				1,75	3					
		Suplantación De La Identidad Del Usuario		6	8	6,75			50%	75%	75%			3	2	1,688			
		Abuso De Privilegios De Acceso	3,5	6	8			50%	50%	75%			1,75	3	2				
		Uso No Previsto	3,5	4	4			50%	25%	75%			1,75	3	1				
		Difusión De Software Dañino	7	8	8			50%	50%	75%			3,5	4	2				
		Acceso No Autorizado		6	8				50%	75%				3	2				
		Modificación Deliberada De La Información		8					50%					4					
		Destrucción De Información	3,5					50%					1,75						
		Divulgación De Información			8					75%					2				
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	5,25					50%					2,625						
		Errores De Usuarios	3,5	6	4			25%	50%	50%			2,625	3	2				
		Errores De Administración	5,25	4	4			50%	25%	50%			2,625	3	2				
		Alteración Accidental De La Información		6					50%					3					
		Destrucción De Información	7					75%					1,75						
		Fugas De Información			8					50%					4				
		Vulnerabilidades De Los Programas	3,5	6	8			25%	50%	50%			2,625	3	4				
		Errores De Mantenimiento/Actualización De Programas	3,5	6				50%	50%				1,75	3					
		Suplantación De La Identidad Del Usuario		6	8	6,75			50%	75%	75%			3	2	1,688			
		Abuso De Privilegios De Acceso	3,5	6	8			50%	50%	75%			1,75	3	2				
		Uso No Previsto	3,5	4	4			50%	25%	75%			1,75	3	1				
		Difusión De Software Dañino	7	8	8			50%	50%	75%			3,5	4	2				
		Acceso No Autorizado		6	8				50%	75%				3	2				
		Modificación Deliberada De La Información		8					50%					4					
		Destrucción De Información	3,5					50%					1,75						
		Divulgación De Información			8					75%					2				
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	6					75%					1,5						
		Errores De Administración	6	6,75	4,5			50%	50%	50%			3	3,375	2,25				
		Alteración Accidental De La Información		9					50%					4,5					
		Destrucción De Información	8					50%					4						
		Fugas De Información			9					50%					4,5				
		Vulnerabilidades De Los Programas	4	6,75	9			50%	50%	50%			2	3,375	4,5				
		Errores De Mantenimiento/Actualización De Programas	4	9				50%	50%				2	4,5					
		Suplantación De La Identidad Del Usuario		9	9	9			50%	50%	100%			4,5	4,5				
		Abuso De Privilegios De Acceso	6	9	9			50%	50%	50%			3	4,5	4,5				
		Uso No Previsto	6	6,75	9			50%	50%	50%			3	3,375	4,5				
		Difusión De Software Dañino	8	9	9			75%	50%	50%			2	4,5	4,5				
		Acceso No Autorizado		9	9				50%	50%				4,5	4,5				
		Modificación Deliberada De La Información		9					50%					4,5					
		Destrucción De Información	8					75%					2						
		Divulgación De Información			9					50%					4,5				
SW6	Aplicación de Página web	Fallo De Origen Lógico	5,25					75%					1,313						
		Errores De Usuarios	1,75	2	2			25%	25%	25%			1,313	1,5	1,5				
		Errores De Administración	5,25	4	6			50%	50%	50%			2,625	2	3				
		Alteración Accidental De La Información		6					50%					3					
		Destrucción De Información	5,25					50%					2,625						
		Fugas De Información			4					50%					2				
		Vulnerabilidades De Los Programas	5,25	6	6			50%	50%	50%			2,625	3	3				
		Errores De Mantenimiento/Actualización De Programas	3,5	6				50%	50%				1,75	3					
		Suplantación De La Identidad Del Usuario		4	8	9			50%	50%	100%			2	4				
		Abuso De Privilegios De Acceso	3,5	6	8			50%	50%	50%			1,75	3	4				
		Uso No Previsto	3,5	4	8			50%	50%	50%			1,75	2	4				
		Difusión De Software Dañino	3,5	4	8			50%	50%	50%			1,75	2	4				
		Acceso No Autorizado		6	8				50%	50%				3	4				
		Modificación Deliberada De La Información		6					50%					3					
		Destrucción De Información	3,5					50%					1,75						
		Divulgación De Información			6					50%					3				
		Manipulación De Programas	3,5	6	6			50%	75%	50%			1,75	1,5	3				
SW7	Aplicación de Intranet	Fallo De Origen Lógico	6					50%					3						
		Errores De Usuarios	4	6	4			25%	50%	50%			3	3	2				
		Errores De Administración	6	4	4			50%	25%	50%			3	3	2				
		Alteración Accidental De La Información		6					50%					3					
		Destrucción De Información	8					75%					2						
		Fugas De Información			8					50%					4				
		Vulnerabilidades De Los Programas	4	6	8			25%	50%	50%			3	3	4				
		Errores De Mantenimiento/Actualización De Programas	4	6				50%	50%				2	3					
		Suplantación De La Identidad Del Usuario		6	8	6,75			50%	75%	75%			3	2	1,688			
		Abuso De Privilegios De Acceso	4	6	8			50%	50%	75%			2	3	2				
		Uso No Previsto	4	4	4			50%	25%	75%			2	3	1				
		Difusión De Software Dañino	8	8	8			50%	50%	75%			4	4	2				
		Acceso No Autorizado		6	8				50%	75%				3	2				
		Modificación Deliberada De La Información		6					50%					3					
		Destrucción De Información	4					50%					2						
		Divulgación De Información			8					75%					2				

Figura 172. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (b) (Fuente propia)

SW8	Aplicación del Sistema de tickets de incidencias	Fallo De Origen Lógico	3					50%					1,5					
		Errores De Usuarios	2	4,5	3			25%	50%	50%			1,5	2,25	1,5			
		Errores De Administración	3	3	3			50%	25%	50%			1,5	2,25	1,5			
		Alteración Accidental De La Información		4,5					50%					2,25				
		Destrucción De Información	4					75%					1					
		Fugas De Información			6					50%					3			
		Vulnerabilidades De Los Programas	2	4,5	6			25%	50%	50%			1,5	2,25	3			
		Errores De Mantenimiento/Actualización De Programas	2	4,5				50%	50%				1	2,25				
		Suplantación De La Identidad Del Usuario		4,5	6	6,75			50%	75%	75%			2,25	1,5	1,688		
		Abuso De Privilegios De Acceso	2	4,5	6			50%	50%	75%			1	2,25	1,5			
		Uso No Previsto	2	3	3			50%	25%	75%			1	2,25	0,75			
		Difusión De Software Dañino	4	6	6			50%	50%	75%			2	3	1,5			
		Acceso No Autorizado		4,5	6				50%	75%				2,25	1,5			
		Modificación Deliberada De La Información		6					50%					3				
		Destrucción De Información	2					50%					1					
		Divulgación De Información			6					75%					1,5			
SW9	Aplicación de Correo electrónico Gmail	Errores De Usuarios	0,35	0,4	2			5%	5%	25%			0,333	0,38	1,5			
		Errores De Administración	1,75	0,4	4			25%	5%	50%			1,313	0,38	2			
		Difusión De Software Dañino	0,35	0,4	8			5%	5%	50%			0,333	0,38	4			
		Alteración Accidental De La Información		0,4					5%					0,38				
		Destrucción De Información	1,75					25%					1,313					
		Fugas De Información			8					50%					4			
		Vulnerabilidades De Los Programas	0,35	4	8			5%	50%	50%			0,333	2	4			
		Errores De Mantenimiento/Actualización De Programas	1,75	4	6			25%	50%	50%			1,313	2	3			
		Suplantación De La Identidad Del Usuario		4	8	9			50%	50%	75%			2	4	2,25		
		Abuso De Privilegios De Acceso	0,35	6	6			5%	75%	50%			0,333	1,5	3			
		Uso No Previsto	3,5	6	8			50%	75%	50%			1,75	1,5	4			
		Difusión De Software Dañino	0,35	4	8			5%	50%	50%			0,333	2	4			
		Acceso No Autorizado		4	8				50%	50%				2	4			
		Modificación Deliberada De La Información		8					50%					4				
		Destrucción De Información	7					75%					1,75					
		Divulgación De Información			8					50%					4			
SW10	E-apsa	Fallo De Origen Lógico	6					75%					1,5					
		Errores De Usuarios	0,4	0,4	1,75			5%	5%	25%			0,38	0,38	1,313			
		Errores De Administración	4	4	5,25			50%	25%	50%			2	3	2,625			
		Alteración Accidental De La Información		2					25%					1,5				
		Destrucción De Información	0,4					5%					0,38					
		Fugas De Información			1,75					25%					1,313			
		Vulnerabilidades De Los Programas	0,4	2	3,5			5%	25%	50%			0,38	1,5	1,75			
		Errores De Mantenimiento/Actualización De Programas	2	2				25%	25%				1,5	1,5				
		Suplantación De La Identidad Del Usuario		2	5,25	8			25%	75%	75%			1,5	1,313	2		
		Abuso De Privilegios De Acceso	0,4	2	5,25			5%	25%	75%			0,38	1,5	1,313			
		Uso No Previsto	2	0,4	3,5			25%	5%	50%			1,5	0,38	1,75			
		Difusión De Software Dañino	0,4	2	3,5			5%	25%	50%			0,38	1,5	1,75			
		Acceso No Autorizado		2	7				25%	75%				1,5	1,75			
		Modificación Deliberada De La Información		2					25%					1,5				
		Destrucción De Información	6					75%					1,5					
		Divulgación De Información			5,25					75%					1,313			
SW11	Aplicaciones en móviles	Fallo De Origen Lógico	2					50%					1					
		Errores De Usuarios	0,2	2	3,5			5%	25%	50%			0,19	1,5	1,75			
		Errores De Administración	1	2	3,5			25%	25%	50%			0,75	1,5	1,75			
		Difusión De Software Dañino	0,2	2	5,25			5%	25%	50%			0,19	1,5	2,625			
		Alteración Accidental De La Información		2					25%					1,5				
		Destrucción De Información	1					25%					0,75					
		Fugas De Información			5,25					50%					2,625			
		Vulnerabilidades De Los Programas	1	2	5,25			25%	25%	50%			0,75	1,5	2,625			
		Errores De Mantenimiento/Actualización De Programas	2	2				50%	25%				1	1,5				
		Suplantación De La Identidad Del Usuario		2	5,25	6			25%	50%	50%			1,5	2,625	3		
		Abuso De Privilegios De Acceso	1	6	5,25			25%	75%	50%			0,75	1,5	2,625			
		Uso No Previsto	3	4	5,25			50%	50%	50%			1,5	2	2,625			
		Difusión De Software Dañino	3	4	7			75%	50%	50%			0,75	2	3,5			
		Acceso No Autorizado		2	7				25%	50%				1,5	3,5			
		Modificación Deliberada De La Información		2					25%					1,5				
		Destrucción De Información	2					50%					1					
		Divulgación De Información			7					50%					3,5			
SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	6,75					50%					3,375					
		Errores De Administración	9	6,75	9			75%	50%	75%			2,25	3,375	2,25			
		Alteración Accidental De La Información		6,75					50%					3,375				
		Destrucción De Información	9					75%					2,25					
		Vulnerabilidades De Los Programas	6,75	6,75	9			75%	50%	75%			1,688	3,375	2,25			
		Errores De Mantenimiento/Actualización De Programas	6,75	6,75				75%	50%				1,688	3,375				
		Suplantación De La Identidad Del Usuario		6,75	9	9			50%	75%	90%			3,375	2,25	0,9		
		Abuso De Privilegios De Acceso	4,5	6,75	9			50%	50%	75%			2,25	3,375	2,25			
		Uso No Previsto	4,5	6,75	9			50%	50%	75%			2,25	3,375	2,25			
		Difusión De Software Dañino	9	9	9			50%	75%	75%			4,5	2,25	2,25			
		Acceso No Autorizado		9	9				75%	75%				2,25	2,25			
		Modificación Deliberada De La Información		9					75%					2,25				
		Destrucción De Información	9					75%					2,25					
		Divulgación De Información			9					75%					2,25			
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	6,75					50%					3,375					
		Errores De Administración	9	6,75	9			75%	50%	75%			2,25	3,375	2,25			
		Alteración Accidental De La Información		6,75					50%					3,375				
		Destrucción De Información	9					75%					2,25					
		Vulnerabilidades De Los Programas	6,75	6,75	9			75%	50%	75%			1,688	3,375	2,25			
		Errores De Mantenimiento/Actualización De Programas	6,75	6,75				75%	50%				1,688	3,375				
		Suplantación De La Identidad Del Usuario		6,75	9	9			50%	75%	75%			3,375	2,25	2,25		
		Abuso De Privilegios De Acceso	4,5	6,75	9			50%	50%	75%			2,25	3,375	2,25			
		Uso No Previsto	4,5	6,75	9			50%	50%	75%			2,25	3,375	2,25			
		Difusión De Software Dañino	9	9	9			50%	75%	75%			4,5	2,25	2,25			
		Acceso No Autorizado		9	9				75%	75%				2,25	2,25			
		Modificación Deliberada De La Información		9					75%					2,25				
		Destrucción De Información	9					75%					2,25					
		Divulgación De Información			9					75%					2,25			

Figura 173. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (c) (Fuente propia)

SW14	Sistema operativo Windows 7	Fallo De Origen Lógico	4					25%					3						
		Errores De Usuarios	1	0,45	1,25			25%	5%	25%			0,75	0,428	0,938				
		Errores De Administración	2	2,25	2,5			50%	25%	25%			1	1,688	1,875				
		Difusión De Software Dañino	3	4,5	3,75			75%	25%	50%			0,75	3,375	1,875				
		Alteración Accidental De La Información		6,75					75%					1,688					
		Destrucción De Información	4					50%					2						
		Vulnerabilidades De Los Programas	1	2,25	5			25%	25%	50%			0,75	1,688	2,5				
		Errores De Mantenimiento/Actualización De Programas	1	2,25				25%	25%				0,75	1,688					
		Suplantación De La Identidad Del Usuario		0,45	5	8			5%	75%	75%			0,428	1,25	2			
		Abuso De Privilegios De Acceso	0,2	0,45	3,75			5%	5%	75%			0,19	0,428	0,938				
		Uso No Previsto	1	2,25	5			25%	25%	75%			0,75	1,688	1,25				
		Difusión De Software Dañino	3	6,75	5			75%	75%	75%			0,75	1,688	1,25				
		Acceso No Autorizado		2,25	5				25%	75%				1,688	1,25				
		Modificación Deliberada De La Información		6,75					75%					1,688					
		Destrucción De Información	4					25%					3						
		Divulgación De Información			5					75%					1,25				
SW15	Sistema operativo Windows 10	Fallo De Origen Lógico	4					25%					3						
		Errores De Usuarios	1	0,45	1,25			25%	5%	25%			0,75	0,428	0,938				
		Errores De Administración	2	2,25	2,5			50%	25%	25%			1	1,688	1,875				
		Difusión De Software Dañino	3	4,5	3,75			75%	25%	50%			0,75	3,375	1,875				
		Alteración Accidental De La Información		6,75					75%					1,688					
		Destrucción De Información	4					50%					2						
		Vulnerabilidades De Los Programas	1	2,25	5			25%	25%	50%			0,75	1,688	2,5				
		Errores De Mantenimiento/Actualización De Programas	1	2,25				25%	25%				0,75	1,688					
		Suplantación De La Identidad Del Usuario		0,45	5	8			5%	75%	75%			0,428	1,25	2			
		Abuso De Privilegios De Acceso	0,2	0,45	3,75			5%	5%	75%			0,19	0,428	0,938				
		Uso No Previsto	1	2,25	5			25%	25%	75%			0,75	1,688	1,25				
		Difusión De Software Dañino	3	6,75	5			75%	75%	75%			0,75	1,688	1,25				
		Acceso No Autorizado		2,25	5				25%	75%				1,688	1,25				
		Modificación Deliberada De La Información		6,75					75%					1,688					
		Destrucción De Información	4					25%					3						
		Divulgación De Información			5					75%					1,25				
SW16	Navegadores Web	Errores De Usuarios	0,2	0,4	6			5%	5%	50%			0,19	0,38	3				
		Errores De Administración	1	0,4	6			25%	5%	50%			0,75	0,38	3				
		Fugas De Información			8					50%					4				
		Vulnerabilidades De Los Programas	1	4	8			25%	50%	50%			0,75	2	4				
		Errores De Mantenimiento/Actualización De Programas	0,2	4				5%	50%				0,19	2					
		Abuso De Privilegios De Acceso	0,2	0,4	6			5%	5%	50%			0,19	0,38	3				
		Uso No Previsto	0,2	2	6			5%	25%	50%			0,19	1,5	3				
		Difusión De Software Dañino	0,2	2	8			5%	25%	100%			0,19	1,5					
		Modificación Deliberada De La Información		2					25%					1,5					
		Destrucción De Información	1					25%					0,75						
		Divulgación De Información			2					25%					1,5				
SW17	Antivirus	Fallo De Origen Lógico	6					50%					3						
		Errores De Administración	4	2	1,25			25%	25%	25%			3	1,5	0,938				
		Errores De Mantenimiento/Actualización De Programas	2	8				25%	50%				1,5	4					
		Abuso De Privilegios De Acceso	4	8	1,25			50%	50%	25%			2	4	0,938				
		Uso No Previsto	4	8	1,25			50%	50%	25%			2	4	0,938				
		Acceso No Autorizado		8	1,25				50%	25%				4	0,938				
		Modificación Deliberada De La Información		8					50%					4					
SW18	Software Ofimático	Fallo De Origen Lógico	1,5					50%					0,75						
		Errores De Usuarios	1,5	0,25	1,25			50%	5%	25%			0,75	0,238	0,938				
		Errores De Administración	1,5	0,25	1,25			50%	5%	25%			0,75	0,238	0,938				
		Errores De Mantenimiento/Actualización De Programas	2,25	1,25				75%	25%				0,563	0,938					
		Abuso De Privilegios De Acceso	0,75	1,25	1,25			25%	25%	25%			0,563	0,938	0,938				
		Uso No Previsto	1,5	1,25	1,25			50%	25%	25%			0,75	0,938	0,938				

Figura 174. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (d) (Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Para los equipos informáticos las salvaguardas tienen en su mayoría una efectividad del 50% o menor. En la dimensión de confidencialidad se observan la mayor cantidad de efectividad del 75%. Los resultados de la efectividad de las salvaguardas repercuten directamente sobre el impacto residual, causando una disminución del valor del impacto aunque sea mínima. Existen casos en los que las salvaguardas no tienen efectividad sobre una dimensión de seguridad, por lo que su impacto se mantiene y se presenta generalmente en la dimensión de disponibilidad. Este grupo de activos no presenta salvaguardas con un 100% de efectividad. Las Figuras 175 y 176 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

EQUIPOS INFORMÁTICOS [HW]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
HW1	Servidores APSA	Avería De Origen Físico/Lógico	9										9				
		Errores De Administración	9	9	9			50%	50%	75%			4,5	4,5	2,25		
		Errores De Mantenimiento/Actualización De Equipos	6,75					50%					3,375				
		Caída Del Sistema Por Agotamiento De Recursos	9					55%					4,05				
		Abuso De Privilegios De Acceso	6,75	6,75	9			50%	50%	75%			3,375	3,375	2,25		
		Uso No Previsto	6,75	6,75	9			50%	50%	75%			3,375	3,375	2,25		
		Acceso No Autorizado		6,75	9				50%	75%				3,375	2,25		
		Denegación De Servicio	9					50%					4,5				
HW2	Servidores Sedes	Daños Por Agua	8					75%					2				
		Avería De Origen Físico/Lógico	8					75%					2				
		Corte De Suministro Eléctrico	8					50%					4				
		Fallas De Climatización	2					50%					1				
		Errores De Administración	6	6	9			75%	50%	75%			1,5	3	2,25		
		Errores De Mantenimiento/Actualización De Equipos	6					75%					1,5				
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Abuso De Privilegios De Acceso	6	6	9			75%	50%	75%			1,5	3	2,25		
		Uso No Previsto	4	4	9			50%	50%	75%			2	2	2,25		
		Acceso No Autorizado		6	9				50%	75%				3	2,25		
		Manipulación De Equipos	6		6,75			50%		75%			3		1,688		
		Denegación De Servicio	8					50%					4				
		Robo	8		6,75			75%		75%			2		1,688		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	5,25					25%					3,938				
		Avería De Origen Físico/Lógico	7					25%					5,25				
		Corte De Suministro Eléctrico	7										7				
		Errores De Administración	3,5	4	6			25%	75%	75%			2,625	1	1,5		
		Errores De Mantenimiento/Actualización De Equipos	3,5					25%					2,625				
		Caída Del Sistema Por Agotamiento De Recursos	5,25					50%					2,625				
		Perdida De Equipos	7		8			25%		25%			5,25		6		
		Abuso De Privilegios De Acceso	3,5	4	8			50%	25%	50%			1,75	3	4		
		Uso No Previsto	5,25	2	8			25%	25%	50%			3,938	1,5	4		
		Acceso No Autorizado		2	8				25%	50%				1,5	4		
		Manipulación De Equipos	3,5		8			25%		75%			2,625		2		
		Robo	7		8			25%		25%			5,25		6		
HW4	Ordenadores de escritorio empleados	Daños Por Agua	2,25					50%					1,125				
		Avería De Origen Físico/Lógico	3					50%					1,5				
		Corte De Suministro Eléctrico	3										3				
		Errores De Administración	1,5	3,5	5,25			50%	10%	50%			0,75	3,15	2,625		
		Errores De Mantenimiento/Actualización De Equipos	1,5					50%					0,75				
		Caída Del Sistema Por Agotamiento De Recursos	2,25					50%					1,125				
		Perdida De Equipos	3		5,25			50%		25%			1,5		3,938		
		Abuso De Privilegios De Acceso	1,5	3,5	5,25			50%	10%	25%			0,75	3,15	3,938		
		Uso No Previsto	2,25	1,75	5,25			50%	10%	50%			1,125	1,575	2,625		
		Acceso No Autorizado		1,75	5,25				10%	25%				1,575	3,938		
		Manipulación De Equipos	1,5		5,25			50%		50%			0,75		2,625		
		Robo	3		7			50%		25%			1,5		5,25		
HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	7										7				
		Corte De Suministro Eléctrico	1,75					10%					1,575				
		Errores De Administración	3,5	2	8			25%	25%	50%			2,625	1,5	4		
		Errores De Mantenimiento/Actualización De Equipos	3,5					25%					2,625				
		Caída Del Sistema Por Agotamiento De Recursos	5,25					50%					2,625				
		Perdida De Equipos	7		8			10%		50%			6,3		4		
		Abuso De Privilegios De Acceso	1,75	2	8			25%	25%	50%			1,313	1,5	4		
		Uso No Previsto	3,5	2	8			25%	75%	50%			2,625	0,5	4		
		Acceso No Autorizado		6	8				25%	50%				4,5	4		
		Manipulación De Equipos	5,25		8			25%		50%			3,938		4		
		Robo	7		8			10%		50%			6,3		4		
HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	3										3				
		Corte De Suministro Eléctrico	0,75										0,75				
		Errores De Administración	1,5	1,75	1,75			25%	25%	75%			1,125	1,313	0,438		
		Errores De Mantenimiento/Actualización De Equipos	1,5					25%					1,125				
		Caída Del Sistema Por Agotamiento De Recursos	2,25					50%					1,125				
		Perdida De Equipos	3		5,25			25%		50%			2,25		2,625		
		Abuso De Privilegios De Acceso	0,75	1,75	5,25			25%	25%	50%			0,563	1,313	2,625		
		Uso No Previsto	1,5	1,75	5,25			25%	75%	50%			1,125	0,438	2,625		
		Acceso No Autorizado		3,5	5,25				25%	50%				2,625	2,625		
		Manipulación De Equipos	1,5		5,25			25%		50%			1,125		2,625		
		Robo	3		7			25%		50%			2,25		3,5		
HW7	Portátiles TIC	Daños Por Agua	8										8				
		Avería De Origen Físico/Lógico	8					10%					7,2				
		Corte De Suministro Eléctrico	6					50%					3				
		Errores De Administración	4	6,75	9			25%	75%	75%			3	1,688	2,25		
		Errores De Mantenimiento/Actualización De Equipos	6					25%					4,5				
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Abuso De Privilegios De Acceso	4	6,75	9			25%	25%	75%			3	5,063	2,25		
		Acceso No Autorizado		6,75	9				25%	75%				5,063	2,25		
		Manipulación De Equipos	4		9			25%		75%			3		2,25		

Figura 175. Efectividad de las salvaguardas e impacto residual del grupo Equipos informáticos. (a) (Fuente propia)

HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	3					25%					2,25					
		Errores De Administración	1	1,75	3,5			50%	25%	50%			0,5	1,313	1,75			
		Errores De Mantenimiento/Actualización De Equipos	3					25%					2,25					
		Caída Del Sistema Por Agotamiento De Recursos	2					50%					1					
		Perdida De Equipos	4		7					50%			4		3,5			
		Abuso De Privilegios De Acceso	2	3,5	7				25%	50%			2	2,625	3,5			
		Uso No Previsto	2	3,5	7				25%	50%			2	2,625	3,5			
		Acceso No Autorizado		5,25	7				25%	50%				3,938	3,5			
		Manipulación De Equipos	3		7			10%		50%			2,7		3,5			
		Robo	4		7					50%			4		3,5			
HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	3					75%					0,75					
		Corte De Suministro Eléctrico	3										3					
		Errores De Administración	1,5	1	0,15			50%	25%				0,75	0,75	0,15			
		Errores De Mantenimiento/Actualización De Equipos	1,5					50%					0,75					
		Caída Del Sistema Por Agotamiento De Recursos	2,25					50%					1,125					
		Perdida De Equipos	3		0,75								3		0,75			
		Abuso De Privilegios De Acceso	1,5	0,5	0,15			10%	25%	10%			1,35	0,375	0,135			
		Uso No Previsto	0,75	0,5	0,75			10%	25%	10%			0,675	0,375	0,675			
		Acceso No Autorizado		0,5	0,75				25%	10%				0,375	0,675			
		Manipulación De Equipos	1,5		0,75			10%		10%			1,35		0,675			
		Robo	3		0,75								3		0,75			
HW10	Router	Avería De Origen Físico/Lógico	8					25%					6					
		Corte De Suministro Eléctrico	8										8					
		Fallas De Climatización	4					10%					3,6					
		Errores De Administración	6	4	8			25%	50%	50%			4,5	2	4			
		Errores De Mantenimiento/Actualización De Equipos	6					25%					4,5					
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4					
		Abuso De Privilegios De Acceso	6	4	8			25%	50%	50%			4,5	2	4			
		Uso No Previsto	6	4	8				50%	50%			6	2	4			
		Acceso No Autorizado		6	8				50%	50%				3	4			
		Manipulación De Equipos	6		8			25%		50%			4,5		4			
		Denegación De Servicio	8										8					
HW11	Router inalámbrico	Daños Por Agua	8										8					
		Avería De Origen Físico/Lógico	6					25%					4,5					
		Corte De Suministro Eléctrico	8										8					
		Errores De Administración	6	4	8			25%	50%	50%			4,5	2	4			
		Errores De Mantenimiento/Actualización De Equipos	6					25%					4,5					
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4					
		Perdida De Equipos	8		4					50%			8		2			
		Abuso De Privilegios De Acceso	4	4	6			25%	50%	50%			3	2	3			
		Uso No Previsto	6	6	6				50%	50%			6	3	3			
		Acceso No Autorizado		6	8				50%	50%				3	4			
		Manipulación De Equipos	6		4			25%		50%			4,5		2			
		Denegación De Servicio	8										8					
		Robo	8		4					50%			8		2			
HW12	Switch	Avería De Origen Físico/Lógico	8					25%					6					
		Corte De Suministro Eléctrico	8										8					
		Fallas De Climatización	4					10%					3,6					
		Errores De Administración	6	4	8			25%	50%	50%			4,5	2	4			
		Errores De Mantenimiento/Actualización De Equipos	6					25%					4,5					
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4					
		Abuso De Privilegios De Acceso	6	4	8			25%	50%	50%			4,5	2	4			
		Uso No Previsto	6	4	8				50%	50%			6	2	4			
		Acceso No Autorizado		6	8				50%	50%				3	4			
		Manipulación De Equipos	6		8			25%		50%			4,5		4			
		Denegación De Servicio	8										8					
HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	8					25%					6					
		Corte De Suministro Eléctrico	8										8					
		Errores De Administración	6	1,25	2			50%	10%	25%			3	1,125	1,5			
		Errores De Mantenimiento/Actualización De Equipos	6					50%					3					
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4					
		Abuso De Privilegios De Acceso	4	2,5	1			25%	10%	25%			3	2,25	0,75			
		Uso No Previsto	6	2,5	1				25%	25%			6	1,875	0,75			
		Acceso No Autorizado		2,5	1				10%	25%				2,25	0,75			
		Manipulación De Equipos	6		1			25%		25%			4,5		0,75			
HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	6					25%					4,5					
		Corte De Suministro Eléctrico	6										6					
		Errores De Administración	3	1,25	2			50%	10%	25%			1,5	1,125	1,5			
		Errores De Mantenimiento/Actualización De Equipos	4,5					50%					2,25					
		Abuso De Privilegios De Acceso	3	1,25	3			25%	10%	25%			2,25	1,125	2,25			
		Uso No Previsto	4,5	1,25	3				25%	25%			4,5	0,938	2,25			
		Acceso No Autorizado		2,5	3					25%				2,5	2,25			
		Manipulación De Equipos	4,5		3			25%		25%			3,375		2,25			
		Robo	6		0,2								6		0,2			

Figura 176. Efectividad de las salvaguardas e impacto residual del grupo Equipos informáticos. (b) (Fuente propia)

- [COM] Redes de Comunicaciones

Para este grupo de activos las salvaguardas tienen una efectividad mayormente del 50% o menores. Se destacan que en la dimensión de confidencialidad los errores de administración en redes inalámbricas y locales tienen una efectividad del 90% en la dimensión de confidencialidad. El valor del impacto residual es inversamente proporcional a la efectividad de las salvaguardas, reduciendo su valor mientras mayor efectividad exista. En el activo de red telefónica, las

salvaguardas no tienen efectividad, por lo que su valor de impacto se mantiene. Esto último también ocurre en el uso no previsto de las redes inalámbricas y locales. En el caso de las redes de comunicaciones, no existe ninguna salvaguarda con una efectividad del 100%. La Figura 177 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

REDES DE COMUNICACIONES [COM]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	7					50%					3,5				
		Errores De Administración	5,25	2	6,75			50%	25%	90%			2,625	1,5	0,675		
		Alteración Accidental De La Información		4					25%					3			
		Caída Del Sistema Por Agotamiento De Recursos	7					50%					3,5				
		Suplantación De La Identidad Del Usuario		4	9	9			25%	50%	50%			3	4,5	4,5	
		Abuso De Privilegios De Acceso	3,5	4	6,75			75%	25%	50%			0,875	3	3,375		
		Uso No Previsto	3,5	2	6,75			50%		50%			1,75	2	3,375		
		Acceso No Autorizado		4	9				25%	50%				3	4,5		
		Análisis De Trafico			9					50%					4,5		
		Interceptación De Información (Escucha)			9					50%					4,5		
		Modificación Deliberada De La Información		6					25%					4,5			
		Divulgación De Información			6,75					50%					3,375		
		Denegación De Servicio	7					75%					1,75				
COM2	Redes locales	Fallo Servicios De Comunicaciones	8					50%					4				
		Errores De Administración	6	4	9			50%	25%	90%			3	3	0,9		
		Alteración Accidental De La Información		4					25%					3			
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Suplantación De La Identidad Del Usuario		6	9	9			25%	50%	75%			4,5	4,5	2,25	
		Abuso De Privilegios De Acceso	4	6	9			75%	25%	50%			1	4,5	4,5		
		Uso No Previsto	4	4	9			50%		50%			2	4	4,5		
		Acceso No Autorizado		4	9				25%	50%				3	4,5		
		Análisis De Trafico			9					50%					4,5		
		Interceptación De Información (Escucha)			9					50%					4,5		
		Modificación Deliberada De La Información		6					25%					4,5			
		Divulgación De Información			6,75					50%					3,375		
		Denegación De Servicio	8					75%					2				
COM3	Red telefónica	Fallo Servicios De Comunicaciones	8					50%					4				
		Errores De Administración	6	3,5	6			50%	25%	50%			3	2,625	3		
		Alteración Accidental De La Información		3,5					25%					2,625			
		Caída Del Sistema Por Agotamiento De Recursos	8					50%					4				
		Abuso De Privilegios De Acceso	4	1,75	6			50%	25%	50%			2	1,313	3		
		Uso No Previsto	4	1,75	6			50%	25%	50%			2	1,313	3		
		Acceso No Autorizado		1,75	8				25%	50%				1,313	4		
		Análisis De Trafico			8					50%					4		
		Interceptación De Información (Escucha)			8					50%					4		
		Modificación Deliberada De La Información		3,5					25%					2,625			
		Divulgación De Información			6					50%					3		
		Denegación De Servicio	8					25%					6				
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	8										8				
		Caída Del Sistema Por Agotamiento De Recursos	6										6				
		Suplantación De La Identidad Del Usuario		0,35	6	5,25				10%	10%			0,35	5,4	4,725	
		Abuso De Privilegios De Acceso	0,4	0,35	4			75%		10%			0,1	0,35	3,6		
		Uso No Previsto	0,4	0,35	6			75%		10%			0,1	0,35	5,4		
		Acceso No Autorizado		0,35	6					10%				0,35	5,4		
		Análisis De Trafico			8										8		
		Interceptación De Información (Escucha)			8										8		
		Divulgación De Información			8										8		

Figura 177. Efectividad de las salvaguardas e impacto residual del grupo Redes de comunicaciones (Fuente propia)

- [MEDIA] Soportes de Información

En la dimensión de confidencialidad, los soportes de información tienen una efectividad del 100% en casi todos los casos. En contraste con la dimensión de disponibilidad en donde los valores son bajos. Esto último se cumple excepto en el activo del material impreso. Los valores del impacto residual son inversamente proporcionales a la efectividad de las salvaguardas. En los casos en que la efectividad es del 100% el valor del impacto se reduce a 0. Existen casos en los que las salvaguardas no tienen efectividad sobre una dimensión de seguridad, por lo que su impacto se mantiene y estos casos son: en las copias de seguridad los errores o ataques de

destrucción y fugas de información. La Figura 178 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	8										8				
		Daños Por Agua	8										8				
		Avería De Origen Físico/Lógico	6					10%					5,4				
		Degradación De Los Soportes De Almacenamiento De La Información	6					10%					5,4				
		Errores De Usuarios	2	6,75	9				25%	100%			2	5,063			
		Errores De Administración	2	6,75	9				50%	90%			2	3,375	0,9		
		Alteración Accidental De La Información		6,75					10%					6,075			
		Destrucción De Información	8										8				
		Fugas De Información			9					100%							
		Errores De Mantenimiento del soporte	2					10%					1,8				
		Perdida del soporte	8		9					100%			8				
		Uso No Previsto	8	9	9			10%	25%	100%			7,2	6,75			
		Acceso No Autorizado		9	9				50%	100%				4,5			
		Modificación Deliberada De La Información		9					25%					6,75			
		Destrucción De Información	8										8				
		Divulgación De Información			9					100%							
		Manipulación del soporte	4		9			10%		100%			3,6				
		Robo	8		9					100%			8				
MEDIA2	Pendrives USB	Daños Por Agua	7										7				
		Daños Por Agua	7										7				
		Avería De Origen Físico/Lógico	5,25					10%					4,725				
		Degradación De Los Soportes De Almacenamiento De La Información	5,25					10%					4,725				
		Errores De Usuarios	1,75	4	9			10%	25%	100%			1,575	3			
		Errores De Administración	1,75	4	9			10%	50%	100%			1,575	2			
		Alteración Accidental De La Información		8					10%					7,2			
		Destrucción De Información	7										7				
		Fugas De Información			9					100%							
		Errores De Mantenimiento del soporte	3,5					10%					3,15				
		Perdida del soporte	7		9					100%			7				
		Uso No Previsto	5,25	8	9			10%	25%	100%			4,725	6			
		Acceso No Autorizado		8	9				50%	100%				4			
		Modificación Deliberada De La Información		8					25%					6			
		Destrucción De Información	7					25%					5,25				
		Divulgación De Información			9					100%							
		Manipulación del soporte	5,25		9			10%		100%			4,725				
		Robo	7		9					100%			7				
MEDIA3	CD/DVD	Daños Por Agua	7										7				
		Daños Por Agua	7										7				
		Avería De Origen Físico/Lógico	5,25					10%					4,725				
		Degradación De Los Soportes De Almacenamiento De La Información	5,25					10%					4,725				
		Errores De Usuarios	1,75	4	9			10%	25%	100%			1,575	3			
		Errores De Administración	1,75	4	9			10%	50%	100%			1,575	2			
		Alteración Accidental De La Información		8					10%					7,2			
		Destrucción De Información	7										7				
		Fugas De Información			9					100%							
		Errores De Mantenimiento del soporte	3,5					10%					3,15				
		Perdida del soporte	7		9					90%			7		0,9		
		Uso No Previsto	5,25	8	9			10%	25%	100%			4,725	6			
		Acceso No Autorizado		8	9				50%	100%				4			
		Modificación Deliberada De La Información		8					25%					6			
		Destrucción De Información	7					25%					5,25				
		Divulgación De Información			9					100%							
		Manipulación del soporte	5,25		9			10%		100%			4,725				
		Robo	7		9					90%			7		0,9		
MEDIA4	Material impreso	Daños Por Agua	7										7				
		Daños Por Agua	7										7				
		Degradación por Almacenamiento	5,25					75%					1,313				
		Errores De Usuarios	3,5	6	6,75			25%	25%	75%			2,625	4,5	1,688		
		Errores De Administración	3,5	6	6,75			25%	25%	75%			2,625	4,5	1,688		
		Alteración Accidental De La Información		4					25%					3			
		Destrucción	7					50%					3,5				
		Fugas De Información			9					25%					6,75		
		Errores De Almacenamiento	3,5					50%					1,75				
		Perdida	3,5		9			75%		10%			0,875		8,1		
		Uso No Previsto	7	6	9			75%	25%	50%			1,75	4,5	4,5		
		Acceso No Autorizado		6	9				25%	25%				4,5	6,75		
		Modificación Deliberada De La Información		8					25%					6			
		Destrucción	7					75%					1,75				
		Divulgación			9					25%					6,75		
		Manipulación	3,5		9			75%		25%			0,875		6,75		
		Robo	3,5		9			75%					0,875		9		

Figura 178. Efectividad de las salvaguardas e impacto residual del grupo Soportes de información (Fuente propia)

- [AUX] Equipamiento Auxiliar

Para este grupo de activos las salvaguardas tienen una efectividad del 10% al 80%. Los resultados de la efectividad de las salvaguardas repercuten directamente sobre el impacto residual, causando una disminución en el valor del impacto. Existen casos en los que las salvaguardas no tienen efectividad, por lo que su impacto se mantiene y estos casos son: daños por agua, fuego

y los impactos que afectan la confidencialidad en el generador eléctrico, fuentes de alimentación, climatización y cableado UTP. Para el equipamiento auxiliar no existen salvaguardas con una efectividad del 100%. La Figura 179 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	3,75										3,75				
		Fuego	3,75										3,75				
		Daños Por Agua	3,75										3,75				
		Contaminación Mecánica	2,5					75%					0,625				
		Degradación por almacenamiento	2,5					75%					0,625				
		Avería De Origen Físico/ Lógico	3,75					75%					0,938				
		Errores De Mantenimiento/ Actualización De Equipos	3,75					75%					0,938				
		Uso No Previsto	3,75	1,25	0,15			50%	50%				1,875	0,625	0,15		
		Acceso No Autorizado		1,25	0,15				50%					0,625	0,15		
		Manipulación De Equipos	3,75		0,15			50%					1,875		0,15		
AUX2	Fuentes de alimentación	Daños Por Agua	3,75										3,75				
		Fuego	3,75										3,75				
		Daños Por Agua	3,75										3,75				
		Contaminación Mecánica	2,5					75%					0,625				
		Degradación por almacenamiento	2,5					75%					0,625				
		Avería De Origen Físico/ Lógico	3,75					75%					0,938				
		Corte De Suministro Eléctrico	5										5				
		Errores De Mantenimiento/ Actualización De Equipos	3,75					75%					0,938				
		Perdida De Equipos	5		0,15								5		0,15		
		Uso No Previsto	5	1,75	0,15			50%	50%	25%			2,5	0,875	0,113		
		Acceso No Autorizado		1,75	0,15			25%	50%					0,875	0,15		
		Manipulación De Equipos	3,75		0,15			50%		25%			1,875		0,113		
		Robo	5		0,15								5		0,15		
AUX3	Climatización	Daños Por Agua	3,75										3,75				
		Fuego	3,75										3,75				
		Daños Por Agua	3,75										3,75				
		Contaminación Mecánica	2,5					75%					0,625				
		Avería De Origen Físico/Lógico	3,75					75%					0,938				
		Corte De Suministro Eléctrico	5										5				
		Errores De Mantenimiento/Actualización De Equipos	3,75					75%					0,938				
		Uso No Previsto	2,5	1	0,15			50%	50%				1,25	0,5	0,15		
		Acceso No Autorizado		1	0,15				50%					0,5	0,15		
		Manipulación De Equipos	2,5		0,15			50%					1,25		0,15		
AUX4	Cableado UTP	Daños Por Agua	5,25										5,25				
		Fuego	7										7				
		Daños Por Agua	5,25										5,25				
		Avería De Origen Físico/Lógico	5,25					75%					1,313				
		Errores De Mantenimiento/Actualización De Equipos	5,25					75%					1,313				
		Uso No Previsto	3,5	2	1			25%	25%	25%			2,625	1,5	0,75		
		Acceso No Autorizado		2	3				25%	25%				1,5	2,25		
		Manipulación De Equipos	3,5		3			25%		25%			2,625		2,25		
AUX5	Armarios	Daños Por Agua	4					10%					3,6				
		Fuego	6					10%					5,4				
		Daños Por Agua	4					10%					3,6				
		Degradación por almacenamiento	2					75%					0,5				
		Avería De Origen Físico/Lógico	4					75%					1				
		Uso No Previsto	2	2	6				25%	75%			2	1,5	1,5		
		Acceso No Autorizado		2	6				25%	75%				1,5	1,5		
		Manipulación De Equipos	2		6			50%		75%			1		1,5		
AUX6	Cajas fuertes	Daños Por Agua	2					25%					1,5				
		Fuego	2					25%					1,5				
		Daños Por Agua	2					25%					1,5				
		Avería De Origen Físico/Lógico	6					50%					3				
		Corte De Suministro Eléctrico	6					50%					3				
		Errores De Mantenimiento/Actualización De Equipos	6					50%					3				
		Perdida De Equipos	8		9			50%		80%			4		1,8		
		Uso No Previsto	6	0,4	9			50%	75%	80%			3	0,1	1,8		
		Acceso No Autorizado		0,4	9				75%	80%				0,1	1,8		
		Manipulación De Equipos	2		9			50%		80%			1		1,8		

Figura 179. Efectividad de las salvaguardas e impacto residual del grupo Equipamiento auxiliar (Fuente propia)

- [L]Instalaciones

Para las instalaciones la mayoría de las salvaguardas tienen una efectividad del 50%. Las salvaguardas definidas para las fugas de información, uso no previsto y acceso no autorizado en edificios y cuartos de servidores solo tienen una eficiencia del 25%. Por otro lado, la efectividad del 75% se observa en la dimensión de integridad en el caso de uso no previsto de los edificios y cuartos de servidores. Los resultados de la efectividad de las salvaguardas repercuten

directamente sobre el impacto residual, causando una disminución considerable en el valor del impacto, exceptuando los casos en los que la efectividad es baja. En el caso del activo coches, al no tener salvaguardas su impacto residual es igual a su impacto potencial. Para estos activos no existe ninguna salvaguarda con una eficiencia del 100%. La Figura 180 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE INSTALACIONES [L]			Impacto					Efectividad de Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
L1	Edificios	Fuego	6					50%					3				
		Daños Por Agua	4,5					50%					2,25				
		Fuego	4,5					50%					2,25				
		Daños Por Agua	3					50%					1,5				
		Fugas De Información			6					50%					3		
		Uso No Previsto	1,5	1,75	6			50%	75%	25%			0,75	0,438	4,5		
		Acceso No Autorizado		1,75	8				25%	50%				1,313	4		
L2	Cuartos servidores	Fuego	8					50%					4				
		Daños Por Agua	8					50%					4				
		Fuego	8					50%					4				
		Daños Por Agua	8					50%					4				
		Fugas De Información			8					25%					6		
		Uso No Previsto	6	6	6			50%	75%	50%			3	1,5	3		
		Acceso No Autorizado		4	8				25%	50%				3	4		
L3	Coche	Daños mecánicos	2										2				
		Accidente de tránsito	2										2				

Figura 180. Efectividad de las salvaguardas e impacto residual del grupo Instalaciones (Fuente propia)

- [P] Personal

Para este grupo de activos todas las salvaguardas tienen un 50% de efectividad en todas las dimensiones de seguridad. Es decir que, los valores del impacto residual son la mitad de los valores del impacto potencial. La Figura 181 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE PERSONAL [P]			Impacto					Efectividad de las Salvaguardas					Impacto Residual				
Código	Nombre	Amenazas	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
P1	Administradores	Fugas De Información			9					50%					4,5		
		Indisponibilidad Del Personal	6					50%					3				
		Indisponibilidad Del Personal	6					50%					3				
		Extorsión	2	6	9			50%	50%	50%			1	3	4,5		
		Ingeniería Social	2	6	9			50%	50%	50%			1	3	4,5		
P2	Técnicos	Fugas De Información			9					50%					4,5		
		Indisponibilidad Del Personal	3,5					50%					1,75				
		Indisponibilidad Del Personal	3,5					50%					1,75				
		Extorsión	1,75	4	9			50%	50%	50%			0,875	2	4,5		
		Ingeniería Social	1,75	4	9			50%	50%	50%			0,875	2	4,5		
P3	Empleados	Fugas De Información			9					50%					4,5		
		Indisponibilidad Del Personal	3,5					50%					1,75				
		Indisponibilidad Del Personal	3,5					50%					1,75				
		Extorsión	1,75	4	9			50%	50%	50%			0,875	2	4,5		
		Ingeniería Social	1,75	4	9			50%	50%	50%			0,875	2	4,5		
P4	Usuarios	Fugas De Información			9					50%					4,5		
		Extorsión	1,25	3	9			50%	50%	50%			0,625	1,5	4,5		
		Ingeniería Social	1,25	3	9			50%	50%	50%			0,625	1,5	4,5		

Figura 181. Efectividad de las salvaguardas e impacto residual del grupo Personal (Fuente propia)

4.5.3. Cálculos de Riesgos Residual

Además de disminuir el grado de degradación de un activo, ciertas salvaguardas también disminuyen la probabilidad de ocurrencia de una amenaza. Si las amenazas redujeron la probabilidad, el valor de la frecuencia cambia y si no el valor de la frecuencia se mantiene.

Antes del cálculo del riesgo residual, se define la eficacia de las salvaguardas sobre la frecuencia de riesgos de un activo. La eficacia se mide en porcentaje con valores de 0% como mínimo y del 100% como máximo. Se procede entonces al cálculo de la frecuencia residual, con la fórmula:

$$FR = F * (1 - EF)$$

Donde

FR= Frecuencia residual

F= Probabilidad de materialización de la amenaza (frecuencia)

EF= Eficacia de la salvaguarda sobre la frecuencia

Definido el valor de la frecuencia residual se procedió a calcular el nuevo riesgo, denominado riesgo residual, con la siguiente fórmula:

$$RR = IR * FR$$

Donde

RR= Riesgo residual

IR = Impacto residual

FR = Frecuencia residual

Calculado el riesgo residual, se logra percibir con mayor claridad la eficacia de las salvaguardas, concluyendo que la mayoría de los valores de los riesgos residuales se encuentran dentro de los rangos definidos en el apartado 4.5.1 Salvaguardas (Tratamiento del riesgo para cada activo).

Teniendo en consideración que en todos los grupos de activos los valores de la frecuencia residual son inversamente proporcionales a la efectividad de la frecuencia, los resultados y análisis del riesgo residual se pueden ver a continuación.

- [D] Datos/Información

Para los datos o información, las salvaguardas definidas producen una disminución considerable de la frecuencia de ocurrencia de las amenazas, por lo tanto tienen una efectividad cercana al 100%. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 0,1, pero se observa que en el caso de los errores de usuarios el riesgo residual sobrepasa ese valor, entendiéndose que esos errores son difíciles de evitar y que la asociación asume los riesgos. Finalmente, existen casos en los que no existe riesgo porque han sido eliminados completamente porque su impacto residual es 0. Las Figuras 182, 183 y 184 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

DATOS / INFORMACIÓN [D]			Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas		F´	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
D1	Datos de configuración	Errores De Administración	80%	0,06	1,5	1,5	0,5			0,09	0,09	0,03		
		Errores De Configuración	80%	0,06		1					0,06			
		Alteración Accidental De La Información	90%	0,03		1					0,03			
		Destrucción De Información	90%	0,03	2					0,06				
		Fugas De Información	90%	0,01			1					0,01		
		Manipulación De Los Registros De Actividad	80%	0,02		0,3			3,375		0,006			0,0675
		Manipulación De La Configuración	90%	0,01		2		2,25			0,02		0,0225	
		Abuso De Privilegios De Acceso	90%	0,01	1,5	1,5				0,015	0,015			
		Acceso No Autorizado	90%	0,01		1,5					0,015			
		Repudio	90%	0,01		1,5			4,5		0,015			0,045
		Modificación Deliberada De La Información	90%	0,01		2					0,02			
		Destrucción De Información	90%	0,01	2					0,02				
D2	Código fuente de aplicaciones	Errores De Administración	80%	0,06	1	1,688	0,5			0,06	0,1013	0,03		
		Errores De Configuración	80%	0,06		1,688					0,1013			
		Alteración Accidental De La Información	90%	0,01		2,25					0,0225			
		Manipulación De Los Registros De Actividad	80%	0,02		0,338			3,375		0,0068			0,0675
		Manipulación De La Configuración	90%	0,01		1,688		1,125			0,0169		0,0113	
		Abuso De Privilegios De Acceso	90%	0,01	0,5	1,688				0,005	0,0169			
		Acceso No Autorizado	90%	0,01		2,25					0,0225			
		Repudio	90%	0,01		1,688			4,5		0,0169			0,045
		Modificación Deliberada De La Información	90%	0,01		2,25					0,0225			
		Destrucción De Información	90%	0,01	2					0,02				
D3	Ficheros almacenados en PC	Errores De Usuarios	50%	0,35	0,563	2,625	1,25			0,1969	0,9188	0,4375		
		Errores De Administración	90%	0,03	0,563	1,313	1,25			0,0169	0,0394	0,0375		
		Errores De Configuración	90%	0,03		0,438					0,0131			
		Alteración Accidental De La Información	50%	0,35		2,625					0,9188			
		Destrucción De Información	50%	0,25	0,75					0,1875				
		Fugas De Información	75%	0,025			0,313					0,0078		
		Manipulación De Los Registros De Actividad	80%	0,02		1,75			1,75		0,035			0,035
		Manipulación De La Configuración	80%	0,02		1,05	0,625	1,125			0,021	0,0125	0,0225	
		Suplantación De La Identidad Del Usuario	80%	0,06		1,05	0,938	3,375			0,063	0,0563	0,2025	
		Abuso De Privilegios De Acceso	80%	0,02	0,188	1,05	0,938			0,0038	0,021	0,0188		
		Acceso No Autorizado	80%	0,06		1,575	1,25				0,0945	0,075		
		Repudio	80%	0,02		0,525			3,5		0,0105			0,07
		Modificación Deliberada De La Información	80%	0,02		2,1					0,042			
		Destrucción De Información	80%	0,02	0,563					0,0113				
D4	Ficheros almacenados en servidores en la nube	Errores De Usuarios	50%	0,35	0,625	1,75	0,175			0,2188	0,6125	0,0613		
		Errores De Administración	90%	0,03	0,938	1,313	0,35			0,0281	0,0394	0,0105		
		Errores De Monitorización Log	90%	0,01		0,875			1,5		0,0088			0,015
		Errores De Configuración	90%	0,03		0,875					0,0263			
		Alteración Accidental De La Información	90%	0,07		1,313					0,0919			
		Destrucción De Información	90%	0,03	0,938					0,0281				
		Manipulación De Los Registros De Actividad	90%	0,01		0,438			1,5		0,0044			0,015
		Manipulación De La Configuración	90%	0,01		0,438	0,35	2			0,0044	0,0035	0,02	
		Suplantación De La Identidad Del Usuario	90%	0,03		0,438	0,525	3			0,0131	0,0158	0,09	
		Abuso De Privilegios De Acceso	90%	0,01	0,313	0,438	0,525			0,0031	0,0044	0,0053		
		Acceso No Autorizado	90%	0,01		0,875	0,7				0,0088	0,007		
		Repudio	90%	0,01		0,175			0,8		0,0018			0,008
		Modificación Deliberada De La Información	90%	0,01		1,75					0,0175			
		Destrucción De Información	90%	0,01	1,25					0,0125				

Figura 182. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (a) (Fuente propia)

D5	Ficheros almacenados en servidores locales	Errores De Usuarios	50%	0,35	0,938	1,75	0,175			0,3281	0,6125	0,0613		
		Errores De Administración	90%	0,03	0,938	1,313	0,7			0,0281	0,0394	0,021		
		Errores De Monitorización Log	90%	0,01		0,875			1,5		0,0088			0,015
		Errores De Configuración	90%	0,03		0,875					0,0263			
		Alteración Accidental De La Información	90%	0,05		1,313					0,0656			
		Destrucción De Información	90%	0,03	0,938					0,0281				
		Manipulación De Los Registros De Actividad	90%	0,01		0,438			1,5		0,0044			0,015
		Manipulación De La Configuración	90%	0,01		0,438	0,7	2			0,0044	0,007	0,02	
		Suplantación De La Identidad Del Usuario	90%	0,03		0,438	1,05	3			0,0131	0,0315	0,09	
		Abuso De Privilegios De Acceso	90%	0,01	0,313	0,438	1,05			0,0031	0,0044	0,0105		
		Acceso No Autorizado	90%	0,01		0,875	1,4				0,0088	0,014		
		Repudio	90%	0,01		0,175			0,8		0,0018			0,008
		Modificación Deliberada De La Información	90%	0,01		1,75					0,0175			
		Destrucción De Información	90%	0,01	1,25					0,0125				
D6	Bases de datos en servidores locales	Errores De Administración	90%	0,03	0,6	0,675				0,018	0,0203			
		Errores De Monitorización Log	90%	0,01		0,675					0,0068			
		Errores De Configuración	90%	0,03		0,675					0,0203			
		Alteración Accidental De La Información	90%	0,05		0,675					0,0338			
		Destrucción De Información	90%	0,01	0,8					0,008				
		Manipulación De Los Registros De Actividad	90%	0,01		0,45					0,0045			
		Manipulación De La Configuración	90%	0,01		0,45		0,9			0,0045		0,009	
		Suplantación De La Identidad Del Usuario	90%	0,01		0,45		1,35			0,0045		0,0135	
		Abuso De Privilegios De Acceso	90%	0,01	0,6	0,45				0,006	0,0045			
		Acceso No Autorizado	90%	0,01		0,675					0,0068			
		Repudio	90%	0,01		0,45					0,0045			
		Modificación Deliberada De La Información	90%	0,01		0,9					0,009			
		Destrucción De Información	90%	0,01	0,8					0,008				
D7	Bases de datos en servidores en la nube	Errores De Administración	90%	0,03	0,675	0,675				0,0203	0,0203			
		Errores De Monitorización Log	90%	0,01		0,675					0,0068			
		Errores De Configuración	90%	0,03		0,675					0,0203			
		Alteración Accidental De La Información	90%	0,05		0,675					0,0338			
		Destrucción De Información	90%	0,01	0,9					0,009				
		Manipulación De Los Registros De Actividad	90%	0,01		0,45					0,0045			
		Manipulación De La Configuración	90%	0,01		0,45		0,9			0,0045		0,009	
		Suplantación De La Identidad Del Usuario	90%	0,01		0,45		1,35			0,0045		0,0135	
		Abuso De Privilegios De Acceso	90%	0,01	0,675	0,45				0,0068	0,0045			
		Acceso No Autorizado	90%	0,01		0,675					0,0068			
		Repudio	90%	0,01		0,45					0,0045			
		Modificación Deliberada De La Información	90%	0,01		0,9					0,009			
		Destrucción De Información	90%	0,01	0,9					0,009				
D8	Copias de seguridad en la nube	Errores De Administración	90%	0,01	1,35	0,6	0,45			0,0135	0,006	0,0045		
		Errores De Monitorización Log	90%	0,03		0,4			2,25		0,012			0,0675
		Errores De Configuración	90%	0,03		2					0,06			
		Alteración Accidental De La Información	90%	0,03		2					0,06			
		Destrucción De Información	90%	0,01	4,5					0,045				
		Manipulación De Los Registros De Actividad	90%	0,01		0,5			1,688		0,005			0,0169
		Manipulación De La Configuración	90%	0,01		1,5	0,675	1,688			0,015	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	90%	0,01		1	0,9	1,688			0,01	0,009	0,0169	
		Abuso De Privilegios De Acceso	90%	0,01	1,125	1,5	0,9			0,0113	0,015	0,009		
		Acceso No Autorizado	90%	0,01		1,5	0,9				0,015	0,009		
		Repudio	90%	0,01		1			2,25		0,01			0,0225
		Modificación Deliberada De La Información	90%	0,01		2					0,02			
		Destrucción De Información	90%	0,01	4,5					0,045				
		Divulgación De Información	90%	0,01			0,9					0,009		
D9	Copias de Seguridad en servidores locales	Errores De Administración	90%	0,01	1,2	1,5	0,45			0,012	0,015	0,0045		
		Errores De Monitorización Log	90%	0,03		1			2,25		0,03			0,0675
		Errores De Configuración	90%	0,03		2					0,06			
		Alteración Accidental De La Información	90%	0,03		2					0,06			
		Destrucción De Información	90%	0,01	8					0,08				
		Fugas De Información	90%	0,01			6,75					0,0675		
		Manipulación De La Configuración	90%	0,01		4,5	0,675	1,688			0,045	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	90%	0,01		3	0,9	1,688			0,03	0,009	0,0169	
		Abuso De Privilegios De Acceso	90%	0,01	2	4,5	0,9			0,02	0,045	0,009		
		Acceso No Autorizado	90%	0,01		4,5	0,9				0,045	0,009		
		Repudio	90%	0,01		3			2,25		0,03			0,0225
		Modificación Deliberada De La Información	90%	0,01		6					0,06			
		Destrucción De Información	90%	0,01	8					0,08				
		Divulgación De Información	90%	0,01			0,9					0,009		
D10	Copias de Seguridad en discos externos	Errores De Administración	90%	0,01	1,05	1,5	0,45			0,0105	0,015	0,0045		
		Errores De Monitorización Log	90%	0,03		2			2,25		0,06			0,0675
		Errores De Configuración	90%	0,03		2					0,06			
		Alteración Accidental De La Información	80%	0,06		2					0,12			
		Destrucción De Información	90%	0,01	7					0,07				
		Manipulación De Los Registros De Actividad	90%	0,01		1,5			1,688		0,015			0,0169
		Manipulación De La Configuración	90%	0,01		4,5	0,675	1,688			0,045	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	90%	0,01		3	0,9	1,688			0,03	0,009	0,0169	
		Abuso De Privilegios De Acceso	90%	0,01	1,75	4,5	0,9			0,0175	0,045	0,009		
		Acceso No Autorizado	80%	0,02		4,5	0,9				0,09	0,018		
		Repudio	90%	0,01		3			2,25		0,03			0,0225
		Modificación Deliberada De La Información	80%	0,02		6					0,12			
		Destrucción De Información	90%	0,01	7					0,07				
		Divulgación De Información	90%	0,01			0,9					0,009		
D11	Ficheros de contraseñas	Errores De Administración	90%	0,01	3,375	1,688				0,0338	0,0169			
		Errores De Configuración	90%	0,01		0,113					0,0011			
		Alteración Accidental De La Información	75%	0,025		1,688					0,0422			
		Destrucción De Información	90%	0,01	2,25					0,0225				
		Manipulación De Los Registros De Actividad	90%	0,01		0,563			2,25		0,0056			0,0225
		Suplantación De La Identidad Del Usuario	90%	0,01		1,125		2,25			0,0113		0,0225	
		Abuso De Privilegios De Acceso	90%	0,01	1,688	1,125				0,0169	0,0113			
		Acceso No Autorizado	90%	0,01		1,688					0,0169			
		Repudio	90%	0,01		0,563			2,25		0,0056			0,0225
		Modificación Deliberada De La Información	90%	0,01		2,25					0,0225			
		Destrucción De Información	90%	0,01	2,25					0,0225				
		Divulgación De Información	90%	0,01			2,25					0,0225		

Figura 183. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (b) (Fuente propia)

D12	Registros de actividades en servidores	Errores De Administración	90%	0,03	1,5	1	0,8			0,045	0,03	0,024		
		Errores De Configuración	90%	0,03		1,5					0,045			
		Destrucción De Información	90%	0,03	1,5					0,045				
		Manipulación De La Configuración	90%	0,01		1,5	0,8	0,675			0,015	0,008	0,0068	
		Suplantación De La Identidad Del Usuario	90%	0,01		1,5	1,6	0,45			0,015	0,016	0,0045	
		Abuso De Privilegios De Acceso	90%	0,01	1,5	2	0,8			0,015	0,02	0,008		
		Acceso No Autorizado	90%	0,01		1,5	1,6				0,015	0,016		
		Repudio	90%	0,03		1			2,25		0,03			0,0675
		Modificación Deliberada De La Información	90%	0,01		2					0,02			
		Destrucción De Información	90%	0,01	2					0,02				
D13	Ficheros compartidos Google Drive	Errores De Administración	75%	0,075	1,313	0,4	0,4			0,0984	0,03	0,03		
		Errores De Configuración	75%	0,025		0,2					0,005			
		Alteración Accidental De La Información	75%	0,075		0,6					0,045			
		Destrucción De Información	75%	0,075	1,313					0,0984				
		Manipulación De La Configuración	75%	0,025		0,4	0,4	1,75			0,01	0,01	0,0438	
		Suplantación De La Identidad Del Usuario	75%	0,025		0,6	0,8	1,75			0,015	0,02	0,0438	
		Abuso De Privilegios De Acceso	75%	0,025	0,875	0,4	0,4			0,0219	0,01	0,01		
		Acceso No Autorizado	75%	0,025		0,6	0,8				0,015	0,02		
		Repudio	75%	0,025		0,2					0,005			
		Modificación Deliberada De La Información	75%	0,025		0,8					0,02			
		Destrucción De Información	75%	0,025	1,75					0,0438				
		Divulgación De Información	75%	0,025			0,8					0,02		

Figura 184. Efectividad de las salvaguardas e impacto residual del grupo Datos/Información. (c) (Fuente propia)

- [S] Servicios

Para este grupo de activos, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia del 50% en adelante. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al Riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 0,5, pero se observa que tres valores de riesgo residual sobrepasan ese valor, entendiéndose que son errores difíciles de evitar (errores de usuarios) y que la asociación asume los riesgos. Además, todos los activos poseen riesgos residuales aunque sean de valores muy pequeños, causado porque ninguna salvaguarda tiene una eficacia del 100%. Las Figuras 185 y 186 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

SERVICIOS [S]			Efectividad	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	de Frecuencia	F´	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
S1	Página web	Errores De Usuarios	50%	0,25	0,088	0,2	0,4			0,0219	0,05	0,1		
		Errores De Administración	90%	0,01	1,75	1,5	1,2			0,0175	0,015	0,012		
		Alteración Accidental De La Información	50%	0,05		1,5					0,075			
		Fugas De Información	50%	0,05			0,8					0,04		
		Caída Del Sistema Por Agotamiento De Recursos	75%	0,075	1,75					0,1313				
		Suplantación De La Identidad Del Usuario	90%	0,07		1,5	1,2	1			0,105	0,084	0,07	
		Abuso De Privilegios De Acceso	90%	0,03	0,875	1,5	1,2			0,0263	0,045	0,036		
		Uso No Previsto	90%	0,03	0,875	1,5	1,2			0,0263	0,045	0,036		
		Acceso No Autorizado	90%	0,05		2	1,2				0,1	0,06		
		Repudio	90%	0,01		1			0,525		0,01			0,0053
		Modificación Deliberada De La Información	90%	0,01		2					0,02			
		Destrucción De Información	90%	0,01	1,313					0,0131				
		Divulgación De Información	90%	0,03			1,6					0,048		
		Denegación De Servicio	90%	0,03	3,5					0,105				
S2	Correo electrónico	Errores De Usuarios	75%	0,175	1,75	1,5	2			0,3063	0,2625	0,35		
		Errores De Administración	90%	0,01	2,625	1,5	3			0,0263	0,015	0,03		
		Alteración Accidental De La Información	90%	0,03		2					0,06			
		Fugas De Información	75%	0,025			3					0,075		
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	3,5					0,035				
		Suplantación De La Identidad Del Usuario	90%	0,05		2	3	1,313			0,1	0,15	0,0656	
		Abuso De Privilegios De Acceso	80%	0,06	1,75	1,5	3			0,105	0,09	0,18		
		Uso No Previsto	80%	0,06	2,625	1,5	3			0,1575	0,09	0,18		
		Acceso No Autorizado	90%	0,05		1,5	2				0,075	0,1		
		Repudio	80%	0,02		2			1,5		0,04			0,03
		Modificación Deliberada De La Información	90%	0,01		1,5					0,015			
		Divulgación De Información	80%	0,06			3					0,18		
		Denegación De Servicio	90%	0,01	3,5					0,035				

Figura 185. Efectividad de las salvaguardas e impacto residual del grupo Servicios. (a) (Fuente propia)

S3	Intranet documental - Servicio FTP	Errores De Usuarios	75%	0,175	0,3	3	1			0,0525	0,525	0,175		
		Errores De Administración	90%	0,03	4,5	4,5	1			0,135	0,135	0,03		
		Alteración Accidental De La Información	80%	0,1		3					0,3			
		Destrucción De Información	80%	0,1	3					0,3				
		Fugas De Información	80%	0,02			1,5					0,03		
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	90%	0,03		2	1,5	1			0,06	0,045	0,03	
		Abuso De Privilegios De Acceso	80%	0,02	1	2	1,5			0,02	0,04	0,03		
		Uso No Previsto	80%	0,06	2	2	1,5			0,12	0,12	0,09		
		Acceso No Autorizado	90%	0,05		2	2				0,1	0,1		
		Repudio	90%	0,03		1,5			1,5		0,045			0,045
		Modificación Deliberada De La Información	80%	0,02		3					0,06			
		Destrucción De Información	80%	0,02	4					0,08				
		Divulgación De Información	80%	0,02			1,5					0,03		
		Denegación De Servicio	80%	0,06	4					0,24				
S4	Sistema de tickets de incidencias	Errores De Usuarios	75%	0,175	0,15	1,125	0,375			0,0263	0,1969	0,0656		
		Errores De Administración	90%	0,03	2,25	2,25	0,375			0,0675	0,0675	0,0113		
		Alteración Accidental De La Información	80%	0,06		1,5					0,09			
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	2					0,04				
		Suplantación De La Identidad Del Usuario	90%	0,03		1,5	1,125	1			0,045	0,0338	0,03	
		Acceso No Autorizado	80%	0,1		2,25	1,125				0,225	0,1125		
		Repudio	90%	0,01		2,25			0,938		0,0225			0,0094
		Modificación Deliberada De La Información	80%	0,02		1,5					0,03			
		Divulgación De Información	80%	0,02			0,75					0,015		
		Denegación De Servicio	80%	0,06	2					0,12				
S5	Educación Virtual	Errores De Usuarios	75%	0,175	0,3	1,5	0,875			0,0525	0,2625	0,1531		
		Errores De Administración	90%	0,03	4,5	3	0,875			0,135	0,09	0,0263		
		Alteración Accidental De La Información	75%	0,125		3					0,375			
		Destrucción De Información	75%	0,125	4					0,5				
		Fugas De Información	50%	0,25			0,875					0,2188		
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	50%	0,25		1	1,313	0,75			0,25	0,3281	0,1875	
		Abuso De Privilegios De Acceso	75%	0,075	1	3	0,875			0,075	0,225	0,0656		
		Uso No Previsto	80%	0,1	2	1	0,875			0,2	0,1	0,0875		
		Acceso No Autorizado	75%	0,125		3	1,313				0,375	0,1641		
		Repudio	90%	0,01		1			1,313		0,01			0,0131
		Modificación Deliberada De La Información	75%	0,025		3					0,075			
		Divulgación De Información	75%	0,075			0,875					0,0656		
		Denegación De Servicio	80%	0,06	4					0,24				
S6	Servicio de financiero	Errores De Usuarios	75%	0,125	1,5	5,063	2,25			0,1875	0,6328	0,2813		
		Errores De Administración	90%	0,03	4,5	3,375	1,688			0,135	0,1013	0,0506		
		Alteración Accidental De La Información	80%	0,1		4,5					0,45			
		Destrucción De Información	80%	0,06	3					0,18				
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,06	4					0,24				
		Suplantación De La Identidad Del Usuario	90%	0,03		3,375	2,25	1,688			0,1013	0,0675	0,0506	
		Abuso De Privilegios De Acceso	80%	0,06	1	3,375	1,688			0,06	0,2025	0,1013		
		Uso No Previsto	80%	0,06	2	2,25	1,125			0,12	0,135	0,0675		
		Acceso No Autorizado	80%	0,06		4,5	2,25				0,27	0,135		
		Repudio	90%	0,01		2,25			2,25		0,0225			0,0225
		Modificación Deliberada De La Información	80%	0,02		4,5					0,09			
		Destrucción De Información	80%	0,02	4					0,08				
		Divulgación De Información	80%	0,02			2,25					0,045		
		Denegación De Servicio	80%	0,06	4					0,24				
S7	Gestión de usuarios Socios	Errores De Usuarios	75%	0,125	1,5	4,5	1			0,1875	0,5625	0,125		
		Errores De Administración	90%	0,03	4,5	3	1,5			0,135	0,09	0,045		
		Alteración Accidental De La Información	80%	0,06		3					0,18			
		Destrucción De Información	80%	0,02	3					0,06				
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	90%	0,03		3	2	0,875			0,09	0,06	0,0263	
		Abuso De Privilegios De Acceso	80%	0,02	1	2	1			0,02	0,04	0,02		
		Uso No Previsto	80%	0,06	2	1	1,5			0,12	0,06	0,09		
		Acceso No Autorizado	90%	0,05		3	2				0,15	0,1		
		Repudio	90%	0,01		1			2		0,01			0,02
		Modificación Deliberada De La Información	80%	0,02		4					0,08			
		Destrucción De Información	80%	0,02	4					0,08				
		Divulgación De Información	80%	0,06			2					0,12		
		Denegación De Servicio	80%	0,06	4					0,24				
S8	Gestión empresarial	Errores De Usuarios	75%	0,125	1,313	2	2			0,1641	0,25	0,25		
		Errores De Administración	90%	0,03	2,625	2	2			0,0788	0,06	0,06		
		Alteración Accidental De La Información	80%	0,06		3					0,18			
		Destrucción De Información	80%	0,02	2,625					0,0525				
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	2,625					0,0525				
		Suplantación De La Identidad Del Usuario	90%	0,03		2	3	1,75			0,06	0,09	0,0525	
		Abuso De Privilegios De Acceso	80%	0,02	0,875	2	2			0,0175	0,04	0,04		
		Uso No Previsto	80%	0,06	0,875	2	3			0,0525	0,12	0,18		
		Acceso No Autorizado	90%	0,05		3	4				0,15	0,2		
		Repudio	90%	0,01		2			2		0,02			0,02
		Modificación Deliberada De La Información	80%	0,02		3					0,06			
		Destrucción De Información	80%	0,02	3,5					0,07				
		Divulgación De Información	80%	0,06			4					0,24		
		Denegación De Servicio	80%	0,06	3,5					0,21				
S9	Gestión de recursos humanos, nóminas	Errores De Usuarios	75%	0,125	1,313	3	1,5			0,1641	0,375	0,1875		
		Errores De Administración	90%	0,03	2,625	3	1,5			0,0788	0,09	0,045		
		Alteración Accidental De La Información	80%	0,06		3					0,18			
		Destrucción De Información	80%	0,02	2,625					0,0525				
		Caída Del Sistema Por Agotamiento De Recursos	80%	0,02	3,5					0,07				
		Suplantación De La Identidad Del Usuario	90%	0,03		3	2	1			0,09	0,06	0,03	
		Abuso De Privilegios De Acceso	80%	0,02	0,875	2	1,5			0,0175	0,04	0,03		
		Uso No Previsto	80%	0,06	0,875	2	1,5			0,0525	0,12	0,09		
		Acceso No Autorizado	80%	0,1		3	2				0,3	0,2		
		Repudio	90%	0,01		2			2,25		0,02			0,0225
		Modificación Deliberada De La Información	80%	0,02		4					0,08			
		Destrucción De Información	80%	0,02	3,5					0,07				
		Divulgación De Información	80%	0,06			2					0,12		
		Denegación De Servicio	80%	0,06	3,5					0,21				

Figura 186. Efectividad de las salvaguardas e impacto residual del grupo Servicios. (b) (Fuente propia)

- [SW] Software – Aplicaciones Informáticas

Para el software, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia entre el 25% y 90%, excepto en la destrucción de información en los navegadores web, modificación deliberada de la información en el antivirus y, el abuso de privilegios de acceso y uso no previsto en el software ofimático. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 1, pero se observa que en el caso errores de usuarios en navegadores web sobrepasa su valor, entendiéndose que esos errores son difíciles de evitar y que la asociación asume los riesgos. Finalmente, existen casos en los que el riesgo han sido eliminados completamente porque su impacto residual es 0. Las Figuras 187, 188, 189 y 190 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	Frecuencia	F´	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
SW1	Aplicación de Financiero	Fallo De Origen Lógico	80%	0,02	3,375					0,0675				
		Errores De Usuarios	50%	0,25	1,688	3,375	2,25			0,4219	0,8438	0,5625		
		Errores De Administración	90%	0,01	3,375	3,375	2,25			0,0338	0,0338	0,0225		
		Alteración Accidental De La Información	75%	0,075		3,375					0,2531			
		Destrucción De Información	25%	0,075	2,25					0,1688				
		Fugas De Información	25%	0,075			4,5					0,3375		
		Vulnerabilidades De Los Programas	90%	0,03	3,375	3,375	4,5			0,1013	0,1013	0,135		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	2,25	3,375				0,1688	0,2531			
		Suplantación De La Identidad Del Usuario	25%	0,075		3,375	2,25	1,688			0,2531	0,1688	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	2,25	3,375	2,25			0,1688	0,2531	0,1688		
		Uso No Previsto	50%	0,15	3,375	3,375	1,125			0,5063	0,5063	0,1688		
		Difusión De Software Dañino	90%	0,01	4,5	4,5	2,25			0,045	0,045	0,0225		
		Acceso No Autorizado	90%	0,01		3,375	2,25				0,0338	0,0225		
		Modificación Deliberada De La Información	50%	0,05		4,5					0,225			
		Destrucción De Información	50%	0,05	2,25					0,1125				
		Divulgación De Información	25%	0,075			2,25					0,1688		
SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	80%	0,02	3					0,06				
		Errores De Usuarios	50%	0,25	3	3	2			0,75	0,75	0,5		
		Errores De Administración	90%	0,01	3	3	2			0,03	0,03	0,02		
		Alteración Accidental De La Información	75%	0,075		3					0,225			
		Destrucción De Información	25%	0,075	2					0,15				
		Fugas De Información	25%	0,075			4					0,3		
		Vulnerabilidades De Los Programas	90%	0,03	3	3	4			0,09	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	2	3				0,15	0,225			
		Suplantación De La Identidad Del Usuario	25%	0,075		3	2	1,688			0,225	0,15	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	2	3	2			0,15	0,225	0,15		
		Uso No Previsto	50%	0,15	2	3	1			0,3	0,45	0,15		
		Difusión De Software Dañino	90%	0,01	4	4	2			0,04	0,04	0,02		
		Acceso No Autorizado	90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	50%	0,05		4					0,2			
		Destrucción De Información	50%	0,05	2					0,1				
		Divulgación De Información	25%	0,075			2					0,15		
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	80%	0,02	2,625					0,0525				
		Errores De Usuarios	50%	0,25	2,625	3	2			0,6563	0,75	0,5		
		Errores De Administración	90%	0,01	2,625	3	2			0,0263	0,03	0,02		
		Alteración Accidental De La Información	75%	0,075		3					0,225			
		Destrucción De Información	25%	0,075	1,75					0,1313				
		Fugas De Información	25%	0,075			4					0,3		
		Vulnerabilidades De Los Programas	90%	0,03	2,625	3	4			0,0788	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	1,75	3				0,1313	0,225			
		Suplantación De La Identidad Del Usuario	25%	0,075		3	2	1,688			0,225	0,15	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	1,75	3	2			0,1313	0,225	0,15		
		Uso No Previsto	50%	0,15	1,75	3	1			0,2625	0,45	0,15		
		Difusión De Software Dañino	90%	0,01	3,5	4	2			0,035	0,04	0,02		
		Acceso No Autorizado	90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	50%	0,05		4					0,2			
		Destrucción De Información	50%	0,05	1,75					0,0875				
		Divulgación De Información	25%	0,075			2					0,15		

Figura 187. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (a) (Fuente propia)

SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	80%	0,02	2,625					0,0525				
		Errores De Usuarios	50%	0,25	2,625	3	2			0,6563	0,75	0,5		
		Errores De Administración	90%	0,01	2,625	3	2			0,0263	0,03	0,02		
		Alteración Accidental De La Información	75%	0,075		3					0,225			
		Destrucción De Información	25%	0,075	1,75					0,1313				
		Fugas De Información	25%	0,075			4					0,3		
		Vulnerabilidades De Los Programas	90%	0,03	2,625	3	4			0,0788	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	1,75	3				0,1313	0,225			
		Suplantación De La Identidad Del Usuario	25%	0,075		3	2	1,688			0,225	0,15	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	1,75	3	2			0,1313	0,225	0,15		
		Uso No Previsto	50%	0,15	1,75	3	1			0,2625	0,45	0,15		
		Difusión De Software Dañino	90%	0,01	3,5	4	2			0,035	0,04	0,02		
		Acceso No Autorizado	90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	50%	0,05		4					0,2			
		Destrucción De Información	50%	0,05	1,75					0,0875				
		Divulgación De Información	25%	0,075			2					0,15		
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	80%	0,02	1,5					0,03				
		Errores De Administración	90%	0,01	3	3,375	2,25			0,03	0,0338	0,0225		
		Alteración Accidental De La Información	75%	0,075		4,5					0,3375			
		Destrucción De Información	50%	0,05	4					0,2				
		Fugas De Información	50%	0,05			4,5					0,225		
		Vulnerabilidades De Los Programas	90%	0,03	2	3,375	4,5			0,06	0,1013	0,135		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	2	4,5				0,15	0,3375			
		Suplantación De La Identidad Del Usuario	75%	0,025		4,5	4,5				0,1125	0,1125		
		Abuso De Privilegios De Acceso	75%	0,075	3	4,5	4,5			0,225	0,3375	0,3375		
		Uso No Previsto	75%	0,075	3	3,375	4,5			0,225	0,2531	0,3375		
		Difusión De Software Dañino	90%	0,01	2	4,5	4,5			0,02	0,045	0,045		
		Acceso No Autorizado	90%	0,01		4,5	4,5				0,045	0,045		
		Modificación Deliberada De La Información	75%	0,025		4,5					0,1125			
		Destrucción De Información	75%	0,025	2					0,05				
		Divulgación De Información	50%	0,05			4,5					0,225		
SW6	Aplicación de Página web	Fallo De Origen Lógico	80%	0,02	1,313					0,0263				
		Errores De Usuarios	75%	0,125	1,313	1,5	1,5			0,1641	0,1875	0,1875		
		Errores De Administración	90%	0,01	2,625	2	3			0,0263	0,02	0,03		
		Alteración Accidental De La Información	75%	0,075		3					0,225			
		Destrucción De Información	75%	0,025	2,625					0,0656				
		Fugas De Información	75%	0,025			2					0,05		
		Vulnerabilidades De Los Programas	90%	0,03	2,625	3	3			0,0788	0,09	0,09		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	1,75	3				0,1313	0,225			
		Suplantación De La Identidad Del Usuario	75%	0,025		2	4				0,05	0,1		
		Abuso De Privilegios De Acceso	75%	0,075	1,75	3	4			0,1313	0,225	0,3		
		Uso No Previsto	50%	0,25	1,75	2	4			0,4375	0,5	1		
		Difusión De Software Dañino	75%	0,025	1,75	2	4			0,0438	0,05	0,1		
		Acceso No Autorizado	75%	0,025		3	4				0,075	0,1		
		Modificación Deliberada De La Información	75%	0,025		3					0,075			
		Destrucción De Información	75%	0,025	1,75					0,0438				
		Divulgación De Información	50%	0,05			3					0,15		
		Manipulación De Programas	75%	0,025	1,75	1,5	3			0,0438	0,0375	0,075		
SW7	Aplicación de Intranet	Fallo De Origen Lógico	80%	0,02	3					0,06				
		Errores De Usuarios	50%	0,25	3	3	2			0,75	0,75	0,5		
		Errores De Administración	90%	0,01	3	3	2			0,03	0,03	0,02		
		Alteración Accidental De La Información	75%	0,075		3					0,225			
		Destrucción De Información	25%	0,075	2					0,15				
		Fugas De Información	25%	0,075			4					0,3		
		Vulnerabilidades De Los Programas	90%	0,03	3	3	4			0,09	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	2	3				0,15	0,225			
		Suplantación De La Identidad Del Usuario	25%	0,075		3	2	1,688			0,225	0,15	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	2	3	2			0,15	0,225	0,15		
		Uso No Previsto	50%	0,15	2	3	1			0,3	0,45	0,15		
		Difusión De Software Dañino	90%	0,01	4	4	2			0,04	0,04	0,02		
		Acceso No Autorizado	90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	50%	0,05		3					0,15			
		Destrucción De Información	50%	0,05	2					0,1				
		Divulgación De Información	25%	0,075			2					0,15		
SW8	Aplicación del Sistema de tickets de incidencias	Fallo De Origen Lógico	80%	0,02	1,5					0,03				
		Errores De Usuarios	50%	0,25	1,5	2,25	1,5			0,375	0,5625	0,375		
		Errores De Administración	90%	0,01	1,5	2,25	1,5			0,015	0,0225	0,015		
		Alteración Accidental De La Información	75%	0,075		2,25					0,1688			
		Destrucción De Información	25%	0,075	1					0,075				
		Fugas De Información	25%	0,075			3					0,225		
		Vulnerabilidades De Los Programas	90%	0,03	1,5	2,25	3			0,045	0,0675	0,09		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	1	2,25				0,075	0,1688			
		Suplantación De La Identidad Del Usuario	25%	0,075		2,25	1,5	1,688			0,1688	0,1125	0,1266	
		Abuso De Privilegios De Acceso	75%	0,075	1	2,25	1,5			0,075	0,1688	0,1125		
		Uso No Previsto	50%	0,15	1	2,25	0,75			0,15	0,3375	0,1125		
		Difusión De Software Dañino	90%	0,01	2	3	1,5			0,02	0,03	0,015		
		Acceso No Autorizado	90%	0,01		2,25	1,5				0,0225	0,015		
		Modificación Deliberada De La Información	50%	0,05		3					0,15			
		Destrucción De Información	50%	0,05	1					0,05				
		Divulgación De Información	25%	0,075			1,5					0,1125		
SW9	Aplicación de Correo electrónico Gmail	Errores De Usuarios	50%	0,25	0,333	0,38	1,5			0,0831	0,095	0,375		
		Errores De Administración	90%	0,01	1,313	0,38	2			0,0131	0,0038	0,02		
		Difusión De Software Dañino	80%	0,02	0,333	0,38	4			0,0067	0,0076	0,08		
		Alteración Accidental De La Información	75%	0,075		0,38					0,0285			
		Destrucción De Información	75%	0,025	1,313					0,0328				
		Fugas De Información	50%	0,15			4					0,6		
		Vulnerabilidades De Los Programas	90%	0,03	0,333	2	4			0,01	0,06	0,12		
		Errores De Mantenimiento/Actualización De Programas	90%	0,01	1,313	2	3			0,0131	0,02	0,03		
		Suplantación De La Identidad Del Usuario	75%	0,025		2	4	2,25			0,05	0,1	0,0563	
		Abuso De Privilegios De Acceso	75%	0,025	0,333	1,5	3			0,0083	0,0375	0,075		
		Uso No Previsto	50%	0,15	1,75	1,5	4			0,2625	0,225	0,6		
		Difusión De Software Dañino	75%	0,025	0,333	2	4			0,0083	0,05	0,1		
		Acceso No Autorizado	75%	0,025		2	4				0,05	0,1		
		Modificación Deliberada De La Información	75%	0,025		4					0,1			
		Destrucción De Información	75%	0,025	1,75					0,0438				
		Divulgación De Información	75%	0,025			4					0,1		

Figura 188. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (b) (Fuente propia)

SW10	E-apsa	Fallo De Origen Lógico	80%	0,02	1,5					0,03				
		Errores De Usuarios	25%	0,375	0,38	0,38	1,313			0,1425	0,1425	0,4922		
		Errores De Administración	90%	0,01	2	3	2,625			0,02	0,03	0,0263		
		Alteración Accidental De La Información	50%	0,15		1,5					0,225			
		Destrucción De Información	25%	0,225	0,38					0,0855				
		Fugas De Información	25%	0,075			1,313					0,0984		
		Vulnerabilidades De Los Programas	90%	0,03	0,38	1,5	1,75			0,0114	0,045	0,0525		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	1,5	1,5				0,1125	0,1125			
		Suplantación De La Identidad Del Usuario	25%	0,225		1,5	1,313	2			0,3375	0,2953	0,45	
		Abuso De Privilegios De Acceso	75%	0,075	0,38	1,5	1,313			0,0285	0,1125	0,0984		
		Uso No Previsto	50%	0,05	1,5	0,38	1,75			0,075	0,019	0,0875		
		Difusión De Software Dañino	90%	0,01	0,38	1,5	1,75			0,0038	0,015	0,0175		
		Acceso No Autorizado	90%	0,01		1,5	1,75				0,015	0,0175		
		Modificación Deliberada De La Información	50%	0,05		1,5					0,075			
		Destrucción De Información	50%	0,05	1,5					0,075				
		Divulgación De Información	25%	0,075			1,313					0,0984		
SW11	Aplicaciones en móviles	Fallo De Origen Lógico	90%	0,01	1					0,01				
		Errores De Usuarios	25%	0,375	0,19	1,5	1,75			0,0713	0,5625	0,6563		
		Errores De Administración	90%	0,01	0,75	1,5	1,75			0,0075	0,015	0,0175		
		Difusión De Software Dañino	50%	0,15	0,19	1,5	2,625			0,0285	0,225	0,3938		
		Alteración Accidental De La Información	10%	0,27		1,5					0,405			
		Destrucción De Información	10%	0,27	0,75					0,2025				
		Fugas De Información	25%	0,225			2,625					0,5906		
		Vulnerabilidades De Los Programas	75%	0,075	0,75	1,5	2,625			0,0563	0,1125	0,1969		
		Errores De Mantenimiento/Actualización De Programas	90%	0,05	1	1,5				0,05	0,075			
		Suplantación De La Identidad Del Usuario	90%	0,03		1,5	2,625	3			0,045	0,0788	0,09	
		Abuso De Privilegios De Acceso	25%	0,225	0,75	1,5	2,625			0,1688	0,3375	0,5906		
		Uso No Previsto	10%	0,09	1,5	2	2,625			0,135	0,18	0,2363		
		Difusión De Software Dañino	50%	0,05	0,75	2	3,5			0,0375	0,1	0,175		
		Acceso No Autorizado	75%	0,025		1,5	3,5				0,0375	0,0875		
		Modificación Deliberada De La Información	25%	0,075		1,5					0,1125			
		Destrucción De Información	25%	0,075	1					0,075				
		Divulgación De Información	50%	0,05			3,5					0,175		
SW12	Sistema operativo Ubuntu Server	Fallo De Origen Lógico	90%	0,01	3,375					0,0338				
		Errores De Administración	90%	0,01	2,25	3,375	2,25			0,0225	0,0338	0,0225		
		Alteración Accidental De La Información	75%	0,025		3,375					0,0844			
		Destrucción De Información	75%	0,025	2,25					0,0563				
		Vulnerabilidades De Los Programas	90%	0,01	1,688	3,375	2,25			0,0169	0,0338	0,0225		
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	1,688	3,375				0,0506	0,1013			
		Suplantación De La Identidad Del Usuario	90%	0,03		3,375	2,25	0,9			0,1013	0,0675	0,027	
		Abuso De Privilegios De Acceso	80%	0,06	2,25	3,375	2,25			0,135	0,2025	0,135		
		Uso No Previsto	80%	0,02	2,25	3,375	2,25			0,045	0,0675	0,045		
		Difusión De Software Dañino	90%	0,01	4,5	2,25	2,25			0,045	0,0225	0,0225		
		Acceso No Autorizado	90%	0,01		2,25	2,25				0,0225	0,0225		
		Modificación Deliberada De La Información	80%	0,02		2,25					0,045			
		Destrucción De Información	80%	0,02	2,25					0,045				
		Divulgación De Información	90%	0,01			2,25					0,0225		
SW13	Sistema Operativo Windows Server	Fallo De Origen Lógico	90%	0,01	3,375					0,0338				
		Errores De Administración	90%	0,01	2,25	3,375	2,25			0,0225	0,0338	0,0225		
		Alteración Accidental De La Información	75%	0,025		3,375					0,0844			
		Destrucción De Información	75%	0,025	2,25					0,0563				
		Vulnerabilidades De Los Programas	90%	0,01	1,688	3,375	2,25			0,0169	0,0338	0,0225		
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	1,688	3,375				0,0506	0,1013			
		Suplantación De La Identidad Del Usuario	90%	0,03		3,375	2,25	2,25			0,1013	0,0675	0,0675	
		Abuso De Privilegios De Acceso	80%	0,06	2,25	3,375	2,25			0,135	0,2025	0,135		
		Uso No Previsto	80%	0,02	2,25	3,375	2,25			0,045	0,0675	0,045		
		Difusión De Software Dañino	90%	0,01	4,5	2,25	2,25			0,045	0,0225	0,0225		
		Acceso No Autorizado	90%	0,01		2,25	2,25				0,0225	0,0225		
		Modificación Deliberada De La Información	80%	0,02		2,25					0,045			
		Destrucción De Información	80%	0,02	2,25					0,045				
		Divulgación De Información	90%	0,01			2,25					0,0225		
SW14	Sistema operativo Windows 7	Fallo De Origen Lógico	90%	0,01	3					0,03				
		Errores De Usuarios	25%	0,375	0,75	0,428	0,938			0,2813	0,1603	0,3516		
		Errores De Administración	90%	0,01	1	1,688	1,875			0,01	0,0169	0,0188		
		Difusión De Software Dañino	50%	0,05	0,75	3,375	1,875			0,0375	0,1688	0,0938		
		Alteración Accidental De La Información	10%	0,09		1,688					0,1519			
		Destrucción De Información	10%	0,09	2					0,18				
		Vulnerabilidades De Los Programas	90%	0,03	0,75	1,688	2,5			0,0225	0,0506	0,075		
		Errores De Mantenimiento/Actualización De Programas	75%	0,075	0,75	1,688				0,0563	0,1266			
		Suplantación De La Identidad Del Usuario	90%	0,03		0,428	1,25	2			0,0128	0,0375	0,06	
		Abuso De Privilegios De Acceso	25%	0,225	0,19	0,428	0,938			0,0428	0,0962	0,2109		
		Uso No Previsto	10%	0,27	0,75	1,688	1,25			0,2025	0,4556	0,3375		
		Difusión De Software Dañino	75%	0,025	0,75	1,688	1,25			0,0188	0,0422	0,0313		
		Acceso No Autorizado	90%	0,03		1,688	1,25				0,0506	0,0375		
		Modificación Deliberada De La Información	25%	0,075		1,688					0,1266			
		Destrucción De Información	25%	0,075	3					0,225				
		Divulgación De Información	10%	0,09			1,25					0,1125		
SW15	Sistema operativo Windows 10	Fallo De Origen Lógico	90%	0,01	3					0,03				
		Errores De Usuarios	25%	0,375	0,75	0,428	0,938			0,2813	0,1603	0,3516		
		Errores De Administración	90%	0,01	1	1,688	1,875			0,01	0,0169	0,0188		
		Difusión De Software Dañino	50%	0,05	0,75	3,375	1,875			0,0375	0,1688	0,0938		
		Alteración Accidental De La Información	10%	0,09		1,688					0,1519			
		Destrucción De Información	10%	0,09	2					0,18				
		Vulnerabilidades De Los Programas	90%	0,03	0,75	1,688	2,5			0,0225	0,0506	0,075		
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	0,75	1,688				0,0225	0,0506			
		Suplantación De La Identidad Del Usuario	90%	0,03		0,428	1,25	2			0,0128	0,0375	0,06	
		Abuso De Privilegios De Acceso	25%	0,225	0,19	0,428	0,938			0,0428	0,0962	0,2109		
		Uso No Previsto	10%	0,27	0,75	1,688	1,25			0,2025	0,4556	0,3375		
		Difusión De Software Dañino	80%	0,02	0,75	1,688	1,25			0,015	0,0338	0,025		
		Acceso No Autorizado	90%	0,03		1,688	1,25				0,0506	0,0375		
		Modificación Deliberada De La Información	25%	0,075		1,688					0,1266			
		Destrucción De Información	25%	0,075	3					0,225				
		Divulgación De Información	10%	0,09			1,25					0,1125		
SW16	Navegadores Web	Errores De Usuarios	25%	0,375	0,19	0,38	3			0,0713	0,1425	1,125		
		Errores De Administración	90%	0,01	0,75	0,38	3			0,0075	0,0038	0,03		
		Fugas De Información	75%	0,025			4					0,1		
		Vulnerabilidades De Los Programas	75%	0,025	0,75	2	4			0,0188	0,05	0,1		
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	0,19	2				0,0057	0,06			
		Abuso De Privilegios De Acceso	25%	0,225	0,19	0,38	3			0,0428	0,0855	0,675		
		Uso No Previsto	90%	0,03	0,19	1,5	3			0,0057	0,045	0,09		
		Difusión De Software Dañino	50%	0,25	0,19	1,5				0,0475	0,375			
		Modificación Deliberada De La Información	25%	0,075		1,5					0,1125			
		Destrucción De Información		0,1	0,75					0,075				
		Divulgación De Información	10%	0,09			1,5					0,135		

Figura 189. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (c) (Fuente propia)

SW17	Antivirus	Fallo De Origen Lógico	90%	0,01	3					0,03					
		Errores De Administración	90%	0,01	3	1,5	0,938			0,03	0,015	0,0094			
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	1,5	4				0,045	0,12				
		Abuso De Privilegios De Acceso	50%	0,05	2	4	0,938			0,1	0,2	0,0469			
		Uso No Previsto	25%	0,075	2	4	0,938			0,15	0,3	0,0703			
		Acceso No Autorizado	50%	0,05		4	0,938				0,2	0,0469			
		Modificación Deliberada De La Información		0,1		4					0,4				
SW18	Software Ofimático	Fallo De Origen Lógico	90%	0,03	0,75					0,0225					
		Errores De Usuarios	10%	0,45	0,75	0,238	0,938			0,3375	0,1069	0,4219			
		Errores De Administración	50%	0,05	0,75	0,238	0,938			0,0375	0,0119	0,0469			
		Errores De Mantenimiento/Actualización De Programas	90%	0,03	0,563	0,938				0,0169	0,0281				
		Abuso De Privilegios De Acceso		0,1	0,563	0,938	0,938			0,0563	0,0938	0,0938			
		Uso No Previsto		0,1	0,75	0,938	0,938			0,075	0,0938	0,0938			

Figura 190. Efectividad de las salvaguardas e impacto residual del grupo Aplicaciones informáticas. (d) (Fuente propia)

- [HW] Equipos Informáticos (Hardware)

Para estos activos, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia mayormente superior a 75%, excepto para las amenazas de corte de suministro eléctrico. En correlación, la frecuencia residual tiene valores bajos que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido de 4 y 1 en el tratamiento de riesgo de este activo. Finalmente, existen casos en los que el riesgo ha sido eliminado completamente porque la efectividad de la frecuencia es 100%. Las Figuras 191, 192 y 193 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

EQUIPOS INFORMÁTICOS [HW]			Efectividad de Frecuencias	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas		F'	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
HW1	Servidores APSA	Avería De Origen Físico/Lógico	75%	0,075	9					0,675				
		Errores De Administración	90%	0,01	4,5	4,5	2,25			0,045	0,045	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	75%	0,075	3,375					0,2531				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4,05					0,0405				
		Abuso De Privilegios De Acceso	90%	0,01	3,375	3,375	2,25			0,0338	0,0338	0,0225		
		Uso No Previsto	90%	0,03	3,375	3,375	2,25			0,1013	0,1013	0,0675		
		Acceso No Autorizado	90%	0,07		3,375	2,25				0,2363	0,1575		
		Denegación De Servicio	75%	0,075	4,5					0,3375				
HW2	Servidores Sedes	Daños Por Agua	100%		2									
		Avería De Origen Físico/Lógico	75%	0,075	2					0,15				
		Corte De Suministro Eléctrico	100%		4									
		Fallas De Climatización	50%	0,05	1					0,05				
		Errores De Administración	90%	0,01	1,5	3	2,25			0,015	0,03	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,03	1,5					0,045				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	90%	0,03	1,5	3	2,25			0,045	0,09	0,0675		
		Uso No Previsto	90%	0,03	2	2	2,25			0,06	0,06	0,0675		
		Acceso No Autorizado	75%	0,125		3	2,25				0,375	0,2813		
		Manipulación De Equipos	90%	0,03	3		1,688			0,09		0,0506		
		Denegación De Servicio	75%	0,075	4					0,3				
		Robo	75%	0,025	2		1,688			0,05		0,0422		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	100%		3,938									
		Avería De Origen Físico/Lógico	75%	0,075	5,25					0,3938				
		Corte De Suministro Eléctrico		0,3	7					2,1				
		Errores De Administración	90%	0,01	2,625	1	1,5			0,0263	0,01	0,015		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,05	2,625					0,1313				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,03	2,625					0,0788				
		Perdida De Equipos	90%	0,01	5,25		6			0,0525		0,06		
		Abuso De Privilegios De Acceso	50%	0,05	1,75	3	4			0,0875	0,15	0,2		
		Uso No Previsto	50%	0,15	3,938	1,5	4			0,5906	0,225	0,6		
		Acceso No Autorizado	90%	0,01		1,5	4				0,015	0,04		
		Manipulación De Equipos	10%	0,27	2,625		2			0,7088		0,54		
		Robo	75%	0,025	5,25		6			0,1313		0,15		

Figura 191. Efectividad de las salvaguardas e impacto residual del grupo Equipos informáticos. (a) (Fuente propia)

HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	75%	0,075	7					0,525				
		Corte De Suministro Eléctrico		0,1	1,575					0,1575				
		Errores De Administración	90%	0,03	2,625	1,5	4			0,0788	0,045	0,12		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,05	2,625					0,1313				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,03	2,625					0,0788				
		Perdida De Equipos	25%	0,075	6,3		4			0,4725		0,3		
		Abuso De Privilegios De Acceso	50%	0,15	1,313	1,5	4			0,1969	0,225	0,6		
		Uso No Previsto	50%	0,15	2,625	0,5	4			0,3938	0,075	0,6		
		Acceso No Autorizado	90%	0,01		4,5	4				0,045	0,04		
		Manipulación De Equipos	25%	0,225	3,938		4			0,8859		0,9		
		Robo	75%	0,025	6,3		4			0,1575		0,1		
HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	75%	0,075	3					0,225				
		Corte De Suministro Eléctrico		0,1	0,75					0,075				
		Errores De Administración	90%	0,03	1,125	1,313	0,438			0,0338	0,0394	0,0131		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,05	1,125					0,0563				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,03	1,125					0,0338				
		Perdida De Equipos	25%	0,075	2,25		2,625			0,1688		0,1969		
		Abuso De Privilegios De Acceso	50%	0,15	0,563	1,313	2,625			0,0844	0,1969	0,3938		
		Uso No Previsto	50%	0,15	1,125	0,438	2,625			0,1688	0,0656	0,3938		
		Acceso No Autorizado	90%	0,03		2,625	2,625				0,0788	0,0788		
		Manipulación De Equipos	25%	0,225	1,125		2,625			0,2531		0,5906		
		Robo	75%	0,025	2,25		3,5			0,0563		0,0875		
HW7	Portátiles TIC	Daños Por Agua	100%		8									
		Avería De Origen Físico/Lógico	75%	0,025	7,2					0,18				
		Corte De Suministro Eléctrico	90%	0,01	3					0,03				
		Errores De Administración	90%	0,01	3	1,688	2,25			0,03	0,0169	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,03	4,5					0,135				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	50%	0,05	3	5,063	2,25			0,15	0,2531	0,1125		
		Acceso No Autorizado	90%	0,01		5,063	2,25				0,0506	0,0225		
		Manipulación De Equipos	50%	0,05	3		2,25			0,15		0,1125		
HW8	Móviles/Tablets	Avería De Origen Físico/Lógico	50%	0,15	2,25					0,3375				
		Errores De Administración	50%	0,05	0,5	1,313	1,75			0,025	0,0656	0,0875		
		Errores De Mantenimiento/Actualización De Equipos	75%	0,125	2,25					0,2813				
		Caída Del Sistema Por Agotamiento De Recursos	25%	0,225	1					0,225				
		Perdida De Equipos	10%	0,45	4		3,5			1,8		1,575		
		Abuso De Privilegios De Acceso	50%	0,15	2	2,625	3,5			0,3	0,3938	0,525		
		Uso No Previsto	10%	0,45	2	2,625	3,5			0,9	1,1813	1,575		
		Acceso No Autorizado	50%	0,05		3,938	3,5				0,1969	0,175		
		Manipulación De Equipos	25%	0,375	2,7		3,5			1,0125		1,3125		
		Robo	10%	0,27	4		3,5			1,08		0,945		
HW9	Impresoras oficinas	Avería De Origen Físico/Lógico	50%	0,15	0,75					0,1125				
		Corte De Suministro Eléctrico		0,1	3					0,3				
		Errores De Administración	90%	0,01	0,75	0,75	0,15			0,0075	0,0075	0,0015		
		Errores De Mantenimiento/Actualización De Equipos	90%	0,03	0,75					0,0225				
		Caída Del Sistema Por Agotamiento De Recursos	75%	0,125	1,125					0,1406				
		Perdida De Equipos	75%	0,025	3		0,75			0,075		0,0188		
		Abuso De Privilegios De Acceso	25%	0,225	1,35	0,375	0,135			0,3038	0,0844	0,0304		
		Uso No Previsto	25%	0,225	0,675	0,375	0,675			0,1519	0,0844	0,1519		
		Acceso No Autorizado	25%	0,075		0,375	0,675				0,0281	0,0506		
		Manipulación De Equipos	25%	0,225	1,35		0,675			0,3038		0,1519		
		Robo	75%	0,025	3		0,75			0,075		0,0188		
HW10	Router	Avería De Origen Físico/Lógico	75%	0,025	6					0,15				
		Corte De Suministro Eléctrico		0,1	8					0,8				
		Fallas De Climatización	25%	0,075	3,6					0,27				
		Errores De Administración	90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	80%	0,06	4,5					0,27				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Uso No Previsto	90%	0,01	6	2	4			0,06	0,02	0,04		
		Acceso No Autorizado	90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	90%	0,03	4,5		4			0,135		0,12		
		Denegación De Servicio	90%	0,03	8					0,24				
HW11	Router inalámbrico	Daños Por Agua	100%		8									
		Avería De Origen Físico/Lógico	75%	0,025	4,5					0,1125				
		Corte De Suministro Eléctrico		0,1	8					0,8				
		Errores De Administración	90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	80%	0,06	4,5					0,27				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4					0,04				
		Perdida De Equipos	75%	0,025	8		2			0,2		0,05		
		Abuso De Privilegios De Acceso	90%	0,03	3	2	3			0,09	0,06	0,09		
		Uso No Previsto	90%	0,03	6	3	3			0,18	0,09	0,09		
		Acceso No Autorizado	90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	90%	0,03	4,5		2			0,135		0,06		
		Denegación De Servicio	90%	0,03	8					0,24				
		Robo	75%	0,025	8		2			0,2		0,05		
HW12	Switch	Avería De Origen Físico/Lógico	75%	0,025	6					0,15				
		Corte De Suministro Eléctrico		0,1	8					0,8				
		Fallas De Climatización	25%	0,075	3,6					0,27				
		Errores De Administración	90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	80%	0,06	4,5					0,27				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Uso No Previsto	90%	0,01	6	2	4			0,06	0,02	0,04		
		Acceso No Autorizado	90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	90%	0,03	4,5		4			0,135		0,12		
		Denegación De Servicio	90%	0,03	8					0,24				

Figura 192. Efectividad de las salvaguardas e impacto residual del grupo Equipos informáticos. (b) (Fuente propia)

HW13	Impresoras repositorios	Avería De Origen Físico/Lógico	75%	0,075	6					0,45				
		Corte De Suministro Eléctrico		0,1	8					0,8				
		Errores De Administración	90%	0,03	3	1,125	1,5			0,09	0,0338	0,045		
		Errores De Mantenimiento/Actualización De Equipos	75%	0,075	3					0,225				
		Caída Del Sistema Por Agotamiento De Recursos	90%	0,03	4					0,12				
		Abuso De Privilegios De Acceso	50%	0,15	3	2,25	0,75			0,45	0,3375	0,1125		
		Uso No Previsto	50%	0,15	6	1,875	0,75			0,9	0,2813	0,1125		
		Acceso No Autorizado	90%	0,01		2,25	0,75				0,0225	0,0075		
		Manipulación De Equipos	50%	0,15	4,5		0,75			0,675		0,1125		
HW14	Teléfonos de sobremesa	Avería De Origen Físico/Lógico	75%	0,025	4,5					0,1125				
		Corte De Suministro Eléctrico		0,1	6					0,6				
		Errores De Administración	90%	0,01	1,5	1,125	1,5			0,015	0,0113	0,015		
		Errores De Mantenimiento/Actualización De Equipos	80%	0,06	2,25					0,135				
		Abuso De Privilegios De Acceso	90%	0,03	2,25	1,125	2,25			0,0675	0,0338	0,0675		
		Uso No Previsto	90%	0,03	4,5	0,938	2,25			0,135	0,0281	0,0675		
		Acceso No Autorizado	90%	0,01		2,5	2,25				0,025	0,0225		
		Manipulación De Equipos	75%	0,125	3,375		2,25			0,4219		0,2813		
		Robo	75%	0,025	6		0,2			0,15		0,005		

Figura 193. Efectividad de las salvaguardas e impacto residual del grupo Equipos informáticos. (c) (Fuente propia)

- [COM] Redes de Comunicaciones

Para las redes de comunicaciones, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia entre el 25% y 90%, excepto en el caso de la caída del sistema por agotamiento de recursos, suplantación de identidad de usuarios, análisis de tráfico e interceptación de información en el activo red de telefonía móvil. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 1, pero se observa que la condición no se cumple en el caso del abuso de privilegios de acceso y uso no previsto de las redes telefónicas y el fallo de las comunicaciones en el caso de la telefonía móvil, entendiéndose que esos errores son difíciles de evitar y que la asociación asume los riesgos. Finalmente, para estos activos siempre hay un riesgo aunque sea mínimo. Las Figuras 194 y 195 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

REDES DE COMUNICACIONES [COM]			Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	Frecuencia	F'	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	25%	0,225	3,5					0,7875				
		Errores De Administración	90%	0,01	2,625	1,5	0,675			0,0263	0,015	0,0068		
		Alteración Accidental De La Información	90%	0,03		3					0,09			
		Caída Del Sistema Por Agotamiento De Recursos	75%	0,075	3,5					0,2625				
		Suplantación De La Identidad Del Usuario	90%	0,07		3	4,5	4,5			0,21	0,315	0,315	
		Abuso De Privilegios De Acceso	50%	0,15	0,875	3	3,375			0,1313	0,45	0,5063		
		Uso No Previsto	50%	0,15	1,75	2	3,375			0,2625	0,3	0,5063		
		Acceso No Autorizado	75%	0,125		3	4,5				0,375	0,5625		
		Análisis De Trafico	50%	0,05			4,5					0,225		
		Interceptación De Información (Escucha)	50%	0,05			4,5					0,225		
		Modificación Deliberada De La Información	90%	0,03		4,5					0,135			
		Divulgación De Información	50%	0,25			3,375					0,8438		
		Denegación De Servicio	75%	0,125	1,75					0,2188				
COM2	Redes locales	Fallo Servicios De Comunicaciones	25%	0,225	4					0,9				
		Errores De Administración	90%	0,01	3	3	0,9			0,03	0,03	0,009		
		Alteración Accidental De La Información	90%	0,03		3					0,09			
		Caída Del Sistema Por Agotamiento De Recursos	75%	0,075	4					0,3				
		Suplantación De La Identidad Del Usuario	90%	0,05		4,5	4,5	2,25			0,225	0,225	0,1125	
		Abuso De Privilegios De Acceso	50%	0,15	1	4,5	4,5			0,15	0,675	0,675		
		Uso No Previsto	75%	0,075	2	4	4,5			0,15	0,3	0,3375		
		Acceso No Autorizado	75%	0,125		3	4,5				0,375	0,5625		
		Análisis De Trafico	50%	0,05			4,5					0,225		
		Interceptación De Información (Escucha)	50%	0,05			4,5					0,225		
		Modificación Deliberada De La Información	90%	0,03		4,5					0,135			
		Divulgación De Información	50%	0,25			3,375					0,8438		
		Denegación De Servicio	75%	0,125	2					0,25				

Figura 194. Efectividad de las salvaguardas e impacto residual del grupo Redes de comunicaciones. (a) (Fuente propia)

COM3	Red telefónica	Fallo Servicios De Comunicaciones	25%	0,225	4					0,9				
		Errores De Administración	90%	0,01	3	2,625	3			0,03	0,0263	0,03		
		Alteración Accidental De La Información	90%	0,03		2,625					0,0788			
		Caída Del Sistema Por Agotamiento De Recursos	50%	0,05	4					0,2				
		Abuso De Privilegios De Acceso	25%	0,375	2	1,313	3			0,75	0,4922	1,125		
		Uso No Previsto	25%	0,375	2	1,313	3			0,75	0,4922	1,125		
		Acceso No Autorizado	25%	0,225		1,313	4				0,2953	0,9		
		Análisis De Trafico	25%	0,075			4					0,3		
		Interceptación De Información (Escucha)	25%	0,075			4					0,3		
		Modificación Deliberada De La Información	50%	0,05		2,625					0,1313			
		Divulgación De Información	25%	0,225			3					0,675		
		Denegación De Servicio	50%	0,05	6					0,3				
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	25%	0,225	8					1,8				
		Caída Del Sistema Por Agotamiento De Recursos		0,1	6					0,6				
		Suplantación De La Identidad Del Usuario		0,1		0,35	5,4	4,725			0,035	0,54	0,4725	
		Abuso De Privilegios De Acceso	25%	0,225	0,1	0,35	3,6			0,0225	0,0788	0,81		
		Uso No Previsto	25%	0,225	0,1	0,35	5,4			0,0225	0,0788	1,215		
		Acceso No Autorizado	25%	0,225		0,35	5,4				0,0788	1,215		
		Análisis De Trafico		0,1			8					0,8		
		Interceptación De Información (Escucha)		0,1			8					0,8		
		Divulgación De Información	50%	0,15			8					1,2		

Figura 195. Efectividad de las salvaguardas e impacto residual del grupo Redes de comunicaciones. (b) (Fuente propia)

- [MEDIA] Soportes de Información

Para las redes de comunicaciones, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia entre el 25% y 100%, excepto en el caso de las fugas de información en el activo material impreso. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento del riesgo para este activo. Se definió un nivel mínimo de aceptación de 4 y todos los valores de riesgo cumplen con esta condición. Finalmente, existen casos en los que el riesgo ha sido eliminado porque el impacto residual es cero o la efectividad de la frecuencia es 100%. Las Figuras 196 y 197 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	Frecuencia	F'	D	I	C	A	T	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	100%		8									
		Daños Por Agua	100%		8									
		Avería De Origen Físico/Lógico	50%	0,05	5,4					0,27				
		Degradación De Los Soportes De Almacenamiento De La Información	50%	0,05	5,4					0,27				
		Errores De Usuarios	50%	0,15	2	5,063				0,3	0,7594			
		Errores De Administración	90%	0,01	2	3,375	0,9			0,02	0,0338	0,009		
		Alteración Accidental De La Información	50%	0,15		6,075					0,9113			
		Destrucción De Información	50%	0,05	8					0,4				
		Fugas De Información	25%	0,075										
		Errores De Mantenimiento del soporte	25%	0,225	1,8					0,405				
		Perdida del soporte	50%	0,05	8					0,4				
		Uso No Previsto	75%	0,075	7,2	6,75				0,54	0,5063			
		Acceso No Autorizado	75%	0,075		4,5					0,3375			
		Modificación Deliberada De La Información	75%	0,025		6,75					0,1688			
		Destrucción De Información	75%	0,025	8					0,2				
		Divulgación De Información	25%	0,075										
		Manipulación del soporte	50%	0,15	3,6					0,54				
		Robo	25%	0,075	8					0,6				
MEDIA2	Pendrives USB	Daños Por Agua	100%		7									
		Daños Por Agua	100%		7									
		Avería De Origen Físico/Lógico	50%	0,05	4,725					0,2363				
		Degradación De Los Soportes De Almacenamiento De La Información	50%	0,15	4,725					0,7088				
		Errores De Usuarios	50%	0,25	1,575	3				0,3938	0,75			
		Errores De Administración	90%	0,01	1,575	2				0,0158	0,02			
		Alteración Accidental De La Información	50%	0,25		7,2					1,8			
		Destrucción De Información	50%	0,25	7					1,75				
		Fugas De Información	25%	0,225										
		Errores De Mantenimiento del soporte		0,1	3,15					0,315				
		Perdida del soporte	25%	0,525	7					3,675				
		Uso No Previsto	50%	0,35	4,725	6				1,6538	2,1			
		Acceso No Autorizado	75%	0,025		4					0,1			
		Modificación Deliberada De La Información	75%	0,025		6					0,15			
		Destrucción De Información	75%	0,025	5,25					0,1313				
		Divulgación De Información	25%	0,225										
		Manipulación del soporte	50%	0,05	4,725					0,2363				
		Robo	25%	0,225	7					1,575				

Figura 196. Efectividad de las salvaguardas e impacto residual del grupo Soportes de información. (a) (Fuente propia)

MEDIA3	CD/DVD	Daños Por Agua	100%		7										
		Daños Por Agua	100%		7										
		Avería De Origen Físico/Lógico	25%	0,075	4,725					0,3544					
		Degradación De Los Soportes De Almacenamiento De La Información	25%	0,225	4,725					1,0631					
		Errores De Usuarios	50%	0,25	1,575	3				0,3938	0,75				
		Errores De Administración	90%	0,01	1,575	2				0,0158	0,02				
		Alteración Accidental De La Información	50%	0,25		7,2					1,8				
		Destrucción De Información	50%	0,25	7					1,75					
		Fugas De Información	25%	0,225											
		Errores De Mantenimiento del soporte	50%	0,05	3,15					0,1575					
		Perdida del soporte	25%	0,525	7		0,9			3,675		0,4725			
		Uso No Previsto	50%	0,35	4,725	6				1,6538	2,1				
		Acceso No Autorizado	50%	0,05		4					0,2				
		Modificación Deliberada De La Información	50%	0,05		6					0,3				
		Destrucción De Información	50%	0,05	5,25					0,2625					
		Divulgación De Información	25%	0,225											
		Manipulación del soporte	50%	0,05	4,725					0,2363					
		Robo	25%	0,225	7		0,9			1,575		0,2025			
MEDIA4	Material impreso	Daños Por Agua	100%		7										
		Daños Por Agua	100%		7										
		Degradación por Almacenamiento	75%	0,075	1,313					0,0984					
		Errores De Usuarios	50%	0,25	2,625	4,5	1,688			0,6563	1,125	0,4219			
		Errores De Administración	50%	0,05	2,625	4,5	1,688			0,1313	0,225	0,0844			
		Alteración Accidental De La Información	25%	0,375		3					1,125				
		Destrucción	25%	0,375	3,5					1,3125					
		Fugas De Información		0,1			6,75					0,675			
		Errores De Almacenamiento	25%	0,375	1,75					0,6563					
		Perdida	75%	0,125	0,875		8,1			0,1094		1,0125			
		Uso No Previsto	50%	0,15	1,75	4,5	4,5			0,2625	0,675	0,675			
		Acceso No Autorizado	50%	0,15		4,5	6,75				0,675	1,0125			
		Modificación Deliberada De La Información	25%	0,075		6					0,45				
		Destrucción	75%	0,025	1,75					0,0438					
		Divulgación	25%	0,075			6,75					0,5063			
		Manipulación	50%	0,05	0,875		6,75			0,0438		0,3375			
		Robo	75%	0,075	0,875		9			0,0656		0,675			

Figura 197. Efectividad de las salvaguardas e impacto residual del grupo Soportes de Información. (b) (Fuente propia)

- [AUX] Equipamiento Auxiliar

Para el equipamiento auxiliar, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia entre el 10% y 100%, excepto en el caso de el corte de suministro eléctrico en la climatización y fuentes de alimentación. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al Riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 4 y todos los valores de riesgo cumplen con esta condición. Finalmente, para estos activos siempre hay un riesgo aunque sea mínimo. Las Figuras 198 y 199 muestran los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenaza	Frecuencia	F´	D	I	C	A	T	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	90%	0,03	3,75					0,1125				
		Fuego	75%	0,025	3,75					0,0938				
		Daños Por Agua	75%	0,075	3,75					0,2813				
		Contaminación Mecánica	25%	0,075	0,625					0,0469				
		Degradación por almacenamiento	50%	0,15	0,625					0,0938				
		Avería De Origen Físico/ Lógico	50%	0,15	0,938					0,1406				
		Errores De Mantenimiento/ Actualización De Equipos	75%	0,025	0,938					0,0234				
		Uso No Previsto	25%	0,225	1,875	0,625	0,15			0,4219	0,1406	0,0338		
		Acceso No Autorizado	25%	0,225		0,625	0,15				0,1406	0,0338		
		Manipulación De Equipos	25%	0,225	1,875		0,15			0,4219		0,0338		
AUX2	Fuentes de alimentación	Daños Por Agua	90%	0,03	3,75					0,1125				
		Fuego	75%	0,025	3,75					0,0938				
		Daños Por Agua	75%	0,075	3,75					0,2813				
		Contaminación Mecánica	25%	0,075	0,625					0,0469				
		Degradación por almacenamiento	50%	0,15	0,625					0,0938				
		Avería De Origen Físico/ Lógico	50%	0,15	0,938					0,1406				
		Corte De Suministro Eléctrico		0,3	5					1,5				
		Errores De Mantenimiento/ Actualización De Equipos	75%	0,075	0,938					0,0703				
		Perdida De Equipos	25%	0,075	5		0,15			0,375		0,0113		
		Uso No Previsto	25%	0,225	2,5	0,875	0,113			0,5625	0,1969	0,0253		
		Acceso No Autorizado	25%	0,225		0,875	0,15				0,1969	0,0338		
		Manipulación De Equipos	25%	0,225	1,875		0,113			0,4219		0,0253		
		Robo	25%	0,075	5		0,15			0,375		0,0113		

Figura 198. Efectividad de las salvaguardas e impacto residual del grupo equipamiento auxiliar. (a) (Fuente propia)

AUX3	Climatización	Daños Por Agua	90%	0,03	3,75					0,1125					
		Fuego	75%	0,025	3,75					0,0938					
		Daños Por Agua	75%	0,075	3,75					0,2813					
		Contaminación Mecánica	75%	0,025	0,625					0,0156					
		Avería De Origen Físico/Lógico	50%	0,15	0,938					0,1406					
		Corte De Suministro Eléctrico		0,3	5					1,5					
		Errores De Mantenimiento/Actualización De Equipos	75%	0,075	0,938					0,0703					
		Uso No Previsto	25%	0,225	1,25	0,5	0,15			0,2813	0,1125	0,0338			
		Acceso No Autorizado	10%	0,27		0,5	0,15				0,135	0,0405			
		Manipulación De Equipos	25%	0,375	1,25		0,15			0,4688		0,0563			
AUX4	Cableado UTP	Daños Por Agua	90%	0,03	5,25					0,1575					
		Fuego	75%	0,025	7					0,175					
		Daños Por Agua	75%	0,075	5,25					0,3938					
		Avería De Origen Físico/Lógico	50%	0,15	1,313					0,1969					
		Errores De Mantenimiento/Actualización De Equipos	75%	0,075	1,313					0,0984					
		Uso No Previsto	50%	0,15	2,625	1,5	0,75			0,3938	0,225	0,1125			
		Acceso No Autorizado	25%	0,075		1,5	2,25				0,1125	0,1688			
		Manipulación De Equipos	25%	0,075	2,625		2,25			0,1969		0,1688			
AUX5	Armarios	Daños Por Agua	90%	0,03	3,6					0,108					
		Fuego	75%	0,025	5,4					0,135					
		Daños Por Agua	75%	0,075	3,6					0,27					
		Degradación por almacenamiento	75%	0,025	0,5					0,0125					
		Avería De Origen Físico/Lógico	75%	0,075	1					0,075					
		Uso No Previsto	90%	0,03	2	1,5	1,5			0,06	0,045	0,045			
		Acceso No Autorizado	90%	0,03		1,5	1,5				0,045	0,045			
		Manipulación De Equipos	90%	0,05	1		1,5			0,05		0,075			
AUX6	Cajas fuertes	Daños Por Agua	90%	0,01	1,5					0,015					
		Fuego	90%	0,01	1,5					0,015					
		Daños Por Agua	90%	0,01	1,5					0,015					
		Avería De Origen Físico/Lógico	75%	0,025	3					0,075					
		Corte De Suministro Eléctrico	50%	0,05	3					0,15					
		Errores De Mantenimiento/Actualización De Equipos	90%	0,03	3					0,09					
		Perdida De Equipos	90%	0,01	4		1,8			0,04		0,018			
		Uso No Previsto	90%	0,01	3	0,1	1,8			0,03	0,001	0,018			
		Acceso No Autorizado	90%	0,03		0,1	1,8				0,003	0,054			
		Manipulación De Equipos	90%	0,05	1		1,8			0,05		0,09			

Figura 199. Efectividad de las salvaguardas e impacto residual del grupo equipamiento auxiliar. (b) (Fuente propia)

- [L]Instalaciones

Para este grupo de activos, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia del 25% y 50%, excepto para el activo coche porque sus riesgos serán asumidos. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 4 y todos los valores de riesgo cumplen con esta condición. Finalmente, para estos activos siempre hay un riesgo aunque sea mínimo. La Figura 200 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE INSTALACIONES [L]			Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas		F'	D	I	C	A	T	D	I	C	A	T
L1	Edificios	Fuego	50%	0,05	3					0,15				
		Daños Por Agua	50%	0,15	2,25					0,3375				
		Fuego	50%	0,05	2,25					0,1125				
		Daños Por Agua	50%	0,15	1,5					0,225				
		Fugas De Información	25%	0,225			3					0,675		
		Uso No Previsto	25%	0,075	0,75	0,438	4,5			0,0563	0,0328	0,3375		
		Acceso No Autorizado	25%	0,225		1,313	4				0,2953	0,9		
L2	Cuartos servidores	Fuego	50%	0,05	4					0,2				
		Daños Por Agua	50%	0,05	4					0,2				
		Fuego	50%	0,05	4					0,2				
		Daños Por Agua	50%	0,15	4					0,6				
		Fugas De Información	25%	0,075			6					0,45		
		Uso No Previsto	25%	0,225	3	1,5	3			0,675	0,3375	0,675		
		Acceso No Autorizado	25%	0,225		3	4				0,675	0,9		
L3	Coche	Daños mecánicos		0,1	2					0,2				
		Accidente de tránsito		0,1	2					0,2				

Figura 200. Efectividad de las salvaguardas e impacto residual del grupo Instalaciones. (Fuente propia)

- [P] Personal

Para el Personal, las salvaguardas definidas tienen una efectividad en la frecuencia de ocurrencia de 25% y 50%, excepto en el caso de indisponibilidad del personal. En correlación, la frecuencia residual tiene valores pequeños que afectan directamente al riesgo residual y reducen sus valores hasta alcanzar el nivel definido en el tratamiento de riesgo de este activo. Se definió un nivel mínimo de aceptación de 4 y todos los valores de riesgo cumplen con esta condición. Finalmente, para estos activos siempre hay un riesgo aunque sea mínimo. La Figura 201 muestra los resultados del cálculo de la efectividad de las salvaguardas y el impacto residual de este grupo de activos.

ACTIVOS DE PERSONAL [P]			Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	Frecuencia	F´	D	I	C	A	T	D	I	C	A	T
P1	Administradores	Fugas De Información	50%	0,05			4,5					0,225		
		Indisponibilidad Del Personal		0,3	3					0,9				
		Indisponibilidad Del Personal		0,1	3					0,3				
		Extorsión	25%	0,075	1	3	4,5			0,075	0,225	0,3375		
		Ingeniería Social	25%	0,075	1	3	4,5			0,075	0,225	0,3375		
P2	Técnicos	Fugas De Información	50%	0,05			4,5					0,225		
		Indisponibilidad Del Personal		0,3	1,75					0,525				
		Indisponibilidad Del Personal		0,1	1,75					0,175				
		Extorsión	25%	0,075	0,875	2	4,5			0,0656	0,15	0,3375		
		Ingeniería Social	25%	0,075	0,875	2	4,5			0,0656	0,15	0,3375		
P3	Empleados	Fugas De Información	50%	0,05			4,5					0,225		
		Indisponibilidad Del Personal		0,3	1,75					0,525				
		Indisponibilidad Del Personal		0,1	1,75					0,175				
		Extorsión	25%	0,075	0,875	2	4,5			0,0656	0,15	0,3375		
		Ingeniería Social	25%	0,075	0,875	2	4,5			0,0656	0,15	0,3375		
P4	Usuarios	Fugas De Información	50%	0,15			4,5					0,675		
		Extorsión	25%	0,075	0,625	1,5	4,5			0,0469	0,1125	0,3375		
		Ingeniería Social	25%	0,075	0,625	1,5	4,5			0,0469	0,1125	0,3375		

Figura 201. Efectividad de las salvaguardas e impacto residual del grupo Personal. (Fuente propia)

4.6. Planes de Seguridad

4.6.1. Tratamiento del Riesgo

Después de todo el análisis del impacto y riesgos de los activos se detectó los siguientes riesgos graves:

- Servicios: suplantación de la identidad de usuarios, acceso no autorizado, destrucción de la información, errores de usuarios y alteración accidental de la información.
- Software: Uso no previsto, modificación deliberada de la información y difusión de software dañino.
- Hardware: acceso no autorizado
- Redes de comunicaciones: suplantación de identidad de usuarios y acceso no autorizado.

- Soportes de información: errores de usuarios alteración accidental de la información, pérdida del soporte y uso no previsto.
- Equipamiento auxiliar: manipulación de equipos.

Además de otros riesgos graves que involucran protección de la información, copias de seguridad y registros de actividad (logs). Por lo tanto, todas aquellas salvaguardas que mitiguen los riesgos listados anteriormente se agrupan para crear 5 planes de seguridad y recomendaciones adicionales.

4.6.2. Planes de Seguridad

A continuación, se presentan planes de seguridad que deben implementarse para mejorar la seguridad de la asociación:

CONTROL DE ACCESO

Proyecto: Protección de Datos e Información – Control de Acceso

Objetivo: Identificar los accesos a los activos de la asociación

Preservar la confidencialidad, integridad y autenticidad de los activos

Activos Afectados: Datos/Información, Servicios, Software, Equipos informáticos, Redes de comunicaciones, Soportes de información, Equipamiento auxiliar e Instalaciones.

Participantes: Todos los departamentos de la asociación.

Salvaguarda: Protección lógica y física para evitar el acceso no autorizado

Descripción: Uno de los aspectos críticos dentro de la asociación es el riesgo que puede causar el acceso no autorizado. Por ello, se deben tomar medidas se seguridad tanto para empleados y usuarios. Para cubrir todos los aspectos de los activos, el plan de seguridad se divide en dos partes: control de acceso lógico y control de acceso físico

Control de Acceso Lógico

- Este control cubre los activos: Datos/Información, Servicios, Aplicaciones y Redes de Comunicaciones.
- El primer punto es la gestión de empleados y usuarios, que para facilitar el trabajo del departamento TIC, será a través de grupos. Para clasificar a los grupos se puede considerar: lugar de trabajo, tipo de profesional, de acuerdo con la información y

servicios que puede acceder, y en función de las acciones que puede ejecutar en el sistema e información.

- Definidos los grupos y a qué tienen acceso, se debe establecer el tipo de perfil que tendrán los usuarios de cada grupo. El perfil irá definido a través de la asignación de permisos de acciones sobre el sistema y la información a los que tienen acceso. Como norma general a los grupos se les debe asignar el mínimo privilegio y después cambiará conforme a los requerimientos.
- Principalmente se identifican dos tipos de perfiles: usuarios y administradores. Para los administradores se recomienda: crear cuentas para realizar acciones que requieran permisos de administración, usar doble factor de autenticación, tener registro de logs, notificar este tipo de accesos, evitar privilegios heredados, las claves de accesos deben ser lo más robustas posibles y cambiarlas con frecuencia, y ser sometidas a auditorias. Para los usuarios se recomienda: elaborar un procedimiento de creación, modificación y borrado de cuentas, entregar de forma confidencial las credenciales de acceso, definir la caducidad de las contraseñas y definir procesos de bloqueos.
- Para acceder al sistema y la información se deben definir mecanismos de autenticación adecuados. Estos pueden ser: contraseñas, dispositivos o tokens, ya sean con mecanismos internos o basados en un servicio de terceros de autenticación.
- Todas las actividades que se realicen cuando un empleado o usuario ingresa al sistema debe quedar registrado para evitar ataques de no repudio.
- Finalmente, periódicamente se debe realizar una revisión de las cuentas de usuarios, grupos, perfiles y los permisos que cada uno tiene. Esta revisión ayuda a no otorgar más permisos de los que se requiere y retirar otros servicios como correo electrónico y equipos informáticos a usuarios dados de baja.

Control de Acceso Físico

- Este control cubre los activos: Equipos informáticos, Soportes de información, Equipamiento auxiliar e Instalaciones.
- Al igual que el acceso lógico, para controlar el acceso físico se crearán grupos de empleados, usuarios y personas externas para crearles un perfil de permisos de acceso.
- Lo primero que se debe controlar es el acceso físico a las Instalaciones. Todos los edificios deben poseer seguridad en todos sus accesos para cuando las actividades diarias culminen. Seguridad extra deben tener oficinas de administradores, el departamento TIC y todos los cuartos en los que se encuentren equipos informáticos,

soportes de información o activos críticos para la asociación. La protección puede ser con llaves, acceso electrónico y cámaras de seguridad.

- En todas las instalaciones deberán registrarse las personas que accedan y cuál es su motivo. Por ello, se deben dar credenciales a los empleados y usuarios para facilitar el acceso a quien ya tiene permiso. Las personas externas obligatoriamente realizarán un registro en la recepción.
- Para evitar accesos no autorizados, es esencial la señalización de aquellas zonas en las que se prohíbe el ingreso, especialmente de equipos informáticos.
- Para los lugares, cuartos, ubicaciones o armarios en donde se encuentren dispositivos informáticos se debe crear registros de quién accede, a la hora que lo hace y cuál será la acción que realiza. Este procedimiento ayuda a evitar ataques o errores de no repudio.
- Para almacenar llaves de cuartos, armarios o seguros de los equipos informáticos serán almacenadas en una caja fuerte a la que tengan acceso solo personal del departamento TIC.
- Se crearán manuales de uso correcto de las instalaciones que contengan equipos informáticos para los empleados de limpieza. De igual manera todos los laboratorios informáticos deberán poseer un informativo de normas y buenas prácticas.

Subtareas: Para el cumplimiento de esta salvaguarda se deben realizar las siguientes tareas:

Control de Acceso Físico

- Revisar la creación de grupos y perfiles de empleados y usuarios.
- Reestablecer, quitar u otorgar permisos a cada perfil o grupo.
- Verificar el sistema de registros de actividades informáticas: logs.
- Crear manuales para empleados, para el acceso a sistemas y aplicaciones así como para el uso de las contraseñas.

Control de Acceso Físico

- Crear los registros para personas externas.
- Entregar credenciales a empleados y usuarios de uso obligatorio.
- Verificar la señalización de las instalaciones especialmente en las ubicaciones de equipos informáticos.
- Guardar todas las llaves de acceso a equipos informáticos en una caja fuerte.
- Crear manuales de uso y buenas prácticas para las instalaciones críticas.

Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la asociación.

Costes: Requiere un alto esfuerzo del departamento TIC.

Tiempo de ejecución: 3 meses

Riesgo Residual: El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad de logs o no se ha realizado correctamente. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.

Indicadores de eficacia y eficiencia: Revisar el cumplimiento del plan de seguridad a través de un checklist y verificando los registros de actividades.

PROTECCIÓN DE DATOS

Proyecto: Protección de Datos e Información – Formalización del cifrado

Objetivo: Preservar la confidencialidad, integridad, transmisión y almacenamiento de la información.

Activos Afectados: Datos/Información y activos que manejen la información: Servicios, Software, Equipos Informáticos, Redes de Comunicaciones y Soportes de Información.

Participantes: Departamento TIC.

Salvaguarda: Cifrado de la Información

Descripción: El departamento TIC esta consiente de la importancia de la confidencialidad de la información, por ello ya tienen políticas de seguridad implementadas en la asociación. Este plan de seguridad pretende reforzar y formalizar los procesos de la política existente.

La encriptación de la información engloba datos, servicios, aplicaciones y equipos informáticos, pero también hay que considerar aspectos legales, políticas internas y niveles de confidencialidad de los datos. Por ello, la responsabilidad de mantener la confidencialidad e integridad de la información recae sobre todos los empleados de la asociación.

El proceso de cifrado empieza con la clasificación de la información para saber qué cifrar. Para la clasificación legalmente hay que cumplir el Reglamento General de Protección de Datos vigente y, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Además de que su cumplimiento es obligatorio, juntamente con las políticas internas

de la asociación, estos documentos ayudan a clasificar la información dependiendo del tipo y grado de confidencialidad para determinar el método de cifrado adecuado.

Se considera que toda información sensible, de carácter personal o confidencial requiere de cifrado. Además requiere protección toda información crítica almacenada en soportes de información y equipos informáticos. Para esta protección se puede elegir un cifrado simétrico, asimétricas o híbridas, conjuntamente se pueden agregar más seguridad como control de acceso, firmas electrónicas (personal, empresarial, factura electrónica) y certificados web (wildcard).

Es conveniente realizar una lista del software de cifrado aprobado y su función, que puede ser: cifrado de discos (arranque, internos, extraíbles), correo, copias de seguridad, ficheros y directorios y dispositivos móviles. Al igual que se puede crear una lista con los algoritmos y tipos de cifrados aprobados, que sean actualizados y estén enmarcados en los algoritmos y métodos más seguros que existen hoy en día, como: el cifrado AES-256.

La seguridad de datos no está completa sin la protección de las redes de comunicaciones. Para ello se pueden usar protocolos como SSL y cifrados de redes inalámbricas con el protocolo más seguro actualmente: WPA2. Además, se requiere tener herramientas que permitan a los empleados transmitir información de forma segura. Las herramientas tienen que incluir protocolos como: SSH (acceso remoto seguro), SFTP/FTPS (transmisión segura de ficheros) y HTTPS (transferencia segura de datos en servicios web).

El plan de seguridad no está completo sin pasar por una revisión de cumplimiento, para hablar de un cifrado eficaz de la información. Así se puede asegurar la confidencialidad e integridad de la información a pesar de ser víctimas de errores o ataques. Esta revisión se puede hacer mediante un registro de incidentes, errores y como se actúa ante ellos.

Subtareas: Para el cumplimiento de esta salvaguarda se deben realizar las siguientes tareas:

- Clasificar los datos con su nivel de confidencialidad
- Definir las técnicas y algoritmos de cifrado que se van a utilizar
- Instalar software de cifrado
- Verificar el cumplimiento de la política de seguridad de cifrado
- Subsanar errores y ausencias de cifrado
- Definir un programa de revisión de cumplimiento de la política de seguridad

Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.

Costes: Requiere un esfuerzo alto del departamento TIC. Para las aplicaciones de cifrado hay opciones de software de código abierto (sin costo) o de pago (desde 5€ para móviles a 100€ para ordenadores) que se pueden instalar en los equipos informáticos.

Tiempo de ejecución: 2 meses para revisión de cumplimiento

Riesgo residual: El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.

Indicadores de eficacia y eficiencia: Evaluar en los registros: errores, incidentes, como se responde ante una contingencia, daños y responsables.

COPIAS DE SEGURIDAD

Proyecto: Protección de Datos e Información - Formalización de las Copias de Seguridad

Objetivo: Verificar que se realicen copias de seguridad

Preservar la disponibilidad de la información y la continuidad de la asociación.

Activos Afectados: Datos/Información y activos que manejen la información: Servicios, Software, Equipos Informáticos y Soportes de Información.

Participantes: Departamento TIC.

Salvaguarda: Copias de seguridad

Descripción: El departamento TIC conoce la importancia de la disponibilidad de la información para la continuidad de los servicios y por lo tanto de la asociación, por ello posee una política de copias de seguridad. Este plan de seguridad pretende reforzar y formalizar los procesos de la política existente.

Para las copias de seguridad se deben considerar los activos: datos, servicios, aplicaciones, equipos informáticos y soportes de información, pero también los aspectos legales, políticas internas y tratamiento de las copias. Por ello, la responsabilidad de mantener la confidencialidad e integridad de la información recae sobre todos los empleados de la asociación.

Determinados los activos de la asociación, se decide de qué datos, aplicaciones o sistemas hay que sacar copias de seguridad. Estas decisiones se deben basar en el Reglamento General de Protección de Datos, la Ley Orgánica de Protección de Datos Personales y las políticas internas de APSA.

Determinados los datos críticos, se define el tipo de copias y la periodicidad con las que se van a realizar. La frecuencia de copias puede ser teniendo en cuenta: la variación de datos generados, obligaciones legales y coste de almacenamiento. Las copias pueden ser de tres tipos: completa, incremental y diferencial. La completa es copia integral de los datos. La copia incremental solo graba los datos que han cambiado desde la última copia. La diferencial solo graba los datos que ha cambiado desde la última copia completa.

Otro aspecto relevante es el almacenamiento de las copias de seguridad. Dependiendo del tipo y grado de confidencialidad, las copias se pueden almacenar en: la nube, servidores locales y soportes externos. También se requiere decidir si las copias de seguridad relevantes se las almacena dentro o fuera de la asociación. Pero sin importar el lugar en donde se almacenen las copias de seguridad, estas deben tener un control de acceso y fundamentalmente ir cifradas.

El almacenamiento de copias está ligada a la caducidad de estas. Se debe entonces determinar cuánto tiempo hay que conservar las copias, en función de: la vigencia de los datos de la copia, duración del soporte y la necesidad de conservar copias anteriores a la última realizada.

Todas estas actividades deben formalizarse creando procedimientos de copias pero también procesos de restauración y eliminación. Realizar un proceso de restauración de copias de seguridad anualmente y se podrá usar como un indicador de eficacia del plan de seguridad. Esta también es una prueba para identificar errores y corregirlos para asegurar la continuidad del negocio en caso de una incidencia. Finalmente, debe definirse un proceso de eliminación de soporte dependiendo de su tipo y la caducidad de los datos.

Subtareas: Para el cumplimiento de esta salvaguarda se deben realizar las siguientes tareas:

- Clasificar la Información para identificar cuál es su grado de criticidad
- Definir el proceso de elaboración, restauración y eliminación de las copias de seguridad
- Elegir el soporte de almacenamiento de las copias de seguridad según: coste, fiabilidad y capacidad. Incluye etiquetado del soporte
- Actualizar o cambiar el software para copias de seguridad
- Crear un registro con la siguiente información: de que se hace copia, tipo de copia, software requerido, soportes de almacenamiento, periodicidad, vigencia, ubicación y verificación.
- Verificar el cumplimiento de la política de seguridad de copias para subsanar errores y ausencias de copias de seguridad
- Definir un programa de revisión de cumplimiento del plan seguridad

Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la asociación.

Costes: Requiere de un esfuerzo medio de la asociación. Los costes pueden producirse por gastos extras en copias de seguridad como: contratación del servicio en la nube (500€), adquisición de equipos (500€ a 1000€), soportes de almacenamiento, software especializado en copias de seguridad (100€).

Tiempo de ejecución: 3 meses para revisión de cumplimiento y actualización del sistema de copias de seguridad.

Riesgo residual: El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad o las copias de seguridad no se realizaron correctamente. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.

Indicadores de eficacia y eficiencia: Evaluar en los registros: errores, incidentes, como se responde ante una contingencia, daños y responsables.

REGISTRO DE ACTIVIDAD INFORMÁTICA

Proyecto: Sistema activo de Registro de Actividad Informática

Objetivo: Determinar eventos significativos dentro del sistema de la asociación.

Establecer mecanismos de monitorización de errores y amenazas.

Activos Afectados: Datos/Información, Servicios, Software, Equipos Informáticos y Redes informáticas.

Participantes: Departamento TIC.

Salvaguarda: Logs, registros de incidencias

Descripción: Todas las soluciones y procesos tecnológicos usados junto con el trabajo de los empleados genera actividad informática. Registrar toda esta actividad ayuda a la gestión y monitorización de todo el sistema y así detectar errores e incidentes. Y para recopilar la información generada por las actividades se usan los ficheros log.

Estos ficheros logs se puede usar con fines estadísticos, detectar fallos, mal funcionamiento, errores, vulnerabilidades y ataques. Por ello se debe establecer una política de gestión de Logs y monitorización para generar alertas en tiempo real.

Las actividades que deben ser registradas pertenecen a los activos críticos para el funcionamiento de la asociación. Se pueden registrar:

- Acceso y modificación de la información confidencial
- Inicio y fin de: conexión a red, ejecución de aplicaciones, sesiones de usuarios incluidos los intentos de sesión fallidos.
- Cambios de configuración en aplicaciones y sistemas
- Modificación de permisos de acceso a red, aplicaciones o sistemas
- Límites de recursos de los equipos informáticos: capacidad de disco, memoria, ancho de banda, uso de CPU.
- Inicio de actividad sospechosa detectada por antivirus y sistemas de detección de intrusos.
- Transacciones importantes dentro de las aplicaciones

Los registros deben tener la siguiente información: identificador de usuario, identificador del elemento (ficheros, servicios, aplicaciones, bases de datos, equipos, etc), identificación del equipo dentro de la red, identificación de protocolos, fecha y hora de ocurrencia, y tipología del evento. Estos datos recolectados deben tener un formato predefinido y generalizado para la simplificación del análisis.

Una vez configurados los sistemas de gestión en los activos necesarios, se requiere configurar un sistema de monitorización y registro adecuadas. Además, todos estos registros deben estar debidamente protegidos ya sea cifrados o con copias de seguridad para no ser manipulados y así evitar ataques de no repudio. Todo este sistema funciona si todo en la asociación esta sincronizado a través de un reloj, y así garantizar el correcto registro de eventos.

Subtareas: Para el cumplimiento de esta salvaguarda se deben realizar las siguientes tareas:

- Seleccionar servicios, aplicaciones, redes y equipos que van a ser monitorizados.
- Definir formatos de logs
- Determinar la solución para monitorización
- Configuración y comprobación del sistema de monitorización
- Verificar el cumplimiento de registro de actividades informáticas para subsanar errores
- Difundir el plan de seguridad a toda la organización
- Definir un programa de revisión de cumplimiento del plan de seguridad

Todos los registros, procedimientos y programas consisten en documentos legalizados y aprobados por el Departamento TIC y la administración de la organización.

Costes: Requiere un alto esfuerzo del departamento TIC. El costo de una solución de monitorización es de 2000€ a 3500€.

Tiempo de ejecución: 4 meses para tener el sistema en funcionamiento.

Riesgo residual: El riesgo residual puede generarse cuando un empleado no cumpla con este plan de seguridad de logs o no se ha realizado correctamente. Según el análisis realizado previamente, el riesgo alcanza un valor mínimo, que según la escala de evaluación es un riesgo asumible para la asociación.

Indicadores de eficacia y eficiencia: Efectuar pruebas controladas de incidentes y verificar el sistema de monitorización.

FORMALIZACIÓN DE PROCESOS DE SEGURIDAD

Proyecto: Formalización de Procesos de Seguridad

Objetivo: Formalizar y legalizar todas las políticas de seguridad de la asociación.

Activos Afectados: Datos/Información y activos que manejen la información: Servicios, Software, Equipos Informáticos, Redes de Comunicaciones, Soportes de Información y Personal.

Participantes: Departamento TIC.

Salvaguarda: Manuales, registros y documentación

Descripción: APSA posee políticas de seguridad que se efectúan en toda la asociación, pero que requieren un proceso de formalización. Este proceso consiste en redactar la política de seguridad, crear manuales para empleados y usuarios, y crear registros de control de activos. Todos estos documentos deben realizarse dentro del departamento y ser aprobados por su director y la Dirección de la asociación.

En las políticas de seguridad debe constar la siguiente información: proyecto, objetivo, fecha, activos afectados, participantes, descripción, coste, duración e indicadores de eficacia. Además de una hoja donde conste el responsable de la elaboración de la política y las firmas de revisión y aceptación del director del departamento de TIC y un representante de la dirección administrativa de la asociación.

En los manuales debe constar la siguiente información: título, objetivos, fecha, responsables de la elaboración del manual, hacia quién o qué actividad va dirigido, descripción, pasos a seguir, recomendaciones. Al igual que las políticas de seguridad, en los manuales debe constar las

firmas de revisión y aceptación del director del departamento de TIC y un representante de la dirección administrativa de la asociación.

Muchas de las salvaguardas y políticas de seguridad requieren un sistema de registro. Estos registros deberán ser digitales e irse llenando conforme los eventos se vayan presentando. Para cada área o uso, los registros deberán contener distinta información, pero en general debe constar de: título, fecha, actividad o equipo y responsable.

Los manuales, registro y documentos que se deben crear son:

- Para los empleados se debe crear manuales para: la protección del puesto de trabajo, uso de redes inalámbricas y redes externas, uso del correo electrónico, uso de equipos informáticos, soportes de información y dispositivos móviles, contraseñas, uso de servicios y aplicaciones, y uso de internet.
- Para los administrativos se debe crear manuales para: uso y configuración de dispositivos informáticos, soportes de información y equipamiento auxiliar, configuraciones de redes de comunicaciones, configuraciones de servicios y aplicaciones, guías para respuesta ante incidentes, registros de configuración en el sistema y servicios, y usos de contraseñas.
- Los registros deben ser de: lista de activos, registros de actividades y cambios de sistemas o equipos, entrega de permisos, software y equipos, directorios telefónicos, acceso de personas externas a la asociación, direccionamiento IP y acceso a equipamiento crítico.

Subtareas: Para el cumplimiento de esta salvaguarda se deben realizar las siguientes tareas:

- Redactar las políticas de seguridad existentes y definir un proceso de revisión, actualización y aprobación.
- Crear manuales para todos los empleados y usuarios que tengan acceso al sistema, además de definir un proceso de revisión, actualización y aprobación.
- Difusión de las políticas de seguridad y manuales

Costes: Requiere un gran esfuerzo del departamento TIC**.**

Tiempo de ejecución: 3 meses

Riesgo residual: Este plan de seguridad es más administrativa por lo que el riesgo residual es mínimo.

Indicadores de eficacia y eficiencia: Crear una checklist para la elaboración de los documentos que cubran todas las áreas de la asociación.

RECOMENDACIONES ADICIONALES

Para tener mayor seguridad se pueden realizar las siguientes acciones:

- Crear un programa anual de concienciación y formación de seguridad para todos los empleados: puede ser a través de reuniones o un archivo multimedia enviado por correo electrónico.
- Para los empleados del departamento TIC se recomienda asistir a cursos de seguridad para estar actualizados en nuevos sistemas y vulnerabilidades.
- Inscribirse en foros oficiales de ciberseguridad para compartir experiencias con otras empresas
- Cuando se requiera actualizar una aplicación revisar el tipo de actualización, y determinar si es o no necesario realizar el cambio.
- Tener siempre actualizado el antivirus o software que ayude a la seguridad de la asociación.
- Pedir informes de cumplimiento de seguridad a las empresas que les prestan servicios a APSA.
- Realizar auditorías de sistemas y seguridad periódicamente. Incluye un análisis de vulnerabilidades a través de pruebas de pentesting.
- Realizar planes de continuidad de Negocio.

5. Conclusiones y trabajo futuro

- El análisis de la situación actual de la seguridad de APSA resultó más larga de lo previsto, pues la mayor parte de información recolectada provino de entrevistas con los administradores TIC. La documentación que entregaron no tuvo un aporte considerable por no ser completa o no estar actualizada.
- Por falta de registros, la clasificación de los activos resultó complicada. Por otro lado, la gran cantidad de activos que APSA maneja, obligaron a que el Inventario de Activos sea generalizada y solo se considere los más críticos. De esta dificultad también se originó la creación del archivo Análsis_APSA, una herramienta ofimática en Excel para facilitar el uso y análisis de la gran cantidad de información que generó este trabajo y que queda a disposición de la asociación.
- El inventario de APSA consistió en 75 activos organizados en 9 grupos: Datos/Información, Servicios, Software, Equipos informáticos, Redes de comunicaciones, Soportes de Información, Equipamiento auxiliar, Instalaciones y Personal. Además a todos ellos, se los analizó en las 5 dimensiones de seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.
- APSA no posee un historial de ataques y errores, por lo que es difícil establecer exactamente cuáles son las amenazas que afectan a la asociación. Entonces, para establecer las amenazas se consideraron aquellas que ya habían ocurrido y las que son comunes para una empresa.
- Para determinar el impacto y riesgo que causan las amenazas sobre los activos, se requirió asignar una valoración de 0 a 10 a los activos, y para la ocurrencia de las amenazas de 0,1 a 1. La valoración de los activos y la frecuencia de ocurrencia de las amenazas depende de un criterio personal, pero se intentó que los valores sean los más cercanos a la realidad en base a toda la información recolectada de la asociación.
- Según los resultados de los riesgos, estos no excedieron un valor de 6,3 dentro de una escala de valoración de 0 a 10. La mayor parte de los riesgos se encuentran en un rango apreciable, por lo que se decidió que todos los valores a partir de 4 sean considerados como graves y de inmediato tratamiento. Para activos como Datos/Información, Servicios, Software y Redes de comunicaciones esta condición cambió por ser activos críticos para la asociación.
- Para reducir los riesgos, se determinaron salvaguardas sin importar si están o no implementadas en APSA, facilitando el análisis de la eficiencia de las salvaguardas para

el cálculo del impacto y riesgo residuales. Esta decisión se basa en que algunas de las políticas de seguridad no están completas o se han ido implementando mientras se desarrolló este trabajo.

- Caracterizadas las salvaguardas se determinó el valor de la efectividad en las dimensiones de seguridad y en la frecuencia de ocurrencia con una escala de valoración de 0% a 100%. Estos valores dependen mucho del criterio personal pero se intentó que fueran lo más cercano a la realidad en base a la investigación de las salvaguardas.
- Los resultados del impacto y riesgo residual fueron los esperados. Salvo pocas excepciones, se cumplieron con los niveles mínimos aceptados para cada activo y los riesgos residuales recaen sobre la escala asumible de riesgo.
- El resultado del análisis realizado se refleja en la creación de una herramienta ofimática de análisis de activos, cinco planes de seguridad y un listado de acciones adicionales en base a las salvaguardas determinadas. Estos planes de seguridad abarcan acciones que contrarresten los valores altos de riesgos potenciales y mejoren las políticas de seguridad críticas dentro de la organización.

Para el trabajo posterior se puede considerar un análisis de riesgos exclusivo para el grupo de activos Datos/Información. Además, se puede completar el análisis desarrollando un inventario completo de los activos. Finalmente, se podría automatizar la herramienta ofimática desarrollada en el trabajo.

Referencias

AEDP. *Normativa y circulares.* [En línea] [Consulta: 25 de mayo 2019]. Disponible en: https://www.aepd.es/normativa/index.html

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método* [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 10 de enero 2019]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas* [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 10 de enero 2019]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

AMUTIO GÓMEZ, M. A., CANDAU, J. & MAÑAS, J. A. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elemento* [en línea]. Madrid: Portal de Administración Electrónica, 2012. [Consulta: 10 de enero 2019]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

AMUTIO, M. A., CANDAU, J. & MAÑAS, J. A. *MAGERIT MAGERIT – version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method* [en línea]. Madrid: Portal de Administración Electrónica, 2014. [Consulta: 16 de enero 2019]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXu2nCgzbIV

Asociación APSA. *APSA.* [En línea] [Consulta: 22 de Mayo 2019]. Disponible en: https://www.asociacionapsa.com/

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *UNE-EN ISO/IEC 27000 Tecnología de la Información, Técnicas de seguridad,Sistemas de Gestión de Seguridad de la Información (SGSI), Visión de conjunto y vocabulario,* Madrid: AENOR Internacional, 2017.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *UNE-EN ISO/IEC 27001 Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos,* Madrid: AENOR Internacional, 2017.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *UNE-EN ISO/IEC 27002 Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información,* Madrid: AENOR Internacional, 2017.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Magerit,* 2005-2019 [en línea] [Consulta: 22 de enero 2019]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

EUROPEAN UNION AGENCY FOR NETWORK AND NFORMATION SECURITY. *Inventory of Risk Management / Risk Assessment Methods.* 2005-2019 [en línea] [Consulta: 22 de enero 2019]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

GONZÁLEZ MATAIX, P. *Auditoría TI en la Asociación APSA.* Trabajo Fin de Grado. J. V Berná Martínez (dir.). Universidad de Alicante, 2018. [Consulta: 10 de diciembre 2018]. Disponible en:http://hdl.handle.net/10045/80391

INCIBE. *Hoja de verificación (checklist) para llevar a cabo una evaluación de controles* [en línea], 2019 [Consulta: 19 de febrero 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

INCIBE. *¿Todavía no haces copias de seguridad? ¡A qué esperas!* [en línea]. [Consulta: 20 de febrero 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/todavia-no-haces-copias-seguridad-esperas

INCIBE. *Clasificación de la información - Políticas de seguridad para la pyme* [en línea]. [Consulta: 125 de julio 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

INCIBE. *Copias de seguridad - Políticas de seguridad para la pyme.* [en línea]. [Consulta: 25 de julio 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf

INCIBE. *Copias de seguridad una guía de aproximación para el empresario.* [en línea]. [Consulta: 25 de julio 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

INCIBE. *ERP desactualizado, incidente asegurado.* [en línea]. [Consulta: 15 de enero 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/erp-desactualizado-incidente-asegurado

INCIBE. *Gestión de logs - Polítias de seguridad para la pyme.* [en línea]. [Consulta: 25 de julio 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

INCIBE. *Plan Director de Seguridad Colección: protege tu empresa.* [en línea]. [Consulta: 15 de diciembre 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INCIBE. *Protección de la Información.* [en línea]. [Consulta: 15 de diciembre 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

INCIBE. *Uso de técnicas criptográficas - Políticas de seguridad para la pyme.* [en línea]. [Consulta: 15 de julio 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO/IEC Information technology — Security techniques — Information security management systems — Overview and vocabulary,* Suiza: 2018.

Anexo A

Estado Inicial - Controles de Seguridad de la Información en APSA según ISO/IEC 27001:2017

CUESTIONARIO

1. Políticas de seguridad de la información

1.1. Directrices de gestión de la seguridad de la información

1.1.1. Políticas para la seguridad de la información

- **¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?** Existe un marco e indicios de estructura pero que no está definida claramente. Existen políticas que se aplican a distintos aspectos de APSA pero no cubren todas las áreas.
- **¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?** Existen políticas razonables y se van creando nuevas de acuerdo con las necesidades que se van presentando con el tiempo
- **¿Cómo se autorizan, comunican, comprenden y aceptan las políticas?** Las políticas para implementarse se comunican de alguna forma pero no existe un claro procedimiento de comunicación y aceptación por departamentos superiores.
- **¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores?** Si, a los trabajadores se les hace firmar un documento en donde se comprometen a cumplir cláusulas, funciones y obligaciones en cuanto a seguridad informática, pero no se hace un seguimiento de cumplimiento de estas.
- **¿Hay acuerdos adecuados de cumplimiento y refuerzo?** Al firmar un documento que contiene las cláusulas de seguridad, los empleados están comprometidos a cumplir, pero posteriormente no existe un seguimiento de cumplimiento.
- **¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)?** Como se van implementando según vayan apareciendo nuevas necesidades, los empleados del departamento de TIC buscan la mejor solución y estas se toman de diferentes normas.
- **¿Están las políticas bien escritas, legible, razonable y viable?** No existe un documento físico como tal, pero el personal tiene bien definidas las que tienen y que ejecutan.
- **¿Incorporan controles adecuados y suficientes?** Realizan controles que ellos requieren convenientes pero no existe un procedimiento escrito.
- **¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?** La gran mayoría, pero no se ha realizado un análisis de si son las adecuadas, suficientes o hay que mejorarlas.
- **¿Cuán madura es la organización en esta área?** Existe indicios de tener políticas de seguridad estructuradas pero que necesitan mejorar. Existen áreas en las que todavía falta tener políticas de seguridad.

RESULTADO	COMENTARIO
REPETIBLE	No existe una maduración de las políticas de seguridad. Existen políticas pero a base de intuición

1.1.2. Revisión de las políticas para la seguridad de la información

- **¿Todas las políticas tienen un formato y estilo consistentes?** No existe documento físico con un formato, pero las políticas que tienen establecidas están estructuradas pero todo lo llevan en la cabeza.
- **¿Están todos al día, habiendo completado todas las revisiones debidas?** Están al día, pues aplican seguridad según aparecen nuevas necesidades.
- **¿Se han vuelto a autorizar y se han distribuido?** No existe un proceso claro de autorización y distribución de las políticas de seguridad. Se tiene evidencia que a los empleados se les comunica algunas de las políticas de seguridad, porque deben firmar un documento de políticas de seguridad que los empleados tienen que cumplir, pero es una única vez.

RESULTADO	COMENTARIO
INICIAL	No existe documentación de Políticas de Seguridad

2. Organización de la seguridad de la información

2.1. Organización interna

2.1.1. Roles y responsabilidades en seguridad de la información

- **¿Se le da suficiente énfasis a la seguridad y al riesgo de la información?** Solo dentro del departamento de TIC.
- **¿Hay apoyo de la administración?** Si, pero no tienen muy claro la importancia y el impacto de la seguridad informática por lo que no se le da la importancia necesaria.
- **¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad?** No, poco interés de parte de la junta directiva, los esfuerzos están orientados a los servicios que APSA ofrece a sus usuarios.
- **¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas?** La responsabilidad recae únicamente sobre el departamento de TIC tanto de la parte informática como de la seguridad. Dentro del departamento se intenta llevar un orden en cuanto a responsabilidad.
- **¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información?** Dentro del departamento se definen responsabilidades informáticas, que dentro de estos se sobreentiende que incluye la seguridad**.** Las responsabilidades intentan mantenerlo definidas pero no tienen un documento claro que describa dichas responsabilidades.
- **¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información?** Existe presupuesto pero el mínimo requerido pues por ser una asociación de ayuda social la mayor parte de los recursos económicos son destinados al cumplimiento de los servicios que ofrecen a sus usuarios. Pero si que se trabaja dando cursos al personal del departamento de TIC

- **¿Hay coordinación dentro de la organización entre las unidades de negocio?** La comunicación es buena y se intenta mantenerla, pero se necesita más comunicación y por lo tanto más coordinación de los otros departamentos y sedes especialmente con el de TIC.
- **¿Funciona efectivamente en la práctica?** Por ahora, todo lo que esta implementado funciona, pero requiere mejorar en muchos aspectos.
- **¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?** No existe una conciencia clara del impacto que tiene la ciberseguridad dentro de una empresa especialmente de parte de gerencia. Los indicios de seguridad existen y se aplican pero necesita establecer una estructura, un orden de tal manera que lo puedan tener todo mejor organizado.

RESULTADO	COMENTARIO
REPETIBLE	La responsabilidad solo recae en el departamento de TIC. Falta de interés de administración y documentación de asignación de roles y responsabilidades. Las funciones están designadas en cuanto a informática pero no a seguridad.

2.1.2. Segregación de tareas

- **¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas?** Dentro de APSA, los deberes y funciones están claramente definidas por el departamento de RRHH. En caso del departamento de TIC existe solo dos personas que están encargadas de la infraestructura informática, y en donde cada uno tiene definido sus responsabilidades de la parte informática por lo que sobreentienden y asumen la responsabilidad también de la seguridad de las áreas que ellos manejan.
- **¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed** No tiene un documento claro definido de responsabilidades de seguridad, el documento en donde si tienen responsabilidades en el que maneja RRHH.
- **¿Existe una política que cubra la segregación de deberes?** Tienen definidas sus responsabilidades, pero no se requiere tanto una política de segregación de tareas pues solo son dos los que están a cargo de toda la infraestructura.
- **¿Cómo llegan las decisiones con respecto a tal segregación?** Las tereas se asignan según sus funcionen dentro del departamento, también si hay nuevas tareas lo definen internamente dentro del departamento para ver la mejor manera de ejecutarlo.
- **¿Quién tiene la autoridad para tomar tales decisiones?** Lo toman entre todos los del departamento pero el director de TIC es la autoridad.
- **¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?** Si realizan un seguimiento de tareas pero no tan documentadas. Usan un pizarrón donde están las tareas que tienen que hacer, lo que han hecho y lo que les falta hacer.

RESULTADO	COMENTARIO
REPETIBLE	No existe documentación de seguridad y tampoco roles asignados en cuanto a seguridad.

2.1.3. Contacto con las autoridades

- **¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?** Dentro de APSA tienen lista de contactos de todas las autoridades de la empresa. También una lista de contactos de empresas externas a las que pueden recurrir. En caso de eventos con proveedores de servicios que ellos trabajan se comunican a través de las líneas de servicio al cliente o atención técnica, además de un correo electrónico.
- **¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo?** Cualquier persona del departamento de TIC que este manejando el incidente en el momento.
- **¿La lista es actual y correcta?** Si
- **¿Hay un proceso de mantenimiento?** Si, cuando se cambia algún contacto pues se va actualizando la lista, pero un proceso como tal periódico de verificación no.

RESULTADO	COMENTARIO
DEFINIDO	Está establecido que es lo que se debe hacer en caso de un incidente pero no está documentado una lista de contactos, porque solo se lo hace a través de servicio al cliente

2.1.4. Contacto con grupos de interés especial

- **¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k?** Para buscar información sobre una mejor práctica en cuanto a la seguridad, se accede a información de foros o noticias en internet, pero no hay algo al que si pertenezcan. No comparten experiencias con otras empresas
- **¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?** No, todo se lo hace de manera interna y de igual manera para encontrar una solución se lo hace de manera interna. Además que no tienen muchos eventos de seguridad que requiera de compartir información ante amenazas de seguridad.

RESULTADO	COMENTARIO
DEFINIDO	El departamento de TIC intenta mantenerse actualizado por noticias y lecturas de interés

2.1.5. Seguridad de la información en la gestión de proyectos

- **¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de**

proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? Los proyectos informáticos van de la mano con los de seguridad, es decir que cuando se va a implementar un proyecto de informática o que requiera de recursos informáticos, se abordan siempre aspectos de seguridad en distintas medidas.

- **¿La etapa del proyecto incluye actividades apropiadas?** Si, siempre se trata de definir los pasos a seguir para un cumplimiento adecuado. Además que cuando se presenta un proyecto se lo debe aprobar primero por la administración donde se presenta un informe.

RESULTADO	COMENTARIO
DEFINIDO	Actualmente, sí están considerados los aspectos de seguridad para nuevos proyectos

2.2. Los dispositivos móviles y el teletrabajo

2.2.1. Política de dispositivos móviles

- **¿Existen política y controles seguridad relacionados con los usuarios móviles?** Sí, existe una política de seguridad para todos los dispositivos móviles, que está definida en un anexo que les hacen firmar para que lo manejen de manera correcta.
- **¿Se distinguen los dispositivos personales de los empresariales?** Si, dentro de la asociación se entregan a todos dispositivos informáticos, ordenadores, portátiles y móviles por lo que no requieren el uso de dispositivos personales para el trabajo.
- **¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad?** Los dispositivos móviles no cuentan con un antivirus, manifiestan que no lo necesitan. En cuanto a portátiles usan la misma política de los ordenadores de escritorio.
- **¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco**? La versión de Windows que se usa en los ordenadores portátiles y de escritorio en Windows home y este no viene con cifrado por defecto por lo que no cifran, algunos que ya tienen Windows pro sí que cifran. En cuento a los dispositivos móviles no lo cifran. En los portátiles, los usuarios no tienen permisos de administrador entonces no pueden instalar nada, por lo que solo pueden acceder a lo que tenga el ordenador. Los dispositivos móviles en principio están libres de instalarse cualquier aplicación.

RESULTADO	COMENTARIO
ADMINISTRADO	Poseen buenas políticas de seguridad para dispositivos portátiles, hay ciertas cosas que se debe mejorar.

2.2.2. Teletrabajo

- **¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina?** No se usa Teletrabajo, solamente lo hace el personal del departamento de TIC en caso de extrema emergencia.
- **¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches,**

registro de seguridad y monitoreo, encriptación y continuidad del negocio? En caso de que se requiera conectar desde el exterior, se usa UltraVNC que es un software de acceso remoto, que se conecta a un servidor propio y desde este se conecta a los otros servidores que se encuentran en la nube.

RESULTADO	COMENTARIO
ADMINISTRADO	Lo tienen bien administrado aunque no es de uso común si no para casos de emergencia.

3. Seguridad relativa a los recursos humanos

3.1. Antes del empleo

3.1.1. Investigación de antecedentes

- **¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo?** Si, las marca la empresa que colabora en la implantación del nuevo RGPDatos y las ejecuta la empresa.
- **¿Se hace en la empresa o se subcontrata a un tercero?** Se hace en la propia empresa.
- **Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables?** Si, cuando se contrata a un tercero hay un intercambio de documentación y certificaciones.
- **¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?** Si, sobre todo se solicita el certificado negativo de antecedentes sexuales para trabajar con nuestro colectivo
- **¿Existen procesos de selección mejorados para los trabajadores en roles críticos?** No hemos tenido roles críticos
- **¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?** Si, tienen el proceso de selección de personal por promoción interna o externa.

RESULTADO	COMENTARIO
OPTIMIZADO	Tienen muy claras las políticas para establecer los procesos de antecedentes de nuevo personal como de empresas externas.

3.1.2. Términos y condiciones del empleo

- **¿Están claramente definidos los términos y condiciones de empleo?** Sí, tienen un único convenio colectivo para las 4 empresas con sus diferentes funciones y tablas salariales
- **¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general?** Si
- **¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles?** Si, el documento de seguridad especifica quien tiene acceso o no a cierta información y cómo actuar
- **¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?** El documento se entrega, explica y sólo se firma cuando ha quedado todo claro.

RESULTADO	COMENTARIO
OPTIMIZADO	Tienen muy claras las políticas para nuevas contrataciones donde incluye términos de aceptación de acciones de seguridad que deben seguir.

3.2. Durante el empleo

3.2.1. Responsabilidades de gestión

- **¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia?** Firman una hoja en donde constan las políticas de seguridad que un empleado debe cumplir, pero no existe un seguimiento o programas de educación de seguridad.
- **¿Se hace de forma regular y está a día?** No, solo al inicio que empieza a trabajar.
- **¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados?** No existe un documento
- **¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad?** Autoridades muy poco interesadas en parte de seguridad informática por lo que delegan directamente la responsabilidad al departamento de TIC
- **¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?** Los empleados y usuarios conocen que sire la seguridad de la información.

RESULTADO	COMENTARIO
REPETIBLE	Existe indicios de seguridad al entregarles documentos al inicio de su trabajo a los empleados, pero no existe ni seguimiento ni programas de seguridad.

3.2.2. Concienciación, educación y capacitación en seguridad de la información

- **¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente?** El personal del departamento de TIC, está consciente en cuento a seguridad e intentan siempre mantenerse al día con nuevas actualizaciones y prepararse en cursos.
- **¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores?** Existe capacitaciones que pueden tomar todos los empleados. En el caso de los empleados en general que no tienen mucho conocimiento en informática reviven cursos de eso y los demás dependiendo de s área puede acceder a dichos cursos de capacitación.
- **¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos?** No hay comunicación en ese sentido. Existen cosas que se les comunica en un inicio y se les exige como cambiar la clave que ellos lo proporcionan de tal manera que los empleados son totalmente responsables de su clave y nadie más la conoce.

- **¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos?** Todo lo que llevan realizado, sí.
- **¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas?** No tienen un documento físico que actualizar, pero el departamento trata de actualizarse siempre. En cuanto a capacitaciones no existen.
- **¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento?** Evaluación como tal no existe pero si pueden acceder a capacitaciones. Las capacitaciones que reciben lo hacen a través de la fundación Tripartita. Al finalizar cada curso, ellos dan una prueba de conocimientos y entregan un informe. Dentro de seguridad de la información para empleados no tienen capacitación.
- **¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?** A pesar de que la empresa da la posibilidad y los recursos para capacitarse, es personal por lo que solo piden que se sigan capacitando pero no toman algún tipo de acción si tienen algún problema durante las capacitaciones.

RESULTADO	COMENTARIO
INICIAL	En el departamento TIC si existe la concientización necesaria pero con los demás empleados falta un programa de capacitación en el aspecto de seguridad.

3.2.3. Proceso disciplinario

- **¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores?** Hasta el momento no se ha presentado ningún evento importante de infracción de seguridad por parte de un empleado o de un usuario. Si suceden cosas son muy pequeñas que generalmente solo requieren de una llamada de atención. Los incidentes que pueden llegar a pasar son muy escasos y generalmente ocurre por desconocimiento de un empleado, pues algunos no tienen un conocimiento alto en informática.
- **¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos?** No tienen evidencia de sanciones por faltas cometidas en relación con seguridad de la información que merezcan sanciones.
- **¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo?** No existe sanciones.
- **¿Se actualiza el proceso de forma regular?** No existe sanciones

RESULTADO	COMENTARIO
REPETIBLE	Aunque no han existido casos, por parte de recursos humanos si contemplan sanciones en caso de faltas provocadas por los trabajadores, pero no específicas para seguridad informática.

3.3. Finalización del empleo o cambio en el puesto de trabajo

3.3.1. Responsabilidades ante la finalización o cambio

- **¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización?** Sí existen políticas y procedimientos, pero no un procedimiento escrito como tal.
- **¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos?** Sí
- **¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?** Sí

RESULTADO	COMENTARIO
DEFINIDO	Existen procedimientos establecidos por recursos humanos, aunque falta un poco tener mayor comunicación entre departamentos para optimizar el proceso.

4. Gestión de activos

4.1. Responsabilidad sobre los activos

4.1.1. Inventario de activos

- **¿Hay un inventario de activos de la información?** Si, pero solo de portátiles, ordenadores y servidores. Inventario que no está actualizado ni completo.
- **¿Contiene la siguiente información?**
    - **Datos digitales** SI
    - **Información impresa** NO
    - **Software** NO
    - **Infraestructura** SI
    - **Servicios de información y proveedores de servicios** NO
    - **Seguridad física** NO
    - **Relaciones comerciales** NO
    - **Las personas** No, solo de pocos activos está escrito un responsable, puesto que en la empresa más se trabaja por puestos de trabajo con varios empleados. Pocos son los que tienen uso exclusivo para una persona. Generalmente el responsable superior a cargo es el director de cada sede.
- **¿A quién pertenece el inventario?** Al departamento de TIC
- **¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI?** Si a la medida de las posibilidades se intenta actualizar cada año
- **¿Es suficientemente detallado y está estructurado adecuadamente?** Esta detallado pero si se puede mejorar agregando otra información de cada uno de los activos sobre todo para manejarlos con facilidad.

RESULTADO	COMENTARIO
REPETIBLE	El inventario de activos existe pero no actualizado, ni completo. Faltan muchos activos y más campos de información.

4.1.2. Propiedad de los activos

- **¿Los activos tienen propietario de riesgo?** Todos los equipos de riesgo (servidores) están bajo la responsabilidad del personal del departamento de TIC.
- **¿Los activos tienen responsable técnico?** Sí, existe una persona dentro del departamento de TIC que se encarga de revisión técnica de los equipos. Si existe un incidente la persona que está usando el equipo notifica el problema mediante el sistema de Tickets o por teléfono.
- **¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos?** Los activos críticos están bajo la responsabilidad exclusiva del personal del departamento de TIC
- **¿Cómo se etiquetan los activos?** No tienen ningún proceso de etiquetado, solo se pone en el inventario asignándole a una sede pero sin ninguna numeración o código.
- **¿Cómo se informa ante incidentes de seguridad de la información que los afectan?** Se manifiesta que generalmente no suceden eventos importantes de seguridad en cuanto a empleados. Si existe tienen un proceso de notificación mediante Tickets. Por otro lado, como los servidores están manejados por los empleados el departamento de TIC, ellos manejan los riegos directamente y se informa a la asamblea general en caso de incidentes graves.

RESULTADO	COMENTARIO
REPETIBLE	Los activos más importantes poseen responsables. Hay un sistema de notificación de incidentes de seguridad para empleados. No hay etiquetado de los activos.

4.1.3. Uso aceptable de los activos

- **¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?** Si, al momento de realizar el contrato y cuando se le indica en la parte informática a que va a tener acceso y los activos que están bajo su nombre, el encargado entrega un documento con políticas de seguridad para el usuario que debe firmar como constancia.
- **¿Cubre el comportamiento del usuario en Internet y en las redes sociales? Puede ser en el contrato?** Dentro del documento que les hacen firmar de la parte de informática, esta una sección de uso del internet.
- **¿Se permite el uso personal de los activos de la empresa?** Existen lineamientos a seguir por parte de los usuarios, donde se da a conocer el uso que se debe dar a los activos, especialmente móviles, que son los más propensos a tener un uso personal.
- **En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto?** Existen lineamientos y ciertas restricciones como no conectar a redes públicas, poseen tarifas de datos para uso mínimo y no usarlo de manera personal si no solo para el trabajo.
- **¿Se describe de forma explícita lo que constituye un uso inapropiado?** Si
- **¿Se distribuye esta información a toda la empresa?** Si, al momento de contratar a una persona.
- **¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?** Sí en todo lo que requiere encriptación.

RESULTADO	COMENTARIO
ADMINISTRADO	Existen procedimientos establecidos solo falta realizar un seguimiento de cumplimiento.

4.1.4. Devolución de activos

- **¿Existe un procedimiento para recuperar los activos tras una baja o despido?** Si, pero no se tiene documento escrito
- **¿Es un procedimiento automatizado o manual?** Manual
- **Si es manual, ¿Cómo se garantiza que no haya desvíos?** Generalmente, se trata con el empleado y se pide que entregue el equipo que va a ser retirado, como no son muchos pues no tienen inconvenientes de desvíos.
- **¿Cómo se abordan los casos en los que los activos no han sido devueltos?** No hay constancia, existe poco movimiento de empleados por lo tanto no presentan casos de no devolución.

RESULTADO	COMENTARIO
ADMINISTRADO	Tienen bastante definido a través de un manual de procedimientos.

4.2. Clasificación de la información

4.1.1. Clasificación de la información

- **¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información?** Sí, el procedimiento e instrucción de uso de cajetín y documentación.
- **¿La clasificación es impulsada por obligaciones legales o contractuales?** Legal
- **¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad?** Si
- **¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen?** Si
- **¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?** Si

RESULTADO	COMENTARIO
OPTIMIZADO	Proceso que tiene exteriorizado en cuanto a seguridad de la información, por lo tanto su clasificación.

4.1.2. Etiquetado de la información

- **¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?** Si
- **¿Está sincronizado con la política de clasificación de la información?** Si
- **¿Cómo se garantiza el correcto etiquetado?** Porque se sigue la normativa de uso de cajetín y documentación.
- **¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante?** Mediante medios informáticos

- **¿Cómo se garantiza que no haya acceso no autorizado?** Controlando el sistema de acceso.
- **¿Se revisan los niveles de clasificación en intervalos predefinidos?** Si

RESULTADO	COMENTARIO
OPTIMIZADO	Proceso que tiene exteriorizado en cuanto a seguridad de la información, por lo tanto usan etiquetado.

4.1.3. Manipulado de la información

- **¿Están los niveles de clasificación adecuadamente asignados a los activos?** si
- **Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.** Existen manuales para cumplir con estas actividades.

RESULTADO	COMENTARIO
OPTIMIZADO	Proceso que tiene exteriorizado en cuanto a seguridad de la información, poseen manuales para manipulado de información.

4.2. Manipulación de los soportes

4.2.1. Gestión de soportes extraíbles

- **¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles?** Si, se registra al entregar a un empleado
- **¿Los medios extraíbles están debidamente etiquetados y clasificados?** Clasificados pero no etiquetados
- **¿Los medios se mantienen y almacenan de forma adecuada?** Almacenados por distintos motivos y bien clasificados
- **¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?** Si, los que se usan en la empresa van encriptados y son los que la propia empresa les entrega.

RESULTADO	COMENTARIO
ADMINISTRADO	Soportes extraíbles bien administrados, solo hace falta un proceso de etiquetado.

4.2.2. Eliminación de soportes

- **¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios?** Si, pero no un documento escrito.
- **¿Se documenta la aprobación en cada etapa para la eliminación de los medios?** Los aprueba directamente el departamento de TIC pero no existe un documento a menos que sea necesario.
- **¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación?** Si
- **¿Se tiene en cuenta los periodos de retención?** Si

- **¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?** No existe ese tipo de eliminación dentro de la organización.

RESULTADO	COMENTARIO
DEFINIDO	Existen procedimientos claros y establecidos para la eliminación se soportes, solo hay un aspecto que no está definido.

4.2.3. Soportes físicos en tránsito

- **¿Se utiliza un transporte o servicio de mensajería confiable?** Correo interno manual, transporte de valija en vehículo o a pie, también se usa mensajería externa.
- **¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia?** Si la información es digital se usa cifrado, pero si es física no usa ningún tipo de protección.
- **¿Se verifica la recepción por el destino?** Firma de recepción

RESULTADO	COMENTARIO
ADMINISTRADO	Existen procesos de mensajería, pero se podrían mejorarse en el sentido de protección de la información y recepción de la mensajería.

5. Control de acceso

5.1. Requisitos de negocio para el control de acceso

5.1.1. Política de control de acceso

- **¿Existe una política de control de acceso?** Para ingresar al sistema todos deben acceder mediante su usuario.
- **¿Es consistente con la política de clasificación?** Si, depende de cada departamento al que pertenece el empleado.
- **¿Hay una segregación de deberes apropiada?** Si, depende de cada departamento al que pertenece el empleado
- **¿Existe un proceso documentado de aprobación de acceso?** Si, depende de cada departamento al que pertenecen entonces, lo define recursos humanos y los directores de cada área.
- **¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?** Recursos humanos, departamento TIC y director del área.

RESULTADO	COMENTARIO
DEFINIDO	El control de acceso es simple pero cumple con su función, dar acceso a las aplicaciones y datos de acuerdo con su puesto de trabajo y necesidades.

5.1.2. Acceso a las redes y a los servicios de red

- **¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado?** Solo para aplicaciones, pocas personas lo usan y está controlado.
- **¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?** Poseen un procedimiento de autenticación que primero acceden mediante un software a un

servidor físico que posee la empresa para que desde allí se conecten a los servidores que se encuentran fuera de esta o en la nube. Este procedimiento solo lo hacen los del departamento TIC está controlado pero generalmente no se usa.

- **¿Cómo monitoriza la red para detectar acceso no autorizado?** No
- **¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)?** Lo hablan entre el departamento, pero no existe procesos de control
- **¿La organización mide la identificación y los tiempos de respuesta ante incidentes?** No tienen definido, 24 a 48 horas, dependiendo de las incidencias pero que en general no son de gravedad.

RESULTADO	COMENTARIO
REPETIBLE	Tienen control de acceso a los servicios, pero a la red no. También no poseen un mecanismo automático de monitorización de incidentes, ni realizan pruebas de pentesting.

5.2. Gestión de acceso de usuario

5.2.1. Registro y baja de usuario

- **¿Se utiliza un ID de usuario únicos para cada usuario?** Único
- **¿Se genera en función a una solicitud con aprobaciones y registros apropiados?** Si
- **¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido?** No porque no existe una comunicación inmediata de parte de recursos humanos
- **¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos?** No, generalmente en el departamento se enteran al ver que un usuario pierde actividad dentro de la empresa.
- **¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes**? No
- **¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios?** Si
- **¿Qué impide que los ID de usuario sean reasignados a otros usuarios?** Es único porque el sistema lo requiere

RESULTADO	COMENTARIO
REPETIBLE	El proceso de identificación de usuario como único está correcto, pero no existe un abuena comunicación para dar de baja a los usuarios.

5.2.2. Provisión de acceso de usuario

- **¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio**? Si
- **¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones?** En lo posible un 90%
- **¿Existe un registro documental de la solicitud y aprobación de acceso?** Correo o llamada los dos directores o empleados depende de la criticidad.

RESULTADO	COMENTARIO
ADMINISTRADO	Esta bastante claro la forma de otorgar permisos, generalmente se realiza por petición verbal.

5.2.3. Gestión de privilegios de acceso

- **¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios?** Son muy pocas las cuentas que tienen privilegios de acceso y que generalmente no las usan por lo que no tienen un proceso de revisión de privilegios de usuarios.
- **¿Se genera un ID de usuario separado para otorgar privilegios elevados?** No, manifiestan que al ser pocos no es necesario.
- **¿Se ha establecido una caducidad para los ID de usuario con privilegios?** No, no es necesario porque solo ellos manejan esos usuarios, gerencia las tiene pero no las maneja
- **¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?** No, no es necesario porque solo ellos manejan esos usuarios, gerencia las tiene pero no las maneja, pero no tienen controlado.

RESULTADO	COMENTARIO
ADMINISTRADO	Manifiestan que no es necesario tener procesos de control pues solo el departamento TIC y gerencia tienen accesos privilegiados, de los cuales gerencia generalmente no hace uso de sus privilegios.

5.2.4. Gestión de la información secreta de autenticación de los usuarios nóminas

- **¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.?** Información financiera, de salud. Solo contraseña para tener acceso al servidor y no se tenía ningún proceso de caducidad de contraseñas.
- **¿Se verifica rutinariamente si hay contraseñas débiles?** Si se verifica
- **¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas?** Teléfono interno, reconocimiento por voz.
- **¿Se transmite dicha información por medios seguros?** Si
- **¿Se generan contraseñas temporales suficientemente fuertes?** Son contraseñas definitivas pero fuertes
- **¿Se cambian las contraseñas por defecto de los fabricantes?** Si
- **¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas?** No
- **¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?** En algunos casos las contraseñas no están cifradas y no se recomienda a los empleados almacenarlas de forma segura.

RESULTADO	COMENTARIO
DEFINIDO	Se controla las contraseñas, aunque falta su almacenamiento seguro. El cambio de contraseña podría mejorarse.

5.2.5. Revisión de los derechos de acceso de usuarios

- **¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones?** No se revisa
- **¿Participan en dicha revisión los ""propietarios"" para verificar cambios en las funciones de los usuarios?** No, puesto que no se revisa.
- **¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?** No se realiza una revisión y los usuarios con privilegios no han cambiado.

RESULTADO	COMENTARIO
INICIAL	Generalmente al inicio de sus funcionales se les da acceso según su puesto de trabajo y no se realiza una revisión posterior a menos que se solicite por parte de algún director o derechos humanos.

5.2.6. Retirada o reasignación de los derechos de acceso

- **¿Existe un proceso de ajuste de derechos de acceso?** Se tiene un proceso, pero si no se notifica que se requiere algún cambio por parte de algún director o recursos humanos, no se realiza un proceso de reajuste de acceso.
- **¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo?** En caso de reajuste va a para todos
- **¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red?** Si
- **En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?** Generalmente no se usan las credenciales compartidas pero al no poseer una política definida para el cambio de contraseñas, las contraseñas se mantienen.

RESULTADO	COMENTARIO
REPETIBLE	Existe un proceso de cambio de derechos de acceso pero que no se ejecuta hasta que se requiera, no existe un proceso de control posterior a la asignación inicial de derechos.

5.3. Responsabilidades del usuario

5.3.1. Uso de la información secreta de autorización

- **¿Cómo se asegura la confidencialidad de las credenciales de autenticación?** No se asegura.
- **¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?** Se pide por teléfono o correo electrónico al departamento TIC, se cambia inmediatamente asignando una contraseña provisional hasta que el usuario ingrese y la cambie.
- **¿Existen controles de seguridad relativas a las cuentas compartidas?** No existen cuentas compartidas para usuarios generales, estas cuentas las usan dentro del departamento TIC y por ser pocos pues se sabe quién hace algo dentro del sistema.

RESULTADO	COMENTARIO
REPETIBLE	Existe proceso de cambio de contraseña adecuado, pero no documentado además que no se asegura la confidencialidad de las credenciales.

5.4. Control de acceso a sistemas y aplicaciones

5.4.1. Restricción del acceso a la información

- **¿Existen controles de acceso adecuados?** De usuario y contraseña, registro logs de intentos de inicio de sesión.
- **¿Se identifican los usuarios de forma individual individuales?** De forma individual
- **¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?** Se gestiona el acceso a aplicaciones a cada usuario dependiendo de su puesto de trabajo, si se requiere que se le otorguen o retiren permisos se notifica al departamento TIC que realice el cambio correspondiente.

RESULTADO	COMENTARIO
REPETIBLE	El control solo se puede hacer por logs, y no hay registros de cambios de permisos solo se ejecuta de acuerdo con las necesidades pero el proceso es relativamente claro.

5.4.2. Procedimientos seguros de inicio de sesión

- **¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado?** No hay mensajes, pero si realiza un control de acceso
- **¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión?** Usuario y contraseña
- **¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.?** No se usa.
- **¿La información de inicio de sesión solo se valida una vez imputadas las credenciales?** Si
- **¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas?** Se generan alertas en logs de intentos de inicio de sesión.
- **¿Se registran los inicios de sesión exitosos?** Si, en logs.
- **¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?** Si, mediante correo electrónico, o vía telefónica.

RESULTADO	COMENTARIO
DEFINIDO	Existe un proceso controlado de inicio de sesión pero que puede mejorar en aspectos de mensajes de advertencia y monitorización automática de accesos fallidos.

5.4.3. Sistema de gestión de contraseñas

- **¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos?** Si
- **¿Las reglas tienen en cuenta lo siguiente?**
    - **Longitud mínima de la contraseña** SI

- **Evitan la reutilización de un número específico de contraseñas** SI
- **Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.)** SI
- **Requiere el cambio forzado de contraseñas** Solo en el primer inicio de sesión
- **Esconde la contraseña durante la imputación** SI
- **¿Se almacenan y transmiten de forma segura (cifrado)?** SI, por vía telefónica o correo electrónico.

RESULTADO	COMENTARIO
DEFINIDO	Existen procedimientos establecidos por recursos humanos, aunque falta un poco tener mayor comunicación entre departamentos para optimizar el proceso.

5.4.4. Uso de utilidades con privilegios del sistema

- **¿Quién controla los servicios privilegiados?** Si solo empleados del departamento TIC.
- **¿Quién puede acceder a ellos, en qué condiciones y con qué fines?** Aunque existen empleados de gerencia que podrían hacerlo, muy pocas veces o hacen. Los únicos que acceden son los empleados del departamento de TIC para administración del sistema y aplicaciones.
- **¿Se verifica que estas personas tengan necesidad comercial para otorgar el acceso según su roles y responsabilidades?** Muy pocas personas tienen acceso y se verifica sus razones para acceder.
- **¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado?** No existe registro, solo los logs.
- **¿Se tiene en cuenta la segregación de tareas?** Si

RESULTADO	COMENTARIO
DEFINIDO	Existe un claro procesos de uso de privilegios puesto que son muy pocas las personas o entidades que tendrían acceso al sistema o concretamente a una aplicación, pero se requiere un registro oficial en caso de ser personas externas.

5.4.5. Control de acceso al código fuente de los programas

- **¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios?** Solo tienen el departamento TIC.
- **¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.?** Es seguro, si se cambia algo se tiene un registro.
- **¿Cómo se modifica el código fuente?** Si, se hace pruebas y luego se cambia definitivamente después de comprobar su funcionalidad.
- **¿Cómo se publica y se compila el código?** Todo el proceso lo realiza el departamento TIC y solo se envía una alerta de actualización de las aplicaciones
- **¿Se almacenan y revisan los registros de acceso y cambios?** Si

RESULTADO	COMENTARIO
ADMINISTRADO	El código fuente esta almacenado de forma correcta y solo tienen acceso el departamento TIC. Los cambios que se realizan se verifican y registran, para proceder a una actualización de la aplicación en todos los ordenadores que se use.

6. Criptografía

6.1. Controles criptográficos

6.1.1. Políticas de uso de los controles criptográficos veracript zip servidores

- **¿Existe una política que cubra el uso de controles criptográficos?** Para servidores y dispositivos de almacenamiento de información confidencial.
- **¿Cubre lo siguiente?**
  - **Los casos en los que información debe ser protegida a través de la criptografía** SI
  - **Normas que deben aplicarse para la aplicación efectiva** SI
  - **Un proceso basado en el riesgo para determinar y especificar la protección requerida** Todos tienen el mismo proceso de protección al tratarse de información confidencial
  - **Uso de cifrado para información almacenada o transferida** SI
  - **Los efectos de cifrado en la inspección de contenidos de software** SI
  - **Cumplimiento de las leyes y normativas aplicables** SI
- **¿Se cumple con la política y requerimientos de cifrado?** SI

RESULTADO	COMENTARIO
ADMINISTRADO	El proceso de cifrado está claramente establecido pues se maneja información confidencial y se requiere el cumplimiento de esta política para cumplir con lo establecido en la Normativa de Protección de Datos.

6.1.2. Gestión de claves

- **¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)?** SI
- **¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas?** SI
- **¿Se generan claves diferentes para sistemas y aplicaciones?** SI
- **¿Se evitan claves débiles?** SI
- **¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)?** SI, depende en cada aplicación
- **¿Se hacen copias de respaldo de las claves?** No
- **¿Se registran las actividades clave de gestión?** SI
- **¿Cómo se cumplen todos estos requisitos?** La gestión de claves criptográficas depende exclusivamente de las reglas que tiene la aplicación que maneja la criptografía. En el caso de las aplicaciones, depende del diseño de cada una de ellas.

RESULTADO	COMENTARIO
ADMINISTRADO	Existen procesos definición para el control de las claves de criptografía, cada una manejada adecuadamente pero distinta para cada aplicación.

7. Seguridad física y del entorno

7.1. Áreas seguras

7.1.1. Perímetro de seguridad física

- **¿Las instalaciones se encuentran en una zona de riesgo?** No
- **¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)?** Si, pero no existe señalización.
- **¿El techo exterior, las paredes y el suelo son de construcción sólida?** Si
- **¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?** Todo ingreso se registra en la recepción, y en caso de ser en horas no laborables se tienen alarmas en todos los edificios.
- **¿Las puertas y ventanas son fuertes y con cerradura?** Si
- **¿Se monitorea los puntos de acceso con cámaras?** No
- **¿Existe un sistema de detección de intrusos y se prueba periódicamente?** Ciertos puntos critico como cuartos de almacenamiento de servidores, no están físicamente protegidos. En ninguno de los casos se realiza una prueba de detección de intrusos.

RESULTADO	COMENTARIO
REPETIBLE	Está definido el control de acceso a edificios, pero falta el control de accesos a ciertos lugares como cuartos de almacenamiento de edificios. Además falta realización de pruebas de detección de intrusos.

7.1.2. Controles físicos de entrada

- **¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)?** Timbres para dar accesos solo desde adentro, y alarmas para horas no laborables.
- **¿Hay procedimientos que cubran las siguientes áreas?**
  - **Cambio regular código de acceso** No aplica
  - **Inspecciones de las guardias de seguridad** Si
  - **Visitantes siempre acompañados y registrados en el libro de visitantes no, cuando los trabajadores entran firman** No aplica, muchas personas ingresan a las instalaciones y solo se deben anunciar en la recepción.
  - **Registro de movimiento de material** No aplica
  - **Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas)** Solo accede a quien se le otorgue permisos. Ciertas áreas críticas no están controladas
- **¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)?** No aplica
- **¿Se requiere para las áreas críticas?** Se requiere autorización.

- **¿Existe un registro de todas las entradas y salidas?** A áreas críticas no.

RESULTADO	COMENTARIO
INICIAL	Los controles físicos a edificios son pocos pero es por la afluencia de personas y al ser una organización que brinda ayuda a personas con discapacidad muchas personas ingresan a sus instalaciones. Falta de control en algunos cuartos considerados como críticos.

7.1.3. Seguridad de oficinas, despachos y recursos

- **¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)?** Se restringe el acceso a despacho de psicólogas y los expedientes bajo llave
- **¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?** Algunas oficinas
- **¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?** Si

RESULTADO	COMENTARIO
DEFINIDO	Existen restricciones para algunas oficinas y recursos de los empleados, pero en algunos casos como cuarto de servidores o recursos TIC falta seguridad física.

7.1.4. Protección contra las amenazas externas y ambientales

- **¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.?** Detector de incendios, extintores, alarmas.
- **¿Existe un procedimiento de recuperación de desastres?** Recuperar las copias de seguridad que están en otro lado. Una copia externa mensual y está fuera del edificio y las copias de los datos está en otro equipo.
- **¿Se contemplan sitios remotos?** Si

RESULTADO	COMENTARIO
OPTIMIZADO	No poseen muchas amenazas de tipo externas ambientales y en caso de sufrirlas están bastante preparados para afrontar y recuperarse de un incidente.

7.1.5. El trabajo en áreas seguras

- **¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo?** Si, si hay incidencia se comunica
- **¿Se hace un análisis para evaluar que los controles adecuados están implementados?** Mantenimiento una vez al año
- **Controles de acceso físico** no, pero si es necesario.
- **Alarmas de intrusión** solo en edificios pero no en cuartos
- **Monitoreo de CCTV (verificar la retención y frecuencia de revisión)** No tienen
- **Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación** No (actualizada a SI)
- **Políticas, procedimientos y pautas** SI, establecidas dependiendo el área de trabajo.

- **¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?** Bajo llave

RESULTADO	COMENTARIO
ADMINISTRADO	Tienen bastante definidos las políticas y la seguridad en los lugares de trabajo.

7.1.6. Áreas de carga y descarga

- **¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado?** Se entrega en la recepción y se firma registrando las entregas.
- **¿Se verifica que el material recibido coincide con un número de pedido autorizado?** Si
- **¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?** Si

RESULTADO	COMENTARIO
OPTIMIZADO	Los procesos de recepción y entregas de mensajería lo tienen definido y con registros. Todo siguiendo las políticas de seguridad establecidas en la organización

7.2. Seguridad de los equipos

7.2.1. Emplazamiento y protección de equipos

- **¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?** No todas están protegidas, o las llaves se encuentran en el mismo lugar.
- **¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?** Los que necesitan protección sí, pero hay equipos a los que deben acceder muchas personas por lo que no se puede cumplir con esta política.
- **¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales?** Inundación – NO, fuego – SI, Temperatura – SI, Polvo – mantenimiento.
    - **Agua / inundación**
    - **Fuego y humo**
    - **Temperatura, humedad y suministro eléctrico**
    - **Polvo**
    - **Rayos, electricidad estática y seguridad del personal**
- **¿Se prueban estos controles periódicamente y después de cambios importantes?** No

RESULTADO	COMENTARIO
REPETIBLE	Existen algunas protecciones para los equipos pero falta mecanismos de protección o establecer en el lugar políticas de uso de los equipos.

7.2.2. Instalaciones de suministro

- **¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad?** Poseen un sistema para servidores dando 5 minutos para ejecutar un apagado seguro

- **¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente?** SI
- **¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante?** Si mantenimiento anual.
- **¿Son probados con regularidad?** No se verifica
- **¿Hay una red de suministro eléctrico redundante?** No, se emite alarma cuando ya no funciona por falta de suministro eléctrico.
- **¿Se realizan pruebas de cambio?** NO
- **¿Se ven afectados los sistemas y servicios?** Se afecta por la interrupción de servicios, pero es menor.
- **¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos?** Si
- **¿Están ubicados apropiadamente?** Si
- **¿Hay una capacidad adecuada de A / C para soportar la carga de calor?** SI
- **¿Hay unidades redundantes, de repuesto o portátiles disponibles?** Disco de reserva, si hay un equipo de reserva en caso de que el principal falle.
- **¿Hay detectores de temperatura con alarmas de temperatura?** No

RESULTADO	COMENTARIO
ADMINISTRADO	Poseen un sistema de suministro y climatización adecuado para las instalaciones, no se requiere grandes sistemas. Solo faltaría revisión del funcionamiento, aunque cuando sucede un incidente eléctrico no ha fallado.

7.2.3. Seguridad del cableado

- **¿Hay protección física adecuada para cables externos, cajas de conexiones?** Pocas
- **¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias?** A nivel de instalaciones si, en algunos puertos de trabajo no
- **¿Se controla el acceso a los paneles de conexión y las salas de cableado?** Está protegido bajo llave, otras veces no está protegido.
- **¿Existen procedimientos adecuados para todo ello?** No

RESULTADO	COMENTARIO
INICIAL	No tienen incidentes de cableado, la seguridad esta y a veces puede ser mínima pero si se debe establecer una mejor política de seguridad para este tipo de instalaciones.

7.2.4. Mantenimiento de los equipos

- **¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)?** SI
- **¿Hay programas de mantenimiento y registros / informes actualizados?** Una vez al año se revisa todo en todas las sedes se hace un mantenimiento**.**
- **¿Se aseguran los equipos?** Mínima seguridad

RESULTADO	COMENTARIO
REPETIBLE	Existe políticas de mantenimiento de equipos una vez al año, pero se podría formalizar más documentando las acciones.

7.2.5. Retirada de materiales propiedad de la empresa

- **¿Existen procedimiento relativos al traslado de activos de información?** En cada sede hay taller de reparación y llevar el personal autorizado.
- **¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados?** Muy manual, si no son equipos sumamente importantes todas las decisiones las toma los administradores del departamento TIC.
- **¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo?** No aplica
- **¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?** No aplica

RESULTADO	COMENTARIO
DEFINIDO	Tienen claramente establecidos los procedimientos, falta un poco de formalización en caso de ser incidentes considerables.

7.2.6. Seguridad de los equipos fuera de las instalaciones

- **¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas?** Se entrega un manual de uso al inicio del contrato o cuando se entrega el dispositivo móvil o portátil. Para los equipos remotos que en este caso son servidores, la seguridad depende directamente de la empresa que presta sus servicios.
- **¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras?** Uso de cifrado, y conexiones seguras.
- **¿Existen controles para asegurar todo esto?** No para dispositivos portátiles, pero si para los servidores.
- **¿Cómo se les informa a los trabajadores sobre sus obligaciones?** Se les entrega un manual de buenas prácticas para su uso de dispositivos móviles. Para los servidores no es necesario.
- **¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?** Si.

RESULTADO	COMENTARIO
DEFINIDO	Existen políticas de seguridad establecidas que se deben cumplir en cuanto a seguridad en dispositivos móviles, no existen controles para verificar que así es pero no han tenido incidentes. En cuanto a servidores remotos existe mucha seguridad pero que depende exclusivamente de la empresa que presta el servicio.

7.2.7. Reutilización o eliminación segura de equipos

- **¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación?** Eliminan la información que contiene el equipo

- **¿Se utiliza cifrado fuerte o borrado seguro?** Se usa cifrado y como la información se almacena en servidores de respaldo se puede eliminar la información de los equipos.
- **¿Se mantienen registros adecuados de todos los medios que se eliminan?** No
- **¿La política y el proceso cubren todos los dispositivos y medios de TIC?** Si

RESULTADO	COMENTARIO
DEFINIDO	Se tienen respaldos de información para luego ser eliminada de los quipos y que estos se puedan reutilizar o eliminar, pero se necesita de un registro más formal de estas actividades.

7.2.8. Equipo de usuario desatendido

- **¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción?** No a nivel de aplicaciones, pero si a nivel físico a veces.
- **¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado?** Si
- **¿Se protegen los bloqueos de pantalla con contraseña?** En algunos equipos
- **¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC?** A casi todos
- **¿Cómo se verifica el cumplimiento?** No

RESULTADO	COMENTARIO
REPETIBLE	Existen indicios de políticas en este sentido pero falta generalizarla y aplicar a todos los dispositivos con verificación de funcionalidad.

7.2.9. Política de puesto de trabajo despejado y pantalla limpia

- **¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?** Cuando entran dejan limpio y cuando se van no se puede asegurar que dejen despejada y limpia
- **¿Funciona en la práctica?** No se puede asegurar, depende del trabajador
- **¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos?** Si, pero no todos lo tienen activado.
- **¿Se activa automáticamente tras de un tiempo inactivo definido?** No en todos los dispositivos esta activo
- **¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?** Si

RESULTADO	COMENTARIO
DEFINIDO	Existen políticas de trabajo despejado y protección de salvaguardas, pero que es necesario controlar que se ejecuten en todos los puestos de trabajo

8. Seguridad de las operaciones

8.1. Procedimientos y responsabilidades operacionales

8.1.1. Documentación de procedimientos operacionales

- **¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.?** Si más o menos, no hay registro de algunas actividades o no se realiza una gestión adecuada o periódica.
- **¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez?** Lo intentan hacer cada vez que se requiera, pero no lo hacen con periodicidad.
- **¿Los procesos son razonablemente seguros y están bien controlados?** Si
- **¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal?** Si, tienen un plan
- **¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)?** Lo máximo posible.
- **¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?** Cuando se lo requiere

RESULTADO	COMENTARIO
REPETIBLE	Existen procedimientos establecidos pero que se deben formalizar y hacerlo periódicamente. Se deben enforcar los controles no solo en operaciones correctas si no también en seguridad.

8.1.2. Gestión de cambios

- **¿Existe una política de gestión de cambios?** Si
- **¿Existen registros relacionados a la gestión de cambios?** Si, se registra cada cambio en aplicaciones o en bases de datos
- **¿Se planifican y gestionan los cambios?** Si, se realizan planificaciones anuales o cuando se requiera
- **¿Se evalúan los riesgos potenciales asociados con los cambios?** SI
- **¿Los cambios están debidamente documentados, justificados y autorizados por la administración?** Si, lo planes son grandes se realiza planes aprobados por la directiva. Si los cambios son menos se consensa en el departamento TIC.

RESULTADO	COMENTARIO
OPTIMIZADO	Tienen todos los procedimientos claros. Se crean planes de cambios cuando son importantes o se llega a un consenso dentro del departamento TIC. Todos los cambios se comprueban y registran.

8.1.3. Gestión de capacidades

- **¿Existe una política de gestión de capacidad?** Si
- **¿Existen registros relacionados a la gestión de capacidad?** Si, pero no actualizados

- **¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante?** Logs de alerta de memoria
- **¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?** Si

RESULTADO	COMENTARIO
DEFINIDO	Las políticas están definidas, falta actualización y un control más definido de capacidad especialmente en los equipos más críticos.

8.1.4. Separación de los recursos de desarrollo, prueba y operación

- **¿Se segregan entornos de TIC de desarrollo, prueba y operacionales?**
- **¿Cómo se logra la separación a un nivel de seguridad adecuado?**
- **¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)?**
- **¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos?**
- **¿Cómo se promueve y se lanza el software?**
- **¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección?**
- **¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros?**
- **¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?**

RESULTADO	COMENTARIO
NO APLICABLE	La organización es pequeña y no se maneja el desarrollo de software por lo que no existe segregación en este sentido.

8.2. Protección contra el software malicioso (malware)

8.2.1. Controles contra el código malicioso

- **¿Existen políticas y procedimientos asociados a controles antimalware?** Si
- **¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?** Se usan las dos.
- **¿Cómo se compila, gestiona y mantiene la lista y por quién?** Lo administra el departamento de TIC
- **¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT?** En ordenadores hay antivirus pero no actualizados, en el caso de los servidores el control es más estricto.

- **¿Se actualiza el software antivirus de forma automática?** En servidores si, demás dispositivos no.
- **¿Se general alertas accionables tras una detección?** Si
- **¿Se toma acción de forma rápida y apropiada para minimizar sus efectos?** Si
- **¿Cómo se gestionan las vulnerabilidades técnicas?** Se realiza un estudio de la amenaza y se toma acciones inmediatas para mitigarlo.
- **¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte?** Un poco
- **¿Existe un mecanismo de escalación para incidentes graves?** Si

RESULTADO	COMENTARIO
DEFINIDO	Existen procesos de control de malware en equipos de riesgo como servidores, pero en los ordenadores falta procesos de control, además de actualización que no se lo realiza periódicamente.

8.3. Copias de seguridad

8.3.1. Copias de seguridad de la información

- **¿Existen políticas y procedimientos asociados a las copias de seguridad?** SI
- **¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio?** En lo máximo posible.
- **¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.?** Se cubre la mayor parte de dispositivos
- **¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales?** Servidores de respaldo si, dispositivos portátiles de almacenamiento podrían mejorarse su seguridad física.
- **¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido?** Si
- **¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica?** En algunos casos
- **¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar?** Se realiza una prueba anual de recuperación de sistemas en base a copias de seguridad.
- **¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?** Si

RESULTADO	COMENTARIO
ADMINISTRADO	Se tienen claros las copias, pero debe haber un mayor control de copias realizadas, organizar mejor la información y procurar también copias de ordenadores.

8.4. Registros y supervisión

8.4.1. Registro de eventos

- **¿Existen políticas y procedimientos para el registro de eventos?** Si son importantes se realiza un registro del evento.
- **¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí?** Se tiene solo logs, y se revisa cuando se requiere no poseen un sistema automatizado.
- **¿Se registra lo siguiente?**
    - **cambios en los ID de usuario** SI
    - **permisos y controles de acceso** SI
    - **actividades privilegiadas del sistema** SI
    - **intentos de acceso exitosos y fallidos** SI
    - **inicio de sesión y cierre de sesión** SI
    - **identidades y ubicaciones de dispositivos** NO
    - **direcciones de red, puertos y protocolos** MÁS O MENOS
    - **instalación de software** NO
    - **cambios a las configuraciones del sistema** SI
    - **uso de utilidades y aplicaciones del sistema** SI
    - **archivos accedidos y el tipo de acceso** NO
    - **filtros de acceso web** SI
- **¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados?** Los administradores del departamento
- **¿Cuál es el periodo de retención de eventos?** Depende del evento, no hay un periodo definido
- **¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?** Si

RESULTADO	COMENTARIO
REPETIBLE	Existen registros de eventos, pero que no se los revisa a menos que sea necesario. No es una tarea automatizada. Tienen que definir mejor como tratar los eventos de seguridad.

8.4.2. Protección de la información del registro

- **¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable?** En logs, con protección que provee los servidores
- **¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado?** Solo tienen acceso los administradores del departamento TIC, no hay proceso de autorización.
- **¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos?** Solo tienen acceso los administradores del departamento TIC
- **¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención?** Si
- **¿Existen copias de seguridad de los registros?** Si, cuando se hace una copia de seguridad de los servidores.

RESULTADO	COMENTARIO
DEFINIDO	Tienen registros de eventos pero no automatizado, toda la revisión es manual y protegido por seguridad que ofrece el servidor.

8.4.3. Registros de administración y operación

- **Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)?** SI
- **¿Cómo se recogen, almacenan y aseguran, analizan los registros?** Proceso manual
- **¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?** No, lo hacer los administradores

RESULTADO	COMENTARIO
ADMINISTRADO	El proceso es manual y solo los administradores lo realizan. Se puede mejorar el proceso.

8.4.4. Sincronización del reloj

- **¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión?** SI
- **¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)?** NTP
- **¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales?** SI
- **¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.?** Parte de ellos
- **¿Existe una configuración de respaldo para la referencia de tiempo?** SI

RESULTADO	COMENTARIO
OPTIMIZADO	Poseen un sistema de sincronización de reloj para todo el sistema y mecanismos de control de acceso y registro manuales.

8.5. Control del software en explotación

8.5.1. Instalación del software en explotación

- **¿Existe una política acerca de la instalación de software?**
- **¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción?**
- **¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)?**
- **¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.?**
- **¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados?**
- **¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas?**
- **¿Existe un control de cambio y aprobación adecuado para la aprobación de software?**

RESULTADO	COMENTARIO
NO APLICABLE	No existe proceso de explotación, sin embargo mantiene controlado las instalaciones en todos los dispositivos.

8.6. Gestión de la vulnerabilidad técnica

8.6.1. Gestión de las vulnerabilidades técnicas

- **¿Existe una política la gestión de vulnerabilidades técnicas?** Si, establecen un proceso pero no está documentado.
- **¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada?** No se ha hecho un proceso de escaneo para detectar vulnerabilidades periódicas y automatizadas
- **¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes?** Siguen un protocolo de aviso y mitigación de la vulnerabilidad
- **¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?** NO
- **¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC?** NO
- **¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo?** NO
- **¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución?** SI
- **¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados?** SI
- **¿Se emplea una administración automatizada de parches?** Si, cuando sea posible
- **¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?** Si, se conversa las soluciones en el departamento TIC.

RESULTADO	COMENTARIO
REPETIBLE	Solo tienen políticas para parches, les hace falta implementar muchos procesos de seguridad que no tienen considerados, especialmente de detección de vulnerabilidades.

8.6.2. Restricción en la instalación de software

- **¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?** SI
- **¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos?** Solo tienen una categoría, no se requiere más.
- **¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?** SI

RESULTADO	COMENTARIO
ADMINISTRADO	Existen controles y restricciones para instalaciones adecuada pero se puede efectivizar el proceso porque causa inconvenientes en la actualización de aplicaciones.

8.7. Consideraciones sobre la auditoria de sistemas de información

8.7.1. Controles de auditoría de sistemas de información

- **¿Existe una política que requiera auditorias de seguridad de la información?** No
- **¿Existe un programa definido y procedimientos para auditoría?** No
- **¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales?** No
- **¿Se define el alcance de la auditoría en coordinación con la administración?** No
- **¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?** No hay evidencia de herramientas

RESULTADO	COMENTARIO
INICIAL	Se ha realizado auditorias informáticas pero con pocas consideraciones en cuanto a seguridad. No tienen madres y nunca se ha realizado una auditoria de seguridad completa de toda la organización. Pero se intenta mantener controlado la seguridad.

9. Seguridad de las comunicaciones

9.1. Gestión de la seguridad de las redes

9.1.1. Controles de red

- **¿Existen políticas de redes físicas e inalámbricas?** SI, segmentación de redes
- **¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red?** No
- **¿Existe un mecanismo de registro y monitorización de la red y los dispositivos que se conectan ella?** NO
- **¿Hay un sistema de autenticación para todos los accesos a la red de la organización?** No para todas las redes
- **¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?** SI
- **¿Los usuarios se autentican adecuadamente al inicio de sesión?** En algunos casos no hay autenticación, pero en los que se el proceso es adecuado. Usuario y contraseña.
- **¿Cómo se autentican los dispositivos de red?** No hay proceso de autenticación de los dispositivos de red.
- **¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?** SI
- **¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?** SI

RESULTADO	COMENTARIO
DEFINIDO	Existen políticas de seguridad para redes, pero que se podrían mejorar en ciertos aspectos que no están controlados.

9.1.2. Seguridad de los servicios de red

- **¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?** Se gestionan los servicios.
- **¿Existe un monitoreo de servicios de red?** No hay tantos servicios como para monitorizarlos

- **¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?** SI
- **¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?** SI
- **¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?** En lo posible

RESULTADO	COMENTARIO
DEFINIDO	No existen muchos servicios de red, pero los que se tiene poseen seguridad, considerando que se podría mejorar.

9.1.3. Segregación en redes

- **¿Existe una política de segmentación de red?** SI
- **¿Qué tipo de segmentación existe?** Separación de la red priva con red pública para redes inalámbricas.
- **¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)?** En niveles de confianza
- **¿Cómo se monitorea y controla la segregación?** No se realiza un proceso de control y monitorización.
- **¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados?** SI
- **¿Hay controles adecuados entre ellos?** No
- **¿Cómo se controla la segmentación con proveedores y clientes?** No posee ese tipo de segmentación, no es necesario.
- **¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?** En lo máximo que se pueda.

RESULTADO	COMENTARIO
DEFINIDO	Poseen segmentación de redes adecuado, pero no un proceso de control y monitorización.

9.2. Intercambio de información

9.2.1. Políticas y procedimientos de intercambio de información

- **¿Existen políticas y procedimientos relacionados con la transmisión segura de información?** SI
- **¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.?** Correo electrónico (actualmente sí), FTO, dispositivos de almacenamiento.
- **¿Está basado en la clasificación de la información?** SI
- **¿Existen controles de acceso adecuados para esos mecanismos?** NO
- **¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)?** Por configuración de red, correo electrónico, y programas de criptografía.
- **¿Se sigue el principio de confidencialidad y privacidad?** SI
- **¿Existen un programa de concientización, capacitación y cumplimiento?** no

RESULTADO	COMENTARIO
DEFINIDO	Existen políticas de protección para el intercambio de información, aunque faltan procesos de control, verificación y concientización.

9.2.2. Acuerdos de intercambio de información

- **¿Qué tipos de comunicaciones se implementan las firmas digitales?** No aplica
- **¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?** Sanciones a nivel de Recursos humanos
- **¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas?** SI
- **¿Cómo se mantiene una cadena de custodia para las transferencias de datos?** No aplica

RESULTADO	COMENTARIO
ADMINISTRADO	Existen procedimientos establecidos para el intercambio de información y se mantiene la confidencialidad de esta.

9.2.3. Mensajería electrónica

- **Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?** SI
- **¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?** SI
- **¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?** NO

RESULTADO	COMENTARIO
ADMINISTRADO	La mensajería electrónica está protegida pero no posee mecanismos de control o concientización por parte de los empleados para realizar procedimientos de verificación.

9.2.4. Acuerdos de confidencialidad o no revelación

- **¿Existen acuerdos de confidencialidad?** SI
- **¿Han sido revisados y aprobados por el Departamento Legal?** SI
- **¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?** Basados en cambios
- **¿Han sido aprobados y firmados por las personas adecuadas?** SI
- **¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?** SI

RESULTADO	COMENTARIO
DEFINIDO	Por el tipo de información que maneja la organización existen acuerdos de confidencialidad por parte de todos aquellos involucrados con la organización.

10. Adquisición, desarrollo y mantenimiento de los sistemas de información

10.1. Requisitos de seguridad en los sistemas de información

10.1.1. Análisis de requisitos y especificaciones de seguridad de la información

- **¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software?** Si se evalúa la seguridad para nuevas adquisiciones pero no existe una política específica de cómo proceder.
- **¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo?** Se verifica la seguridad pero no existe un procedimiento claro a seguir.
- **¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.)** Se revisa la seguridad en cambios, actualizaciones y nuevas adquisiciones.
- **¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados?** Se revisa aspectos de seguridad al inicio del cambio o adquisición.

RESULTADO	COMENTARIO
REPETIBLE	Se revisa la seguridad en cambios, actualizaciones y adquisición, pero no existen procesos formalizados.

10.1.2. Asegurar los servicios de aplicaciones en redes públicas

- **¿La organización usa o proporciona aplicaciones web de comercio electrónico?**
- **¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio?**
- **¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad?**
- **¿Se fuerza https?**
- **¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)?**
- **¿Se analizan y documentan las amenazas de forma rutinaria?**
- **¿Existe una gestión de incidentes y cambios para tratarlos?**

RESULTADO	COMENTARIO
OPTIMIZADO	A nivel público ofrecen una aplicación web, pero que la desarrolla otra empresa.

10.1.3. Protección de las transacciones de servicios de aplicaciones

- **¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet?**
- **¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.?**
- **¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?**

RESULTADO	COMENTARIO
NO APLICABLE	No se realizan transacciones en los servicios de aplicaciones que la organización ofrece.

10.2. Seguridad en el desarrollo y en los procesos de soporte

10.2.1. Política de desarrollo seguro

- **¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad?** SI
- **¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios?** SI
- **¿Los métodos de desarrollo incluyen pautas de programación segura?** SI
- **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?** Pueden buscar ese tipo de capacitación, pero están conscientes de que así debe ser.

RESULTADO	COMENTARIO
ADMINISTRADO	Aunque no existe un área específica de desarrollo, el que se realiza dentro de la organización, se realiza en base a requisitos de seguridad, pero falta formalización.

10.2.2. Procedimiento de control de cambios en sistemas

- **¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios?** SI
- **¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión?** Si, se verifica su funcionalidad antes de realizar el cambio en el sistema.
- **¿Incluye un procedimiento para cambios de emergencia?** Si
- **¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones?** No
- **¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?** Un poco, los cambios se documentan pero no existe un proceso formal de autorización excepto si es un cambio considerable.

RESULTADO	COMENTARIO
ADMINISTRADO	Tienen claro el proceso seguro a la hora de realizar un cambio en el sistema, pero se debe formalizar todos los procesos y autorizaciones no solo cuando el cambio sea considerable, sino, en todos.

10.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

- **¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado?** Se realiza una verificación de funcionalidad
- **¿Hay registros de estas actividades?** Cuando es necesario

RESULTADO	COMENTARIO
NO APLICABLE	Se verifica que este funcionado una aplicación después de un cambio, pero se requiere un proceso formal de documentado de las verificaciones en todos los tipos de cambios, mínimos o considerables.

10.2.4. Restricciones a los cambios en los paquetes de software

- **¿Se hacen cambios a paquetes software adquiridos?** Cuando sea necesario, pero pocas veces se lo ha realizado
- **¿Se verifica que los controles originales no han sido comprometidos?** SI
- **¿Se obtuvo el consentimiento y la participación del proveedor?** Depende del software
- **¿El proveedor continúa dando soporte tras los cambios?** Depende del software
- **¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores?** Si
- **¿Se hace una comprobación de compatibilidad con otro software en uso?** SI

RESULTADO	COMENTARIO
DEFINIDO	Cuando se trata de software que proporciona otra empresa, se trata de mantener actualizado, pero si son comerciales los paquetes pues no se realiza seguimiento. Cuando se lanza un a una actualización se ve sus pros y contras y se toma una decisión para el cambio o no. Falta establecer procesos claros

10.2.5. Principios de ingeniería de sistemas seguros

- **¿Se siguen principios de SDLC que incluye controles de seguridad?**
- **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?**

RESULTADO	COMENTARIO
NO APLICABLE	No existe desarrollo como tal en la organización, solo se realizan pequeños cambios en los códigos.

10.2.6. Entorno de desarrollo seguro

- **¿Se aíslan los entornos de desarrollo?**
- **¿Cómo se desarrolla, prueba y lanza el software?**
- **¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones?**
- **¿Se realizan comprobaciones de antecedentes de los desarrolladores?**
- **¿Tienen que cumplir con un NDA?**
- **¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo?**
- **¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?**

RESULTADO	COMENTARIO
NO APLICABLE	No existen entonces de desarrollo dentro de la organización porque no se dedican a esta área, solo se realizan cambios en las complicaciones que ya se encuentran en el sistema.

10.2.7. Externalización del desarrollo de software

- **¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero?**

- **Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual** SI
- **Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba** SI
- **Acceso al código fuente si el código ejecutable necesita ser modificado** SI
- **Controles de prueba de seguridad de aplicaciones** SI
- **Evaluación de vulnerabilidad y tratamiento** dependiendo de la aplicación

RESULTADO	COMENTARIO
NO APLICABLE	Todos estos aspectos son considerados a la hora de establecer una colaboración o contrato con otra empresa que ofrecerá este tipo de servicio.

10.2.8. Pruebas funcionales de seguridad de sistemas

- **¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados?** Se revisa cuando hay cambios, pero no hay revisión periódica
- **¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?** Si

RESULTADO	COMENTARIO
ADMINISTRADO	Se realizan pruebas con todas las consideraciones necesarias, pero no periódicas, se podrían mejorar los tiempos de revisión.

10.2.9. Pruebas de aceptación de sistemas

- **¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red?** SI
- **¿Las pruebas replican situaciones y entornos operativos realistas?** SI
- **¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado?** SI
- **¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo?** NO
- **¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?** Si hay un incidente se lo corrige en todas las aplicaciones que sea necesario.

RESULTADO	COMENTARIO
ADMINISTRADO	Se realizan pruebas de aceptación para nuevos sistemas, pero no se considera al usuario, sino que depende del departamento TIC y luego se da capacitación a los usuarios, si es necesario.

10.3. Datos de prueba

10.3.1. Protección de los datos de prueba

- **¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.?**
- **¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas?**

- **¿Existen registros de estas actividades?**

RESULTADO	COMENTARIO
NO APLICABLE	La organización no se maneja con este tipo de datos, datos de prueba.

11. Relación con proveedores

11.1. Seguridad en las relaciones con proveedores

11.1.1. Política de seguridad de la información en las relaciones con los proveedores

- **¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI?** SI
- **¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?** SI
- **¿Los contratos y acuerdos abordan lo siguiente?**
    - **Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada** SI
    - **Información / propiedad intelectual, y obligaciones / limitaciones derivadas**
    - **Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información** SI
    - **Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001**
    - **Identificación de controles físicos y lógicos** SI
    - **Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio** En algunos casos
    - **Habilitación de seguridad de los empleados y concienciación** NO
    - **Derecho de auditoría de seguridad por parte de la organización** En algunos casos
- **¿Existe una obligación contractual de cumplimento?** SI
- **¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?** NO

RESULTADO	COMENTARIO
ADMINISTRADO	Los contratos y acuerdos están claramente establecidos y se confía en los servicios que los proveedores pueden dar en cuento a seguridad.

11.1.2. Requisitos de seguridad en contratos con terceros

- **¿Los contratos o acuerdos formales con proveedores cubren lo siguiente?**
    - **Gestión de las relaciones, incluyendo riesgos** SI
    - **Cláusulas de confidencialidad vinculantes** SI
    - **Descripción de la información que se maneja y el método de acceder a dicha información** SI
    - **Estructura de la clasificación de la información a usar** SI

- **La Inmediata notificación de incidentes de seguridad** Si en algunos casos
- **Aspectos de continuidad del negocio** SI
- **Subcontratación y restricciones en las relaciones con otros proveedores** SI
- **Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)** SI

RESULTADO	COMENTARIO
ADMINISTRADO	Se tienen contratos con terceros claramente establecidos, pero tal vez falta un poco más de énfasis en seguridad estableciendo más requerimientos.

11.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones

- **¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos?** Se revisan las características de los equipos y se ve si se adapta a las necesidades de la organización.
- **¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros?** Aunque sean suministrado por terceros, el control lo tiene el departamento TIC de la organización por lo que se puede realizar una recuperación inicial. Si se requiere de los terceros, se tiene una buena comunicación y cláusulas de contratos de los que valerse para una recuperación correcta.
- **¿Se puede rastrear el origen del producto o servicio?** SI

RESULTADO	COMENTARIO
OPTIMIZADO	Se mantiene comunicación con todas las empresas de las cuales se adquiere tecnología por lo que se puede realizar una recuperación adecuada, además que la organización tiene el control sobre ellos.

11.2. Gestión de la provisión de servicios del proveedor

11.2.1. Control y revisión de la provisión de servicios del proveedor

- **¿Existe una monitorización de servicios y quien responsable de esta actividad?** NO
- **¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia?** Solo cuando se requiere
- **¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas?** SI
- **¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría?** Todo lo que conlleva la prestación del servicio
- **¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?** Depende del tipo de contrato

RESULTADO	COMENTARIO
DEFINIDO	Se realizan reuniones y se revisa el servicio pero solo se realiza pocas veces, cuando se requiere. No existe un seguimiento completo del servicio con auditorias.

11.2.2. Gestión de cambios en la provisión del servicio del proveedor

- **¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados?** Mediante reuniones
- **¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización?** Mediante comunicados a las empresas y con reuniones
- **¿Se actualizan los acuerdos relacionados con los cambios?** SI

RESULTADO	COMENTARIO
OPTIMIZADO	Se mantiene buena comunicación con proveedores de servicios cuando se deben cambiar las políticas dentro de la organización.

12. Gestión de incidentes de seguridad de la información

12.1. Gestión de incidentes de seguridad de la información y mejoras

12.1.1. Responsabilidades y procedimientos

- **¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes?** Se sabe que debe hacer pero no tienen claramente establecidos políticas para gestión de incidentes
- **¿Qué cubre?**
    - **El plan de respuesta a incidentes** Saben que hacer
    - **Puntos de contacto para la notificación de incidentes, seguimiento y evaluación** SI
    - **Monitoreo, detección y reporte de eventos de seguridad** SI
    - **Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio** NO
    - **Método de recolección de evidencias y pruebas forenses digitales** NO
    - **Revisión post-evento de seguridad y procesos de aprendizaje / mejora** NO
- **¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?** SI

RESULTADO	COMENTARIO
REPETIBLE	Los administradores saben que acciones tomar pero se debe formalizar con procedimientos claros a seguir. Además se deben realizar registros y revisiones después de solucionar el incidente.

12.1.2. Notificación de los eventos de seguridad de la información

- **¿Cómo se informan los eventos de seguridad de la información?** Por el sistema te tickets, correo electrónico o por teléfono.
- **¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen?** Si, pero no se puede asegurar que lo haga inmediatamente cuando no son emergentes.
- **¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.** Si en caso de que los eventos sean muy relevantes, en caso contrario solo se soluciona.
- **¿Qué pasa con esos informes?** Se los archivan

RESULTADO	COMENTARIO
DEFINIDO	Tienen muy claro que se debe hacer en caso de que los eventos sean emergentes, en caso contrario se sigue el proceso pero no existe documentación.

12.1.3. Notificación de puntos débiles de la seguridad

- **¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual?** Si, se espera que los empleados lo hagan.
- **¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?** SI

RESULTADO	COMENTARIO
ADMINISTRADO	Los empleados saben que en caso de ventos de seguridad u ocurrencias anuales deben notificar inmediatamente. Se espera que todos los empleados lo hagan.

12.1.4. Evaluación y decisión sobre los eventos de seguridad de información

- **¿Qué tipos de eventos se espera que informen los empleados?** Todo evento que no esté dentro de lo normal.
- **¿A quién informan?** Mediante el sistema te tickets, por correo o teléfono a su jefe inmediato, director de la sede, o en casos relevantes directamente al departamento TIC.
- **¿Cómo se evalúan estos eventos para decidir si califican como incidentes?** No se tiene una escala de evaluación
- **¿Hay una escala de clasificación?** No
- **¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves?** No, para lo que es seguridad. Se puede usar la de informática normal pero que es generalizada.
- **¿En qué se basa?**

RESULTADO	COMENTARIO
REPETIBLE	En cuanto a seguridad no se tiene una escala de medición de incidentes para que los empleados sepan a quién o como informarlos.

12.1.5. Respuesta a incidentes de seguridad de la información

- **¿Cómo se recolecta, almacena y evalúa la evidencia?** Se hace el proceso dependiendo del tipo incidente.
- **¿Hay una matriz de escalación para usar según sea necesario?** Si, pero no claramente establecida.
- **¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes?** SI
- **¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?** Se documenta todo lo que realiza necesario.

RESULTADO	COMENTARIO
DEFINIDO	Se realiza las actividades correspondientes para atender un incidente dependiendo de su gravedad, pero no es un proceso formalizado.

12.1.6. Aprendizaje de los incidentes de seguridad de la información

- **¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes?** Solo si se lo requiere
- **¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?** SI
- **Además, ¿Se está utilizado para formación y concienciación?** No
- **¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro?** Más o menos
- **¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?** Más o menos

RESULTADO	COMENTARIO
NO APLICABLE	Conocer los procedimientos para tratar las incidencias, pero no se tiene un proceso de realimentación y aprendizaje adecuado.

12.1.7. Recopilación de evidencias

- **¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área?**
- **¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol?**
- **(cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas)**
- **¿Quién decide emprender un análisis forense, y en qué criterio se base?**
- **¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?**

RESULTADO	COMENTARIO
INEXISTENTE	No ha ocurrido eventos que se requiera de la recolección de evidencias, por lo que este aspecto no se puede evaluar. Se puede indicar que ante un incidente han actuado de la forma correspondiente.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

13.1. Continuidad de la seguridad de la información

13.1.1. Planificación de la continuidad de la seguridad de la información

- **¿Cómo se determinan los requisitos de continuidad del negocio?** Planes realizados a inicio de año
- **¿Existe un plan de continuidad de negocio?** SI
- **¿Existen un diseño adecuado de ""alta disponibilidad"" para sistemas de TI, redes y procesos críticos?** Más o menos

- **¿Se identifica el impacto potencial de los incidentes?** SI
- **¿Se evalúan los planes de continuidad del negocio?** SI
- **¿Se llevan a cabo ensayos de continuidad?** SI

RESULTADO	COMENTARIO
ADMINISTRADO	Existen planes de continuidad de negocio que se presenta una vez al año y acciones que se ejecutan para verificar igual una vez al año. Falta un poco de enfoque a la seguridad.

13.1.2. Implementar la continuidad de la seguridad de la información

- **¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción?** SI
- **¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares?** SI
- **¿La planificación de la continuidad es consistente e identifica las prioridades de restauración?** SI
- **¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades?** Depende directamente de la coordinación del departamento TIC
- **¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?** No aplica

RESULTADO	COMENTARIO
OPTIMIZADO	Los planes de continuidad de negocio cubren todos los aspectos que a organización requiere y se ejecuta cuando se realiza las pruebas.

13.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

- **¿Existe un método de pruebas del plan de continuidad?** SI
- **¿Con qué frecuencia se llevan a cabo dichas pruebas?** Se intenta que sea una vez al año
- **¿Hay evidencia de las pruebas reales y sus resultados?** SI
- **¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?** SI

RESULTADO	COMENTARIO
NO APLICABLE	Las pruebas que se realizan siguen un proceso de ejecución, informe y revisión de todo lo que se realizó para evaluar si se identifican deficiencias.

13.2. Redundancias

13.2.1. Disponibilidad de los recursos de tratamiento de la información

- **¿Cómo se identifican los requisitos de disponibilidad de servicios?** Evaluando los servicios mínimos con los que la organización debe funcionar
- **¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga?** No te toman en cuenta estos aspectos en específico, pero si otros.

- **¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí?** SI
- **¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?** No aplica no poseen sitios de recuperación de desastres

RESULTADO	COMENTARIO
ADMINISTRADO	Se tienen en consideración varios aspectos para tener una disponibilidad de información.

14. Cumplimiento

14.1. Cumplimiento de los requisitos

14.1.1. Identificación de la legislación aplicable y de los requisitos contractuales

- **¿Existe una política acerca del cumplimiento de requisitos legales?** SI
- **LOPD, GDPR, etc.** SI
- **¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?** SI
- **¿Hay una persona encargada de mantener, usar y controlar el registro?** SI
- **¿Cómo se logra y se garantiza el cumplimiento?** Contratación con empresa externa
- **¿Existen controles adecuados para cumplir con los requisitos?** SI

RESULTADO	COMENTARIO
OOTIMIZADO	La organización se basa el normativas y leyes legares y en cuento a protección de la información lo tiene externalizado y son ellos quienes les ayuda a cumplir con las obligaciones legales.

14.1.2. Derechos de Propiedad Intelectual (DPI)

- **¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?** SI

RESULTADO	COMENTARIO
OPTIMIZADO	La organización se maneja dentro del marco legal.

14.1.3. Protección de los registros de la organización

- **¿Existe una política que contemple lo siguiente?** SI
- **Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.** SI
- **¿Se almacenan las firmas digitales de forma segura?**
- **¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado?** SI
- **¿Se verifica periódicamente la integridad de los registros?** Se verifica cuando se puede
- **¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?** SI

RESULTADO	COMENTARIO
ADMINISTRADO	Los registros de la organización como una información más se encuentran gestionados de manera adecuada. Faltaría hacer un poco más de control.

14.1.4. Protección y privacidad de la información de carácter personal

- **¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal?** SI
- **¿Hay un responsable de privacidad en la organización?** SI
- **¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización?** SI
- **¿Cuáles son los controles de acceso a información de carácter personal?** Se accede dependiendo del tipo de empleado y la función que desempeña dentro de la organización, es decir por roles.
- **¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?** Profesionales y administrativos.

RESULTADO	COMENTARIO
OPTIMIZADO	La protección y privacidad de la información se maneja con cautela y está bien gestionado por el tipo de información que se maneja.

14.1.5. Regulación de los controles criptográficos

- **¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico?** SI
- **¿Estas actividades cumplen con los requisitos legales y reglamentarios?** SI

RESULTADO	COMENTARIO
OPTIMIZADO	Los controles criptográficos cumplen con los requisitos legales.

14.2. Revisiones de la seguridad de la información

14.2.1. Revisión independiente de la seguridad de la información

- **¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información?** No
- **¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos?** No
- **¿Están los objetivos y el alcance de auditoria autorizados por la gerencia?** No
- **¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información?** No
- **¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?**

RESULTADO	COMENTARIO
INICIAL	No existe una maduración en la revisión de la seguridad de la información dentro de la organización.

14.2.2. Cumplimiento de las políticas y normas de seguridad

- **¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente?** Se espera que cumplan con todas sus obligaciones los empleados.
- **¿Se hace una verificación periódica?** NO

RESULTADO	COMENTARIO
REPETIBLE	No existen procesos claro que garanticen el cumplimiento de las políticas de seguridad si se trata de empleados. El departamento TIC cumple las políticas.

14.2.3. Comprobación del cumplimiento técnico

- **¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares?**
- **¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables?**
- **¿Cómo informa, analiza y utilizan los resultados de dichas pruebas?**
- **¿La prioridad de tratamiento se basa en un análisis de riesgos?**
- **¿Hay evidencias de medidas tomadas para abordar los problemas identificados?**

RESULTADO	COMENTARIO
INEXISTENTE	No se han realizado pruebas de pentesting o de cumplimiento técnico de seguridad por lo que no se puede evaluar este aspecto.

Anexo B

Tablas de los tipos de datos con sus dimensiones de seguridad y las amenazas que afecta a cada uno de ellos.

- [D] Datos /Información:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1					
Daños por agua	N2					
Fenómeno climático	N3					
Fenómeno sísmico	N4					
Fuego	I1					
Daños por agua	I2					
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4					
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10					
Errores de usuarios	E1	X	X	X		
Errores de administración	E2	X	X	X		
Errores de monitorización log	E3		X			X
Errores de configuración	E4		X			
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17					
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1		X			X
Manipulación de la configuración	A2		X	X	X	
Suplantación de la identidad del usuario	A3		X	X	X	
Abuso de privilegios de acceso	A4	X	X	X		
Uso no previsto	A5					

Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11		X			X
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13		X			
Destrucción de información	A14	X				
Divulgación de información	A15			X		
Manipulación de programas	A16					
Manipulación de equipos	A17					
Denegación de servicio	A18					
Robo	A19					
Ataque destructivo	A20					
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [S] Servicios:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1					
Daños por agua	N2					
Fenómeno climático	N3					
Fenómeno sísmico	N4					
Fuego	I1					
Daños por agua	I2					
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4					
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10					
Errores de usuarios	E1	X	X	X		
Errores de administración	E2	X	X	X		
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7			X		
Errores de secuencia	E8		X			
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				

Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16	X				
Perdida de equipos	E17					
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3		X	X	X	
Abuso de privilegios de acceso	A4	X	X	X		
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7			X		
Alteración de secuencia	A8		X			
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11		X			X
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13		X			
Destrucción de información	A14	X				
Divulgación de información	A15			X		
Manipulación de programas	A16					
Manipulación de equipos	A17					
Denegación de servicio	A18	X				
Robo	A19					
Ataque destructivo	A20					
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [SW] Software – Aplicaciones Informáticas:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1					
Daños por agua	N2					
Fenómeno climático	N3					
Fenómeno sísmico	N4					
Fuego	I1					
Daños por agua	I2					
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4	X				
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					

Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10					
Errores de usuarios	E1	X	X	X		
Errores de administración	E2	X	X	X		
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6	X	X	X		
Errores de (re)encaminamiento	E7			X		
Errores de secuencia	E8		X			
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13	X	X	X		
Errores de mantenimiento/actualización de programas	E14	X	X			
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17					
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3		X	X	X	
Abuso de privilegios de acceso	A4	X	X	X		
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6	X	X	X		
(re) Encaminamiento de mensajes	A7			X		
Alteración de secuencia	A8		X			
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13		X			
Destrucción de información	A14	X				
Divulgación de información	A15			X		
Manipulación de programas	A16	X	X	X		
Manipulación de equipos	A17					
Denegación de servicio	A18					
Robo	A19					
Ataque destructivo	A20					
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [HW] Equipos Informáticos (Hardware):

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1	X				
Daños por agua	N2	X				
Fenómeno climático	N3	X				
Fenómeno sísmico	N4	X				
Fuego	I1	X				
Daños por agua	I2	X				
Contaminación mecánica	I3	X				
Avería de origen físico/lógico	I4	X				
Corte de suministro eléctrico	I5	X				
Fallas de climatización	I6	X				
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10			X		
Errores de usuarios	E1					
Errores de administración	E2	X	X	X		
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10					
Destrucción de información	E11					
Fugas de información	E12					
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15	X				
Caída del sistema por agotamiento de recursos	E16	X				
Perdida de equipos	E17	X		X		
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3					
Abuso de privilegios de acceso	A4	X	X	X		
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					

Modificación deliberada de la información	A13					
Destrucción de información	A14					
Divulgación de información	A15					
Manipulación de programas	A16					
Manipulación de equipos	A17	X		X		
Denegación de servicio	A18	X				
Robo	A19	X		X		
Ataque destructivo	A20	X				
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [COM] Redes de Comunicaciones:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1					
Daños por agua	N2					
Fenómeno climático	N3					
Fenómeno sísmico	N4					
Fuego	I1					
Daños por agua	I2					
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4					
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					
Fallo servicios de comunicaciones	I7	X				
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10					
Errores de usuarios	E1					
Errores de administración	E2	X	X	X		
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7			X		
Errores de secuencia	E8		X			
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16	X				
Perdida de equipos	E17					

Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3		X	X	X	
Abuso de privilegios de acceso	A4	X	X	X		
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7			X		
Alteración de secuencia	A8		X			
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10			X		
Repudio	A11					
Interceptación de información (escucha)	A12			X		
Modificación deliberada de la información	A13		X			
Destrucción de información	A14					
Divulgación de información	A15			X		
Manipulación de programas	A16					
Manipulación de equipos	A17					
Denegación de servicio	A18	X				
Robo	A19					
Ataque destructivo	A20					
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [MEDIA] Soportes de Información:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1	X				
Daños por agua	N2	X				
Fenómeno climático	N3	X				
Fenómeno sísmico	N4	X				
Fuego	I1	X				
Daños por agua	I2	X				
Contaminación mecánica	I3	X				
Avería de origen físico/lógico	I4	X				
Corte de suministro eléctrico	I5	X				
Fallas de climatización	I6	X				
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9	X				
Emanaciones electromagnéticas	I10			X		
Errores de usuarios	E1	X	X	X		
Errores de administración	E2	X	X	X		

Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15	X				
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17	X		X		
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3					
Abuso de privilegios de acceso	A4					
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13		X			
Destrucción de información	A14	X				
Divulgación de información	A15			X		
Manipulación de programas	A16					
Manipulación de equipos	A17	X		X		
Denegación de servicio	A18					
Robo	A19	X		X		
Ataque destructivo	A20	X				
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [AUX] Equipamiento Auxiliar:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1	X				
Daños por agua	N2	X				
Fenómeno climático	N3	X				
Fenómeno sísmico	N4	X				
Fuego	I1	X				
Daños por agua	I2	X				
Contaminación mecánica	I3	X				
Avería de origen físico/lógico	I4	X				
Corte de suministro eléctrico	I5	X				
Fallas de climatización	I6	X				
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8	X				
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10			X		
Errores de usuarios	E1					
Errores de administración	E2					
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10					
Destrucción de información	E11					
Fugas de información	E12					
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15	X				
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17	X		X		
Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3					
Abuso de privilegios de acceso	A4					
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					

Modificación deliberada de la información	A13					
Destrucción de información	A14					
Divulgación de información	A15					
Manipulación de programas	A16					
Manipulación de equipos	A17	X		X		
Denegación de servicio	A18					
Robo	A19	X		X		
Ataque destructivo	A20	X				
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [L]Instalaciones:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1	X				
Daños por agua	N2	X				
Fenómeno climático	N3	X				
Fenómeno sísmico	N4	X				
Fuego	I1	X				
Daños por agua	I2	X				
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4					
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10			X		
Errores de usuarios	E1					
Errores de administración	E2					
Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10		X			
Destrucción de información	E11	X				
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17					

Indisponibilidad del personal	E18					
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3					
Abuso de privilegios de acceso	A4					
Uso no previsto	A5	X	X	X		
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9		X	X		
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13		X			
Destrucción de información	A14	X				
Divulgación de información	A15			X		
Manipulación de programas	A16					
Manipulación de equipos	A17					
Denegación de servicio	A18					
Robo	A19					
Ataque destructivo	A20	X				
Indisponibilidad del personal	A21					
Extorsión	A22					
Ingeniería social	A23					

- [P] Personal:

AMENAZA	TIPO	D	I	C	A	T
Fuego	N1					
Daños por agua	N2					
Fenómeno climático	N3					
Fenómeno sísmico	N4					
Fuego	I1					
Daños por agua	I2					
Contaminación mecánica	I3					
Avería de origen físico/lógico	I4					
Corte de suministro eléctrico	I5					
Fallas de climatización	I6					
Fallo servicios de comunicaciones	I7					
Interrupción de otros servicios y suministros esenciales	I8					
Degradación de los soportes de almacenamiento de la info.	I9					
Emanaciones electromagnéticas	I10					
Errores de usuarios	E1					
Errores de administración	E2					

Errores de monitorización log	E3					
Errores de configuración	E4					
Difusión de software dañino	E6					
Errores de (re)encaminamiento	E7					
Errores de secuencia	E8					
Alteración accidental de la información	E10					
Destrucción de información	E11					
Fugas de información	E12			X		
Vulnerabilidades de los programas	E13					
Errores de mantenimiento/actualización de programas	E14					
Errores de mantenimiento/actualización de equipos	E15					
Caída del sistema por agotamiento de recursos	E16					
Perdida de equipos	E17					
Indisponibilidad del personal	E18	X				
Manipulación de los registros de actividad	A1					
Manipulación de la configuración	A2					
Suplantación de la identidad del usuario	A3					
Abuso de privilegios de acceso	A4					
Uso no previsto	A5					
Difusión de software dañino	A6					
(re) Encaminamiento de mensajes	A7					
Alteración de secuencia	A8					
Acceso no autorizado	A9					
Análisis de trafico	A10					
Repudio	A11					
Interceptación de información (escucha)	A12					
Modificación deliberada de la información	A13					
Destrucción de información	A14					
Divulgación de información	A15					
Manipulación de programas	A16					
Manipulación de equipos	A17					
Denegación de servicio	A18					
Robo	A19					
Ataque destructivo	A20					
Indisponibilidad del personal	A21	X				
Extorsión	A22	X	X	X		
Ingeniería social	A23	X	X	X		

Anexo C

Este Anexo corresponde a la herramienta ofimática en Excel Analisis_APSA, aquí se puede ver todos los datos recopilados y la magnitud de los cálculos realizados durante el desarrollo de este trabajo.

El orden en que se presenta el documento es:

- Inventario
- Dependencias
- Valoración de Activos
- Amenazas
- Datos/Información
- Servicios
- Software – Aplicaciones
- Equipos Informáticos (Hardware)
- Redes de Comunicaciones
- Soportes de Información
- Equipamiento Auxiliar
- Instalaciones
- Personal
- Tipo
- Salvaguardas

GRUPO	No.	CÓDIGO	NOMBRE	TIPO	RESPONSABLE	DESCRIPCIÓN
D	1	D1	Datos de configuración	[files][conf][int]	Administradores	Datos usados para la configuración de aplicaciones y servidores
D	2	D2	Código fuente de aplicaciones	[files][source]	Administradores	Código fuente de las aplicaciones que APSA maneja y no pertenece a ningún tercero
D	3	D3	Ficheros almacenados en PC	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en sus respectivos ordenadores
D	4	D4	Ficheros almacenados en servidores en la nube	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en los servidores de la nube mediante el servicio de Intranet Documental. Estos ficheros se pueden compartir con otros profesionales
D	5	D5	Ficheros almacenados en servidores locales	[files]	Administradores	Ficheros multimedia (audio, voy, video, texto) y ofimáticos guardados por los empleados de APSA en los servidores que se encuentran en cada una de las sedes mediante el servicio de Intranet Documental. Estos ficheros se pueden compartir con otros profesionales que se encuentran dentro de la misma sede.
D	6	D6	Bases de datos en servidores locales	[int][auth]	Administradores	Se consideran las bases de datos que están en los servidores locales de cada sede para el acceso al servicio de intranet
D	7	D7	Bases de datos en servidores en la nube	[int][auth]	Administradores	Se consideran las bases de datos que pertenecen a las aplicaciones que se encuentran almacenadas en los servidores en la nube
D	8	D8	Copias de seguridad en la nube	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en los servidores en la nube
D	9	D9	Copias de Seguridad en servidores locales	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en los servidores locales
D	10	D10	Copias de Seguridad en discos externos	[files][backup]	Administradores	Aquí se agrupan las copias de seguridad de: servidores, datos de configuración, bases de datos y ficheros que están almacenados en discos externos, pendrives o algún otro equipo de almacenamiento
D	11	D11	Ficheros de contraseñas	[files][password][auth]	Administradores	APSA para el ingreso como administrador tanto para aplicaciones como servidores, cuenta con ficheros de contraseñas compartidos entre administradores
D	12	D12	Registros de actividades en servidores	[files][int][log]	Administradores	Todos los servidores tienen configurados logs que registran las actividades que en ellos se realiza y son los que pertenecen a este grupo
D	13	D13	Ficheros compartidos Google Drive	[files][password[int]	Administradores	Se consideran todos los archivos importantes para APSA que se almacenan en Google Drive y que se comparte entre administradores.
S	1	S1	Página web	[anon][pub][ext][www]	Administradores	Servicio que ofrece APSA a través de su aplicación web
S	2	S2	Correo electrónico	[int][email][edi]	Administradores	Este es un servicio subcontratado con la Suit de correo electrónico de Gmail para empresas.
S	3	S3	Intranet documental - Servicio FTP	[int][file][ftp][edi]	Administradores	Este es el servicio que usan los profesionales para compartir sus ficheros
S	4	S4	Sistema de tickets de incidencias	[int][www]	Administradores	Si ocurre algún tipo de incidencia, todos quienes trabajan en APSA tendrán acceso a un Sistema de tickets de incidencia, mediante el cual se intenta solucionar los problemas con la brevedad posible

GRUPO DE ACTIVO
[D] Datos / Información
[S] Servicios

S	**5**	**S5**	**Educación Virtual**	[ext][int][www][edi]	SR	Este es un servicio que se prondrá en marcha en un futuro por lo que se ha considerado para este análisis. La educación Virtual pretende llegar a más usuarios y sus familias. Ahora no dependerá si está cerca de una sede, un usuario puede recibir clases desde su casa.
S	**6**	**S6**	**Servicio de financiero**	[int]	Administradores	Aquí se involucran los servidores y aplicaciones dedicadas al departamento financiero de APSA
S	**7**	**S7**	**Gestión de usuarios Socios**	[int][dir]	Administradores	Servicio que se ofrece a todos los usuarios inscritos para los tratamientos que se ofrecen en APSA
S	**8**	**S8**	**Gestión empresarial**	[int]	Administradores	Ofrece un control empresarial de distintas áreas a través de módulos
S	**9**	**S9**	**Gestión de recursos humanos, nóminas**	[int][dir]	Administradores	Servicio que se ofrece al departamento de recursos humanos para el tratamiento de nóminas
SW	**1**	**SW1**	**Aplicación de Financiero**	[prp][app]	Administradores	Aplicación dedicada a tesorería, contabilidad y todo tema relacionado con el sector financiero y económico de APSA
SW	**2**	**SW2**	**GUS Gestión de Usuarios Socios**	[prp][app]	Administradores	Aplicación que usan los profesionales de la salud o interesados, en donde se encuentran todos los usuarios que reciben tratamientos o beneficios dentro de APSA
SW	**3**	**SW3**	**G2K Gestión Empresarial**	[sub][app]	Administradores	Aplicación que permite integrar módulos para la gestión empresarial y que contiene aplicaciones para otros departamentos
SW	**4**	**SW4**	**Sage Gestión de Recursos Humanos (nóminas)**	[sub][app]	Administradores	Sub-aplicación que permite al departamento de recursos humanos manejar las nóminas de los empleados de APSA
SW	**5**	**SW5**	**Gestión de Bases de Datos**	[std][dbms]	Administradores	Aplicaciones que configuran las bases de datos según sean MySQL y SQL Server
SW	**6**	**SW6**	**Aplicación de Página web**	[sub][www][app]	Administradores	Aplicación que contiene la página web de APSA a la que todas las personas tienen acceso, que esta creada y controlada por terceros
SW	**7**	**SW7**	**Aplicación de Intranet**	[prp][app][file][backup]	Administradores	Aplicación que permite guardar y compartir ficheros de interés general entre profesionales
SW	**8**	**SW8**	**Aplicación del Sistema de tickets de incidencias**	[prp][app]	Administradores	Aplicación que ayuda a todos los empleados de APSA notificar si tienen algún tipo de problemas para ser atendidos lo antes posible
SW	**9**	**SW9**	**Aplicación de Correo electrónico Gmail**	[sub][std][email_server]	Administradores	Aplicación contratada con Google mediante la Suit de Gmail que ofrece el servicio de correo electrónico empresarial para APSA
SW	**10**	**SW10**	**E-apsa**	[sub][www][app]	Administradores	Es una aplicación que se encuentra en desarrollo y que aún no ha sido integrada a los servicios de APSA, pero que ha sido considerada pues en poco tiempo lo integraran a su infraestructura
SW	**11**	**SW11**	**Aplicaciones en móviles**	[sub][std]	Administradores	A todos los empleados se les entrega un teléfono móvil o en algunas ocasiones tablets, estos dispositivos tienen aplicaciones como correo electrónico, navegadores web, aplicaciones de chat entre otras que se requiere para el trabajo.
SW	**12**	**SW12**	**Sistema operativo Ubuntu Server**	[sub][std][os]	Administradores	Sistema operativo que se encuentra en uno de los servidores de APSA
SW	**13**	**SW13**	**Sistema Operativo Windows Server**	[sub][std][os]	Administradores	Sistema operativo que se encuentra en el resto de los servidores de APSA
SW	**14**	**SW14**	**Sistema operativo Windows 7**	[sub][std][os]	Administradores	Sistema operativo que usan cerca de la mitad de los ordenadores de APSA, aunque ya se ha empezado la migración a Windows 10, se lo considera porque aún se usa.

[SW] Software - Aplicaciones informáticas

SW	**15**	**SW15**	**Sistema operativo Windows 10**	[sub][std][os]	Administradores	Sistema operativo al que están migrado los ordenadores de APSA	
SW	**16**	**SW16**	**Navegadores Web**	[std][browser]	Administradores	Todos los empleados de APSA ingresan a través de navegadores web algunos de las aplicaciones, así también usan para navegar por internet según las necesidades de su trabajo	
SW	**17**	**SW17**	**Antivirus**	[sub][std][av]	Administradores	Este está presente en todos los servidores, así como en los ordenadores que operan con Windows 7	
SW	**18**	**SW18**	**Software Ofimático**	[std][office]	Administradores	Son herramientas que usan a diario los empleados para cumplir con sus actividades, dentro de estas se consideran documentos, fotografías, imágenes, videos, audios.	
HW	**1**	**HW1**	**Servidores APSA**	[vhost]	Administradores	Se consideran los 4 servidores principales de APSA en donde se encuentran alojados sus principales servicios y aplicaciones	**[HW] Equipos Informáticos (Hardware)**
HW	**2**	**HW2**	**Servidores Sedes**	[host]	Administradores	Se consideran a los ordenadores que funcionan como servidores de almacenamiento que existen en cada una de las sedes	
HW	**3**	**HW3**	**Ordenadores de escritorio administrativos**	[pc]	Administradores, técnicos	Ordenadores usados por la directiva y parte gerencial de APSA	
HW	**4**	**HW4**	**Ordenadores de escritorio empleados**	[pc]	Administradores, técnicos	Ordenadores usados por los empleados de los distintos departamentos que conforman APSA	
HW	**5**	**HW5**	**Portátiles de administrativos**	[pc]	Administradores, técnicos	Portátiles usados por la directiva y gerencia de APSA	
HW	**6**	**HW6**	**Portátiles de empleados**	[pc]	Administradores, técnicos	Portátiles usados por los empleados de los distintos departamentos que conforman APSA	
HW	**7**	**HW7**	**Portátiles TIC**	[pc]	Administradores	Portátiles usados por los empleados del departamento de TIC, estos son de importancia pues es desde allí que se tienen el control de servidores y aplicaciones	
HW	**8**	**HW8**	**Móviles/Tablets**	[mobile][pda]	Administradores, técnicos	Dispositivos móviles usados por los empleados de APSA pertenecientes a la organización para comunicación telefónica móvil	
HW	**9**	**HW9**	**Impresoras oficinas**	[peripheral][print][scan]	Administradores, técnicos	Dispositivos de impresión y escaneo que se encuentran en las oficinas de APSA	
HW	**10**	**HW10**	**Router**	[mid][network][router]	Administradores, técnicos	Dispositivos que permiten la conexión de red para entregar el servicio de internet a ordenadores	
HW	**11**	**HW11**	**Router inalámbrico**	[network][modem][wap]	Administradores, técnicos	Dispositivo que permiten la conexión de red para entregar servicio de internet a dispositivos móviles	
HW	**12**	**HW12**	**Switch**	[network][switch]	Administradores, técnicos	Dispositivos que permiten la conexión de red para entregar el servicio de internet a ordenadores	
HW	**13**	**HW13**	**Impresoras repositorios**	[peripheral][print][scan]	Administradores, técnicos	Dispositivos de impresión y escaneo que se encuentran en los dos repositorios en los que trabaja APSA	
HW	**14**	**HW14**	**Teléfonos de sobremesa**	[ipphone]	Administradores, técnicos	Dispositivos para comunicación telefónica	
COM	**1**	**COM1**	**Redes inalámbricas**	[wifi][internet]	Administradores, técnicos	Redes de comunicaciones que se realizan a través de routers inalámbricos para brindar conectividad a dispositivos móviles	**[COM] Redes de comunicaciones**
COM	**2**	**COM2**	**Redes locales**	[LAN][internet]	Administradores, técnicos	Redes de comunicaciones que se realizan a través de routers y switches para dar conectividad a las oficinas y laboratorios de APSA	
COM	**3**	**COM3**	**Red telefónica**	[PSTN]	Administradores, técnicos	Red telefónica mediante la cual se ofrece el servicio de comunicación de telefónica entre empleados	
COM	**4**	**COM4**	**Red telefonía móvil**	[mobile]	Administradores, técnicos	Red telefónica móvil mediante la cual se ofrece el servicio de comunicación de telefónica móvil entre empleados	
MEDIA	**1**	**MEDIA1**	**Discos duros externos**	[electrónica][disk]	Administradores, técnicos	Discos duros usados para realizar copias de seguridad	**[MEDIA] Soportes de Información**

MEDIA	**2**	**MEDIA2**	**Pendrives USB**	[electronic][usb]	Administradores, técnicos	Dispositivos usados para guardar información que usen los empleados de APSA	
MEDIA	**3**	**MEDIA3**	**CD/DVD**	[electronic][cd][dvd]	Administradores, técnicos	Dispositivos usados para guardar información que usen los empleados de APSA	
MEDIA	**4**	**MEDIA4**	**Material impreso**	[non_electronic][printed]	SR	Toda documentación impresa de APSA que sea relevante	
AUX	**1**	**AUX1**	**Generador eléctrico**	[power][gen]	Administradores, técnicos	Generadores eléctricos en caso de fallas eléctricas que permiten proteger momentáneamente los servidores para resguardarlos	**[AUX] Equipamiento Auxiliar**
AUX	**2**	**AUX2**	**Fuentes de alimentación**	[power]	Administradores, técnicos	Fuentes de alimentación usados para distintos elementos informáticos	
AUX	**3**	**AUX3**	**Climatización**	[ac]	Administradores, técnicos	Dispositivos usados en algunos de los cuartos en los que se encuentran dispositivos informativos relevantes	
AUX	**4**	**AUX4**	**Cableado UTP**	[cabling][wire]	Administradores, técnicos	Sistema de cableado para establecer las redes y brindar conectividad entre ordenadores y hacia internet	
AUX	**5**	**AUX5**	**Armarios**	[furniture]	Administradores, técnicos	Armarios en donde se encuentran alojados dispositivos informáticos y dispositivos de red	
AUX	**6**	**AUX6**	**Cajas fuertes**	[safe]	Administradores	Es aquí en donde se almacenan las cosas más críticas que requieran este tipo de protección	
L	**1**	**L1**	**Edificios**	[building]	Administradores, técnicos	Se considera a todos los edificios que conforman APSA	**[L] Instalaciones**
L	**2**	**L2**	**Cuartos servidores**	[local]	Administradores, técnicos	Se consideran los cuartos en donde se encuentran los servidores o dispositivos de red importantes	
L	**3**	**L3**	**Coche**	[car]	SR	Es el medio de transporte en donde se moviliza el personal de TIC a las distintas sedes	
P	**1**	**P1**	**Administradores**	[adm][com][sec]	no aplica	Administradores del departamento de TIC y encargados del manejo de casi todo el sistema informático y manejan bases de datos, aplicaciones y servidores, aunque también puede cumplir con otras funciones	**[P] Personal**
P	**2**	**P2**	**Técnicos**	[dba][sec][des]	no aplica	Encargados de funciones técnicas, mantenimiento infromático y eléctrico	
P	**3**	**P3**	**Empleados**	[ui]	no aplica	Personal que trabaja dentro de la organización como empleado	
P	**4**	**P4**	**Usuarios**	[ue]	no aplica	Son todas las personas y familias que acceden a los servicios o prestan colaboración a la organización	

GRUPO	No.	CÓDIGO	NOMBRE	DEPENDENCIAS GRADO 1
D	1	D1	Datos de configuración	Servidores APSA, Servidores locales
D	2	D2	Código fuente de aplicaciones	Servidores APSA, Servidores locales
D	3	D3	Ficheros almacenados en PC	Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, discos duros externos, pendrives USB
D	4	D4	Ficheros almacenados en servidores en la nube	Servidores APSA, Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, redes inalámbricas, redes locales
D	5	D5	Ficheros almacenados en servidores locales	Servidores locales, Ordenadores de escritorio administrativos, Ordenadores de escritorio empleados, Portátiles de administrativos, Portátiles de empleados, Portátiles TIC, redes inalámbricas, redes locales
D	6	D6	Bases de datos en servidores locales	Servidores locales, redes inalámbricas, redes locales, , discos duros externos, pendrives USB
D	7	D7	Bases de datos en servidores en la nube	Servidores APSA, redes inalámbricas, redes locales
D	8	D8	Copias de seguridad en la nube	Servidores APSA, redes inalámbricas, redes locales
D	9	D9	Copias de Seguridad en servidores locales	Servidores locales, redes inalámbricas, redes locales
D	10	D10	Copias de Seguridad en discos externos	Servidores APSA, Servidores locales, redes inalámbricas, redes locales, , discos duros externos, pendrives USB
D	11	D11	Ficheros de contraseñas	Servidores APSA, Servidores locales
D	12	D12	Registros de actividades en servidores	Servidores APSA, Servidores locales
D	13	D13	Ficheros compartidos Google Drive	Portátiles TIC, redes inalámbricas, redes locales
S	1	S1	Página web	Aplicación de Página Web
S	2	S2	Correo electrónico	Aplicación de correo electrónico Gmail
S	3	S3	Intranet documental - Servicio FTP	Aplicación de intranet
S	4	S4	Sistema de tickets de incidencias	Aplicación del sistema de tickets de incidencias
S	5	S5	Educación Virtual	E-apsa
S	6	S6	Servicio de financiero	Aplicación de Financiero
S	7	S7	Gestión de usuarios Socios	GUS Gestión de Usuarios Socios
S	8	S8	Gestión empresarial	G2K Gestión empresarial

S	9	S9	Gestión de recursos humanos, nóminas	Sage Gestión de Recursos Humanos (nóminas)
SW	**1**	**SW1**	Aplicación de Financiero	
SW	**2**	**SW2**	GUS Gestión de Usuarios Socios	
SW	**3**	**SW3**	G2K Gestión Empresarial	
SW	**4**	**SW4**	Sage Gestión de Recursos Humanos (nóminas)	
SW	**5**	**SW5**	Gestión de Bases de Datos	
SW	**6**	**SW6**	Aplicación de Página web	
SW	**7**	**SW7**	Aplicación de Intranet	
SW	**8**	**SW8**	Aplicación del Sistema de tickets de incidencias	
SW	**9**	**SW9**	Aplicación de Correo electrónico Gmail	
SW	**10**	**SW10**	E-apsa	
SW	**11**	**SW11**	Aplicaciones en móviles	
SW	**12**	**SW12**	Sistema operativo Ubuntu Server	
SW	**13**	**SW13**	Sistema Operativo Windows Server	
SW	**14**	**SW14**	Sistema operativo Windows 7	
SW	**15**	**SW15**	Sistema operativo Windows 10	
SW	**16**	**SW16**	Navegadores Web	
SW	**17**	**SW17**	Antivirus	
SW	**18**	**SW18**	Software Ofimático	
HW	**1**	**HW1**	Servidores APSA	Página web, Intranet documental - Servicio FTP, Sistema de tickets de incidencias, Servicio de financiero, Gestión de usuarios Socios, Gestión empresarial, Gestión de recursos humanos, nóminas, generador eléctrico, fuentes de alimentación, climatización, cableado UTP, edificios, cuartos de servidores
HW	**2**	**HW2**	Servidores Sedes	Intranet documental - Servicio FTP, generador eléctrico, fuentes de alimentación, climatización, cableado UTP, edificios, cuartos de servidores
HW	**3**	**HW3**	Ordenadores de escritorio administrativos	Fuentes de alimentación, cableado UTP, edificios
HW	**4**	**HW4**	Ordenadores de escritorio empleados	Fuentes de alimentación, cableado UTP, edificios
HW	**5**	**HW5**	Portátiles de administrativos	Fuentes de alimentación, cableado UTP, edificios

HW	**6**	**HW6**	Portátiles de empleados	Fuentes de alimentación, cableado UTP, edificios
HW	**7**	**HW7**	Portátiles TIC	Fuentes de alimentación, cableado UTP, edificios
HW	**8**	**HW8**	Móviles/Tablets	Correo electrónico, conectividad
HW	**9**	**HW9**	Impresoras oficinas	Conectividad, cableado UTP, edificios
HW	**10**	**HW10**	Router	Conectividad, cableado UTP, edificios
HW	**11**	**HW11**	Router inalámbrico	Conectividad, cableado UTP, edificios
HW	**12**	**HW12**	Switch	Conectividad, cableado UTP, edificios
HW	**13**	**HW13**	Impresoras repositorios	Conectividad, cableado UTP
HW	**14**	**HW14**	Teléfonos de sobremesa	Conectividad, cableado UTP, edificios
COM	**1**	**COM1**	Redes inalámbricas	Edificios, fuentes de alimentación, armarios, Cableado UTP, router inalámbrico
COM	**2**	**COM2**	Redes locales	Edificios, cuartos servidores, fuentes de alimentación, armarios, Cableado UTP, router, switch
COM	**3**	**COM3**	Red telefónica	Edificios, cableado UTP, router, switch
COM	**4**	**COM4**	Red telefonía móvil	
MEDIA	**1**	**MEDIA1**	Discos duros externos	Armarios y mobiliario
MEDIA	**2**	**MEDIA2**	Pendrives USB	Armarios y mobiliario
MEDIA	**3**	**MEDIA3**	CD/DVD	Armarios y mobiliario
MEDIA	**4**	**MEDIA4**	Material impreso	Armarios y mobiliario
AUX	**1**	**AUX1**	Generador eléctrico	
AUX	**2**	**AUX2**	Fuentes de alimentación	
AUX	**3**	**AUX3**	Climatización	
AUX	**4**	**AUX4**	Cableado UTP	
AUX	**5**	**AUX5**	Armarios	
AUX	**6**	**AUX6**	Cajas fuertes	
L	**1**	**L1**	Edificios	
L	**2**	**L2**	Cuartos servidores	
L	**3**	**L3**	Coche	
P	**1**	**P1**	Administradores	
P	**2**	**P2**	Técnicos	

GRUPO	No.	CÓDIGO	NOMBRE	D	I	C	A	T
D	1	D1	Datos de configuración	8	8	8	9	9
D	2	D2	Código fuente de aplicaciones	8	9	8	9	9
D	3	D3	Ficheros almacenados en PC	3	7	5	6	7
D	4	D4	Ficheros almacenados en servidores en la nube	5	7	7	8	8
D	5	D5	Ficheros almacenados en servidores locales	5	7	7	8	8
D	6	D6	Bases de datos en servidores locales	8	9	9	9	9
D	7	D7	Bases de datos en servidores en la nube	9	9	9	9	9
D	8	D8	Copias de seguridad en la nube	9	8	9	9	9
D	9	D9	Copias de Seguridad en servidores locales	8	8	9	9	9
D	10	D10	Copias de Seguridad en discos externos	7	8	9	9	9
D	11	D11	Ficheros de contraseñas	9	9	9	9	9
D	12	D12	Registros de actividades en servidores	8	8	8	9	9
D	13	D13	Ficheros compartidos Google Drive	7	8	8	7	7
S	1	S1	Página web	7	8	8	5	7
S	2	S2	Correo electrónico	7	8	8	7	8
S	3	S3	Intranet documental - Servicio FTP	8	8	8	8	8
S	4	S4	Sistema de tickets de incidencias	4	6	6	8	5
S	5	S5	Educación Virtual	8	8	7	6	7
S	6	S6	Servicio de financiero	8	9	9	9	9
S	7	S7	Gestión de usuarios Socios	8	8	8	7	8
S	8	S8	Gestión empresarial	7	8	8	7	8
S	9	S9	Gestión de recursos humanos, nóminas	7	8	8	8	9
SW	1	SW1	Aplicación de Financiero	9	9	9	9	9
SW	2	SW2	GUS Gestión de Usuarios Socios	8	8	8	9	9
SW	3	SW3	G2K Gestión Empresarial	7	8	8	9	9
SW	4	SW4	Sage Gestión de Recursos Humanos (nóminas)	7	8	8	9	9
SW	5	SW5	Gestión de Bases de Datos	8	9	9	9	9
SW	6	SW6	Aplicación de Página web	7	8	8	9	8
SW	7	SW7	Aplicación de Intranet	8	8	8	9	7
SW	8	SW8	Aplicación del Sistema de tickets de incidencias	4	6	6	9	5
SW	9	SW9	Aplicación de Correo electrónico Gmail	7	8	8	9	8
SW	10	SW10	E-apsa	8	8	7	8	7
SW	11	SW11	Aplicaciones en móviles	4	8	7	6	5
SW	12	SW12	Sistema operativo Ubuntu Server	9	9	9	9	9
SW	13	SW13	Sistema Operativo Windows Server	9	9	9	9	9
SW	14	SW14	Sistema operativo Windows 7	4	9	5	8	6
SW	15	SW15	Sistema operativo Windows 10	4	9	5	8	6
SW	16	SW16	Navegadores Web	4	8	8	8	6

Dimensiones de Valoración	
D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de la información
A	Autencidad
T	Trazabilidad

Escala de Valoración		
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
8	alto	daño grave
7		
6		
5	medio	daño importante
4		
3		
2	bajo	daño menor
1		
0	despreciable	irrelevante a efectos prácticos

SW	**17**	**SW17**	Antivirus	8	8	5	8	5
SW	**18**	**SW18**	Software Ofimático	3	5	5	4	3
HW	**1**	**HW1**	Servidores APSA	9	9	9	9	9
HW	**2**	**HW2**	Servidores Sedes	8	8	9	9	9
HW	**3**	**HW3**	Ordenadores de escritorio administrativos	7	8	8	7	8
HW	**4**	**HW4**	Ordenadores de escritorio empleados	3	7	7	7	7
HW	**5**	**HW5**	Portátiles de administrativos	7	8	8	7	8
HW	**6**	**HW6**	Portátiles de empleados	3	7	7	7	7
HW	**7**	**HW7**	Portátiles TIC	8	9	9	9	9
HW	**8**	**HW8**	Móviles/Tablets	4	7	7	8	6
HW	**9**	**HW9**	Impresoras oficinas	3	2	3	3	3
HW	**10**	**HW10**	Router	8	8	8	8	8
HW	**11**	**HW11**	Router inalámbrico	8	8	8	8	8
HW	**12**	**HW12**	Switch	8	8	8	8	8
HW	**13**	**HW13**	Impresoras repositorios	8	5	4	6	5
HW	**14**	**HW14**	Teléfonos de sobremesa	6	5	4	4	4
COM	**1**	**COM1**	Redes inalámbricas	7	8	9	9	8
COM	**2**	**COM2**	Redes locales	8	8	9	9	8
COM	**3**	**COM3**	Red telefónica	8	7	8	7	8
COM	**4**	**COM4**	Red telefonía móvil	8	7	8	7	8
MEDIA	**1**	**MEDIA1**	Discos duros externos	8	9	9	9	9
MEDIA	**2**	**MEDIA2**	Pendrives USB	7	8	9	9	8
MEDIA	**3**	**MEDIA3**	CD/DVD	7	8	9	9	8
MEDIA	**4**	**MEDIA4**	Material impreso	7	8	9	9	9
AUX	**1**	**AUX1**	Generador eléctrico	5	5	3	4	4
AUX	**2**	**AUX2**	Fuentes de alimentación	5	7	3	4	4
AUX	**3**	**AUX3**	Climatización	5	4	3	4	4
AUX	**4**	**AUX4**	Cableado UTP	7	8	4	4	4
AUX	**5**	**AUX5**	Armarios	8	8	8	8	8
AUX	**6**	**AUX6**	Cajas fuertes	8	8	9	9	9
L	**1**	**L1**	Edificios	6	7	8	6	5
L	**2**	**L2**	Cuartos servidores	8	8	8	8	7
L	**3**	**L3**	Coche	2	5	3	5	2
P	**1**	**P1**	Administradores	8	8	9	9	9
P	**2**	**P2**	Técnicos	7	8	9	9	8
P	**3**	**P3**	Empleados	7	8	9	9	8
P	**4**	**P4**	Usuarios	5	6	9	9	5

AMENAZA	TIPO	Datos/Información [D]					Servicios [S]					Software – Aplicaciones [SW]					Equipamiento Informático [HW]					Redes de Comunicaciones [COM]					Soportes de Información [MEDIA]					Equipamiento Auxiliar [AUX]					Instalaciones [L]					Personal [P]					OBSERVACIONES
		D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	
Fuego	N1																X										X						X					X									INCENDIO
Daños por agua	N2																X										X						X					X									ININDACIONES
Fenómeno climático	N3																X										X						X					X									
Fenómeno sísmico	N4																X										X						X					X									
Fuego	I1																X										X						X					X									ACCIDENTAL O DELIBERADO
Daños por agua	I2																X										X						X					X									ACCIDENTAL O DELIBERADO
Contaminación mecánica	I3																X										X						X													POLVO, SUCIEDAD
Avería de origen físico/lógico	I4											X					X										X						X													
Corte de suministro eléctrico	I5																X										X						X													
Fallas de climatización	I6																X										X						X													
Fallo servicios de comunicaciones	I7																					X																								
Interrupción de otros servicios y suministros esenciales	I8																																X													
Degradación de los soportes de almacenamiento de la información	I9																										X																			PASO DEL TIEMPO
Emanaciones electromagnéticas	I10																		X										X					X					X						
Errores de usuarios	E1	X		X		X		X		X			X		X												X		X																	ERRORES DE USO
Errores de administración	E2	X		X		X		X		X			X		X		X		X			X		X			X		X																	ERRORES DE USO
Errores de monitorización log	E3		X																																												LOG REGISTROS DE ACTIVIDAD
Errores de configuración	E4		X																																											DATOS DE CONFIGURACIÓN
Difusión de software dañino	E6												X		X																															
Errores de (re)encaminamiento	E7								X					X										X																						
Errores de secuencia	E8							X						X									X																							
Alteración accidental de la información	E10		X					X						X									X						X											X						
Destrucción de información	E11	X					X					X										X					X											X								
Fugas de información	E12			X					X					X										X						X										X					X	
Vulnerabilidades de los programas	E13											X	X	X																										X						
Errores de mantenimiento/actualización de programas	E14											X	X																																	FALLA DE FUNCIONAMIENTO, PERJUICIO A LA MANTENIBILIAD DEL SISTEMA DE INFORMACION
Errores de mantenimiento/actualización de equipos	E15																X										X						X													PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACION
Caída del sistema por agotamiento de recursos	E16						X										X					X																							SATURACION DEL SISTEMA INFORMÁTICO
Perdida de equipos	E17																X		X								X		X			X													RECUPERACION DE SOPORTES RECICLADOS O DESECHADOS
Indisponibilidad del personal	E18																																											X			
Manipulación de los registros de actividad	A1		X			X																																									LOG DE RESGISTROS DE ACTIVIDAD
Manipulación de la configuración	A2		X	X	X																																										LOG DE REGISTROS DE ACTIVIDAD
Suplantación de la identidad del usuario	A3		X	X	X			X	X	X			X	X	X								X	X	X																					USURPACIÓN DE DERECHO
Abuso de privilegios de acceso	A4	X	X	X			X	X	X			X	X	X			X	X	X			X	X	X																						
Uso no previsto	A5						X	X	X			X	X	X			X	X	X			X	X	X			X	X	X			X	X	X			X	X	X						
Difusión de software dañino	A6											X	X	X																																	
(re) Encaminamiento de mensajes	A7								X					X										X																							
Alteración de secuencia	A8							X						X									X																							ALTERACION DE DATOS
Acceso no autorizado	A9		X	X				X	X					X	X				X	X				X	X				X	X										X	X				USO ILICITO DEL HARDWARE
Análisis de trafico	A10																							X																						
Repudio	A11		X			X		X			X																																			DATOS LOG RESGISTROS DE ACTIVIDAD, NEGACION DE ACCIONES
Interceptación de información (escucha)	A12																							X																						ESCUCHA PASIVA
Modificación deliberada de la información	A13		X					X						X									X					X											X						
Destrucción de información	A14	X					X					X										X					X											X								
Divulgación de información	A15			X					X					X										X						X										X					DIVULGACION, GEOLOCALIZACION, COPIA ILEGAL DE SOFTWARE
Manipulación de programas	A16											X	X	X																																	ALTERACION DE PROGRAMAS
Manipulación de equipos	A17																X		X								X		X			X													SABOTAJE DEL HARDWARE
Denegación de servicio	A18						X										X					X																							SATURACION DEL SISTEMA INFORMATICO
Robo	A19																X		X								X		X			X													RODNO DE SOPOERTES O DOCUEMNTOS, RONO DE HARWARE
Ataque destructivo	A20																X										X						X					X									DESTRUCCION DE HARDWARE O DE SOPORTES
Indisponibilidad del personal	A21																																										X			
Extorsión	A22																																										X	X	X	
Ingeniería social	A23																																										X	X	X	

DATOS / INFORMACIÓN [D]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D'	I'	C'	A'	T'	Frecuencia	F´	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
D1	Datos de configuración	Errores De Administración	0,3	75%	75%	25%			8	8	8	9	9	6	6	2			1,8	1,8	0,6			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos	75%	75%	75%			80%	0,06	1,5	1,5	0,5			0,09	0,09	0,03		
		Errores De Configuración	0,3		50%				8	8	8	9	9		4					1,2						75%					80%	0,06		1				0,06				
		Alteración Accidental De La Información	0,3		50%				8	8	8	9	9		4					1,2						75%					90%	0,03		1				0,03				
		Destrucción De Información	0,3	100%					8	8	8	9	9	8					2,4						75%					90%	0,03	2					0,06				
		Fugas De Información	0,1			50%			8	8	8	9	9			4					0,4						75%				90%	0,01			1				0,01			
		Manipulación De Los Registros De Actividad	0,1		5%			75%	8	8	8	9	9		0,4			6,75		0,04			0,68			25%			50%	80%	0,02			0,3			3,38		0,006				0,0675
		Manipulación De La Configuración	0,1		100%	100%	100%		8	8	8	9	9		8	8	9			0,8	0,8	0,9				75%	100%	75%		90%	0,01			2		2,25			0,02		0,0225	
		Abuso De Privilegios De Acceso	0,1	75%	75%	75%			8	8	8	9	9	6	6	6			0,6	0,6	0,6				75%	75%	100%			90%	0,01	1,5	1,5				0,015	0,015				
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	9		6	8				0,6	0,8					75%	100%			90%	0,01		1,5					0,015				
		Repudio	0,1		75%			100%	8	8	8	9	9		6			9		0,6			0,9			75%			50%	90%	0,01		1,5			4,5		0,015				0,045
		Modificación Deliberada De La Información	0,1		100%				8	8	8	9	9		8					0,8						75%				90%	0,01			2				0,02				
		Destrucción De Información	0,1	100%					8	8	8	9	9	8					0,8						75%					90%	0,01	2					0,02				
D2	Código fuente de aplicaciones	Errores De Administración	0,3	50%	75%	25%			8	9	8	9	9	4	6,75	2			1,2	2,03	0,6			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Registro de actualizaciones protegidos	75%	75%	75%			80%	0,06	1	1,69	0,5			0,06	0,1013	0,03		
		Errores De Configuración	0,3		75%				8	9	8	9	9		6,75					2,03						75%					80%	0,06		1,69					0,1013				
		Alteración Accidental De La Información	0,1		100%				8	9	8	9	9		9					0,9						75%					90%	0,01		2,25					0,0225				
		Manipulación De Los Registros De Actividad	0,1		5%			75%	8	9	8	9	9		0,45			6,75		0,05			0,68			25%			50%	80%	0,02			0,34			3,38		0,0068				0,0675
		Manipulación De La Configuración	0,1		75%	50%	50%		8	9	8	9	9		6,75	4	4,5			0,68	0,4	0,45				75%	100%	75%		90%	0,01			1,69		1,13			0,0169		0,0113		
		Abuso De Privilegios De Acceso	0,1	25%	75%	75%			8	9	8	9	9	2	6,75	6			0,2	0,68	0,6				75%	75%	100%			90%	0,01	0,5	1,69				0,005	0,0169				
		Acceso No Autorizado	0,1		100%	100%			8	9	8	9	9		9	8				0,9	0,8					75%	100%			90%	0,01			2,25					0,0225				
		Repudio	0,1		75%			100%	8	9	8	9	9		6,75			9		0,68			0,9			75%			50%	90%	0,01			1,69			4,5		0,0169				0,045
		Modificación Deliberada De La Información	0,1		100%				8	9	8	9	9		9					0,9						75%				90%	0,01			2,25					0,0225				
		Destrucción De Información	0,1	100%					8	9	8	9	9	8					0,8						75%					90%	0,01	2					0,02				
D3	Ficheros almacenados en PC	Errores De Usuarios	0,7	75%	75%	50%			3	7	5	6	7	2,25	5,25	2,5			1,58	3,68	1,75			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad archivos confidenciales • Cifrado de la información • Manual de Usuarios • Depuración	75%	50%	50%			50%	0,35	0,56	2,63	1,25			0,1969	0,9188	0,4375		
		Errores De Administración	0,3	75%	75%	50%			3	7	5	6	7	2,25	5,25	2,5			0,68	1,58	0,75				75%	75%	50%			90%	0,03	0,56	1,31	1,25			0,0169	0,0394	0,0375			
		Errores De Configuración	0,3		25%				3	7	5	6	7		1,75					0,53						75%					90%	0,03		0,44					0,0131				
		Alteración Accidental De La Información	0,7		75%				3	7	5	6	7		5,25					3,68						50%					50%	0,35		2,63					0,9188				
		Destrucción De Información	0,5	100%					3	7	5	6	7	3					1,5						75%					50%	0,25	0,75					0,1875				
		Fugas De Información	0,1			25%			3	7	5	6	7			1,25					0,13						75%				75%	0,025			0,31					0,0078			
		Manipulación De Los Registros De Actividad	0,1		25%			50%	3	7	5	6	7		1,75			3,5		0,18			0,35						50%	80%	0,02			1,75			1,75		0,035				0,035
		Manipulación De La Configuración	0,1		50%	50%	25%		3	7	5	6	7		3,5	2,5	1,5			0,35	0,25	0,15				70%	75%	25%		80%	0,02			1,05	0,63	1,13			0,021	0,0125	0,0225		
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	75%		3	7	5	6	7		3,5	3,75	4,5			1,05	1,13	1,35				70%	75%	25%		80%	0,06			1,05	0,94	3,38			0,063	0,0563	0,2025		
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%			3	7	5	6	7	0,75	3,5	3,75			0,08	0,35	0,38				75%	70%	75%			80%	0,02	0,19	1,05	0,94			0,0038	0,021	0,0188			
		Acceso No Autorizado	0,3		75%	100%			3	7	5	6	7		5,25	5				1,58	1,5					70%	75%			80%	0,06		1,58	1,25				0,0945	0,075			
		Repudio	0,1		25%			100%	3	7	5	6	7		1,75			7		0,18			0,7			70%			50%	80%	0,02			0,53			3,5		0,0105				0,07
		Modificación Deliberada De La Información	0,1		100%				3	7	5	6	7		7					0,7						70%				80%	0,02			2,1					0,042				
		Destrucción De Información	0,1	75%					3	7	5	6	7	2,25					0,23						75%					80%	0,02	0,56					0,0113				
D4	Ficheros almacenados en servidores en la nube	Errores De Usuarios	0,7	50%	50%	5%			5	7	7	8	8	2,5	3,5	0,35			1,75	2,45	0,25			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Usuarios • Depuración	75%	50%	50%			50%	0,35	0,63	1,75	0,18			0,2188	0,6125	0,0613		
		Errores De Administración	0,3	75%	75%	50%			5	7	7	8	8	3,75	5,25	3,5			1,13	1,58	1,05				75%	75%	90%			90%	0,03	0,94	1,31	0,35			0,0281	0,0394	0,0105			
		Errores De Monitorización Log	0,1		50%			75%	5	7	7	8	8		3,5			6		0,35			0,6				75%			75%	90%	0,01			0,88			1,5		0,0088				0,015
		Errores De Configuración	0,3		50%				5	7	7	8	8		3,5					1,05						75%					90%	0,03		0,88					0,0263				
		Alteración Accidental De La Información	0,7		75%				5	7	7	8	8		5,25					3,68						75%					90%	0,07		1,31					0,0919				
		Destrucción De Información	0,3	75%					5	7	7	8	8	3,75					1,13						75%					90%	0,03	0,94					0,0281				
		Manipulación De Los Registros De Actividad	0,1		25%			75%	5	7	7	8	8		1,75			6		0,18			0,6				75%			75%	90%	0,01			0,44			1,5		0,0044				0,015
		Manipulación De La Configuración	0,1		25%	50%	50%		5	7	7	8	8		1,75	3,5	4			0,18	0,35	0,4				75%	90%	50%		90%	0,01			0,44	0,35	2			0,0044	0,0035	0,02		
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	75%		5	7	7	8	8		1,75	5,25	6			0,53	1,58	1,8				75%	90%	50%		90%	0,03			0,44	0,53	3			0,0131	0,0158	0,09		
		Abuso De Privilegios De Acceso	0,1	25%	25%	75%			5	7	7	8	8	1,25	1,75	5,25			0,13	0,18	0,53				75%	75%	90%			90%	0,01	0,31	0,44	0,53			0,0031	0,0044	0,0053			
		Acceso No Autorizado	0,1		50%	100%			5	7	7	8	8		3,5	7				0,35	0,7					75%	90%			90%	0,01			0,88	0,7				0,0088	0,007			
		Repudio	0,1		25%			100%	5	7	7	8	8		1,75			8		0,18			0,8			90%			90%	90%	0,01			0,18			0,8		0,0018				0,008
		Modificación Deliberada De La Información	0,1		100%				5	7	7	8	8		7					0,7						75%				90%	0,01			1,75					0,0175				
		Destrucción De Información	0,1	100%					5	7	7	8	8	5					0,5						75%					90%	0,01	1,25					0,0125				
D5	Ficheros almacenados en servidores locales	Errores De Usuarios	0,7	75%	50%	5%			5	7	7	8	8	3,75	3,5	0,35			2,63	2,45	0,25			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Usuarios • Depuración	75%	50%	50%			50%	0,35	0,94	1,75	0,18			0,3281	0,6125	0,0613		
		Errores De Administración	0,3	75%	75%	50%			5	7	7	8	8	3,75	5,25	3,5			1,13	1,58	1,05				75%	75%	80%			90%	0,03	0,94	1,31	0,7			0,0281	0,0394	0,021			
		Errores De Monitorización Log	0,1		50%			75%	5	7	7	8	8		3,5			6		0,35			0,6				75%			75%	90%	0,01			0,88			1,5		0,0088				0,015
		Errores De Configuración	0,3		50%				5	7	7	8	8		3,5					1,05						75%					90%	0,03		0,88					0,0263				
		Alteración Accidental De La Información	0,5		75%				5	7	7	8	8		5,25					2,63						75%					90%	0,05		1,31					0,0656				
		Destrucción De Información	0,3	75%					5	7	7	8	8	3,75					1,13						75%					90%	0,03	0,94					0,0281				
		Manipulación De Los Registros De Actividad	0,1		25%			75%	5	7	7	8	8		1,75			6		0,18			0,6				75%			75%	90%	0,01			0,44			1,5		0,0044				0,015
		Manipulación De La Configuración	0,1		25%	50%	50%		5	7	7	8	8		1,75	3,5	4			0,18	0,35	0,4				75%	80%	50%		90%	0,01			0,44	0,7	2			0,0044	0,007	0,02		
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	75%		5	7	7	8	8		1,75	5,25	6			0,53	1,58	1,8				75%	80%	50%		90%	0,03			0,44	1,05	3			0,0131	0,0315	0,09		
		Abuso De Privilegios De Acceso	0,1	25%	25%	75%			5	7	7	8	8	1,25	1,75	5,25			0,13	0,18	0,53				75%	75%	80%			90%	0,01	0,31	0,44	1,05			0,0031	0,0044	0,0105			
		Acceso No Autorizado	0,1		50%	100%			5	7	7	8	8		3,5	7				0,35	0,7					75%	80%			90%	0,01			0,88	1,4				0,0088	0,014			
		Repudio	0,1		25%			100%	5	7	7	8	8		1,75			8		0,18			0,8			90%			90%	90%	0,01			0,18			0,8		0,0018				0,008
		Modificación Deliberada De La Información	0,1		100%				5	7	7	8	8		7					0,7						75%				90%	0,01			1,75					0,0175				
		Destrucción De Información	0,1	100%					5	7	7	8	8	5					0,5						75%					90%	0,01	1,25					0,0125				
D6	Bases de datos en servidores locales	Errores De Administración	0,3	75%	75%	50%			8	9	9	9	9	6	6,75	4,5			1,8	2,03	1,35			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Administración • Depuración • Registro de incidencias y actualizaciones • Control de recursos • Configuración de Logs	90%	90%	100%			90%	0,03	0,6	0,68				0,018	0,0203				
		Errores De Monitorización Log	0,1		75%			75%	8	9	9	9	9		6,75			6,75		0,68			0,68				90%			100%	90%	0,01			0,68					0,0068				
		Errores De Configuración	0,3		75%				8	9	9	9	9		6,75					2,03						90%					90%	0,03		0,68					0,0203				
		Alteración Accidental De La Información	0,5		75%				8	9	9	9	9		6,75					3,38						90%					90%	0,05		0,68					0,0338				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8						90%					90%	0,01	0,8					0,008				
		Manipulación De Los Registros De Actividad	0,1		50%			100%	8	9	9	9	9		4,5			9		0,45			0,9				90%			100%	90%	0,01			0,45					0,0045				
		Manipulación De La Configuración	0,1		50%	75%	50%		8	9	9	9	9		4,5	6,75	4,5			0,45	0,68	0,45					90%	100%	80%		90%	0,01			0,45		0,9			0,0045		0,009		
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%		8	9	9	9	9		4,5	9	6,75			0,45	0,9	0,68					90%	100%	80%		90%	0,01			0,45		1,35			0,0045		0,0135		
		Abuso De Privilegios De Acceso	0,1	75%	50%	75%			8	9	9	9	9	6	4,5	6,75			0,6	0,45	0,68					90%	100%			90%	0,01	0,6	0,45				0,006	0,0045				
		Acceso No Autorizado	0,1		75%	100%			8	9	9	9	9		6,75	9				0,68	0,9						90%	100%			90%	0,01			0,68					0,0068				
		Repudio	0,1		50%			100%	8	9	9	9	9		4,5			9		0,45			0,9				90%			100%	90%	0,01			0,45					0,0045				
		Modificación Deliberada De La Información	0,1		100%				8	9	9	9	9		9					0,9							90%				90%	0,01			0,9					0,009				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8						90%					90%	0,01	0,8					0,008				
D7	Bases de datos en servidores en la nube	Errores De Administración	0,3	75%	75%	50%			9	9	9	9	9	6,75	6,75	4,5			2,03	2,03	1,35			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Copias de seguridad • Cifrado de la información • Manual de Administración • Depuración	90%	90%	100%			90%	0,03	0,68	0,68				0,0203	0,0203				
		Errores De Monitorización Log	0,1		75%			75%	9	9	9	9	9		6,75			6,75		0,68			0,68				90%			100%	90%	0,01			0,68					0,0068				
		Errores De Configuración	0,3		75%				9	9	9	9	9		6,75					2,03							90%				90%	0,03			0,68					0,0203				
		Alteración Accidental De La Información	0,5		75%				9	9	9	9	9		6,75					3,38							90%				90%	0,05			0,68					0,0338				
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9						90%					90%	0,01	0,9					0,009				
		Manipulación De Los Registros De Actividad	0,1		50%			100%	9	9	9	9	9		4,5			9		0,45			0,9				90%			100%	90%	0,01			0,45					0,0045				
		Manipulación De La Configuración	0,1		50%	75%	50%		9	9	9	9	9		4,5	6,75	4,5			0,45	0,68	0,45						90%	100%	80%	90%	0,01			0,45		0,9			0,0045		0,009		
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%		9	9	9	9	9		4,5	9	6,75			0,45	0,9	0,68						90%	100%	80%	90%	0,01			0,45		1,35			0,0045		0,0135		

		Abuso De Privilegios De Acceso	0,1	75%	50%	75%			9	9	9	9	9	6,75	4,5	6,75			0,68	0,45	0,68			• Depuración • Registro de incidencias y actualizaciones • Control de recursos • Configuración de Logs	90%	90%	100%			90%	0,01	0,68	0,45				0,0068	0,0045			
		Acceso No Autorizado	0,1		75%	100%			9	9	9	9	9		6,75	9				0,68	0,9					90%	100%			90%	0,01		0,68					0,0068			
		Repudio	0,1		50%			100%	9	9	9	9	9		4,5			9		0,45			0,9			90%			100%	90%	0,01		0,45					0,0045			
		Modificación Deliberada De La Información	0,1		100%				9	9	9	9	9		9					0,9						90%				90%	0,01		0,9					0,009			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9						90%					90%	0,01	0,9					0,009				
D8	**Copias de seguridad en la nube**	Errores De Administración	0,1	75%	75%	50%			9	8	9	9	9	6,75	6	4,5			0,68	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Configuración de Logs • Comprobación de efectividad de las copias de seguridad	80%	90%	90%			90%	0,01	1,35	0,6	0,45			0,0135	0,006	0,0045		
		Errores De Monitorización Log	0,3		50%			50%	9	8	9	9	9		4			4,5		1,2			1,35			90%			50%	90%	0,03		0,4			2,25		0,012			0,0675
		Errores De Configuración	0,3		100%				9	8	9	9	9		8					2,4						75%				90%	0,03		2					0,06			
		Alteración Accidental De La Información	0,3		100%				9	8	9	9	9		8					2,4						75%				90%	0,03		2					0,06			
		Destrucción De Información	0,1	100%					9	8	9	9	9	9					0,9						50%					90%	0,01	4,5					0,045				
		Manipulación De Los Registros De Actividad	0,1		25%			75%	9	8	9	9	9		2			6,75		0,2			0,68			75%			75%	90%	0,01		0,5			1,69		0,005			0,0169
		Manipulación De La Configuración	0,1		75%	75%	75%		9	8	9	9	9		6	6,75	6,75			0,6	0,68	0,68				75%	90%	75%		90%	0,01		1,5	0,68	1,69			0,015	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%		9	8	9	9	9		4	9	6,75			0,4	0,9	0,68				75%	90%	75%		90%	0,01		1	0,9	1,69			0,01	0,009	0,0169	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%			9	8	9	9	9	4,5	6	9			0,45	0,6	0,9				75%	75%	90%			90%	0,01	1,13	1,5	0,9			0,0113	0,015	0,009		
		Acceso No Autorizado	0,1		75%	100%			9	8	9	9	9		6	9				0,6	0,9					75%	90%			90%	0,01		1,5	0,9				0,015	0,009		
		Repudio	0,1		50%			100%	9	8	9	9	9		4			9		0,4			0,9			75%			75%	90%	0,01		1			2,25		0,01			0,0225
		Modificación Deliberada De La Información	0,1		100%				9	8	9	9	9		8					0,8						75%				90%	0,01		2					0,02			
		Destrucción De Información	0,1	100%					9	8	9	9	9	9					0,9						50%					90%	0,01	4,5					0,045				
		Divulgación De Información	0,1			100%			9	8	9	9	9			9					0,9						90%			90%	0,01			0,9					0,009		
D9	**Copias de Seguridad en servidores locales**	Errores De Administración	0,1	75%	75%	50%			8	8	9	9	9	6	6	4,5			0,6	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Configuración de Logs • Comprobación de efectividad de las copias de seguridad	80%	75%	90%			90%	0,01	1,2	1,5	0,45			0,012	0,015	0,0045		
		Errores De Monitorización Log	0,3		50%			50%	8	8	9	9	9		4			4,5		1,2			1,35			75%			50%	90%	0,03		1			2,25		0,03			0,0675
		Errores De Configuración	0,3		100%				8	8	9	9	9		8					2,4						75%				90%	0,03		2					0,06			
		Alteración Accidental De La Información	0,3		100%				8	8	9	9	9		8					2,4						75%				90%	0,03		2					0,06			
		Destrucción De Información	0,1	100%					8	8	9	9	9	8					0,8											90%	0,01	8					0,08				
		Fugas De Información	0,1			75%			8	8	9	9	9			6,75					0,68					25%			75%	90%	0,01			6,75					0,0675		
		Manipulación De La Configuración	0,1		75%	75%	75%		8	8	9	9	9		6	6,75	6,75			0,6	0,68	0,68				25%	90%	75%		90%	0,01		4,5	0,68	1,69			0,045	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%		8	8	9	9	9		4	9	6,75			0,4	0,9	0,68				25%	90%	75%		90%	0,01		3	0,9	1,69			0,03	0,009	0,0169	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%			8	8	9	9	9	4	6	9			0,4	0,6	0,9				50%	25%	90%			90%	0,01	2	4,5	0,9			0,02	0,045	0,009		
		Acceso No Autorizado	0,1		75%	100%			8	8	9	9	9		6	9				0,6	0,9					25%	90%			90%	0,01		4,5	0,9				0,045	0,009		
		Repudio	0,1		50%			100%	8	8	9	9	9		4			9		0,4			0,9			25%			75%	90%	0,01		3			2,25		0,03			0,0225
		Modificación Deliberada De La Información	0,1		100%				8	8	9	9	9		8					0,8						25%				90%	0,01		6					0,06			
		Destrucción De Información	0,1	100%					8	8	9	9	9	8					0,8											90%	0,01	8					0,08				
		Divulgación De Información	0,1			100%			8	8	9	9	9			9					0,9						90%			90%	0,01			0,9					0,009		
D10	**Copias de Seguridad en discos externos**	Errores De Administración	0,1	75%	75%	50%			7	8	9	9	9	5,25	6	4,5			0,53	0,6	0,45			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Manual de Administración • Registro de copias realizadas • Control de recursos • Comprobación de efectividad de las copias de seguridad	80%	75%	90%			90%	0,01	1,05	1,5	0,45			0,0105	0,015	0,0045		
		Errores De Monitorización Log	0,3		50%			50%	7	8	9	9	9		4			4,5		1,2			1,35			50%			50%	90%	0,03		2			2,25		0,06			0,0675
		Errores De Configuración	0,3		100%				7	8	9	9	9		8					2,4						75%				90%	0,03		2					0,06			
		Alteración Accidental De La Información	0,3		100%				7	8	9	9	9		8					2,4						75%				80%	0,06		2					0,12			
		Destrucción De Información	0,1	100%					7	8	9	9	9	7					0,7											90%	0,01	7					0,07				
		Manipulación De Los Registros De Actividad	0,1		25%			75%	7	8	9	9	9		2			6,75		0,2			0,68			25%			75%	90%	0,01		1,5			1,69		0,015			0,0169
		Manipulación De La Configuración	0,1		75%	75%	75%		7	8	9	9	9		6	6,75	6,75			0,6	0,68	0,68				25%	90%	75%		90%	0,01		4,5	0,68	1,69			0,045	0,0068	0,0169	
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	75%		7	8	9	9	9		4	9	6,75			0,4	0,9	0,68				25%	90%	75%		90%	0,01		3	0,9	1,69			0,03	0,009	0,0169	
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%			7	8	9	9	9	3,5	6	9			0,35	0,6	0,9				50%	25%	90%			90%	0,01	1,75	4,5	0,9			0,0175	0,045	0,009		
		Acceso No Autorizado	0,1		75%	100%			7	8	9	9	9		6	9				0,6	0,9					25%	90%			80%	0,02		4,5	0,9				0,09	0,018		
		Repudio	0,1		50%			100%	7	8	9	9	9		4			9		0,4			0,9			25%			75%	90%	0,01		3			2,25		0,03			0,0225
		Modificación Deliberada De La Información	0,1		100%				7	8	9	9	9		8					0,8						25%				80%	0,02		6					0,12			
		Destrucción De Información	0,1	100%					7	8	9	9	9	7					0,7											90%	0,01	7					0,07				
		Divulgación De Información	0,1			100%			7	8	9	9	9			9					0,9						90%			90%	0,01			0,9					0,009		
D11	**Ficheros de contraseñas**	Errores De Administración	0,1	75%	75%	100%			9	9	9	9	9	6,75	6,75	9			0,68	0,68	0,9			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Cifrado de la información • Depuración • Control de acceso • Copias de seguridad	50%	75%	100%			90%	0,01	3,38	1,69				0,0338	0,0169			
		Errores De Configuración	0,1		5%				9	9	9	9	9		0,45					0,05						75%				90%	0,01		0,11					0,0011			
		Alteración Accidental De La Información	0,1		75%				9	9	9	9	9		6,75					0,68						75%				75%	0,025		1,69					0,0422			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9						75%					90%	0,01	2,25					0,0225				
		Manipulación De Los Registros De Actividad	0,1		25%			100%	9	9	9	9	9		2,25			9		0,23			0,9			75%			75%	90%	0,01		0,56			2,25		0,0056			0,0225
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	50%		9	9	9	9	9		4,5	9	4,5			0,45	0,9	0,45				75%	100%	50%		90%	0,01		1,13		2,25			0,0113		0,0225	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%			9	9	9	9	9	2,25	4,5	6,75			0,23	0,45	0,68				25%	75%	100%			90%	0,01	1,69	1,13				0,0169	0,0113			
		Acceso No Autorizado	0,1		75%	100%			9	9	9	9	9		6,75	9				0,68	0,9					75%	100%			90%	0,01		1,69					0,0169			
		Repudio	0,1		25%			100%	9	9	9	9	9		2,25			9		0,23			0,9			75%			75%	90%	0,01		0,56			2,25		0,0056			0,0225
		Modificación Deliberada De La Información	0,1		100%				9	9	9	9	9		9					0,9						75%				90%	0,01		2,25					0,0225			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9						75%					90%	0,01	2,25					0,0225				
		Divulgación De Información	0,1			100%			9	9	9	9	9			9					0,9						75%			90%	0,01			2,25					0,0225		
D12	**Registros de actividades en servidores**	Errores De Administración	0,3	75%	50%	50%			8	8	8	9	9	6	4	4			1,8	1,2	1,2			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Convertirlo en sistema activo • Depuración	75%	75%	80%			90%	0,03	1,5	1	0,8			0,045	0,03	0,024		
		Errores De Configuración	0,3		75%				8	8	8	9	9		6					1,8						75%				90%	0,03		1,5					0,045			
		Destrucción De Información	0,3	75%					8	8	8	9	9	6					1,8						75%					90%	0,03	1,5					0,045				
		Manipulación De La Configuración	0,1		75%	50%	75%		8	8	8	9	9		6	4	6,75			0,6	0,4	0,68				75%	80%	90%		90%	0,01		1,5	0,8	0,68			0,015	0,008	0,0068	
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	50%		8	8	8	9	9		6	8	4,5			0,6	0,8	0,45				75%	80%	90%		90%	0,01		1,5	1,6	0,45			0,015	0,016	0,0045	
		Abuso De Privilegios De Acceso	0,1	75%	50%	50%			8	8	8	9	9	6	4	4			0,6	0,4	0,4				75%	50%	80%			90%	0,01	1,5	2	0,8			0,015	0,02	0,008		
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	9		6	8				0,6	0,8					75%	80%			90%	0,01		1,5	1,6				0,015	0,016		
		Repudio	0,3		50%			100%	8	8	8	9	9		4			9		1,2			2,7			75%			75%	90%	0,03		1			2,25		0,03			0,0675
		Modificación Deliberada De La Información	0,1		100%				8	8	8	9	9		8					0,8						75%				90%	0,01		2					0,02			
		Destrucción De Información	0,1	100%					8	8	8	9	9	8					0,8						75%					90%	0,01	2					0,02				
D13	**Ficheros compartidos Google Drive**	Errores De Administración	0,3	75%	50%	50%			7	8	8	7	7	5,25	4	4			1,58	1,2	1,2			• Seguridad de equipos/dispositivos que los alojan • Seguridad de las aplicaciones que manejan los datos • Depuración • Actualización permanente control de accesos • Cifrado de información confidencial	75%	90%	90%			75%	0,075	1,31	0,4	0,4			0,0984	0,03	0,03		
		Errores De Configuración	0,1		25%				7	8	8	7	7		2					0,2						90%				75%	0,025		0,2					0,005			
		Alteración Accidental De La Información	0,3		75%				7	8	8	7	7		6					1,8						90%				75%	0,075		0,6					0,045			
		Destrucción De Información	0,3	75%					7	8	8	7	7	5,25					1,58						75%					75%	0,075	1,31					0,0984				
		Manipulación De La Configuración	0,1		50%	50%	50%		7	8	8	7	7		4	4	3,5			0,4	0,4	0,35				90%	90%	50%		75%	0,025		0,4	0,4	1,75			0,01	0,01	0,0438	
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	50%		7	8	8	7	7		6	8	3,5			0,6	0,8	0,35				90%	90%	50%		75%	0,025		0,6	0,8	1,75			0,015	0,02	0,0438	
		Abuso De Privilegios De Acceso	0,1	50%	50%	50%			7	8	8	7	7	3,5	4	4			0,35	0,4	0,4				75%	90%	90%			75%	0,025	0,88	0,4	0,4			0,0219	0,01	0,01		
		Acceso No Autorizado	0,1		75%	100%			7	8	8	7	7		6	8				0,6	0,8					90%	90%			75%	0,025		0,6	0,8				0,015	0,02		
		Repudio	0,1		25%			100%	7	8	8	7	7		2			7		0,2			0,7			90%			100%	75%	0,025		0,2					0,005			
		Modificación Deliberada De La Información	0,1		100%				7	8	8	7	7		8					0,8						90%				75%	0,025		0,8					0,02			
		Destrucción De Información	0,1	100%					7	8	8	7	7	7					0,7						75%					75%	0,025	1,75					0,0438				
		Divulgación De Información	0,1			100%			7	8	8	7	7			8					0,8						90%			75%	0,025			0,8					0,02		

SERVICIOS [S]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D'	I'	C'	A'	T'			D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
S1	Página web	Errores De Usuarios	0,5	5%	5%	25%			7	8	8	5	7	0,35	0,4	2			0,18	0,2	1			• Seguridad en la aplicación • Gestión de cambios y mejoras • Registros de incidencias • Pedir informes de actividades • Logs de incidencias	75%	50%	80%			50%	0,25	0,09	0,2	0,4			0,0219	0,05	0,1		
		Errores De Administración	0,1	100%	75%	75%			7	8	8	5	7	7	6	6			0,7	0,6	0,6				75%	75%	80%			90%	0,01	1,75	1,5	1,2			0,0175	0,015	0,012		
		Alteración Accidental De La Información	0,1		75%				7	8	8	5	7		6					0,6					75%					50%	0,05		1,5					0,075			
		Fugas De Información	0,1			50%			7	8	8	5	7			4					0,4					80%				50%	0,05			0,8					0,04			
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%					7	8	8	5	7	7					2,1						75%					75%	0,075	1,75					0,1313				
		Suplantación De La Identidad Del Usuario	0,7		75%	75%	100%		7	8	8	5	7		6	6	5			4,2	4,2	3,5				75%	80%	80%		90%	0,07		1,5	1,2	1			0,105	0,084	0,07	
		Abuso De Privilegios De Acceso	0,3	50%	75%	75%			7	8	8	5	7	3,5	6	6			1,05	1,8	1,8				75%	75%	80%			90%	0,03	0,88	1,5	1,2			0,0263	0,045	0,036		
		Uso No Previsto	0,3	50%	75%	75%			7	8	8	5	7	3,5	6	6			1,05	1,8	1,8				75%	75%	80%			90%	0,03	0,88	1,5	1,2			0,0263	0,045	0,036		
		Acceso No Autorizado	0,5		100%	75%			7	8	8	5	7		8	6				4	3					75%	80%			90%	0,05		2	1,2				0,1	0,06		
		Repudio	0,1		50%			75%	7	8	8	5	7		4			5,25		0,4			0,53			75%			90%	0,01		1		0,53			0,01			0,0053
		Modificación Deliberada De La Información	0,1		100%				7	8	8	5	7		8					0,8						75%				90%	0,01		2					0,02			
		Destrucción De Información	0,1	75%					7	8	8	5	7	5,25					0,53						75%					90%	0,01	1,31					0,0131				
		Divulgación De Información	0,3			100%			7	8	8	5	7			8					2,4					80%				90%	0,03			1,6				0,048			
		Denegación De Servicio	0,3	100%					7	8	8	5	7	7					2,1						50%					90%	0,03	3,5					0,105				
S2	Correo electrónico	Errores De Usuarios	0,7	50%	25%	50%			7	8	8	7	8	3,5	2	4			2,45	1,4	2,8			• Seguridad de la aplicación de correo electrónico • Resgistro de incidencias • Analisis de informes de ataques • Manual de Administración • Manual de Buenas prácticas para Usuario • Logs de incidencias	50%	25%	50%			75%	0,175	1,75	1,5	2			0,3063	0,2625	0,35		
		Errores De Administración	0,1	75%	25%	75%			7	8	8	7	8	5,25	2	6			0,53	0,2	0,6				50%	25%	50%			90%	0,01	2,63	1,5	3			0,0263	0,015	0,03		
		Alteración Accidental De La Información	0,3		50%				7	8	8	7	8		4					1,2						50%				90%	0,03		2					0,06			
		Fugas De Información	0,1			75%			7	8	8	7	8			6					0,6					50%				75%	0,025			3					0,075			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					7	8	8	7	8	7					0,7						50%					90%	0,01	3,5					0,035				
		Suplantación De La Identidad Del Usuario	0,5		50%	75%	75%		7	8	8	7	8		4	6	5,25			2	3	2,63				50%	50%	75%		90%	0,05		2	3	1,31			0,1	0,15	0,0656	
		Abuso De Privilegios De Acceso	0,3	50%	75%	75%			7	8	8	7	8	3,5	6	6			1,05	1,8	1,8				50%	75%	50%			80%	0,06	1,75	1,5	3			0,105	0,09	0,18		
		Uso No Previsto	0,3	75%	75%	75%			7	8	8	7	8	5,25	6	6			1,58	1,8	1,8				50%	75%	50%			80%	0,06	2,63	1,5	3			0,1575	0,09	0,18		
		Acceso No Autorizado	0,5		75%	100%			7	8	8	7	8		6	8				3	4					75%	75%			90%	0,05		1,5	2				0,075	0,1		
		Repudio	0,1		50%			75%	7	8	8	7	8		4			6		0,4			0,6			50%			75%	80%	0,02		2		1,5			0,04			0,03
		Modificación Deliberada De La Información	0,1		75%				7	8	8	7	8		6					0,6						75%				90%	0,01		1,5					0,015			
		Divulgación De Información	0,3			75%			7	8	8	7	8			6					1,8					50%				80%	0,06			3				0,18			
		Denegación De Servicio	0,1	100%					7	8	8	7	8	7					0,7						50%					90%	0,01	3,5					0,035				
S3	Intranet documental - Servicio FTP	Errores De Usuarios	0,7	5%	50%	50%			8	8	8	8	8	0,4	4	4			0,28	2,8	2,8			• Seguridad de la aplicación de Intranet • Resgistro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	25%	25%	75%			75%	0,175	0,3	3	1			0,0525	0,525	0,175		
		Errores De Administración	0,3	75%	75%	50%			8	8	8	8	8	6	6	4			1,8	1,8	1,2				25%	25%	75%			90%	0,03	4,5	4,5	1			0,135	0,135	0,03		
		Alteración Accidental De La Información	0,5		75%				8	8	8	8	8		6					3						50%				80%	0,1		3					0,3			
		Destrucción De Información	0,5	75%					8	8	8	8	8	6					3						50%					80%	0,1	3					0,3				
		Fugas De Información	0,1			75%			8	8	8	8	8			6					0,6					75%				80%	0,02			1,5					0,03			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	8	8	8	8					0,8						50%					80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%		8	8	8	8	8		4	6	4			1,2	1,8	1,2				50%	75%	75%		90%	0,03		2	1,5	1			0,06	0,045	0,03	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%			8	8	8	8	8	2	4	6			0,2	0,4	0,6				50%	50%	75%			80%	0,02	1	2	1,5			0,02	0,04	0,03		
		Uso No Previsto	0,3	50%	50%	75%			8	8	8	8	8	4	4	6			1,2	1,2	1,8				50%	50%	75%			80%	0,06	2	2	1,5			0,12	0,12	0,09		
		Acceso No Autorizado	0,5		50%	100%			8	8	8	8	8		4	8				2	4					50%	75%			90%	0,05		2	2				0,1	0,1		
		Repudio	0,3		25%			75%	8	8	8	8	8		2			6		0,6			1,8			25%			75%	90%	0,03		1,5		1,5			0,045			0,045
		Modificación Deliberada De La Información	0,1		75%				8	8	8	8	8		6					0,6						50%				80%	0,02		3					0,06			
		Destrucción De Información	0,1	100%					8	8	8	8	8	8					0,8						50%					80%	0,02	4					0,08				
		Divulgación De Información	0,1			75%			8	8	8	8	8			6					0,6						75%			80%	0,02			1,5					0,03			
		Denegación De Servicio	0,3	100%					8	8	8	8	8	8					2,4						50%					80%	0,06	4					0,24				
S4	Sistema de tickets de incidencias	Errores De Usuarios	0,7	5%	25%	25%			4	6	6	8	5	0,2	1,5	1,5			0,14	1,05	1,05			• Seguridad de la aplicación de sistema de tockets de incidencias • Resgistro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	0,25	25%	75%			75%	0,175	0,15	1,13	0,38			0,0263	0,1969	0,0656		
		Errores De Administración	0,3	75%	50%	25%			4	6	6	8	5	3	3	1,5			0,9	0,9	0,45				25%	25%	75%			90%	0,03	2,25	2,25	0,38			0,0675	0,0675	0,0113		
		Alteración Accidental De La Información	0,3		50%				4	6	6	8	5		3					0,9						50%				80%	0,06		1,5					0,09			
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					4	6	6	8	5	4					0,4						50%					80%	0,02	2					0,04				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%		4	6	6	8	5		3	4,5	4			0,9	1,35	1,2				50%	75%	75%		90%	0,03		2	1,13	1			0,045	0,0338	0,03	
		Acceso No Autorizado	0,5		75%	75%			4	6	6	8	5		4,5	4,5				2,25	2,25					50%	75%			80%	0,1		2,25	1,13				0,225	0,1125		
		Repudio	0,1		50%			75%	4	6	6	8	5		3			3,75		0,3			0,38			25%			75%	90%	0,01		2,25		0,94			0,0225			0,0094
		Modificación Deliberada De La Información	0,1		50%				4	6	6	8	5		3					0,3						50%				80%	0,02		1,5					0,03			
		Divulgación De Información	0,1			50%			4	6	6	8	5			3					0,3						75%			80%	0,02			0,75					0,015		
		Denegación De Servicio	0,3	100%					4	6	6	8	5	4					1,2						50%					80%	0,06	2					0,12				
S5	Educación Virtual	Errores De Usuarios	0,7	5%	25%	50%			8	8	7	6	7	0,4	2	3,5			0,28	1,4	2,45			• Seguridad de la aplicación E-apsa • Registro de incidencias • Manual de Administración • Manual de Usuarios • Gestión de mejoras • Logs de incidencias	25%	25%	75%			75%	0,175	0,3	1,5	0,88			0,0525	0,2625	0,1531		
		Errores De Administración	0,3	75%	50%	50%			8	8	7	6	7	6	4	3,5			1,8	1,2	1,05				25%	25%	75%			90%	0,03	4,5	3	0,88			0,135	0,09	0,0263		
		Alteración Accidental De La Información	0,5		75%				8	8	7	6	7		6					3						50%				75%	0,125		3					0,375			
		Destrucción De Información	0,5	100%					8	8	7	6	7	8					4						50%					75%	0,125	4					0,5				
		Fugas De Información	0,5			50%			8	8	7	6	7			3,5					1,75					75%				50%	0,25			0,88					0,2188		
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	7	6	7	8					0,8						50%					80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	0,5		25%	75%	50%		8	8	7	6	7		2	5,25	3			1	2,63	1,5				50%	75%	75%		50%	0,25		1	1,31	0,75			0,25	0,3281	0,1875	
		Abuso De Privilegios De Acceso	0,3	25%	75%	50%			8	8	7	6	7	2	6	3,5			0,6	1,8	1,05				50%	50%	75%			75%	0,075	1	3	0,88			0,075	0,225	0,0656		
		Uso No Previsto	0,5	50%	25%	50%			8	8	7	6	7	4	2	3,5			2	1	1,75				50%	50%	75%			80%	0,1	2	1	0,88			0,2	0,1	0,0875		
		Acceso No Autorizado	0,5		75%	75%			8	8	7	6	7		6	5,25				3	2,63					50%	75%			75%	0,125		3	1,31				0,375	0,1641		
		Repudio	0,1		25%			75%	8	8	7	6	7		2			5,25		0,2			0,53			50%			75%	90%	0,01		1		1,31			0,01			0,0131
		Modificación Deliberada De La Información	0,1		75%				8	8	7	6	7		6					0,6						50%				75%	0,025		3					0,075			
		Divulgación De Información	0,3			50%			8	8	7	6	7			3,5					1,05						75%			75%	0,075			0,88					0,0656		
		Denegación De Servicio	0,3	100%					8	8	7	6	7	8					2,4						50%					80%	0,06	4					0,24				
S6	Servicio de financiero	Errores De Usuarios	0,5	25%	75%	100%			8	9	9	9	9	2	6,75	9			1	3,38	4,5			• Seguridad de la aplicación financiero • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	25%	25%	75%			75%	0,125	1,5	5,06	2,25			0,1875	0,6328	0,2813		
		Errores De Administración	0,3	75%	50%	75%			8	9	9	9	9	6	4,5	6,75			1,8	1,35	2,03				25%	25%	75%			90%	0,03	4,5	3,38	1,69			0,135	0,1013	0,0506		
		Alteración Accidental De La Información	0,5		100%				8	9	9	9	9		9					4,5						50%				80%	0,1		4,5					0,45			
		Destrucción De Información	0,3	75%					8	9	9	9	9	6					1,8						50%					80%	0,06	3					0,18				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%					8	9	9	9	9	8					2,4						50%					80%	0,06	4					0,24				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	75%		8	9	9	9	9		6,75	9	6,75			2,03	2,7	2,03				50%	75%	75%		90%	0,03		3,38	2,25	1,69			0,1013	0,0675	0,0506	
		Abuso De Privilegios De Acceso	0,3	25%	75%	75%			8	9	9	9	9	2	6,75	6,75			0,6	2,03	2,03				50%	50%	75%			80%	0,06	1	3,38	1,69			0,06	0,2025	0,1013		
		Uso No Previsto	0,3	50%	50%	50%			8	9	9	9	9	4	4,5	4,5			1,2	1,35	1,35				50%	50%	75%			80%	0,06	2	2,25	1,13			0,12	0,135	0,0675		
		Acceso No Autorizado	0,3		100%	100%			8	9	9	9	9		9	9				2,7	2,7					50%	75%			80%	0,06		4,5	2,25				0,27	0,135		
		Repudio	0,1		50%			100%	8	9	9	9	9		4,5			9		0,45			0,9			50%			75%	90%	0,01		2,25		2,25			0,0225			0,0225
		Modificación Deliberada De La Información	0,1		100%				8	9	9	9	9		9					0,9						50%				80%	0,02		4,5					0,09			
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8						50%					80%	0,02	4					0,08				
		Divulgación De Información	0,1			100%			8	9	9	9	9			9					0,9						75%			80%	0,02			2,25					0,045		
		Denegación De Servicio	0,3	100%					8	9	9	9	9	8					2,4						50%					80%	0,06	4					0,24				
		Errores De Usuarios	0,5	25%	75%	50%			8	8	8	7	8	2	6	4			1	3	2				25%	25%	75%			75%	0,125	1,5	4,5	1			0,1875	0,5625	0,125		

S7	**Gestión de usuarios Socios**	Errores De Administración	0,3	75%	50%	75%			8	8	8	7	8	6	4	6			1,8	1,2	1,8			• Seguridad de la aplicación GUS • Gestión de Usuarios Socios • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	25%	25%	75%			90%	0,03	4,5	3	1,5			0,135	0,09	0,045		
		Alteración Accidental De La Información	0,3		75%				8	8	8	7	8		6					1,8						50%				80%	0,06		3					0,18			
		Destrucción De Información	0,1	75%					8	8	8	7	8	6					0,6						50%					80%	0,02	3					0,06				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	8	7	8	8					0,8						50%					80%	0,02	4					0,08				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	50%		8	8	8	7	8		6	8	3,5			1,8	2,4	1,05				50%	75%	75%		90%	0,03		3	2	0,88			0,09	0,06	0,0263	
		Abuso De Privilegios De Acceso	0,1	25%	50%	50%			8	8	8	7	8	2	4	4			0,2	0,4	0,4				50%	50%	75%			80%	0,02	1	2	1			0,02	0,04	0,02		
		Uso No Previsto	0,3	50%	25%	75%			8	8	8	7	8	4	2	6			1,2	0,6	1,8				50%	50%	75%			80%	0,06	2	1	1,5			0,12	0,06	0,09		
		Acceso No Autorizado	0,5		75%	100%			8	8	8	7	8		6	8				3	4					50%	75%			90%	0,05		3	2				0,15	0,1		
		Repudio	0,1		25%			100%	8	8	8	7	8		2			8		0,2			0,8			50%			75%	90%	0,01		1			2		0,01			0,02
		Modificación Deliberada De La Información	0,1		100%				8	8	8	7	8		8					0,8						50%				80%	0,02		4					0,08			
		Destrucción De Información	0,1	100%					8	8	8	7	8	8					0,8						50%					80%	0,02	4					0,08				
		Divulgación De Información	0,3			100%			8	8	8	7	8			8					2,4						75%			80%	0,06			2					0,12		
		Denegación De Servicio	0,3	100%					8	8	8	7	8	8					2,4						50%					80%	0,06	4					0,24				
S8	**Gestión empresarial**	Errores De Usuarios	0,5	25%	50%	50%			7	8	8	7	8	1,75	4	4			0,88	2	2			• Seguridad de la aplicación G2K • Gestión empresarial • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	25%	50%	50%			75%	0,125	1,31	2	2			0,1641	0,25	0,25		
		Errores De Administración	0,3	50%	50%	50%			7	8	8	7	8	3,5	4	4			1,05	1,2	1,2				25%	50%	50%			90%	0,03	2,63	2	2			0,0788	0,06	0,06		
		Alteración Accidental De La Información	0,3		75%				7	8	8	7	8		6					1,8						50%				80%	0,06		3					0,18			
		Destrucción De Información	0,1	75%					7	8	8	7	8	5,25					0,53						50%					80%	0,02	2,63					0,0525				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	75%					7	8	8	7	8	5,25					0,53						50%					80%	0,02	2,63					0,0525				
		Suplantación De La Identidad Del Usuario	0,3		50%	75%	50%		7	8	8	7	8		4	6	3,5			1,2	1,8	1,05				50%	50%	50%		90%	0,03		2	3	1,75			0,06	0,09	0,0525	
		Abuso De Privilegios De Acceso	0,1	25%	50%	50%			7	8	8	7	8	1,75	4	4			0,18	0,4	0,4				50%	50%	50%			80%	0,02	0,88	2	2			0,0175	0,04	0,04		
		Uso No Previsto	0,3	25%	50%	75%			7	8	8	7	8	1,75	4	6			0,53	1,2	1,8				50%	50%	50%			80%	0,06	0,88	2	3			0,0525	0,12	0,18		
		Acceso No Autorizado	0,5		75%	100%			7	8	8	7	8		6	8				3	4					50%	50%			90%	0,05		3	4				0,15	0,2		
		Repudio	0,1		50%			100%	7	8	8	7	8		4			8		0,4			0,8			50%			75%	90%	0,01		2			2		0,02			0,02
		Modificación Deliberada De La Información	0,1		75%				7	8	8	7	8		6					0,6						50%				80%	0,02		3					0,06			
		Destrucción De Información	0,1	100%					7	8	8	7	8	7					0,7						50%					80%	0,02	3,5					0,07				
		Divulgación De Información	0,3			100%			7	8	8	7	8			8					2,4						50%			80%	0,06			4					0,24		
		Denegación De Servicio	0,3	100%					7	8	8	7	8	7					2,1						50%					80%	0,06	3,5					0,21				
S9	**Gestión de recursos humanos, nóminas**	Errores De Usuarios	0,5	25%	50%	75%			7	8	8	8	9	1,75	4	6			0,88	2	3			• Seguridad de la aplicación Sage • Gestión de Recursos Humanos • Registro de incidencias • Manual de Administración • Manual de Usuario • Gestión de mejoras • Logs de incidencias	25%	25%	75%			75%	0,125	1,31	3	1,5			0,1641	0,375	0,1875		
		Errores De Administración	0,3	50%	50%	75%			7	8	8	8	9	3,5	4	6			1,05	1,2	1,8				25%	25%	75%			90%	0,03	2,63	3	1,5			0,0788	0,09	0,045		
		Alteración Accidental De La Información	0,3		75%				7	8	8	8	9		6					1,8						50%				80%	0,06		3					0,18			
		Destrucción De Información	0,1	75%					7	8	8	8	9	5,25					0,53						50%					80%	0,02	2,63					0,0525				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					7	8	8	8	9	7					0,7						50%					80%	0,02	3,5					0,07				
		Suplantación De La Identidad Del Usuario	0,3		75%	100%	50%		7	8	8	8	9		6	8	4			1,8	2,4	1,2				50%	75%	75%		90%	0,03		3	2	1			0,09	0,06	0,03	
		Abuso De Privilegios De Acceso	0,1	25%	50%	75%			7	8	8	8	9	1,75	4	6			0,18	0,4	0,6				50%	50%	75%			80%	0,02	0,88	2	1,5			0,0175	0,04	0,03		
		Uso No Previsto	0,3	25%	50%	75%			7	8	8	8	9	1,75	4	6			0,53	1,2	1,8				50%	50%	75%			80%	0,06	0,88	2	1,5			0,0525	0,12	0,09		
		Acceso No Autorizado	0,5		75%	100%			7	8	8	8	9		6	8				3	4					50%	75%			80%	0,1		3	2				0,3	0,2		
		Repudio	0,1		50%			100%	7	8	8	8	9		4			9		0,4			0,9			50%			75%	90%	0,01		2			2,25		0,02			0,0225
		Modificación Deliberada De La Información	0,1		100%				7	8	8	8	9		8					0,8						50%				80%	0,02		4					0,08			
		Destrucción De Información	0,1	100%					7	8	8	8	9	7					0,7						50%					80%	0,02	3,5					0,07				
		Divulgación De Información	0,3			100%			7	8	8	8	9			8					2,4						75%			80%	0,06			2					0,12		
		Denegación De Servicio	0,3	100%					7	8	8	8	9	7					2,1						50%					80%	0,06	3,5					0,21				

SOFTWARE - APLICACIONES INFORMÁTICAS [SW]			Frecuencia	Degradación					Valor del Activo						Impacto						Riesgo						Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D'	I'	C'	A'	T'		F´	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
SW1	Aplicación de Financiero	Fallo De Origen Lógico	0,1	75%					9	9	9	9	9	6,75					0,68											50%						80%	0,02	3,38					0,0675				
		Errores De Usuarios	0,5	25%	75%	50%			9	9	9	9	9	2,25	6,75	4,5			1,13	3,38	2,25									25%	50%	50%				50%	0,25	1,69	3,38	2,25			0,4219	0,8438	0,5625		
		Errores De Administración	0,1	75%	50%	50%			9	9	9	9	9	6,75	4,5	4,5			0,68	0,45	0,45									50%	25%	50%				90%	0,01	3,38	3,38	2,25			0,0338	0,0338	0,0225		
		Alteración Accidental De La Información	0,3		75%				9	9	9	9	9		6,75					2,03										50%					75%	0,075		3,38				0,2531				
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9										75%					25%	0,075	2,25					0,1688				
		Fugas De Información	0,1			100%			9	9	9	9	9			9					0,9									50%				25%	0,075			4,5				0,3375			
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			1,35	2,03	2,7									25%	50%	50%				90%	0,03	3,38	3,38	4,5			0,1013	0,1013	0,135		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				9	9	9	9	9	4,5	6,75				1,35	2,03										50%	50%					75%	0,075	2,25	3,38				0,1688	0,2531				
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		9	9	9	9	9		6,75	9	6,75			0,68	0,9	0,68									50%	75%	75%			25%	0,075		3,38	2,25	1,69			0,2531	0,1688	0,1266		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			1,35	2,03	2,7									50%	50%	75%				75%	0,075	2,25	3,38	2,25			0,1688	0,2531	0,1688		
		Uso No Previsto	0,3	75%	50%	50%			9	9	9	9	9	6,75	4,5	4,5			2,03	1,35	1,35									50%	25%	75%				50%	0,15	3,38	3,38	1,13			0,5063	0,5063	0,1688		
		Difusión De Software Dañino	0,1	100%	100%	100%			9	9	9	9	9	9	9	9			0,9	0,9	0,9									50%	50%	75%				90%	0,01	4,5	4,5	2,25			0,045	0,045	0,0225		
		Acceso No Autorizado	0,1		75%	100%			9	9	9	9	9		6,75	9				0,68	0,9										50%	75%				90%	0,01		3,38	2,25				0,0338	0,0225		
		Modificación Deliberada De La Información	0,1		100%				9	9	9	9	9		9					0,9										50%					50%	0,05		4,5				0,225				
		Destrucción De Información	0,1	50%					9	9	9	9	9	4,5					0,45											50%					50%	0,05	2,25					0,1125				
		Divulgación De Información	0,1			100%			9	9	9	9	9			9					0,9											75%			25%	0,075			2,25				0,1688				
SW2	GUS Gestión de Usuarios Socios	Fallo De Origen Lógico	0,1	75%					8	8	8	9	9	6					0,6											50%						80%	0,02	3					0,06				
		Errores De Usuarios	0,5	50%	75%	50%			8	8	8	9	9	4	6	4			2	3	2									25%	50%	50%				50%	0,25	3	3	2			0,75	0,75	0,5		
		Errores De Administración	0,1	75%	50%	50%			8	8	8	9	9	6	4	4			0,6	0,4	0,4									50%	25%	50%				90%	0,01	3	3	2			0,03	0,03	0,02		
		Alteración Accidental De La Información	0,3		75%				8	8	8	9	9		6					1,8										50%					75%	0,075		3				0,225				
		Destrucción De Información	0,1	100%					8	8	8	9	9	8					0,8										75%					25%	0,075	2					0,15				
		Fugas De Información	0,1			100%			8	8	8	9	9			8					0,8									50%				25%	0,075			4				0,3			
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			8	8	8	9	9	4	6	8			1,2	1,8	2,4									25%	50%	50%				90%	0,03	3	3	4			0,09	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				8	8	8	9	9	4	6				1,2	1,8										50%	50%					75%	0,075	2	3				0,15	0,225				
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		8	8	8	9	9		6	8	6,75			0,6	0,8	0,68									50%	75%	75%			25%	0,075		3	2	1,69			0,225	0,15	0,1266		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			8	8	8	9	9	4	6	8			1,2	1,8	2,4									50%	50%	75%				75%	0,075	2	3	2			0,15	0,225	0,15		
		Uso No Previsto	0,3	50%	50%	50%			8	8	8	9	9	4	4	4			1,2	1,2	1,2									50%	25%	75%				50%	0,15	2	3	1			0,3	0,45	0,15		
		Difusión De Software Dañino	0,1	100%	100%	100%			8	8	8	9	9	8	8	8			0,8	0,8	0,8									50%	50%	75%				90%	0,01	4	4	2			0,04	0,04	0,02		
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	9		6	8				0,6	0,8										50%	75%				90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	0,1		100%				8	8	8	9	9		8					0,8										50%					50%	0,05		4				0,2				
		Destrucción De Información	0,1	50%					8	8	8	9	9	4					0,4											50%					50%	0,05	2					0,1				
		Divulgación De Información	0,1			100%			8	8	8	9	9			8					0,8											75%			25%	0,075			2				0,15				
SW3	G2K Gestión Empresarial	Fallo De Origen Lógico	0,1	75%					7	8	8	9	9	5,25					0,53											50%						80%	0,02	2,63					0,0525				
		Errores De Usuarios	0,5	50%	75%	50%			7	8	8	9	9	3,5	6	4			1,75	3	2									25%	50%	50%				50%	0,25	2,63	3	2			0,6563	0,75	0,5		
		Errores De Administración	0,1	75%	50%	50%			7	8	8	9	9	5,25	4	4			0,53	0,4	0,4									50%	25%	50%				90%	0,01	2,63	3	2			0,0263	0,03	0,02		
		Alteración Accidental De La Información	0,3		75%				7	8	8	9	9		6					1,8										50%					75%	0,075		3				0,225				
		Destrucción De Información	0,1	100%					7	8	8	9	9	7					0,7										75%					25%	0,075	1,75					0,1313				
		Fugas De Información	0,1			100%			7	8	8	9	9			8					0,8									50%				25%	0,075			4				0,3			
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			7	8	8	9	9	3,5	6	8			1,05	1,8	2,4									25%	50%	50%				90%	0,03	2,63	3	4			0,0788	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				7	8	8	9	9	3,5	6				1,05	1,8										50%	50%					75%	0,075	1,75	3				0,1313	0,225				
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		7	8	8	9	9		6	8	6,75			0,6	0,8	0,68									50%	75%	75%			25%	0,075		3	2	1,69			0,225	0,15	0,1266		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			7	8	8	9	9	3,5	6	8			1,05	1,8	2,4									50%	50%	75%				75%	0,075	1,75	3	2			0,1313	0,225	0,15		
		Uso No Previsto	0,3	50%	50%	50%			7	8	8	9	9	3,5	4	4			1,05	1,2	1,2									50%	25%	75%				50%	0,15	1,75	3	1			0,2625	0,45	0,15		
		Difusión De Software Dañino	0,1	100%	100%	100%			7	8	8	9	9	7	8	8			0,7	0,8	0,8									50%	50%	75%				90%	0,01	3,5	4	2			0,035	0,04	0,02		
		Acceso No Autorizado	0,1		75%	100%			7	8	8	9	9		6	8				0,6	0,8										50%	75%				90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	0,1		100%				7	8	8	9	9		8					0,8										50%					50%	0,05		4				0,2				
		Destrucción De Información	0,1	50%					7	8	8	9	9	3,5					0,35											50%					50%	0,05	1,75					0,0875				
		Divulgación De Información	0,1			100%			7	8	8	9	9			8					0,8											75%			25%	0,075			2				0,15				
SW4	Sage Gestión de Recursos Humanos (nóminas)	Fallo De Origen Lógico	0,1	75%					7	8	8	9	9	5,25					0,53											50%						80%	0,02	2,63					0,0525				
		Errores De Usuarios	0,5	50%	75%	50%			7	8	8	9	9	3,5	6	4			1,75	3	2									25%	50%	50%				50%	0,25	2,63	3	2			0,6563	0,75	0,5		
		Errores De Administración	0,1	75%	50%	50%			7	8	8	9	9	5,25	4	4			0,53	0,4	0,4									50%	25%	50%				90%	0,01	2,63	3	2			0,0263	0,03	0,02		
		Alteración Accidental De La Información	0,3		75%				7	8	8	9	9		6					1,8										50%					75%	0,075		3				0,225				
		Destrucción De Información	0,1	100%					7	8	8	9	9	7					0,7										75%					25%	0,075	1,75					0,1313				
		Fugas De Información	0,1			100%			7	8	8	9	9			8					0,8									50%				25%	0,075			4				0,3			
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			7	8	8	9	9	3,5	6	8			1,05	1,8	2,4									25%	50%	50%				90%	0,03	2,63	3	4			0,0788	0,09	0,12		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				7	8	8	9	9	3,5	6				1,05	1,8										50%	50%					75%	0,075	1,75	3				0,1313	0,225				
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		7	8	8	9	9		6	8	6,75			0,6	0,8	0,68									50%	75%	75%			25%	0,075		3	2	1,69			0,225	0,15	0,1266		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			7	8	8	9	9	3,5	6	8			1,05	1,8	2,4									50%	50%	75%				75%	0,075	1,75	3	2			0,1313	0,225	0,15		
		Uso No Previsto	0,3	50%	50%	50%			7	8	8	9	9	3,5	4	4			1,05	1,2	1,2									50%	25%	75%				50%	0,15	1,75	3	1			0,2625	0,45	0,15		
		Difusión De Software Dañino	0,1	100%	100%	100%			7	8	8	9	9	7	8	8			0,7	0,8	0,8									50%	50%	75%				90%	0,01	3,5	4	2			0,035	0,04	0,02		
		Acceso No Autorizado	0,1		75%	100%			7	8	8	9	9		6	8				0,6	0,8										50%	75%				90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	0,1		100%				7	8	8	9	9		8					0,8										50%					50%	0,05		4				0,2				
		Destrucción De Información	0,1	50%					7	8	8	9	9	3,5					0,35											50%					50%	0,05	1,75					0,0875				
		Divulgación De Información	0,1			100%			7	8	8	9	9			8					0,8											75%			25%	0,075			2				0,15				
SW5	Gestión de Bases de Datos	Fallo De Origen Lógico	0,1	75%					8	9	9	9	9	6					0,6											75%						80%	0,02	1,5					0,03				
		Errores De Administración	0,1	75%	75%	50%			8	9	9	9	9	6	6,75	4,5			0,6	0,68	0,45									50%	50%	50%				90%	0,01	3	3,38	2,25			0,03	0,0338	0,0225		
		Alteración Accidental De La Información	0,3		100%				8	9	9	9	9		9					2,7										50%					75%	0,075		4,5				0,3375				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8											50%					50%	0,05	4					0,2				
		Fugas De Información	0,1			100%			8	9	9	9	9			9					0,9									50%				50%	0,05			4,5				0,225			
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			8	9	9	9	9	4	6,75	9			1,2	2,03	2,7									50%	50%	50%				90%	0,03	2	3,38	4,5			0,06	0,1013	0,135		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	100%				8	9	9	9	9	4	9				1,2	2,7										50%	50%					75%	0,075	2	4,5				0,15	0,3375				
		Suplantación De La Identidad Del Usuario	0,1		100%	100%	100%		8	9	9	9	9		9	9	9			0,9	0,9	0,9									50%	50%	100%			75%	0,025		4,5	4,5				0,1125	0,1125			
		Abuso De Privilegios De Acceso	0,3	75%	100%	100%			8	9	9	9	9	6	9	9			1,8	2,7	2,7									50%	50%	50%				75%	0,075	3	4,5	4,5			0,225	0,3375	0,3375		
		Uso No Previsto	0,3	75%	75%	100%			8	9	9	9	9	6	6,75	9			1,8	2,03	2,7									50%	50%	50%				75%	0,075	3	3,38	4,5			0,225	0,2531	0,3375		
		Difusión De Software Dañino	0,1	100%	100%	100%			8	9	9	9	9	8	9	9			0,8	0,9	0,9									75%	50%	50%				90%	0,01	2	4,5	4,5			0,02	0,045	0,045		
		Acceso No Autorizado	0,1		100%	100%			8	9	9	9	9		9	9				0,9	0,9										50%	50%				90%	0,01		4,5	4,5				0,045	0,045		
		Modificación Deliberada De La Información	0,1		100%				8	9	9	9	9		9					0,9										50%					75%	0,025		4,5				0,1125				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8											75%					75%	0,025	2					0,05				
		Divulgación De Información	0,1			100%			8	9	9	9	9			9					0,9											50%				50%	0,05			4,5				0,225			
		Fallo De Origen Lógico	0,1	75%					7	8	8	9	8	5,25					0,53											75%						80%	0,02	1,31					0,0263				
		Errores De Usuarios	0,5	25%	25%	25%			7	8	8	9	8	1,75	2	2			0,88	1	1									25%	25%	25%				75%	0,125	1,31	1,5	1,5			0,1641	0,1875	0,1875		
		Errores De Administración	0,1	75%	50%	75%			7	8	8	9	8	5,25	4	6			0,53	0,4	0,6									50%	50%	50%				90%	0,01	2,63	2	3			0,0263	0,02	0,03		
		Alteración Accidental De La Información	0,3		75%				7	8	8	9	8		6					1,8										50%					75%	0,075		3				0,225				
		Destrucción De Información	0,1	75%					7	8	8	9	8	5,25					0,53											50%					75%	0,025	2,63					0,0656				
		Fugas De Información	0,1			50%			7	8	8	9	8			4					0,4											50%				75%	0,025			2				0,05			

Salvaguardas:
- Copias de seguridad
- Revisión de la configuración de seguridad
- Cifrado de información
- Análisis de vulnerabilidades
- Actualizaciones
- Configuración y revisión de logs
- Manual de Administración
- Manual de Usuarios
- Registro de configuración e Incidencias

		Vulnerabilidades De Los Programas	0,3	75%	75%	75%			7	8	8	9	8	5,25	6	6			1,58	1,8	1,8			seguridad	50%	50%	50%			90%	0,03	2,63	3	3			0,0788	0,09	0,09		
		Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				7	8	8	9	8	3,5	6				1,05	1,8				• Análisis de Vulnerabilidades	50%	50%				75%	0,075	1,75	3				0,1313	0,225			
SW6	Aplicación de Página web	Suplantación De La Identidad Del Usuario	0,1		50%	100%	100%		7	8	8	9	8		4	8	9			0,4	0,8	0,9		• Actualizaciones		50%	50%	100%		75%	0,025		2	4				0,05	0,1		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			7	8	8	9	8	3,5	6	8			1,05	1,8	2,4			• Configuración y revisión de logs	50%	50%	50%			75%	0,075	1,75	3	4			0,1313	0,225	0,3		
		Uso No Previsto	0,5	50%	50%	100%			7	8	8	9	8	3,5	4	8			1,75	2	4			• Manual de Administración	50%	50%	50%			50%	0,25	1,75	2	4			0,4375	0,5	1		
		Difusión De Software Dañino	0,1	50%	50%	100%			7	8	8	9	8	3,5	4	8			0,35	0,4	0,8			• Registro de configuración e	50%	50%	50%			75%	0,025	1,75	2	4			0,0438	0,05	0,1		
		Acceso No Autorizado	0,1		75%	100%			7	8	8	9	8		6	8				0,6	0,8			Incidencias		50%	50%			75%	0,025		3	4				0,075	0,1		
		Modificación Deliberada De La Información	0,1		75%				7	8	8	9	8		6					0,6						50%				75%	0,025		3					0,075			
		Destrucción De Información	0,1	50%					7	8	8	9	8	3,5					0,35						50%					75%	0,025	1,75					0,0438				
		Divulgación De Información	0,1			75%			7	8	8	9	8			6					0,6						50%			50%	0,05			3					0,15		
		Manipulación De Programas	0,1	50%	75%	75%			7	8	8	9	8	3,5	6	6			0,35	0,6	0,6				50%	75%	50%			75%	0,025	1,75	1,5	3			0,0438	0,0375	0,075		
		Fallo De Origen Lógico	0,1	75%					8	8	8	9	7	6					0,6						50%					80%	0,02	3					0,06				
		Errores De Usuarios	0,5	50%	75%	50%			8	8	8	9	7	4	6	4			2	3	2				25%	50%	50%			50%	0,25	3	3	2			0,75	0,75	0,5		
		Errores De Administración	0,1	75%	50%	50%			8	8	8	9	7	6	4	4			0,6	0,4	0,4				50%	25%	50%			90%	0,01	3	3	2			0,03	0,03	0,02		
		Alteración Accidental De La Información	0,3		75%				8	8	8	9	7		6					1,8				• Copias de seguridad		50%				75%	0,075		3					0,225			
		Destrucción De Información	0,1	100%					8	8	8	9	7	8					0,8					• Revisión de la configuración de	75%					25%	0,075	2					0,15				
		Fugas De Información	0,1			100%			8	8	8	9	7			8					0,8			seguridad			50%			25%	0,075			4					0,3		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			8	8	8	9	7	4	6	8			1,2	1,8	2,4			• Análisis de Vulnerabilidades	25%	50%	50%			90%	0,03	3	3	4			0,09	0,09	0,12		
SW7	Aplicación de Intranet	Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				8	8	8	9	7	4	6				1,2	1,8				• Actualizaciones	50%	50%				75%	0,075	2	3				0,15	0,225			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		8	8	8	9	7		6	8	6,75			0,6	0,8	0,68		• Configuración y revisión de logs		50%	75%	75%		25%	0,075		3	2	1,69			0,225	0,15	0,1266	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			8	8	8	9	7	4	6	8			1,2	1,8	2,4			• Manual de Administración	50%	50%	75%			75%	0,075	2	3	2			0,15	0,225	0,15		
		Uso No Previsto	0,3	50%	50%	50%			8	8	8	9	7	4	4	4			1,2	1,2	1,2			• Manual de Usuarios	50%	25%	75%			50%	0,15	2	3	1			0,3	0,45	0,15		
		Difusión De Software Dañino	0,1	100%	100%	100%			8	8	8	9	7	8	8	8			0,8	0,8	0,8			• Registro de configuración e	50%	50%	75%			90%	0,01	4	4	2			0,04	0,04	0,02		
		Acceso No Autorizado	0,1		75%	100%			8	8	8	9	7		6	8				0,6	0,8			Incidencias		50%	75%			90%	0,01		3	2				0,03	0,02		
		Modificación Deliberada De La Información	0,1		75%				8	8	8	9	7		6					0,6						50%				50%	0,05		3					0,15			
		Destrucción De Información	0,1	50%					8	8	8	9	7	4					0,4						50%					50%	0,05	2					0,1				
		Divulgación De Información	0,1			100%			8	8	8	9	7			8					0,8						75%			25%	0,075			2					0,15		
		Fallo De Origen Lógico	0,1	75%					4	6	6	9	5	3					0,3						50%					80%	0,02	1,5					0,03				
		Errores De Usuarios	0,5	50%	75%	50%			4	6	6	9	5	2	4,5	3			1	2,25	1,5				25%	50%	50%			50%	0,25	1,5	2,25	1,5			0,375	0,5625	0,375		
		Errores De Administración	0,1	75%	50%	50%			4	6	6	9	5	3	3	3			0,3	0,3	0,3				50%	25%	50%			90%	0,01	1,5	2,25	1,5			0,015	0,0225	0,015		
		Alteración Accidental De La Información	0,3		75%				4	6	6	9	5		4,5					1,35				• Copias de seguridad		50%				75%	0,075		2,25					0,1688			
		Destrucción De Información	0,1	100%					4	6	6	9	5	4					0,4					• Revisión de la configuración de	75%					25%	0,075	1					0,075				
		Fugas De Información	0,1			100%			4	6	6	9	5			6					0,6			seguridad			50%			25%	0,075			3					0,225		
		Vulnerabilidades De Los Programas	0,3	50%	75%	100%			4	6	6	9	5	2	4,5	6			0,6	1,35	1,8			• Análisis de Vulnerabilidades	25%	50%	50%			90%	0,03	1,5	2,25	3			0,045	0,0675	0,09		
SW8	Aplicación del Sistema de tickets de incidencias	Errores De Mantenimiento/Actualización De Programas	0,3	50%	75%				4	6	6	9	5	2	4,5				0,6	1,35				• Actualizaciones	50%	50%				75%	0,075	1	2,25				0,075	0,1688			
		Suplantación De La Identidad Del Usuario	0,1		75%	100%	75%		4	6	6	9	5		4,5	6	6,75			0,45	0,6	0,68		• Configuración y revisión de logs		50%	75%	75%		25%	0,075		2,25	1,5	1,69			0,1688	0,1125	0,1266	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			4	6	6	9	5	2	4,5	6			0,6	1,35	1,8			• Manual de Administración	50%	50%	75%			75%	0,075	1	2,25	1,5			0,075	0,1688	0,1125		
		Uso No Previsto	0,3	50%	50%	50%			4	6	6	9	5	2	3	3			0,6	0,9	0,9			• Manual de Usuarios	50%	25%	75%			50%	0,15	1	2,25	0,75			0,15	0,3375	0,1125		
		Difusión De Software Dañino	0,1	100%	100%	100%			4	6	6	9	5	4	6	6			0,4	0,6	0,6			• Registro de configuración e	50%	50%	75%			90%	0,01	2	3	1,5			0,02	0,03	0,015		
		Acceso No Autorizado	0,1		75%	100%			4	6	6	9	5		4,5	6				0,45	0,6			Incidencias		50%	75%			90%	0,01		2,25	1,5				0,0225	0,015		
		Modificación Deliberada De La Información	0,1		100%				4	6	6	9	5		6					0,6						50%				50%	0,05		3					0,15			
		Destrucción De Información	0,1	50%					4	6	6	9	5	2					0,2						50%					50%	0,05	1					0,05				
		Divulgación De Información	0,1			100%			4	6	6	9	5			6					0,6						75%			25%	0,075			1,5					0,1125		
		Errores De Usuarios	0,5	5%	5%	25%			7	8	8	9	8	0,35	0,4	2			0,18	0,2	1				5%	5%	25%			50%	0,25	0,33	0,38	1,5			0,0831	0,095	0,375		
		Errores De Administración	0,1	25%	5%	50%			7	8	8	9	8	1,75	0,4	4			0,18	0,04	0,4				25%	5%	50%			90%	0,01	1,31	0,38	2			0,0131	0,0038	0,02		
		Difusión De Software Dañino	0,1	5%	5%	100%			7	8	8	9	8	0,35	0,4	8			0,04	0,04	0,8				5%	5%	50%			80%	0,02	0,33	0,38	4			0,0067	0,0076	0,08		
		Alteración Accidental De La Información	0,3		5%				7	8	8	9	8		0,4					0,12						5%				75%	0,075		0,38					0,0285			
		Destrucción De Información	0,1	25%					7	8	8	9	8	1,75					0,18					• Cifrado de correo electrónicos	25%					75%	0,025	1,31					0,0328				
		Fugas De Información	0,3			100%			7	8	8	9	8			8					2,4			• Reglas de Filtro de correos			50%			50%	0,15			4					0,6		
		Vulnerabilidades De Los Programas	0,3	5%	50%	100%			7	8	8	9	8	0,35	4	8			0,11	1,2	2,4			maliciosos	5%	50%	50%			90%	0,03	0,33	2	4			0,01	0,06	0,12		
SW9	Aplicación de Correo electrónico Gmail	Errores De Mantenimiento/Actualización De Programas	0,1	25%	50%	75%			7	8	8	9	8	1,75	4	6			0,18	0,4	0,6			• Actualización	25%	50%	50%			90%	0,01	1,31	2	3			0,0131	0,02	0,03		
		Suplantación De La Identidad Del Usuario	0,1		50%	100%	100%		7	8	8	9	8		4	8	9			0,4	0,8	0,9		• Manual de Administración		50%	50%	75%		75%	0,025		2	4	2,25			0,05	0,1	0,0563	
		Abuso De Privilegios De Acceso	0,1	5%	75%	75%			7	8	8	9	8	0,35	6	6			0,04	0,6	0,6			• Manual de Buenas prácticas para	5%	75%	50%			75%	0,025	0,33	1,5	3			0,0083	0,0375	0,075		
		Uso No Previsto	0,3	50%	75%	100%			7	8	8	9	8	3,5	6	8			1,05	1,8	2,4			Usuario	50%	75%	50%			50%	0,15	1,75	1,5	4			0,2625	0,225	0,6		
		Difusión De Software Dañino	0,1	5%	50%	100%			7	8	8	9	8	0,35	4	8			0,04	0,4	0,8			• Registro de Cambios e incidencias	5%	50%	50%			75%	0,025	0,33	2	4			0,0083	0,05	0,1		
		Acceso No Autorizado	0,1		50%	100%			7	8	8	9	8		4	8				0,4	0,8					50%	50%			75%	0,025		2	4				0,05	0,1		
		Modificación Deliberada De La Información	0,1		100%				7	8	8	9	8		8					0,8						50%				75%	0,025		4					0,1			
		Destrucción De Información	0,1	100%					7	8	8	9	8	7					0,7						75%					75%	0,025	1,75					0,0438				
		Divulgación De Información	0,1			100%			7	8	8	9	8			8					0,8						50%			75%	0,025			4					0,1		
		Fallo De Origen Lógico	0,1	75%					8	8	7	8	7	6					0,6						75%					80%	0,02	1,5					0,03				
		Errores De Usuarios	0,5	5%	5%	25%			8	8	7	8	7	0,4	0,4	1,75			0,2	0,2	0,88				5%	5%	25%			25%	0,375	0,38	0,38	1,31			0,1425	0,1425	0,4922		
		Errores De Administración	0,1	50%	50%	75%			8	8	7	8	7	4	4	5,25			0,4	0,4	0,53				50%	25%	50%			90%	0,01	2	3	2,63			0,02	0,03	0,0263		
		Alteración Accidental De La Información	0,3		25%				8	8	7	8	7		2					0,6				• Copias de seguridad		25%				50%	0,15		1,5					0,225			
		Destrucción De Información	0,3	5%					8	8	7	8	7	0,4					0,12					• Revisión de la configuración de	5%					25%	0,225	0,38					0,0855				
		Fugas De Información	0,1			25%			8	8	7	8	7			1,75					0,18			seguridad			25%			25%	0,075			1,31					0,0984		
		Vulnerabilidades De Los Programas	0,3	5%	25%	50%			8	8	7	8	7	0,4	2	3,5			0,12	0,6	1,05			• Análisis de Vulnerabilidades	5%	25%	50%			90%	0,03	0,38	1,5	1,75			0,0114	0,045	0,0525		
SW10	E-apsa	Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%				8	8	7	8	7	2	2				0,6	0,6				• Actualizaciones	25%	25%				75%	0,075	1,5	1,5				0,1125	0,1125			
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	100%		8	8	7	8	7		2	5,25	8			0,6	1,58	2,4		• Configuración y revisión de logs		25%	75%	75%		25%	0,225		1,5	1,31	2			0,3375	0,2953	0,45	
		Abuso De Privilegios De Acceso	0,3	5%	25%	75%			8	8	7	8	7	0,4	2	5,25			0,12	0,6	1,58			• Manual de Administración	5%	25%	75%			75%	0,075	0,38	1,5	1,31			0,0285	0,1125	0,0984		
		Uso No Previsto	0,1	25%	5%	50%			8	8	7	8	7	2	0,4	3,5			0,2	0,04	0,35			• Manual de Usuarios	25%	5%	50%			50%	0,05	1,5	0,38	1,75			0,075	0,019	0,0875		
		Difusión De Software Dañino	0,1	5%	25%	50%			8	8	7	8	7	0,4	2	3,5			0,04	0,2	0,35			• Registro de configuración e	5%	25%	50%			90%	0,01	0,38	1,5	1,75			0,0038	0,015	0,0175		
		Acceso No Autorizado	0,1		25%	100%			8	8	7	8	7		2	7				0,2	0,7			Incidencias		25%	75%			90%	0,01		1,5	1,75				0,015	0,0175		
		Modificación Deliberada De La Información	0,1		25%				8	8	7	8	7		2					0,2						25%				50%	0,05		1,5					0,075			
		Destrucción De Información	0,1	75%					8	8	7	8	7	6					0,6						75%					50%	0,05	1,5					0,075				
		Divulgación De Información	0,1			75%			8	8	7	8	7			5,25					0,53						75%			25%	0,075			1,31					0,0984		
		Fallo De Origen Lógico	0,1	50%					4	8	7	6	5	2					0,2						50%					90%	0,01	1					0,01				
		Errores De Usuarios	0,5	5%	25%	50%			4	8	7	6	5	0,2	2	3,5			0,1	1	1,75				5%	25%	50%			25%	0,375	0,19	1,5	1,75			0,0713	0,5625	0,6563		
		Errores De Administración	0,1	25%	25%	50%			4	8	7	6	5	1	2	3,5			0,1	0,2	0,35				25%	25%	50%			90%	0,01	0,75	1,5	1,75			0,0075	0,015	0,0175		
		Difusión De Software Dañino	0,3	5%	25%	75%			4	8	7	6	5	0,2	2	5,25			0,06	0,6	1,58				5%	25%	50%			50%	0,15	0,19	1,5	2,63			0,0285	0,225	0,3938		
		Alteración Accidental De La Información	0,3		25%				4	8	7	6	5		2					0,6						25%				10%	0,27		1,5					0,405			
		Destrucción De Información	0,3	25%					4	8	7	6	5	1					0,3					• Configuración de carpeta Segura	25%					10%	0,27	0,75					0,2025				
		Fugas De Información	0,3			75%			4	8	7	6	5			5,25					1,58			• Cifrado de Información			50%			25%	0,225			2,63					0,5906		
		Vulnerabilidades De Los Programas	0,3	25%	25%	75%			4	8	7	6	5	1	2	5,25			0,3	0,6	1,58			• Actualización del Sistema	25%	25%	50%			75%	0,075	0,75	1,5	2,63			0,0563	0,1125	0,1969		
SW11	Aplicaciones en móviles	Errores De Mantenimiento/Actualización De Programas	0,5	50%	25%				4	8	7	6	5	2	2				1	1				Operativo y Aplicaciones	50%	25%				90%	0,05	1	1,5				0,05	0,075			
		Suplantación De La Identidad Del Usuario	0,3		25%	75%	100%		4	8	7	6	5		2	5,25	6			0,6	1,58	1,8		• Instalación/Actualización Antivirus		25%	50%	50%		90%	0,03		1,5	2,63	3			0,045	0,0788	0,09	
		Abuso De Privilegios De Acceso	0,3	25%	75%	75%			4	8	7	6	5	1	6	5,25			0,3	1,8	1,58			• Análisis de Virus	25%	75%	50%			25%	0,225	0,75	1,5	2,63			0,1688	0,3375	0,5906		
		Uso No Previsto	0,1	75%	50%	75%			4	8	7	6	5	3	4	5,25			0,3	0,4	0,53			• Manual de buenas practicas y de Usuarios	50%	50%	50%			10%	0,09	1,5	2	2,63			0,135	0,18	0,2363		

		Difusión De Software Dañino	0,1	75%	50%	100%			4	8	7	6	5	3	4	7			0,3	0,4	0,7			usuarios	75%	50%	50%			50%	0,05	0,75	2	3,5			0,0375	0,1	0,175		
		Acceso No Autorizado	0,1		25%	100%			4	8	7	6	5		2	7				0,2	0,7					25%	50%			75%	0,025		1,5	3,5				0,0375	0,0875		
		Modificación Deliberada De La Información	0,1		25%				4	8	7	6	5		2					0,2						25%				25%	0,075		1,5					0,1125			
		Destrucción De Información	0,1	50%					4	8	7	6	5	2					0,2						50%					25%	0,075	1					0,075				
		Divulgación De Información	0,1			100%			4	8	7	6	5			7					0,7						50%				50%	0,05			3,5					0,175			
		Fallo De Origen Lógico	0,1	75%					9	9	9	9	9	6,75					0,68						50%					90%	0,01	3,38					0,0338				
		Errores De Administración	0,1	100%	75%	100%			9	9	9	9	9	9	6,75	9			0,9	0,68	0,9			• Configuración de Políticas de	75%	50%	75%			90%	0,01	2,25	3,38	2,25			0,0225	0,0338	0,0225		
		Alteración Accidental De La Información	0,1		75%				9	9	9	9	9		6,75					0,68				seguridad Local		50%				75%	0,025		3,38					0,0844			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9					• Cifrado de Información	75%					75%	0,025	2,25					0,0563				
		Vulnerabilidades De Los Programas	0,1	75%	75%	100%			9	9	9	9	9	6,75	6,75	9			0,68	0,68	0,9			• Perfiles de Usuarios	75%	50%	75%			90%	0,01	1,69	3,38	2,25			0,0169	0,0338	0,0225		
		Errores De Mantenimiento/Actualización De Programas	0,3	75%	75%				9	9	9	9	9	6,75	6,75				2,03	2,03				• Actualización del Sistema	75%	50%				90%	0,03	1,69	3,38				0,0506	0,1013			
SW12	Sistema operativo Ubuntu Server	Suplantación De La Identidad Del Usuario	0,3		75%	100%	100%		9	9	9	9	9		6,75	9	9			2,03	2,7	2,7		Operativo		50%	75%	90%		90%	0,03		3,38	2,25	0,9			0,1013	0,0675	0,027	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			1,35	2,03	2,7			• Actualización Antivirus	50%	50%	75%			80%	0,06	2,25	3,38	2,25			0,135	0,2025	0,135		
		Uso No Previsto	0,1	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			0,45	0,68	0,9			• Respaldos de configuración	50%	50%	75%			80%	0,02	2,25	3,38	2,25			0,045	0,0675	0,045		
		Difusión De Software Dañino	0,1	100%	100%	100%			9	9	9	9	9	9	9	9			0,9	0,9	0,9			• Copias de seguridad	50%	75%	75%			90%	0,01	4,5	2,25	2,25			0,045	0,0225	0,0225		
		Acceso No Autorizado	0,1		100%	100%			9	9	9	9	9		9	9				0,9	0,9			• Registro de cambios e incidentes		75%	75%			90%	0,01		2,25	2,25				0,0225	0,0225		
		Modificación Deliberada De La Información	0,1		100%				9	9	9	9	9		9					0,9				• Configuración de logs de		75%				80%	0,02		2,25					0,045			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9					incidencias	75%					80%	0,02	2,25					0,045				
		Divulgación De Información	0,1			100%			9	9	9	9	9			9					0,9						75%				90%	0,01			2,25					0,0225			
		Fallo De Origen Lógico	0,1	75%					9	9	9	9	9	6,75					0,68						50%					90%	0,01	3,38					0,0338				
		Errores De Administración	0,1	100%	75%	100%			9	9	9	9	9	9	6,75	9			0,9	0,68	0,9			• Configuración de Políticas de	75%	50%	75%			90%	0,01	2,25	3,38	2,25			0,0225	0,0338	0,0225		
		Alteración Accidental De La Información	0,1		75%				9	9	9	9	9		6,75					0,68				seguridad Local		50%				75%	0,025		3,38					0,0844			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9					• Cifrado de Información	75%					75%	0,025	2,25					0,0563				
		Vulnerabilidades De Los Programas	0,1	75%	75%	100%			9	9	9	9	9	6,75	6,75	9			0,68	0,68	0,9			• Perfiles de Usuarios	75%	50%	75%			90%	0,01	1,69	3,38	2,25			0,0169	0,0338	0,0225		
		Errores De Mantenimiento/Actualización De Programas	0,3	75%	75%				9	9	9	9	9	6,75	6,75				2,03	2,03				• Actualización del Sistema	75%	50%				90%	0,03	1,69	3,38				0,0506	0,1013			
SW13	Sistema Operativo Windows Server	Suplantación De La Identidad Del Usuario	0,3		75%	100%	100%		9	9	9	9	9		6,75	9	9			2,03	2,7	2,7		Operativo		50%	75%	75%		90%	0,03		3,38	2,25	2,25			0,1013	0,0675	0,0675	
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			1,35	2,03	2,7			• Actualización Antivirus	50%	50%	75%			80%	0,06	2,25	3,38	2,25			0,135	0,2025	0,135		
		Uso No Previsto	0,1	50%	75%	100%			9	9	9	9	9	4,5	6,75	9			0,45	0,68	0,9			• Respaldos de configuración	50%	50%	75%			80%	0,02	2,25	3,38	2,25			0,045	0,0675	0,045		
		Difusión De Software Dañino	0,1	100%	100%	100%			9	9	9	9	9	9	9	9			0,9	0,9	0,9			• Copias de seguridad	50%	75%	75%			90%	0,01	4,5	2,25	2,25			0,045	0,0225	0,0225		
		Acceso No Autorizado	0,1		100%	100%			9	9	9	9	9		9	9				0,9	0,9			• Registro de cambios e incidentes		75%	75%			90%	0,01		2,25	2,25				0,0225	0,0225		
		Modificación Deliberada De La Información	0,1		100%				9	9	9	9	9		9					0,9				• Configuración de logs de		75%				80%	0,02		2,25					0,045			
		Destrucción De Información	0,1	100%					9	9	9	9	9	9					0,9					incidencias	75%					80%	0,02	2,25					0,045				
		Divulgación De Información	0,1			100%			9	9	9	9	9			9					0,9						75%				90%	0,01			2,25					0,0225			
		Fallo De Origen Lógico	0,1	100%					4	9	5	8	6	4					0,4						25%					90%	0,01	3					0,03				
		Errores De Usuarios	0,5	25%	5%	25%			4	9	5	8	6	1	0,45	1,25			0,5	0,23	0,63				25%	5%	25%			25%	0,375	0,75	0,43	0,94			0,2813	0,1603	0,3516		
		Errores De Administración	0,1	50%	25%	50%			4	9	5	8	6	2	2,25	2,5			0,2	0,23	0,25			• Perfiles de usuarios	50%	25%	25%			90%	0,01	1	1,69	1,88			0,01	0,0169	0,0188		
		Difusión De Software Dañino	0,1	75%	50%	75%			4	9	5	8	6	3	4,5	3,75			0,3	0,45	0,38			• Configuración de seguridad	75%	25%	50%			50%	0,05	0,75	3,38	1,88			0,0375	0,1688	0,0938		
		Alteración Accidental De La Información	0,1		75%				4	9	5	8	6		6,75					0,68				• Actualizaciones de Software		75%				10%	0,09		1,69					0,1519			
		Destrucción De Información	0,1	100%					4	9	5	8	6	4					0,4					• Registro de cambio e incidencias	50%					10%	0,09	2					0,18				
		Vulnerabilidades De Los Programas	0,3	25%	25%	100%			4	9	5	8	6	1	2,25	5			0,3	0,68	1,5			• Configuración de la Carpeta	25%	25%	50%			90%	0,03	0,75	1,69	2,5			0,0225	0,0506	0,075		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%				4	9	5	8	6	1	2,25				0,3	0,68				Segura	25%	25%				75%	0,075	0,75	1,69				0,0563	0,1266			
SW14	Sistema operativo Windows 7	Suplantación De La Identidad Del Usuario	0,3		5%	100%	100%		4	9	5	8	6		0,45	5	8			0,14	1,5	2,4		• Cifrado de Información		5%	75%	75%		90%	0,03		0,43	1,25	2			0,0128	0,0375	0,06	
		Abuso De Privilegios De Acceso	0,3	5%	5%	75%			4	9	5	8	6	0,2	0,45	3,75			0,06	0,14	1,13			• Manual de buenas prácticas	5%	5%	75%			25%	0,225	0,19	0,43	0,94			0,0428	0,0962	0,2109		
		Uso No Previsto	0,3	25%	25%	100%			4	9	5	8	6	1	2,25	5			0,3	0,68	1,5			• Configuración de logs de	25%	25%	75%			10%	0,27	0,75	1,69	1,25			0,2025	0,4556	0,3375		
		Difusión De Software Dañino	0,1	75%	75%	100%			4	9	5	8	6	3	6,75	5			0,3	0,68	0,5			incidencias	75%	75%	75%			75%	0,025	0,75	1,69	1,25			0,0188	0,0422	0,0313		
		Acceso No Autorizado	0,3		25%	100%			4	9	5	8	6		2,25	5				0,68	1,5			• Seguridad con otras aplicaciones		25%	75%			90%	0,03		1,69	1,25				0,0506	0,0375		
		Modificación Deliberada De La Información	0,1		75%				4	9	5	8	6		6,75					0,68				• Copias de seguridad		75%				25%	0,075		1,69					0,1266			
		Destrucción De Información	0,1	100%					4	9	5	8	6	4					0,4						25%					25%	0,075	3					0,225				
		Divulgación De Información	0,1			100%			4	9	5	8	6			5					0,5						25%				10%	0,09			1,25					0,1125			
		Fallo De Origen Lógico	0,1	100%					4	9	5	8	6	4					0,4						25%					90%	0,01	3					0,03				
		Errores De Usuarios	0,5	25%	5%	25%			4	9	5	8	6	1	0,45	1,25			0,5	0,23	0,63				25%	5%	25%			25%	0,375	0,75	0,43	0,94			0,2813	0,1603	0,3516		
		Errores De Administración	0,1	50%	25%	50%			4	9	5	8	6	2	2,25	2,5			0,2	0,23	0,25			• Perfiles de usuarios	50%	25%	25%			90%	0,01	1	1,69	1,88			0,01	0,0169	0,0188		
		Difusión De Software Dañino	0,1	75%	50%	75%			4	9	5	8	6	3	4,5	3,75			0,3	0,45	0,38			• Configuración de seguridad	75%	25%	50%			50%	0,05	0,75	3,38	1,88			0,0375	0,1688	0,0938		
		Alteración Accidental De La Información	0,1		75%				4	9	5	8	6		6,75					0,68				• Actualizaciones de Software		75%				10%	0,09		1,69					0,1519			
		Destrucción De Información	0,1	100%					4	9	5	8	6	4					0,4					• Registro de cambio e incidencias	50%					10%	0,09	2					0,18				
		Vulnerabilidades De Los Programas	0,3	25%	25%	100%			4	9	5	8	6	1	2,25	5			0,3	0,68	1,5			• Configuración de la Carpeta	25%	25%	50%			90%	0,03	0,75	1,69	2,5			0,0225	0,0506	0,075		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	25%				4	9	5	8	6	1	2,25				0,3	0,68				Segura	25%	25%				90%	0,03	0,75	1,69				0,0225	0,0506			
SW15	Sistema operativo Windows 10	Suplantación De La Identidad Del Usuario	0,3		5%	100%	100%		4	9	5	8	6		0,45	5	8			0,14	1,5	2,4		• Cifrado de Información		5%	75%	75%		90%	0,03		0,43	1,25	2			0,0128	0,0375	0,06	
		Abuso De Privilegios De Acceso	0,3	5%	5%	75%			4	9	5	8	6	0,2	0,45	3,75			0,06	0,14	1,13			• Manual de buenas prácticas	5%	5%	75%			25%	0,225	0,19	0,43	0,94			0,0428	0,0962	0,2109		
		Uso No Previsto	0,3	25%	25%	100%			4	9	5	8	6	1	2,25	5			0,3	0,68	1,5			• Configuración de logs de	25%	25%	75%			10%	0,27	0,75	1,69	1,25			0,2025	0,4556	0,3375		
		Difusión De Software Dañino	0,1	75%	75%	100%			4	9	5	8	6	3	6,75	5			0,3	0,68	0,5			incidencias	75%	75%	75%			80%	0,02	0,75	1,69	1,25			0,015	0,0338	0,025		
		Acceso No Autorizado	0,3		25%	100%			4	9	5	8	6		2,25	5				0,68	1,5			• Seguridad con otras aplicaciones		25%	75%			90%	0,03		1,69	1,25				0,0506	0,0375		
		Modificación Deliberada De La Información	0,1		75%				4	9	5	8	6		6,75					0,68				copias de seguridad		75%				25%	0,075		1,69					0,1266			
		Destrucción De Información	0,1	100%					4	9	5	8	6	4					0,4						25%					25%	0,075	3					0,225				
		Divulgación De Información	0,1			100%			4	9	5	8	6			5					0,5						25%				10%	0,09			1,25					0,1125			
		Errores De Usuarios	0,5	5%	5%	75%			4	8	8	8	6	0,2	0,4	6			0,1	0,2	3				5%	5%	50%			25%	0,375	0,19	0,38	3			0,0713	0,1425	1,125		
		Errores De Administración	0,1	25%	5%	75%			4	8	8	8	6	1	0,4	6			0,1	0,04	0,6				25%	5%	50%			90%	0,01	0,75	0,38	3			0,0075	0,0038	0,03		
		Fugas De Información	0,1			100%			4	8	8	8	6			8					0,8						50%				75%	0,025			4					0,1			
		Vulnerabilidades De Los Programas	0,1	25%	50%	100%			4	8	8	8	6	1	4	8			0,1	0,4	0,8			• Manual de administración	25%	50%	50%			75%	0,025	0,75	2	4			0,0188	0,05	0,1		
		Errores De Mantenimiento/Actualización De Programas	0,3	5%	50%				4	8	8	8	6	0,2	4				0,06	1,2				• Manual de buenas prácticas de	5%	50%				90%	0,03	0,19	2				0,0057	0,06			
SW16	Navegadores Web	Abuso De Privilegios De Acceso	0,3	5%	5%	75%			4	8	8	8	6	0,2	0,4	6			0,06	0,12	1,8			usuarios	5%	5%	50%			25%	0,225	0,19	0,38	3			0,0428	0,0855	0,675		
		Uso No Previsto	0,3	5%	25%	75%			4	8	8	8	6	0,2	2	6			0,06	0,6	1,8			• Configuración de seguridad	5%	25%	50%			90%	0,03	0,19	1,5	3			0,0057	0,045	0,09		
		Difusión De Software Dañino	0,5	5%	25%	100%			4	8	8	8	6	0,2	2	8			0,1	1	4			• Actualización del software	5%	25%	100%			50%	0,25	0,19	1,5				0,0475	0,375			
		Modificación Deliberada De La Información	0,1		25%				4	8	8	8	6		2					0,2				• Registro de cambio e incidencias		25%				25%	0,075		1,5					0,1125			
		Destrucción De Información	0,1	25%					4	8	8	8	6	1					0,1						25%						0,1	0,75					0,075				
		Divulgación De Información	0,1			25%			4	8	8	8	6			2					0,2								25%		10%	0,09			1,5					0,135			
		Fallo De Origen Lógico	0,1	75%					8	8	5	8	5	6					0,6						50%					90%	0,01	3					0,03				
		Errores De Administración	0,1	50%	25%	25%			8	8	5	8	5	4	2	1,25			0,4	0,2	0,13				25%	25%	25%			90%	0,01	3	1,5	0,94			0,03	0,015	0,0094		
		Errores De Mantenimiento/Actualización De Programas	0,3	25%	100%				8	8	5	8	5	2	8				0,6	2,4				• Manual de administración	25%	50%				90%	0,03	1,5	4				0,045	0,12			
SW17	Antivirus	Abuso De Privilegios De Acceso	0,1	50%	100%	25%			8	8	5	8	5	4	8	1,25			0,4	0,8	0,13			• Actualización de software	50%	50%	25%			50%	0,05	2	4	0,94			0,1	0,2	0,0469		
		Uso No Previsto	0,1	50%	100%	25%			8	8	5	8	5	4	8	1,25			0,4	0,8	0,13			• Análisis con el software	50%	50%	25%			25%	0,075	2	4	0,94			0,15	0,3	0,0703		
		Acceso No Autorizado	0,1		100%	25%			8	8	5	8	5		8	1,25				0,8	0,13			• Registro de cambio e incidencias		50%	25%			50%	0,05		4	0,94				0,2	0,0469		
		Modificación Deliberada De La Información	0,1		100%				8	8	5	8	5		8					0,8						50%					0,1		4					0,4				
		Fallo De Origen Lógico	0,3	50%					3	5	5	4	3	1,5					0,45						50%					90%	0,03	0,75					0,0225				
		Errores De Usuarios	0,5	50%	5%	25%			3	5	5	4	3	1,5	0,25	1,25			0,75	0,13	0,63				50%	5%	25%			10%	0,45	0,75	0,24	0,94			0,3375	0,1069	0,4219		
		Errores De Administración	0,1	50%	5%	25%			3	5	5	4	3	1,5	0,25	1,25			0,15	0,03	0,13			• Manual de usuarios	50%	5%	25%			50%	0,05	0,75	0,24	0,94			0,0375	0,0119	0,0469		
SW18	Software Ofimático	Errores De Mantenimiento/Actualización De Programas	0,3	75%	25%				3	5	5	4	3	2,25	1,25				0,68	0,38				• Actualización de software	75%	25%				90%	0,03	0,56	0,94				0,0169	0,0281			
																								• Registros de Cambio																	

		Abuso De Privilegios De Acceso	0,1	25%	25%	25%			3	5	5	4	3	0,75	1,25	1,25			0,08	0,13	0,13			- Registros de Cambio	25%	25%	25%				0,1	0,56	0,94	0,94			0,0563	0,0938	0,0938		
		Uso No Previsto	0,1	50%	25%	25%			3	5	5	4	3	1,5	1,25	1,25			0,15	0,13	0,13				50%	25%	25%				0,1	0,75	0,94	0,94			0,075	0,0938	0,0938		

EQUIPOS INFORMÁTICOS [HW]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencias	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D'	I'	C'	A'	T'		F'	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
HW1	Servidores APSA	Avería De Origen Físico/Lógico	0,3	100%					9	9	9	9	9	9					2,7					• Configuración de seguridad						75%	0,075	9					0,675				
		Errores De Administración	0,1	100%	100%	100%			9	9	9	9	9	9	9	9			0,9	0,9	0,9			• Seguridad en servicios alojados	50%	50%	75%			90%	0,01	4,5	4,5	2,25			0,045	0,045	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					9	9	9	9	9	6,75					2,03					• Revisión de recursos	50%					75%	0,075	3,38					0,2531				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					9	9	9	9	9	9					0,9					• Copias de seguridad de configuración	55%					90%	0,01	4,05					0,0405				
		Abuso De Privilegios De Acceso	0,1	75%	75%	100%			9	9	9	9	9	6,75	6,75	9			0,68	0,68	0,9			• Registro de accesos	50%	50%	75%			90%	0,01	3,38	3,38	2,25			0,0338	0,0338	0,0225		
		Uso No Previsto	0,3	75%	75%	100%			9	9	9	9	9	6,75	6,75	9			2,03	2,03	2,7			• Manuales de Administración	50%	50%	75%			90%	0,03	3,38	3,38	2,25			0,1013	0,1013	0,0675		
		Acceso No Autorizado	0,7		75%	100%			9	9	9	9	9		6,75	9				4,73	6,3			• Depuración		50%	75%			90%	0,07		3,38	2,25				0,2363	0,1575		
		Denegación De Servicio	0,3	100%					9	9	9	9	9	9					2,7					• Logs de incidencias • Servidores de Respaldo • Cifrado de Información	50%					75%	0,075	4,5					0,3375				
HW2	Servidores Sedes	Daños Por Agua	0,1	100%					8	8	9	9	9	8					0,8					• Configuración de seguridad	75%					100%		2									
		Avería De Origen Físico/Lógico	0,3	100%					8	8	9	9	9	8					2,4					• Seguridad en servicios alojados	75%					75%	0,075	2					0,15				
		Corte De Suministro Eléctrico	0,3	100%					8	8	9	9	9	8					2,4					• Revisión de recursos	50%					100%		4									
		Fallas De Climatización	0,1	25%					8	8	9	9	9	2					0,2					• Copias de seguridad de configuración	50%					50%	0,05	1					0,05				
		Errores De Administración	0,1	75%	75%	100%			8	8	9	9	9	6	6	9			0,6	0,6	0,9			• Manuales de Administración	75%	50%	75%			90%	0,01	1,5	3	2,25			0,015	0,03	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	8	9	9	9	6					1,8					• Depuración	75%					90%	0,03	1,5					0,045				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	9	9	9	8					0,8					• Seguridad física	50%					90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	0,3	75%	75%	100%			8	8	9	9	9	6	6	9			1,8	1,8	2,7			• Registro de accesos lógicos y físicos	75%	50%	75%			90%	0,03	1,5	3	2,25			0,045	0,09	0,0675		
		Uso No Previsto	0,3	50%	50%	100%			8	8	9	9	9	4	4	9			1,2	1,2	2,7			• Asegurar suministro eléctrico	50%	50%	75%			90%	0,03	2	2	2,25			0,06	0,06	0,0675		
		Acceso No Autorizado	0,5		75%	100%			8	8	9	9	9		6	9				3	4,5			• Registro de cambios e incidencias		50%	75%			75%	0,125		3	2,25				0,375	0,2813		
		Manipulación De Equipos	0,3	75%		75%			8	8	9	9	9	6		6,75			1,8		2,03			• Protección física	50%		75%			90%	0,03	3		1,69			0,09		0,0506		
		Denegación De Servicio	0,3	100%					8	8	9	9	9	8					2,4					• Logs de incidencias	50%					75%	0,075	4					0,3				
		Robo	0,1	100%		75%			8	8	9	9	9	8		6,75			0,8		0,68			• Mantenimiento • Servidores de Respaldo • Ubicaciones adecuadas • Cifrado de Información	75%		75%			75%	0,025	2		1,69			0,05		0,0422		
HW3	Ordenadores de escritorio administrativos	Daños Por Agua	0,1	75%					7	8	8	7	8	5,25					0,53					• Seguridad en sistemas operativos	25%					100%		3,94									
		Avería De Origen Físico/Lógico	0,3	100%					7	8	8	7	8	7					2,1					• Revisión de recursos	25%					75%	0,075	5,25					0,3938				
		Corte De Suministro Eléctrico	0,3	100%					7	8	8	7	8	7					2,1					• Depuración							0,3	7					2,1				
		Errores De Administración	0,1	50%	50%	75%			7	8	8	7	8	3,5	4	6			0,35	0,4	0,6			• Copias de seguridad	25%	75%	75%			90%	0,01	2,63	1	1,5			0,0263	0,01	0,015		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%					7	8	8	7	8	3,5					1,75					• Manuales de Administración	25%					90%	0,05	2,63					0,1313				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%					7	8	8	7	8	5,25					1,58					• Registro de accesos lógicos	50%					90%	0,03	2,63					0,0788				
		Perdida De Equipos	0,1	100%		100%			7	8	8	7	8	7		8			0,7		0,8			• Manual de buenas prácticas	25%		25%			90%	0,01	5,25		6			0,0525		0,06		
		Abuso De Privilegios De Acceso	0,1	50%	50%	100%			7	8	8	7	8	3,5	4	8			0,35	0,4	0,8			• Mantenimiento	50%	25%	50%			50%	0,05	1,75	3	4			0,0875	0,15	0,2		
		Uso No Previsto	0,3	75%	25%	100%			7	8	8	7	8	5,25	2	8			1,58	0,6	2,4			• Registro de cambios e incidencias	25%	25%	50%			50%	0,15	3,94	1,5	4			0,5906	0,225	0,6		
		Acceso No Autorizado	0,1		25%	100%			7	8	8	7	8		2	8				0,2	0,8			• Ubicaciones adecuadas		25%	50%			90%	0,01		1,5	4				0,015	0,04		
		Manipulación De Equipos	0,3	50%		100%			7	8	8	7	8	3,5		8			1,05		2,4			• Cifrado de información	25%		75%			10%	0,27	2,63		2			0,7088		0,54		
		Robo	0,1	100%		100%			7	8	8	7	8	7		8			0,7		0,8			• Protección física	25%		25%			75%	0,025	5,25		6			0,1313		0,15		
HW4	Ordenadores de escritorio empleados	Daños Por Agua	0,1	75%					3	7	7	7	7	2,25					0,23					• Seguridad en sistemas operativos	50%					100%		1,13									
		Avería De Origen Físico/Lógico	0,5	100%					3	7	7	7	7	3					1,5					• Revisión de recursos	50%					75%	0,125	1,5					0,1875				
		Corte De Suministro Eléctrico	0,3	100%					3	7	7	7	7	3					0,9					• Depuración							0,3	3					0,9				
		Errores De Administración	0,3	50%	50%	75%			3	7	7	7	7	1,5	3,5	5,25			0,45	1,05	1,58			• Copias de seguridad	50%	10%	50%			90%	0,03	0,75	3,15	2,63			0,0225	0,0945	0,0788		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%					3	7	7	7	7	1,5					0,75					• Manuales de Adnimistración	50%					90%	0,05	0,75					0,0375				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%					3	7	7	7	7	2,25					0,68					• Registro de accesos lógicos	50%					90%	0,03	1,13					0,0338				
		Perdida De Equipos	0,1	100%		75%			3	7	7	7	7	3		5,25			0,3		0,53			• Manual de buenas prácticas	50%		25%			75%	0,025	1,5		3,94			0,0375		0,0984		
		Abuso De Privilegios De Acceso	0,5	50%	50%	75%			3	7	7	7	7	1,5	3,5	5,25			0,75	1,75	2,63			• Mantenimiento	50%	10%	25%			50%	0,25	0,75	3,15	3,94			0,1875	0,7875	0,9844		
		Uso No Previsto	0,5	75%	25%	75%			3	7	7	7	7	2,25	1,75	5,25			1,13	0,88	2,63			• Registro de cambios e incidencias	50%	10%	50%			50%	0,25	1,13	1,58	2,63			0,2813	0,3938	0,6563		
		Acceso No Autorizado	0,3		25%	75%			3	7	7	7	7		1,75	5,25				0,53	1,58			• Ubicaciones adecuadas		10%	25%			90%	0,03		1,58	3,94				0,0473	0,1181		
		Manipulación De Equipos	0,5	50%		75%			3	7	7	7	7	1,5		5,25			0,75		2,63			• Cifrado de Infromación	50%		50%			10%	0,45	0,75		2,63			0,3375		1,1813		
		Robo	0,1	100%		100%			3	7	7	7	7	3		7			0,3		0,7			• Protección física	50%		25%			75%	0,025	1,5		5,25			0,0375		0,1313		
HW5	Portátiles de administrativos	Avería De Origen Físico/Lógico	0,3	100%					7	8	8	7	8	7					2,1												75%	0,075	7					0,525				
		Corte De Suministro Eléctrico	0,1	25%					7	8	8	7	8	1,75					0,18					• Seguridad en sistemas operativos	10%						0,1	1,58					0,1575				
		Errores De Administración	0,3	50%	25%	100%			7	8	8	7	8	3,5	2	8			1,05	0,6	2,4			• Revisión de recursos	25%	25%	50%			90%	0,03	2,63	1,5	4			0,0788	0,045	0,12		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%					7	8	8	7	8	3,5					1,75					• Depuración	25%					90%	0,05	2,63					0,1313				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%					7	8	8	7	8	5,25					1,58					• Copias de seguridad	50%					90%	0,03	2,63					0,0788				
		Perdida De Equipos	0,1	100%		100%			7	8	8	7	8	7		8			0,7		0,8			• Manuales de Adnimistración	10%		50%			25%	0,075	6,3		4			0,4725		0,3		
		Abuso De Privilegios De Acceso	0,3	25%	25%	100%			7	8	8	7	8	1,75	2	8			0,53	0,6	2,4			• Registro de accesos lógicos	25%	25%	50%			50%	0,15	1,31	1,5	4			0,1969	0,225	0,6		
		Uso No Previsto	0,3	50%	25%	100%			7	8	8	7	8	3,5	2	8			1,05	0,6	2,4			• Manual de buenas prácticas	25%	75%	50%			50%	0,15	2,63	0,5	4			0,3938	0,075	0,6		
		Acceso No Autorizado	0,1		75%	100%			7	8	8	7	8		6	8				0,6	0,8			• Mantenimiento		25%	50%			90%	0,01		4,5	4				0,045	0,04		
		Manipulación De Equipos	0,3	75%		100%			7	8	8	7	8	5,25		8			1,58		2,4			• Registro de cambios e incidencias	25%		50%			25%	0,225	3,94		4			0,8859		0,9		
		Robo	0,1	100%		100%			7	8	8	7	8	7		8			0,7		0,8			• Cifrado de Información	10%		50%			75%	0,025	6,3		4			0,1575		0,1		
HW6	Portátiles de empleados	Avería De Origen Físico/Lógico	0,3	100%					3	7	7	7	7	3					0,9												75%	0,075	3					0,225				
		Corte De Suministro Eléctrico	0,1	25%					3	7	7	7	7	0,75					0,08					• Seguridad en sistemas operativos							0,1	0,75					0,075				
		Errores De Administración	0,3	50%	25%	25%			3	7	7	7	7	1,5	1,75	1,75			0,45	0,53	0,53			• Revisión de recursos	25%	25%	75%			90%	0,03	1,13	1,31	0,44			0,0338	0,0394	0,0131		
		Errores De Mantenimiento/Actualización De Equipos	0,5	50%					3	7	7	7	7	1,5					0,75					• Depuración	25%					90%	0,05	1,13					0,0563				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	75%					3	7	7	7	7	2,25					0,68					• Copias de seguridad	50%					90%	0,03	1,13					0,0338				
		Perdida De Equipos	0,1	100%		75%			3	7	7	7	7	3		5,25			0,3		0,53			• Manuales de Adnimistración	25%		50%			25%	0,075	2,25		2,63			0,1688		0,1969		
		Abuso De Privilegios De Acceso	0,3	25%	25%	75%			3	7	7	7	7	0,75	1,75	5,25			0,23	0,53	1,58			• Registro de accesos lógicos	25%	25%	50%			50%	0,15	0,56	1,31	2,63			0,0844	0,1969	0,3938		
		Uso No Previsto	0,3	50%	25%	75%			3	7	7	7	7	1,5	1,75	5,25			0,45	0,53	1,58			• Manual de buenas prácticas	25%	75%	50%			50%	0,15	1,13	0,44	2,63			0,1688	0,0656	0,3938		
		Acceso No Autorizado	0,3		50%	75%			3	7	7	7	7		3,5	5,25				1,05	1,58			• Mantenimiento		25%	50%			90%	0,03		2,63	2,63				0,0788	0,0788		
		Manipulación De Equipos	0,3	50%		75%			3	7	7	7	7	1,5		5,25			0,45		1,58			• Registro de cambios e incidencias	25%		50%			25%	0,225	1,13		2,63			0,2531		0,5906		
		Robo	0,1	100%		100%			3	7	7	7	7	3		7			0,3		0,7			• Cifrado de Infromación	25%		50%			75%	0,025	2,25		3,5			0,0563		0,0875		
HW7	Portátiles TIC	Daños Por Agua	0,1	100%					8	9	9	9	9	8					0,8					• Seguridad en sistemas operativos						100%		8									
		Avería De Origen Físico/Lógico	0,1	100%					8	9	9	9	9	8					0,8					• Revisión de recursos	10%					75%	0,025	7,2					0,18				
		Corte De Suministro Eléctrico	0,1	75%					8	9	9	9	9	6					0,6					• Depuración	50%					90%	0,01	3					0,03				
		Errores De Administración	0,1	50%	75%	100%			8	9	9	9	9	4	6,75	9			0,4	0,68	0,9			• Copias de seguridad	25%	75%	75%			90%	0,01	3	1,69	2,25			0,03	0,0169	0,0225		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	9	9	9	9	6					1,8					• Manuales de Adnimistración	25%					90%	0,03	4,5					0,135				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	9	9	9	9	8					0,8					• Registro de accesos lógicos	50%					90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	0,1	50%	75%	100%			8	9	9	9	9	4	6,75	9			0,4	0,68	0,9			• Manual de buenas prácticas	25%	25%	75%			50%	0,05	3	5,06	2,25			0,15	0,2531	0,1125		
		Acceso No Autorizado	0,1		75%	100%			8	9	9	9	9		6,75	9				0,68	0,9			• Mantenimiento		25%	75%			90%	0,01		5,06	2,25				0,0506	0,0225		
		Manipulación De Equipos	0,1	50%		100%			8	9	9	9	9	4		9			0,4		0,9			• Registro de cambios e incidencias • Seguridad Física • Ubicaciones adecuadas • Cifrado de Información • Asegurar suministro electrico	25%		75%			50%	0,05	3		2,25			0,15		0,1125		
		Avería De Origen Físico/Lógico	0,3	75%					4	7	7	8	6	3					0,9						25%					50%	0,15	2,25					0,3375				
		Errores De Administración	0,1	25%	25%	50%			4	7	7	8	6	1	1,75	3,5			0,1	0,18	0,35				50%	25%	50%			50%	0,05	0,5	1,31	1,75			0,025	0,0656	0,0875		
		Errores De Mantenimiento/Actualización De Equipos	0,5	75%					4	7	7	8	6	3					1,5					• Seguridad en aplicaciones alojadas	25%					75%	0,125	2,25					0,2813				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	50%					4	7	7	8	6	2					0,6					• Revisión de recursos	50%					25%	0,225	1					0,225				

HW8	**Móviles/Tablets**	Perdida De Equipos	0,5	100%		100%			4	7	7	8	6	4		7			2		3,5			• Manual de buenas prácticas, con depuración			50%			10%	0,45	4		3,5			1,8		1,575		
		Abuso De Privilegios De Acceso	0,3	50%	50%	100%			4	7	7	8	6	2	3,5	7			0,6	1,05	2,1			• Mantenimiento		25%	50%			50%	0,15	2	2,63	3,5			0,3	0,3938	0,525		
		Uso No Previsto	0,5	50%	50%	100%			4	7	7	8	6	2	3,5	7			1	1,75	3,5			• Cifrado de Información		25%	50%			10%	0,45	2	2,63	3,5			0,9	1,1813	1,575		
		Acceso No Autorizado	0,1		75%	100%			4	7	7	8	6		5,25	7				0,53	0,7			• Registro de cambios e incidencias		25%	50%			50%	0,05		3,94	3,5				0,1969	0,175		
		Manipulación De Equipos	0,5	75%		100%			4	7	7	8	6	3		7			1,5		3,5				10%		50%			25%	0,375	2,7		3,5			1,0125		1,3125		
		Robo	0,3	100%		100%			4	7	7	8	6	4		7			1,2		2,1						50%			10%	0,27	4		3,5			1,08		0,945		
		Avería De Origen Físico/Lógico	0,3	100%					3	2	3	3	3	3					0,9						75%					50%	0,15	0,75					0,1125				
		Corte De Suministro Eléctrico	0,1	100%					3	2	3	3	3	3					0,3												0,1	3					0,3				
		Errores De Administración	0,1	50%	50%	5%			3	2	3	3	3	1,5	1	0,15			0,15	0,1	0,02			• Revisión de recursos	50%	25%				90%	0,01	0,75	0,75	0,15			0,0075	0,0075	0,0015		
		Errores De Mantenimiento/Actualización De Equipos	0,3	50%					3	2	3	3	3	1,5					0,45					• Depuración	50%					90%	0,03	0,75					0,0225				
		Caída Del Sistema Por Agotamiento De Recursos	0,5	75%					3	2	3	3	3	2,25					1,13					• Manual de buenas prácticas	50%					75%	0,125	1,13					0,1406				
HW9	**Impresoras oficinas**	Perdida De Equipos	0,1	100%		25%			3	2	3	3	3	3		0,75			0,3		0,08			• Mantenimiento						75%	0,025	3		0,75			0,075		0,0188		
		Abuso De Privilegios De Acceso	0,3	50%	25%	5%			3	2	3	3	3	1,5	0,5	0,15			0,45	0,15	0,05			• Registro de cambios e incidencias	10%	25%	10%			25%	0,225	1,35	0,38	0,14			0,3038	0,0844	0,0304		
		Uso No Previsto	0,3	25%	25%	25%			3	2	3	3	3	0,75	0,5	0,75			0,23	0,15	0,23			• Ubicaciones adecuadas	10%	25%	10%			25%	0,225	0,68	0,38	0,68			0,1519	0,0844	0,1519		
		Acceso No Autorizado	0,1		25%	25%			3	2	3	3	3		0,5	0,75				0,05	0,08			• Duplicación		25%	10%			25%	0,075		0,38	0,68				0,0281	0,0506		
		Manipulación De Equipos	0,3	50%		25%			3	2	3	3	3	1,5		0,75			0,45		0,23				10%		10%			25%	0,225	1,35		0,68			0,3038		0,1519		
		Robo	0,1	100%		25%			3	2	3	3	3	3		0,75			0,3		0,08									75%	0,025	3		0,75			0,075		0,0188		
		Avería De Origen Físico/Lógico	0,1	100%					8	8	8	8	8	8					0,8					• Máxima configuracióon de seguridad	25%					75%	0,025	6					0,15				
		Corte De Suministro Eléctrico	0,1	100%					8	8	8	8	8	8					0,8					• Aplicación de perfiles							0,1	8					0,8				
		Fallas De Climatización	0,1	50%					8	8	8	8	8	4					0,4					• Seguridad de redes	10%					25%	0,075	3,6					0,27				
		Errores De Administración	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Revisión de recursos	25%	50%	50%			90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	8	8	8	8	6					1,8					• Depuración	25%					80%	0,06	4,5					0,27				
HW10	**Router**	Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	8	8	8	8					0,8					• Manual de administración	50%					90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Mantenimiento	25%	50%	50%			90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Uso No Previsto	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Registro de cambios e incidencias		50%	50%			90%	0,01	6	2	4			0,06	0,02	0,04		
		Acceso No Autorizado	0,3		75%	100%			8	8	8	8	8		6	8				1,8	2,4			• Protección física		50%	50%			90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	0,3	75%		100%			8	8	8	8	8	6		8			1,8		2,4			• Ubicaciones adecuadas	25%		50%			90%	0,03	4,5		4			0,135		0,12		
		Denegación De Servicio	0,3	100%					8	8	8	8	8	8					2,4											90%	0,03	8					0,24				
		Daños Por Agua	0,1	100%					8	8	8	8	8	8					0,8											100%		8									
		Avería De Origen Físico/Lógico	0,1	75%					8	8	8	8	8	6					0,6					• Máxima configuracióon de seguridad	25%					75%	0,025	4,5					0,1125				
		Corte De Suministro Eléctrico	0,1	100%					8	8	8	8	8	8					0,8					• Aplicación de perfiles							0,1	8					0,8				
		Errores De Administración	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Seguridad de redes inálambricas	25%	50%	50%			90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	8	8	8	8	6					1,8					• Revisión de recursos	25%					80%	0,06	4,5					0,27				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	8	8	8	8					0,8					• Depuración	50%					90%	0,01	4					0,04				
HW11	**Router inalámbrico**	Perdida De Equipos	0,1	100%		50%			8	8	8	8	8	8		4			0,8		0,4			• Manual de administración			50%			75%	0,025	8		2			0,2		0,05		
		Abuso De Privilegios De Acceso	0,3	50%	50%	75%			8	8	8	8	8	4	4	6			1,2	1,2	1,8			• Mantenimiento	25%	50%	50%			90%	0,03	3	2	3			0,09	0,06	0,09		
		Uso No Previsto	0,3	75%	75%	75%			8	8	8	8	8	6	6	6			1,8	1,8	1,8			• Registro de cambios e incidencias		50%	50%			90%	0,03	6	3	3			0,18	0,09	0,09		
		Acceso No Autorizado	0,3		75%	100%			8	8	8	8	8		6	8				1,8	2,4			• Protección física		50%	50%			90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	0,3	75%		50%			8	8	8	8	8	6		4			1,8		1,2			• Ubicaciones adecuadas	25%		50%			90%	0,03	4,5		2			0,135		0,06		
		Denegación De Servicio	0,3	100%					8	8	8	8	8	8					2,4											90%	0,03	8					0,24				
		Robo	0,1	100%		50%			8	8	8	8	8	8		4			0,8		0,4						50%			75%	0,025	8		2			0,2		0,05		
		Avería De Origen Físico/Lógico	0,1	100%					8	8	8	8	8	8					0,8					• Máxima configuracióon de seguridad	25%					75%	0,025	6					0,15				
		Corte De Suministro Eléctrico	0,1	100%					8	8	8	8	8	8					0,8					• Aplicación de perfiles							0,1	8					0,8				
		Fallas De Climatización	0,1	50%					8	8	8	8	8	4					0,4					• Seguridad de redes	10%					25%	0,075	3,6					0,27				
		Errores De Administración	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Revisión de recursos	25%	50%	50%			90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	8	8	8	8	6					1,8					• Depuración	25%					80%	0,06	4,5					0,27				
HW12	**Switch**	Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	8	8	8	8	8					0,8					• Manual de administración	50%					90%	0,01	4					0,04				
		Abuso De Privilegios De Acceso	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Mantenimiento	25%	50%	50%			90%	0,01	4,5	2	4			0,045	0,02	0,04		
		Uso No Previsto	0,1	75%	50%	100%			8	8	8	8	8	6	4	8			0,6	0,4	0,8			• Registro de cambios e incidencias		50%	50%			90%	0,01	6	2	4			0,06	0,02	0,04		
		Acceso No Autorizado	0,3		75%	100%			8	8	8	8	8		6	8				1,8	2,4			• Protección física		50%	50%			90%	0,03		3	4				0,09	0,12		
		Manipulación De Equipos	0,3	75%		100%			8	8	8	8	8	6		8			1,8		2,4			• Ubicaciones adecuadas	25%		50%			90%	0,03	4,5		4			0,135		0,12		
		Denegación De Servicio	0,3	100%					8	8	8	8	8	8					2,4											90%	0,03	8					0,24				
		Avería De Origen Físico/Lógico	0,3	100%					8	5	4	6	5	8					2,4					• Revisión de recursos	25%					75%	0,075	6					0,45				
		Corte De Suministro Eléctrico	0,1	100%					8	5	4	6	5	8					0,8					• Depuración							0,1	8					0,8				
		Errores De Administración	0,3	75%	25%	50%			8	5	4	6	5	6	1,25	2			1,8	0,38	0,6			• Manuales de Administración	50%	10%	25%			90%	0,03	3	1,13	1,5			0,09	0,0338	0,045		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	5	4	6	5	6					1,8					• Manual de buenas prácticas	50%					75%	0,075	3					0,225				
HW13	**Impresoras repositorios**	Caída Del Sistema Por Agotamiento De Recursos	0,3	100%					8	5	4	6	5	8					2,4					• Mantenimiento	50%					90%	0,03	4					0,12				
		Abuso De Privilegios De Acceso	0,3	50%	50%	25%			8	5	4	6	5	4	2,5	1			1,2	0,75	0,3			• Registro de cambios e incidencias	25%	10%	25%			50%	0,15	3	2,25	0,75			0,45	0,3375	0,1125		
		Uso No Previsto	0,3	75%	50%	25%			8	5	4	6	5	6	2,5	1			1,8	0,75	0,3			• Ubicaciones adecuadas		25%	25%			50%	0,15	6	1,88	0,75			0,9	0,2813	0,1125		
		Acceso No Autorizado	0,1		50%	25%			8	5	4	6	5		2,5	1				0,25	0,1			• Seguridad física		10%	25%			90%	0,01		2,25	0,75				0,0225	0,0075		
		Manipulación De Equipos	0,3	75%		25%			8	5	4	6	5	6		1			1,8		0,3				25%		25%			50%	0,15	4,5		0,75			0,675		0,1125		
		Avería De Origen Físico/Lógico	0,1	100%					6	5	4	4	4	6					0,6						25%					75%	0,025	4,5					0,1125				
		Corte De Suministro Eléctrico	0,1	100%					6	5	4	4	4	6					0,6												0,1	6					0,6				
		Errores De Administración	0,1	50%	25%	50%			6	5	4	4	4	3	1,25	2			0,3	0,13	0,2			• Manual de buenas prácticas y administración	50%	10%	25%			90%	0,01	1,5	1,13	1,5			0,015	0,0113	0,015		
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					6	5	4	4	4	4,5					1,35					• Mantenimiento	50%					80%	0,06	2,25					0,135				
HW14	**Teléfonos de sobremesa**	Abuso De Privilegios De Acceso	0,3	50%	25%	75%			6	5	4	4	4	3	1,25	3			0,9	0,38	0,9			• Registro de cambios e incidencias	25%	10%	25%			90%	0,03	2,25	1,13	2,25			0,0675	0,0338	0,0675		
		Uso No Previsto	0,3	75%	25%	75%			6	5	4	4	4	4,5	1,25	3			1,35	0,38	0,9			• Seguridad Red telefónica		25%	25%			90%	0,03	4,5	0,94	2,25			0,135	0,0281	0,0675		
		Acceso No Autorizado	0,1		50%	75%			6	5	4	4	4		2,5	3				0,25	0,3			• Ubicaciones adecuadas			25%			90%	0,01		2,5	2,25				0,025	0,0225		
		Manipulación De Equipos	0,5	75%		75%			6	5	4	4	4	4,5		3			2,25		1,5				25%		25%			75%	0,125	3,38		2,25			0,4219		0,2813		
		Robo	0,1	100%		5%			6	5	4	4	4	6		0,2			0,6		0,02									75%	0,025	6		0,2			0,15		0,005		

REDES DE COMUNICACIONES [COM]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D'	I'	C'	A'	T'		F	D'	I'	C'	A'	T'	D'	I'	C'	A'	T'
COM1	Redes inalámbricas	Fallo Servicios De Comunicaciones	0,3	100%					7	8	9	9	8	7					2,1					• Controlar acceso • Definir perfiles de seguridad • Configuración de seguriad (dispositivo) • Manuales de administración e incidencias • Analisis de vulnerabilidades • Manuales de uso y acceso usuario • Registro de direccionamiento IP • Registro de Incidentes	50%					25%	0,225	3,5					0,7875				
		Errores De Administración	0,1	75%	25%	75%			7	8	9	9	8	5,25	2	6,75			0,53	0,2	0,68				50%	25%	90%			90%	0,01	2,63	1,5	0,68			0,0263	0,015	0,0068		
		Alteración Accidental De La Información	0,3		50%				7	8	9	9	8		4					1,2						25%				90%	0,03		3				0,09				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%					7	8	9	9	8	7					2,1						50%					75%	0,075	3,5					0,2625				
		Suplantación De La Identidad Del Usuario	0,7		50%	100%	100%		7	8	9	9	8		4	9	9			2,8	6,3	6,3				25%	50%	50%		90%	0,07		3	4,5	4,5			0,21	0,315	0,315		
		Abuso De Privilegios De Acceso	0,3	50%	50%	75%			7	8	9	9	8	3,5	4	6,75			1,05	1,2	2,03				75%	25%	50%			50%	0,15	0,88	3	3,38			0,1313	0,45	0,5063		
		Uso No Previsto	0,3	50%	25%	75%			7	8	9	9	8	3,5	2	6,75			1,05	0,6	2,03				50%		50%			50%	0,15	1,75	2	3,38			0,2625	0,3	0,5063		
		Acceso No Autorizado	0,5		50%	100%			7	8	9	9	8		4	9				2	4,5					25%	50%			75%	0,125		3	4,5				0,375	0,5625		
		Análisis De Trafico	0,1			100%			7	8	9	9	8			9					0,9						50%			50%	0,05			4,5					0,225		
		Interceptación De Información (Escucha)	0,1			100%			7	8	9	9	8			9					0,9						50%			50%	0,05			4,5					0,225		
		Modificación Deliberada De La Información	0,3		75%				7	8	9	9	8		6					1,8					25%					90%	0,03		4,5				0,135				
		Divulgación De Información	0,5			75%			7	8	9	9	8			6,75					3,38						50%			50%	0,25			3,38					0,8438		
		Denegación De Servicio	0,5	100%					7	8	9	9	8	7					3,5						75%					75%	0,125	1,75					0,2188				
COM2	Redes locales	Fallo Servicios De Comunicaciones	0,3	100%					8	8	9	9	8	8					2,4					• Controlar acceso • Definir perfiles de seguridad • Configuración de seguriad (dispositivo) • Manuales de administración e incidencias IDS-IPS • Analisis de vulnerabilidades • Manuales de uso y acceso usuario • Registro de direccionamiento IP • Registro de Incidencias	50%					25%	0,225	4					0,9				
		Errores De Administración	0,1	75%	50%	100%			8	8	9	9	8	6	4	9			0,6	0,4	0,9				50%	25%	90%			90%	0,01	3	3	0,9			0,03	0,03	0,009		
		Alteración Accidental De La Información	0,3		50%				8	8	9	9	8		4					1,2						25%				90%	0,03		3				0,09				
		Caída Del Sistema Por Agotamiento De Recursos	0,3	100%					8	8	9	9	8	8					2,4						50%					75%	0,075	4					0,3				
		Suplantación De La Identidad Del Usuario	0,5		75%	100%	100%		8	8	9	9	8		6	9	9			3	4,5	4,5				25%	50%	75%		90%	0,05		4,5	4,5	2,25			0,225	0,225	0,1125		
		Abuso De Privilegios De Acceso	0,3	50%	75%	100%			8	8	9	9	8	4	6	9			1,2	1,8	2,7				75%	25%	50%			50%	0,15	1	4,5	4,5			0,15	0,675	0,675		
		Uso No Previsto	0,3	50%	50%	100%			8	8	9	9	8	4	4	9			1,2	1,2	2,7				50%		50%			75%	0,075	2	4	4,5			0,15	0,3	0,3375		
		Acceso No Autorizado	0,5		50%	100%			8	8	9	9	8		4	9				2	4,5					25%	50%			75%	0,125		3	4,5				0,375	0,5625		
		Análisis De Trafico	0,1			100%			8	8	9	9	8			9					0,9						50%			50%	0,05			4,5					0,225		
		Interceptación De Información (Escucha)	0,1			100%			8	8	9	9	8			9					0,9						50%			50%	0,05			4,5					0,225		
		Modificación Deliberada De La Información	0,3		75%				8	8	9	9	8		6					1,8					25%					90%	0,03		4,5				0,135				
		Divulgación De Información	0,5			75%			8	8	9	9	8			6,75					3,38						50%			50%	0,25			3,38					0,8438		
		Denegación De Servicio	0,5	100%					8	8	9	9	8	8					4						75%					75%	0,125	2					0,25				
COM3	Red telefónica	Fallo Servicios De Comunicaciones	0,3	100%					8	7	8	7	8	8					2,4					• Manual de buenas prácticas para usuarios • Manuales de administración e incidencias • Configuraciones de seguridad • Registro telefónico de empleados • Registro de incidencias	50%					25%	0,225	4					0,9				
		Errores De Administración	0,1	75%	50%	75%			8	7	8	7	8	6	3,5	6			0,6	0,35	0,6				50%	25%	50%			90%	0,01	3	2,63	3			0,03	0,0263	0,03		
		Alteración Accidental De La Información	0,3		50%				8	7	8	7	8		3,5					1,05						25%				90%	0,03		2,63				0,0788				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	100%					8	7	8	7	8	8					0,8						50%					50%	0,05	4					0,2				
		Abuso De Privilegios De Acceso	0,5	50%	25%	75%			8	7	8	7	8	4	1,75	6			2	0,88	3				50%	25%	50%			25%	0,375	2	1,31	3			0,75	0,4922	1,125		
		Uso No Previsto	0,5	50%	25%	75%			8	7	8	7	8	4	1,75	6			2	0,88	3				50%	25%	50%			25%	0,375	2	1,31	3			0,75	0,4922	1,125		
		Acceso No Autorizado	0,3		25%	100%			8	7	8	7	8		1,75	8				0,53	2,4					25%	50%			25%	0,225		1,31	4				0,2953	0,9		
		Análisis De Trafico	0,1			100%			8	7	8	7	8			8					0,8						50%			25%	0,075			4					0,3		
		Interceptación De Información (Escucha)	0,1			100%			8	7	8	7	8			8					0,8						50%			25%	0,075			4					0,3		
		Modificación Deliberada De La Información	0,1		50%				8	7	8	7	8		3,5					0,35						25%				50%	0,05		2,63				0,1313				
		Divulgación De Información	0,3			75%			8	7	8	7	8			6					1,8						50%			25%	0,225			3					0,675		
		Denegación De Servicio	0,1	100%					8	7	8	7	8	8					0,8						25%					50%	0,05	6					0,3				
COM4	Red telefonía móvil	Fallo Servicios De Comunicaciones	0,3	100%					8	7	8	7	8	8					2,4					• Manual de buenas prácticas para usuarios • Manuales de administración e incidencias • Registro telefónico de empleados • Registro de incidencias • Servicio exterior						25%	0,225	8					1,8				
		Caída Del Sistema Por Agotamiento De Recursos	0,1	75%					8	7	8	7	8	6					0,6												0,1	6					0,6				
		Suplantación De La Identidad Del Usuario	0,1		5%	75%	75%		8	7	8	7	8		0,35	6	5,25			0,04	0,6	0,53					10%	10%			0,1		0,35	5,4	4,73			0,035	0,54	0,4725		
		Abuso De Privilegios De Acceso	0,3	5%	5%	50%			8	7	8	7	8	0,4	0,35	4			0,12	0,11	1,2				75%		10%			25%	0,225	0,1	0,35	3,6			0,0225	0,0788	0,81		
		Uso No Previsto	0,3	5%	5%	75%			8	7	8	7	8	0,4	0,35	6			0,12	0,11	1,8				75%		10%			25%	0,225	0,1	0,35	5,4			0,0225	0,0788	1,215		
		Acceso No Autorizado	0,3		5%	75%			8	7	8	7	8		0,35	6				0,11	1,8						10%			25%	0,225		0,35	5,4				0,0788	1,215		
		Análisis De Trafico	0,1			100%			8	7	8	7	8			8					0,8										0,1			8					0,8		
		Interceptación De Información (Escucha)	0,1			100%			8	7	8	7	8			8					0,8										0,1			8					0,8		
		Divulgación De Información	0,3			100%			8	7	8	7	8			8					2,4									50%	0,15			8					1,2		

ACTIVOS DE SOPORTES DE INFORMACIÓN [MEDIA]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D	I	C	A	T		F	D	I	C	A	T	D	I	C	A	T
MEDIA1	Discos duros externos	Daños Por Agua	0,3	100%					8	9	9	9	9	8					2,4											100%		8									
		Daños Por Agua	0,3	100%					8	9	9	9	9	8					2,4											100%		8									
		Avería De Origen Físico/Lógico	0,1	75%					8	9	9	9	9	6					0,6											50%	0,05	5,4					0,27				
		Degradación De Los Soportes De Almacenamiento De La Información	0,1	75%					8	9	9	9	9	6					0,6						10%					50%	0,05	5,4					0,27				
		Errores De Usuarios	0,3	25%	75%	100%			8	9	9	9	9	2	6,75	9			0,6	2,03	2,7					25%	100%			50%	0,15	2	5,06				0,3	0,7594				
		Errores De Administración	0,1	25%	75%	100%			8	9	9	9	9	2	6,75	9			0,2	0,68	0,9			• Protección criptográfica y de		50%	90%			90%	0,01	2	3,38	0,9			0,02	0,0338	0,009			
		Alteración Accidental De La Información	0,3		75%				8	9	9	9	9		6,75					2,03				acceso lógico y físico		10%				50%	0,15		6,08					0,9113				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8					• Establecer ubicaciones						50%	0,05	8					0,4					
		Fugas De Información	0,1		100%				8	9	9	9	9			9					0,9			adecuadas			100%			25%	0,075											
		Errores De Mantenimiento del soporte	0,3	25%					8	9	9	9	9	2					0,6					• Protección de acceso	10%					25%	0,225	1,8					0,405					
		Perdida del soporte	0,1	100%		100%			8	9	9	9	9	8		9			0,8		0,9			• Registro del dispositivo, uso e			100%			50%	0,05	8					0,4					
		Uso No Previsto	0,3	100%	100%	100%			8	9	9	9	9	8	9	9			2,4	2,7	2,7			incidentes	10%	25%	100%			75%	0,075	7,2	6,75				0,54	0,5063				
		Acceso No Autorizado	0,3		100%	100%			8	9	9	9	9		9	9				2,7	2,7			• Manual de uso del dispositivo		50%	100%			75%	0,075		4,5					0,3375				
		Modificación Deliberada De La Información	0,1		100%				8	9	9	9	9		9					0,9						25%				75%	0,025		6,75					0,1688				
		Destrucción De Información	0,1	100%					8	9	9	9	9	8					0,8											75%	0,025	8					0,2					
		Divulgación De Información	0,1			100%			8	9	9	9	9			9					0,9						100%			25%	0,075											
		Manipulación del soporte	0,3	50%		100%			8	9	9	9	9	4		9			1,2		2,7				10%		100%			50%	0,15	3,6					0,54					
		Robo	0,1	100%		100%			8	9	9	9	9	8		9			0,8		0,9						100%			25%	0,075	8					0,6					
MEDIA2	Pendrives USB	Daños Por Agua	0,1	100%					7	8	9	9	8	7					0,7											100%		7									
		Daños Por Agua	0,3	100%					7	8	9	9	8	7					2,1											100%		7									
		Avería De Origen Físico/Lógico	0,1	75%					7	8	9	9	8	5,25					0,53						10%					50%	0,05	4,73					0,2363				
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	75%					7	8	9	9	8	5,25					1,58						10%					50%	0,15	4,73					0,7088				
		Errores De Usuarios	0,5	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,88	2	4,5			• Protección criptográfica y de	10%	25%	100%			50%	0,25	1,58	3				0,3938	0,75				
		Errores De Administración	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9			acceso lógico y físico	10%	50%	100%			90%	0,01	1,58	2				0,0158	0,02				
		Alteración Accidental De La Información	0,5		100%				7	8	9	9	8		8					4				• Manual de uso del dispositivo		10%				50%	0,25		7,2					1,8				
		Destrucción De Información	0,5	100%					7	8	9	9	8	7					3,5					• Registro de la entrega e						50%	0,25	7					1,75					
		Fugas De Información	0,3			100%			7	8	9	9	8			9					2,7			incidentes			100%			25%	0,225											
		Errores De Mantenimiento del soporte	0,1	50%					7	8	9	9	8	3,5					0,35					• Establecer ubicaciones	10%						0,1	3,15					0,315				
		Perdida del soporte	0,7	100%		100%			7	8	9	9	8	7		9			4,9		6,3			adecuadas			100%			25%	0,525	7					3,675					
		Uso No Previsto	0,7	75%	100%	100%			7	8	9	9	8	5,25	8	9			3,68	5,6	6,3			• Copias de seguridad de	10%	25%	100%			50%	0,35	4,73	6				1,6538	2,1				
		Acceso No Autorizado	0,1		100%	100%			7	8	9	9	8		8	9				0,8	0,9			información crucial		50%	100%			75%	0,025		4					0,1				
		Modificación Deliberada De La Información	0,1		100%				7	8	9	9	8		8					0,8				• Limpieza de contenidos		25%				75%	0,025		6					0,15				
		Destrucción De Información	0,1	100%					7	8	9	9	8	7					0,7					• Destrucción de soportes	25%					75%	0,025	5,25					0,1313					
		Divulgación De Información	0,3			100%			7	8	9	9	8			9					2,7						100%			25%	0,225											
		Manipulación del soporte	0,1	75%		100%			7	8	9	9	8	5,25		9			0,53		0,9				10%		100%			50%	0,05	4,73					0,2363					
		Robo	0,3	100%		100%			7	8	9	9	8	7		9			2,1		2,7						100%			25%	0,225	7					1,575					
MEDIA3	CD/DVD	Daños Por Agua	0,1	100%					7	8	9	9	8	7					0,7											100%		7									
		Daños Por Agua	0,3	100%					7	8	9	9	8	7					2,1											100%		7									
		Avería De Origen Físico/Lógico	0,1	75%					7	8	9	9	8	5,25					0,53											25%	0,075	4,73					0,3544				
		Degradación De Los Soportes De Almacenamiento De La Información	0,3	75%					7	8	9	9	8	5,25					1,58						10%					25%	0,225	4,73					1,0631				
		Errores De Usuarios	0,5	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,88	2	4,5			• Protección criptográfica y acceso	10%	25%	100%			50%	0,25	1,58	3				0,3938	0,75				
		Errores De Administración	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9			lógico y físico	10%	50%	100%			90%	0,01	1,58	2				0,0158	0,02				
		Alteración Accidental De La Información	0,5		100%				7	8	9	9	8		8					4				• Manual de uso del dispositivo		10%				50%	0,25		7,2					1,8				
		Destrucción De Información	0,5	100%					7	8	9	9	8	7					3,5					• Registro de la entrega e						50%	0,25	7					1,75					
		Fugas De Información	0,3			100%			7	8	9	9	8			9					2,7			incidentes			100%			25%	0,225											
		Errores De Mantenimiento del soporte	0,1	50%					7	8	9	9	8	3,5					0,35					• Establecer ubicaciones	10%					50%	0,05	3,15					0,1575				
		Perdida del soporte	0,7	100%		100%			7	8	9	9	8	7		9			4,9		6,3			adecuadas			90%			25%	0,525	7		0,9			3,675		0,4725			
		Uso No Previsto	0,7	75%	100%	100%			7	8	9	9	8	5,25	8	9			3,68	5,6	6,3			• Copias de seguridad de	10%	25%	100%			50%	0,35	4,73	6				1,6538	2,1				
		Acceso No Autorizado	0,1		100%	100%			7	8	9	9	8		8	9				0,8	0,9			información confidencial		50%	100%			50%	0,05		4					0,2				
		Modificación Deliberada De La Información	0,1		100%				7	8	9	9	8		8					0,8				• Destrucción de soportes y		25%				50%	0,05		6					0,3				
		Destrucción De Información	0,1	100%					7	8	9	9	8	7					0,7					cambio de almacenamiento de	25%					50%	0,05	5,25					0,2625					
		Divulgación De Información	0,3			100%			7	8	9	9	8			9					2,7			información			100%			25%	0,225											
		Manipulación del soporte	0,1	75%		100%			7	8	9	9	8	5,25		9			0,53		0,9				10%		100%			50%	0,05	4,73					0,2363					
		Robo	0,3	100%		100%			7	8	9	9	8	7		9			2,1		2,7						90%			25%	0,225	7		0,9			1,575		0,2025			
MEDIA4	Material impreso	Daños Por Agua	0,1	100%					7	8	9	9	9	7					0,7											100%		7									
		Daños Por Agua	0,1	100%					7	8	9	9	9	7					0,7											100%		7									
		Degradación por Almacenamiento	0,3	75%					7	8	9	9	9	5,25					1,58						75%					75%	0,075	1,31					0,0984				
		Errores De Usuarios	0,5	50%	75%	75%			7	8	9	9	9	3,5	6	6,75			1,75	3	3,38				25%	25%	75%			50%	0,25	2,63	4,5	1,69			0,6563	1,125	0,4219			
		Errores De Administración	0,1	50%	75%	75%			7	8	9	9	9	3,5	6	6,75			0,35	0,6	0,68				25%	25%	75%			50%	0,05	2,63	4,5	1,69			0,1313	0,225	0,0844			
		Alteración Accidental De La Información	0,5		50%				7	8	9	9	9		4					2				• Establecer ubicaciones		25%				25%	0,375		3					1,125				
		Destrucción	0,5	100%					7	8	9	9	9	7					3,5					adecuadas	50%					25%	0,375	3,5					1,3125					
		Fugas De Información	0,1			100%			7	8	9	9	9			9					0,9			• Manual de uso de información			25%				0,1			6,75					0,675				
		Errores De Almacenamiento	0,5	50%					7	8	9	9	9	3,5					1,75					confidencial, establecer	50%					25%	0,375	1,75					0,6563					
		Perdida	0,5	50%		100%			7	8	9	9	9	3,5		9			1,75		4,5			respondables	75%		10%			75%	0,125	0,88		8,1			0,1094		1,0125			
		Uso No Previsto	0,3	100%	75%	100%			7	8	9	9	9	7	6	9			2,1	1,8	2,7			• Digitalización	75%	25%	50%			50%	0,15	1,75	4,5	4,5			0,2625	0,675	0,675			
		Acceso No Autorizado	0,3		75%	100%			7	8	9	9	9		6	9				1,8	2,7			• Destrucción		25%	25%			50%	0,15		4,5	6,75				0,675	1,0125			
		Modificación Deliberada De La Información	0,1		100%				7	8	9	9	9		8					0,8						25%				25%	0,075		6					0,45				
		Destrucción	0,1	100%					7	8	9	9	9	7					0,7						75%					75%	0,025	1,75					0,0438					
		Divulgación	0,1			100%			7	8	9	9	9			9					0,9						25%			25%	0,075			6,75					0,5063			
		Manipulación	0,1	50%		100%			7	8	9	9	9	3,5		9			0,35		0,9				75%		25%			50%	0,05	0,88		6,75			0,0438		0,3375			
		Robo	0,3	50%		100%			7	8	9	9	9	3,5		9			1,05		2,7				75%					75%	0,075	0,88		9			0,0656		0,675			

ACTIVOS DE EQUIPAMIENTO AUXILIARES [AUX]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenaza	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D	I	C	A	T	Frecuencia	F	D	I	C	A	T	D	I	C	A	T
AUX1	Generador eléctrico	Daños Por Agua	0,3	75%					5	5	3	4	4	3,75					1,13					• Establecer y señalizar ubicaciones adecuadas • Mantenimiento periódico, uso exclusivo del personal técnico • Registro de uso, cambios e incidentes						90%	0,03	3,75					0,1125				
		Fuego	0,1	75%					5	5	3	4	4	3,75					0,38											75%	0,025	3,75					0,0938				
		Daños Por Agua	0,3	75%					5	5	3	4	4	3,75					1,13											75%	0,075	3,75					0,2813				
		Contaminación Mecánica	0,1	50%					5	5	3	4	4	2,5					0,25						75%					25%	0,075	0,63					0,0469				
		Degradación por almacenamiento	0,3	50%					5	5	3	4	4	2,5					0,75						75%					50%	0,15	0,63					0,0938				
		Avería De Origen Físico/ Lógico	0,3	75%					5	5	3	4	4	3,75					1,13						75%					50%	0,15	0,94					0,1406				
		Errores De Mantenimiento/ Actualización De Equipos	0,1	75%					5	5	3	4	4	3,75					0,38						75%					75%	0,025	0,94					0,0234				
		Uso No Previsto	0,3	75%	25%	5%			5	5	3	4	4	3,75	1,25	0,15			1,13	0,38	0,05				50%	50%				25%	0,225	1,88	0,63	0,15			0,4219	0,1406	0,0338		
		Acceso No Autorizado	0,3		25%	5%			5	5	3	4	4		1,25	0,15				0,38	0,05					50%				25%	0,225		0,63	0,15				0,1406	0,0338		
		Manipulación De Equipos	0,3	75%		5%			5	5	3	4	4	3,75		0,15			1,13		0,05				50%					25%	0,225	1,88		0,15			0,4219		0,0338		
AUX2	Fuentes de alimentación	Daños Por Agua	0,3	75%					5	7	3	4	4	3,75					1,13											90%	0,03	3,75					0,1125				
		Fuego	0,1	75%					5	7	3	4	4	3,75					0,38											75%	0,025	3,75					0,0938				
		Daños Por Agua	0,3	75%					5	7	3	4	4	3,75					1,13											75%	0,075	3,75					0,2813				
		Contaminación Mecánica	0,1	50%					5	7	3	4	4	2,5					0,25						75%					25%	0,075	0,63					0,0469				
		Degradación por almacenamiento	0,3	50%					5	7	3	4	4	2,5					0,75					• Registro del equipo, uso, cambios e incidentes • Establecer ubicaciones adecuadas • Mantenimiento periódico, uso exclusivo del personal técnico	75%					50%	0,15	0,63					0,0938				
		Avería De Origen Físico/ Lógico	0,3	75%					5	7	3	4	4	3,75					1,13						75%					50%	0,15	0,94					0,1406				
		Corte De Suministro Eléctrico	0,3	100%					5	7	3	4	4	5					1,5												0,3	5					1,5				
		Errores De Mantenimiento/ Actualización De Equipos	0,3	75%					5	7	3	4	4	3,75					1,13						75%					75%	0,075	0,94					0,0703				
		Perdida De Equipos	0,1	100%		5%			5	7	3	4	4	5		0,15			0,5		0,02									25%	0,075	5		0,15			0,375		0,0113		
		Uso No Previsto	0,3	100%	25%	5%			5	7	3	4	4	5	1,75	0,15			1,5	0,53	0,05				50%	50%	25%			25%	0,225	2,5	0,88	0,11			0,5625	0,1969	0,0253		
		Acceso No Autorizado	0,3		25%	5%			5	7	3	4	4		1,75	0,15				0,53	0,05				25%	50%				25%	0,225		0,88	0,15				0,1969	0,0338		
		Manipulación De Equipos	0,3	75%		5%			5	7	3	4	4	3,75		0,15			1,13		0,05				50%		25%			25%	0,225	1,88		0,11			0,4219		0,0253		
		Robo	0,1	100%		5%			5	7	3	4	4	5		0,15			0,5		0,02									25%	0,075	5		0,15			0,375		0,0113		
AUX3	Climatización	Daños Por Agua	0,3	75%					5	4	3	4	4	3,75					1,13											90%	0,03	3,75					0,1125				
		Fuego	0,1	75%					5	4	3	4	4	3,75					0,38											75%	0,025	3,75					0,0938				
		Daños Por Agua	0,3	75%					5	4	3	4	4	3,75					1,13											75%	0,075	3,75					0,2813				
		Contaminación Mecánica	0,1	50%					5	4	3	4	4	2,5					0,25						75%					75%	0,025	0,63					0,0156				
		Avería De Origen Físico/Lógico	0,3	75%					5	4	3	4	4	3,75					1,13					• Mantenimiento periódico • Establecer ubicaciones adecuadas • Registro de Incidentes	75%					50%	0,15	0,94					0,1406				
		Corte De Suministro Eléctrico	0,3	100%					5	4	3	4	4	5					1,5												0,3	5					1,5				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					5	4	3	4	4	3,75					1,13						75%					75%	0,075	0,94					0,0703				
		Uso No Previsto	0,3	50%	25%	5%			5	4	3	4	4	2,5	1	0,15			0,75	0,3	0,05				50%	50%				25%	0,225	1,25	0,5	0,15			0,2813	0,1125	0,0338		
		Acceso No Autorizado	0,3		25%	5%			5	4	3	4	4		1	0,15				0,3	0,05					50%				10%	0,27		0,5	0,15				0,135	0,0405		
		Manipulación De Equipos	0,5	50%		5%			5	4	3	4	4	2,5		0,15			1,25		0,08				50%					25%	0,375	1,25		0,15			0,4688		0,0563		
AUX4	Cableado UTP	Daños Por Agua	0,3	75%					7	8	4	4	4	5,25					1,58											90%	0,03	5,25					0,1575				
		Fuego	0,1	100%					7	8	4	4	4	7					0,7											75%	0,025	7					0,175				
		Daños Por Agua	0,3	75%					7	8	4	4	4	5,25					1,58					• Mantenimiento periódico • uso exclusivo del personal técnico • Registro de uso, cambios e incidentes						75%	0,075	5,25					0,3938				
		Avería De Origen Físico/Lógico	0,3	75%					7	8	4	4	4	5,25					1,58						75%					50%	0,15	1,31					0,1969				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					7	8	4	4	4	5,25					1,58						75%					75%	0,075	1,31					0,0984				
		Uso No Previsto	0,3	50%	25%	25%			7	8	4	4	4	3,5	2	1			1,05	0,6	0,3				25%	25%	25%			50%	0,15	2,63	1,5	0,75			0,3938	0,225	0,1125		
		Acceso No Autorizado	0,1		25%	75%			7	8	4	4	4		2	3				0,2	0,3					25%	25%			25%	0,075		1,5	2,25				0,1125	0,1688		
		Manipulación De Equipos	0,1	50%		75%			7	8	4	4	4	3,5		3			0,35		0,3				25%		25%			25%	0,075	2,63		2,25			0,1969		0,1688		
AUX5	Armarios	Daños Por Agua	0,3	50%					8	8	8	8	8	4					1,2											90%	0,03	3,6					0,108				
		Fuego	0,1	75%					8	8	8	8	8	6					0,6					• Protección física • Mantenimiento periodico, uso exclusivo del personal técnico • Registro de uso, cambios e incidentes • Establecer ubicaciones adecuadas	10%					75%	0,025	5,4					0,135				
		Daños Por Agua	0,3	50%					8	8	8	8	8	4					1,2						10%					75%	0,075	3,6					0,27				
		Degradación por almacenamiento	0,1	25%					8	8	8	8	8	2					0,2						75%					75%	0,025	0,5					0,0125				
		Avería De Origen Físico/Lógico	0,3	50%					8	8	8	8	8	4					1,2						75%					75%	0,075	1					0,075				
		Uso No Previsto	0,3	25%	25%	75%			8	8	8	8	8	2	2	6			0,6	0,6	1,8					25%	75%			90%	0,03	2	1,5	1,5			0,06	0,045	0,045		
		Acceso No Autorizado	0,3		25%	75%			8	8	8	8	8		2	6				0,6	1,8					25%	75%			90%	0,03		1,5	1,5				0,045	0,045		
		Manipulación De Equipos	0,5	25%		75%			8	8	8	8	8	2		6			1		3				50%		75%			90%	0,05	1		1,5			0,05		0,075		
AUX6	Cajas fuertes	Daños Por Agua	0,1	25%					8	8	9	9	9	2					0,2						25%					90%	0,01	1,5					0,015				
		Fuego	0,1	25%					8	8	9	9	9	2					0,2						25%					90%	0,01	1,5					0,015				
		Daños Por Agua	0,1	25%					8	8	9	9	9	2					0,2					• Uso exclusivo de personal autorizado, protección de acceso y física • Establecer ubicaciones adecuadas • Mantenimiento periódico • Registro de Incidentes	25%					90%	0,01	1,5					0,015				
		Avería De Origen Físico/Lógico	0,1	75%					8	8	9	9	9	6					0,6						50%					75%	0,025	3					0,075				
		Corte De Suministro Eléctrico	0,1	75%					8	8	9	9	9	6					0,6						50%					50%	0,05	3					0,15				
		Errores De Mantenimiento/Actualización De Equipos	0,3	75%					8	8	9	9	9	6					1,8						50%					90%	0,03	3					0,09				
		Perdida De Equipos	0,1	100%		100%			8	8	9	9	9	8		9			0,8		0,9				50%		80%			90%	0,01	4		1,8			0,04		0,018		
		Uso No Previsto	0,1	75%	5%	100%			8	8	9	9	9	6	0,4	9			0,6	0,04	0,9				50%	75%	80%			90%	0,01	3	0,1	1,8			0,03	0,001	0,018		
		Acceso No Autorizado	0,3		5%	100%			8	8	9	9	9		0,4	9				0,12	2,7					75%	80%			90%	0,03		0,1	1,8				0,003	0,054		
		Manipulación De Equipos	0,5	25%		100%			8	8	9	9	9	2		9			1		4,5				50%		80%			90%	0,05	1		1,8			0,05		0,09		

ACTIVOS DE INSTALACIONES [L]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D	I	C	A	T		F'	D	I	C	A	T	D	I	C	A	T
L1	Edificios	Fuego	0,1	100%					6	7	8	6	5	6					0,6					• Control de los accesos físicos • Determinación y señalización de puntos vulnerables a daños físicos • Establecer manuales de uso de las instalaciones • Registro de Incidentes	50%					50%	0,05	3					0,15				
		Daños Por Agua	0,3	75%					6	7	8	6	5	4,5					1,35						50%					50%	0,15	2,25					0,3375				
		Fuego	0,1	75%					6	7	8	6	5	4,5					0,45						50%					50%	0,05	2,25					0,1125				
		Daños Por Agua	0,3	50%					6	7	8	6	5	3					0,9						50%					50%	0,15	1,5					0,225				
		Fugas De Información	0,3			75%			6	7	8	6	5			6					1,8					50%				25%	0,225			3				0,675			
		Uso No Previsto	0,1	25%	25%	75%			6	7	8	6	5	1,5	1,75	6			0,15	0,175	0,6				50%	75%	25%			25%	0,075	0,75	0,438	4,5			0,0563	0,0328	0,3375		
		Acceso No Autorizado	0,3		25%	100%			6	7	8	6	5		1,75	8				0,525	2,4					25%	50%			25%	0,225		1,313	4				0,2953	0,9		
L2	Cuartos servidores	Fuego	0,1	100%					8	8	8	8	7	8					0,8					• Protección física • Control de los accesos físicos • Establecer manuales de uso de las instalaciones • Determinación y señalización de puntos vulnerables a daños físicos • Registro de Incidentes	50%					50%	0,05	4					0,2				
		Daños Por Agua	0,1	100%					8	8	8	8	7	8					0,8						50%					50%	0,05	4					0,2				
		Fuego	0,1	100%					8	8	8	8	7	8					0,8						50%					50%	0,05	4					0,2				
		Daños Por Agua	0,3	100%					8	8	8	8	7	8					2,4						50%					50%	0,15	4					0,6				
		Fugas De Información	0,1			100%			8	8	8	8	7			8					0,8						25%			25%	0,075			6				0,45			
		Uso No Previsto	0,3	75%	75%	75%			8	8	8	8	7	6	6	6			1,8	1,8	1,8				50%	75%	50%			25%	0,225	3	1,5	3			0,675	0,3375	0,675		
		Acceso No Autorizado	0,3		50%	100%			8	8	8	8	7		4	8				1,2	2,4					25%	50%			25%	0,225		3	4				0,675	0,9		
L3	Coche	Daños mecánicos	0,1	100%					2	5	3	5	2	2					0,2					• Riesgos asumibles							0,1	2					0,2				
		Accidente de tránsito	0,1	100%					2	5	3	5	2	2					0,2												0,1	2					0,2				

ACTIVOS DE PERSONAL [P]			Frecuencia	Degradación					Valor del Activo					Impacto					Riesgo					Salvaguardas	Efectividad de las Salvaguardas					Efectividad de Frecuencia	Frecuencia Residual	Impacto Residual					Riesgo Residual				
Código	Nombre	Amenazas	F	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T	D	I	C	A	T		D	I	C	A	T		F´	D	I	C	A	T	D	I	C	A	T
P1	Administradores	Fugas De Información	0,1			100%			8	8	9	9	9			9					0,9							50%				50%	0,05			4,5				0,225			
		Indisponibilidad Del Personal	0,3	75%					8	8	9	9	9	6					1,8					• Capacitación del personal • Actualizar manuales o guías	50%						0,3	3					0,9				
		Indisponibilidad Del Personal	0,1	75%					8	8	9	9	9	6					0,6						50%						0,1	3					0,3				
		Extorsión	0,1	25%	75%	100%			8	8	9	9	9	2	6	9			0,2	0,6	0,9				50%	50%	50%			25%	0,075	1	3	4,5			0,075	0,225	0,3375		
		Ingeniería Social	0,1	25%	75%	100%			8	8	9	9	9	2	6	9			0,2	0,6	0,9				50%	50%	50%			25%	0,075	1	3	4,5			0,075	0,225	0,3375		
P2	Técnicos	Fugas De Información	0,1			100%			7	8	9	9	8			9					0,9							50%				50%	0,05			4,5				0,225			
		Indisponibilidad Del Personal	0,3	50%					7	8	9	9	8	3,5					1,05					• Capacitación del personal	50%						0,3	1,75					0,525				
		Indisponibilidad Del Personal	0,1	50%					7	8	9	9	8	3,5					0,35					• Actualizar manuales o guías	50%						0,1	1,75					0,175				
		Extorsión	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9			• Concientización	50%	50%	50%			25%	0,075	0,88	2	4,5			0,0656	0,15	0,3375		
		Ingeniería Social	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9				50%	50%	50%			25%	0,075	0,88	2	4,5			0,0656	0,15	0,3375		
P3	Empleados	Fugas De Información	0,1			100%			7	8	9	9	8			9					0,9							50%				50%	0,05			4,5				0,225			
		Indisponibilidad Del Personal	0,3	50%					7	8	9	9	8	3,5					1,05						50%						0,3	1,75					0,525				
		Indisponibilidad Del Personal	0,1	50%					7	8	9	9	8	3,5					0,35					• Capacitación del personal	50%						0,1	1,75					0,175				
		Extorsión	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9			• Actualizar manuales o guías	50%	50%	50%			25%	0,075	0,88	2	4,5			0,0656	0,15	0,3375		
		Ingeniería Social	0,1	25%	50%	100%			7	8	9	9	8	1,75	4	9			0,18	0,4	0,9			• Concientización	50%	50%	50%			25%	0,075	0,88	2	4,5			0,0656	0,15	0,3375		
P4	Usuarios	Fugas De Información	0,3			100%			5	6	9	9	5			9					2,7							50%				50%	0,15			4,5				0,675			
		Extorsión	0,1	25%	50%	100%			5	6	9	9	5	1,25	3	9			0,13	0,3	0,9				50%	50%	50%			25%	0,075	0,63	1,5	4,5			0,0469	0,1125	0,3375		
		Ingeniería Social	0,1	25%	50%	100%			5	6	9	9	5	1,25	3	9			0,13	0,3	0,9			• Capacitación del personal • Actualizar manuales o guías • Concientización	50%	50%	50%			25%	0,075	0,63	1,5	4,5			0,0469	0,1125	0,3375		

[D] Datos / Información	
[files]	ficheros
[backup]	copias de respaldo
[conf]	datos de configuración
[int]	datos de gestión interna
[password]	credenciales
[auth]	datos de validación de credenciales
[acl]	datos de control de acceso
[log]	registro de actividad
[source]	código fuente
[exe]	código ejecutable
[test]	datos de prueba
[S] Servicios	
[anon]	anónimo (sin requerir identificación del usuario)
[pub]	al público en general (sin relación contractual)
[ext]	a usuarios externos (bajo una relación contractual)
[int]	interno (a usuarios de la propia organización)
[www]	world wide web
[telnet]	acceso remoto a cuenta local
[email]	correo electrónico
[file]	almacenamiento de ficheros
[ftp]	transferencia de ficheros
[edi]	intercambio electrónico de datos
[dir]	servicio de directorio (1)
[idm]	gestión de identidades (2)
[ipm]	gestión de privilegios
[pki]	PKI - infraestructura de clave pública (3)
[COM] Redes de comunicaciones	
[PSTN]	red telefónica
[ISDN]	rdsi (red digital)
[X25]	X25 (red de datos)
[ADSL]	ADSL
[pp]	punto a punto
[radio]	comunicaciones radio
[wifi]	red inalámbrica
[mobile]	telefonía móvil
[sat]	por satélite
[LAN]	red local
[MAN]	red metropolitana
[Internet]	Internet
[P] Personal	
[ue]	usuarios externos
[ui]	usuarios internos
[op]	operadores
[adm]	administradores de sistemas
[com]	administradores de comunicaciones
[dba]	administradores de BBDD
[sec]	administradores de seguridad
[des]	desarrolladores / programadores
[sub]	subcontratas
[prov]	proveedores

[SW] Software - Aplicaciones informáticas	
[prp]	desarrollo propio (in house)
[sub]	desarrollo a medida (subcontratado)
[std]	estándar (off the shelf)
[browser]	navegador web
[www]	servidor de presentación
[app]	servidor de aplicaciones
[email_client]	cliente de correo electrónico
[email_server]	servidor de correo electrónico
[file]	servidor de ficheros
[dbms]	sistema de gestión de bases de datos
[tm]	monitor transaccional
[office]	ofimática
[av]	anti virus
[os]	sistema operativo
[hypervisor]	gestor de máquinas virtuales
[ts]	servidor de terminales
[backup]	sistema de backup
[HW] Equipos Informáticos (Hardware)	
[host]	grandes equipos
[mid]	equipos medios
[pc]	informática personal
[pda]	informática móvil
[pda]	agendas electrónica
[vhost]	equipo vitual
[backup]	equipamiento de respaldo
[peripheral]	periféricos
[print]	medios de impresión
[scan]	escámeres
[crypto]	dispositivos criptográficos
[bp]	dispositivo de frontera
[network]	soporte de la red
[modem]	módems
[hub]	concentradores
[switch]	conmutadores
[router]	encaminadores
[bridge]	pasarelas
[firewall]	cortafuegos
[wap]	punto de acceso inalámbrico
[pabx]	centralita telefónica
[ipphone]	teléfono IP
[MEDIA] Soportes de Información	
[electronic]	electrónicos
[disk]	discos
[vdisk]	discos virtuales
[san]	almacenamiento en red
[disquette]	disquetes
[cd]	cederrón (CD-ROM)
[usb]	memorias USB
[dvd]	DVD
[tape]	cinta magnética
[mc]	tarjetas de memoria
[ic]	tarjetas inteligentes
[non_electronic]	no electrónicos
[printed]	material impreso
[tape]	cinta de papel
[film]	microfilm
[cards]	tarjetas perforadas
[AUX] Equipamiento Auxiliar	
[power]	fuentes de alimentación
[ups]	sistemas de alimentación ininterrumpida
[gen]	generadores eléctricos
[ac]	equipos de climatización
[cabling]	cableado
[wire]	cable eléctrico
[fiber]	fibra óptica
[robot]	robots
[tape]	... de cintas
[disk]	... de discos
[supply]	suministros esenciales
[destroy]	equipod de destruccion de soportes de información
[furniture]	mobiliario: armarios, etc
[safe]	cajas fuertes
[L] Instalaciones	
[site]	recinto
[building]	edificio
[local]	cuarto
[mobile]	plataformas móviles
[car]	vehículo terrestre: coche, camión,etc.
[plane]	vehículo aéreo: avión, etc
[ship]	vehículo marítimo: buque, lancha, etc.
[shelter]	contenedores
[channel]	canalización
[backup]	instalaciones de respaldo

protección de los datos/información
protección de la información
copias de seguridad de los datos (Backup)
Aseguramiento de la integridad
Cifrado de la información
Uso de firmas electrónicas
Uso de servicios de fechado electrónico

protección de los servicios
protección de los servicio
aseguramiento de la disponibilidad
aceptación y pues en operación
se aplican perfiles de seguridad
explotación
gestión de cambios (mejoras y sustituciones)
Terminación
protección de servicios y aplicaciones web
protección del correo electrónico
protección del directorios
protección del servidor de nombres de dominio (DNS)
Teletrabajo
Voz sobre IP

Protección de las aplicaciones (software)
protección de las aplicaciones informáticas
copias de seguridad
puesta en producción
se aplican perfiles de seguridad
explotación /producción
cambios (actualizaciones y mantenimiento)
Terminación

Protección de los equipos (hardware)
Protección de os Equipos informáticos
puesta en producción
Se aplican perfiles de Seguridad
Aseguramiento de la disponibilidad
Operación
cambios (actualizaciones y mantenimiento)
Terminación
Informática móvil
Reproducción de documentos
Protección de la centralita Telefónica

Protección de las comunicaciones
Protección de las comunicaciones
entrada en servicio
se aplican perfiles de seguridad
aseguramiento de la disponibilidad
Autenticación del canal
Protección de la integridad de los datos intercambiados
Protección criptográfica de la confidencialidad de lis datos intercambiados
Operación
cambios (actualizaciones y mantenimiento)
Terminación
Internet: uso de?, acceso a
Seguridad Wireless (WIFI)
Telefonía móvil
Segregación de las redes en dominios

Protección en los puntos de interconexión con otros sistemas
Puntos de interconexión, conexión entre zonas de confianza
Sistema de protección perimetral
Protección de los equipos de frontera

Protección de los soportes de información
Protección de los Soportes de Información
Aseguramiento de la disponibilidad
Protección criptográfica del contenido
Limpieza de contenido
Destrucción de soportes

Protección de los elementos Auxiliares
Elementos Auxiliares
Aseguramiento de la disponibilidad
Instalación
Suministro eléctrico
Climatización
Protección del cableado

Seguridad Física -Protección de las Instalaciones
Protección de las instalaciones
Diseño
Defensa en profundidad
Control de los accesos físicos
Aseguramiento de la disponibilidad
Terminación

Salvaguardas relativas al personal
Gestión del personal
Formación y consideración

protecciones generales u horizontales
protecciones generales
identificación y autentificación
control de acceso lógico
segregación de tareas
gestión de incidencias
herramientas de seguridad
herramienta contra código dañino
IDS/IPS: Herramienta de detección y prevención de intrusos
herramienta de chequeo de configuración
herramienta de análisis de vulnerabilidades
herramienta de monitorización de trafico
DLP; herramienta de monitorización de contenidos
Herramienta para análisis de logs
Honey net/Honeypot
Verificación de las funciones de seguridad
gestión de vulnerabilidades
registro y auditoria

Salvaguardas de tipo organizativo
Organización
Gestión de riesgos
Planificación de la seguridad
Inspecciones de seguridad

Continuidad de las operaciones
Continuidad del negocio
Análisis de impacto (BIA)
Plan de Recuperación de desastres (DRP)

Externalización
Relaciones externas
Acuerdos para intercambio de información y software
Acceso externo
Servicios proporcionados por otras organizaciones
Personal subcontratado

Adquisición y desarrollo
Adquisición y desarrollo
Servicios: Adquisición o desarrollo
Equipos: Adquisición o desarrollo
Comunicaciones: Adquisición o desarrollo
Soportes de Información: Adquisición o desarrollo
Productos certificados o acreditados

SLA: nivel de servicios, si la disponibilidad es un valor
NDA: compromiso de secreto, si la confidencialidad es un valor
Identificación y calificación del personal encargado
Procedimientos de escalado y resolución de incidencias
Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
Asunción de responsabilidades y penalizaciones por incumplimiento