Escuela Politécnica Superior

Desarrollo del plan director de seguridad para un bufete de abogados

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:
Agustín Peco Moreno

Tutor/es:
Jose Vicente Berna Martínez

Septiembre 2019

Universitat d'Alacant
Universidad de Alicante

Resumen

En este proyecto se aborda el análisis y desarrollo de un Sistema de Gestión de la Seguridad de la Información en un despacho de abogados en el que previamente no se había implantado ninguna medida. Para llevar a cabo este SGSI utilizaremos la metodología MAGERIT en la que estudiaremos punto por punto cómo obtener un catálogo de activos de la empresa, ver las amenazas a las que están expuestos y en base a la valoración de los activos y a la probabilidad de suceso de amenazas, realizar un análisis del riesgo que acumulan para posteriormente tomar decisiones y realizar acciones que disminuyan este riesgo hasta unos valores aceptables.

Una vez hayamos aprendido la metodología MAGERIT la pondremos en práctica para analizar el estado actual del SGSI en el despacho de abogados y realizar el análisis de riesgos para diseñar un plan director de seguridad que nos permita poner en práctica varios proyectos que disminuirán el riesgo de los activos del despacho. Previamente analizaremos mediante un diagrama DAFO un estudio de viabilidad que nos permita orientarnos ante la decisión de llevar a cabo este proyecto y la relación coste/beneficio que podemos obtener.

Realizaremos además a modo de consulta una posible certificación ISO 27001 para conocer qué requisitos sería necesario cumplir y qué pasos se deberían seguir para obtenerla.

Motivación, justificación y objetivo general

Actualmente la “ciberseguridad” o seguridad de la información parece estar reservado o destinado a las grandes empresas. Si bien es cierto que éstas son las que más ataques pueden sufrir o las que pueden ser mayor objetivo de otras empresas o gobiernos que quieran realizarles ataques de cualquier índole, no por eso la pequeñas y medianas empresas deben estar exentas de un plan de seguridad de la información.

La mayoría de pequeñas y medianas empresas tienen un desconocimiento general de las amenazas y riesgos que pueden sufrir sus datos debido precisamente a que carecen de este plan de seguridad. Muchas veces tampoco saben cómo llevarlo a cabo o carecen del personal adecuado para poder implementar uno. En este aspecto puede ser útil la visión de la subcontratación de servicios, ya que se puede considerar la “ciberseguridad” como un servicio más que se puede contratar a una tercera empresa externa para su implementación.

De esta idea surge este proyecto. Lo que pretendo desarrollar aquí es la realización de un plan director de seguridad para un bufete de abogados que conozco personalmente y que carece completamente de medidas de seguridad frente a los datos que almacena. Esto, además de los posibles riesgos de pérdida o robo de datos inherente a la carencia de seguridad, también puede acarrear sanciones económicas debido a que profesiones como la abogacía deben garantizar la no divulgación o filtración de información relativa a los casos que representan.

Con la realización de este proyecto podré poner en práctica habilidades aprendidas en las distintas asignaturas del máster tales como conceptos de Sistemas de gestión de la seguridad, Seguridad en las comunicaciones, Seguridad en Sistemas Operativos, etc… Además de la experiencia de la implantación real de un plan de seguridad en una empresa como es este despacho de abogados.

Dedicatoria

A mi padre (D.E.P.)

Agradecimientos

A mis padres por insistir en mi educación y por enseñarme literalmente el significado de no rendirse nunca.

A mi esposa Alejandra y a mi hija Paula por regalarme mucha parte de su tiempo para que pudiera realizar este Máster y por la comprensión y paciencia que han demostrado.

Citas

“Una persona inteligente se repone pronto de un fracaso. Un mediocre jamás se recupera de un éxito.” — Lucio Anneo Seneca

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

El bufete “CC-Abogados” es un despacho de abogados ubicado en el centro de Alicante que lleva principalmente asuntos de naturaleza civil y mercantil. Está dirigido por D. Gonzalo Calderón Chao abogado de Alicante y que conozco personalmente desde hace más de 30 años.

Este despacho es un claro ejemplo de pequeña empresa emprendedora, ya que Gonzalo montó el despacho después de haber adquirido experiencia en otros bufetes de Alicante y queriendo mejorar muchos de los aspectos con los que no estaba a gusto, fundó su propio bufete hace aproximadamente 10 años.

Como persona inquieta que se considera, además de tener los conocimientos de derecho por su profesión, también tiene ciertos conocimientos técnicos básicos que le permiten gestionar los requerimientos ofimáticos de su bufete, que está compuesto por él mismo como abogado y su secretaria que realiza las tareas administrativas. Aunque estos conocimientos no van mucho más allá, y en cuestión de seguridad no hay ninguna medida adoptada.

Esta estructura ha funcionado durante estos últimos años correctamente, sin embargo, un cierto número de casos ganados y ciertas acciones realizadas han hecho que el bufete empiece a tener cierta notoriedad y animado por este hecho Gonzalo quiere atraer a clientes más grandes e incluso a empresas que puedan tener ciertas necesidades de representación legal.

Esto hace que sea necesario replantearse ciertas estructuras técnicas dentro de la empresa por dos motivos principales. El primero es que el bufete debe tener una imagen de seguridad, ya que ningún gran cliente o empresa quiere que sus datos estén expuestos con facilidad. El otro motivo es que cuando una gran empresa es objeto de ciberataques muchas veces si no pueden atacar directamente a la empresa porque está convenientemente protegida, pueden realizar ataques a otras empresas satélites más pequeñas que sean proveedoras de diversos servicios y que les puedan proporcionar información confidencial y/o de acceso a la empresa principal.

Está claro que el segundo punto se consigue realizando un buen plan director de seguridad de la información. Pero ¿Y en cuanto al primero? Parece obvio que el no haber sufrido ataques es una buena imagen de seguridad, pero ¿Cómo demuestras que no has sufrido ataques porque simplemente no se han interesado en ti hasta este momento? Aquí es donde entra en juego una certificación ISO 27001 por ejemplo.

Una certificación como la ISO 27001 puede acreditarte como una empresa que protege sus activos de forma segura ya que especifica los requisitos para establecer, implementar, mantener y mejorar de manera continua un SGSI.

Cuando una organización quiere cumplir con la norma ISO 27001 debe demostrar que los apartados 4 a 10 de la norma están efectivamente implantados, estos puntos son los siguientes [1]:

4. Contexto de la organización:

Es necesario conocer la organización, sus objetivos de negocio y todas aquellas cuestiones relativas a elementos internos o externos de la empresa que puedan favorecer o perjudicar en el logro de dichos objetivos. El objetivo del SGSI será siempre favorecer el desempeño de la organización y para ello debe estar alineado con los objetivos de negocio, por lo que debe conocer la empresa.

5. Liderazgo

Para lograr la implantación de un SGSI es necesario el compromiso de la dirección. Es imprescindible que la empresa muestre explícitamente que la empresa apoya la consecución del SGSI, aportando recursos económicos y humanos, y además evidenciando su implicación.

También debe establecer una política de seguridad de la información, una documentación en la que se reflejan en términos generales los objetivos de la organización respecto a la seguridad de la información y las principales líneas de acción. Esta documentación debería ser comunicada a todos los empleados y partes interesadas.

Por último, la alta dirección debe determinar los roles y responsabilidades de seguridad, indicando quién tiene que hacer qué, y así evitar que procesos diseñados queden sin implantar por falta de responsabilidad. Es ideal determinar un responsable de seguridad que coordine las actividades en materia de seguridad y reporte a la dirección, y un comité de seguridad que busque soluciones a los temas de seguridad, resuelva temas interdisciplinarios y apruebe directrices y normas.

6. Planificación

Una vez tenido en cuenta el contexto de la organización y sus necesidades se deben llevar a cabo las acciones encaminadas a determinar riesgos y oportunidades. Para ello se llevará a cabo una evaluación de riesgos para lo cual será necesario:

- Definir la metodología de evaluación de riesgos: que ofrezca resultados consistentes, válidos y comparables
- Identificación de los activos de información: indicando su responsable, valoración y dependencias de activos y servicios y procesos
- Identificación de amenazas y vulnerabilidades
- Cálculo del riesgo: calculando la relación entre el valor del activo, la degradación que se produce por la amenaza y la probabilidad de ocurrencia
- Tratamiento de los riesgos: mitigar, asumir, transferir o eliminar
- Selección de controles para el tratamiento de riesgos: considerando hasta qué punto permite reducir el riesgo y su coste
- Gestión del riesgo: reanalizar riesgos para comprobar el riesgo residual y su aceptabilidad
- Declaración de aplicabilidad: indicar los controles incluidos y justificar su inclusión o exclusión.

7. Soporte

Se deben asignar los recursos necesarios para la implantación del SGSI, incluyendo todas las fases mencionadas. Además, se debe asegurar la competencia del personal implicado y la comunicación a los niveles adecuados, ya tanto a nivel interno como externo. Incluso es indicado determinar las comunicaciones: su contenido, cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos mediante los cuales se puede comunicar. Toda la información ha de quedar documentada a través de los diferentes informes y documentos.

8. Operación

Tras la aprobación de los planes de riesgos y su tratamiento se han de poner en práctica. Esto implica que se dotará de los recursos necesarios y de que se realizará el seguimiento pertinente.

9. Evaluación y desempeño

Una vez implantados los procesos se debe evaluar periódicamente su funcionamiento para garantizar el plan de seguridad. Para ello la organización debe determinar qué elementos deben ser evaluados y sobre los que se realizará su seguimiento junto con los métodos de medición, y sus responsables.

Debería llevarse a cabo un proceso de auditoría interna, se aconseja que al menos anualmente, y excepcionalmente cuando se produzcan cambios drásticos, asegurando que se cumple con los requisitos de la norma.

Además, a la dirección se le debe ofrecer una visión global del funcionamiento del SGSI y la situación actual de la empresa respecto a la seguridad. Este proceso es aconsejable también anualmente para que la dirección pueda tomar decisiones al respecto.

10. Mejora

Las organizaciones están sometidas a cambios constantes por lo que el SGSI debe estar en permanente evolución, actualizándose y adaptándose a las circunstancias. Esto conlleva aplicar acciones correctivas a las no conformidades o incidentes de seguridad, corrigiendo los problemas desde su origen una vez localizada la causa. Por otro lado, se ha producir la mejora continua del sistema para adecuar su idoneidad y eficacia.

Este proyecto se dividirá en dos partes bien diferenciadas:

En los apartados siguientes explicaremos cómo abordar estos puntos para la obtención de un SGSI. Y posteriormente veremos la viabilidad de obtener una certificación ISO 27001 con la implantación de este.

La última parte la compondrá el análisis de riesgos y diseño del plan de seguridad del despacho habiendo aplicado la metodología detallada en los apartados de este proyecto.

2. Estudio de viabilidad

El diseño e implantación de un SGSI puede llegar a suponer un presupuesto bastante considerable de una pequeña empresa, y las certificaciones en normativa ISO también suponen un desembolso importante. Así que antes de embarcarnos en la realización material del proyecto puede ser interesante realizar un estudio de viabilidad para obtener una visión global de lo que nos puede aportar el proyecto y qué costes deberemos asumir para llevarlo a cabo. Y si merece la pena asumir el coste frente al posible beneficio.

Para este caso en particular, un esquema que nos puede ser útil es el análisis DAFO, en el que se estudian las características internas de una empresa (Fortalezas y Debilidades) frente a las situaciones externas (Amenazas y Oportunidades). Todo ello en una matriz de 2 por 2:

	Positivo	Negativo
Interno	Fortalezas: Implicación total de la dirección Interés por el aumento de la seguridad	Debilidades: Personal con falta de formación en el campo a tratar Coste del análisis del SGSI y de la certificación elevados Necesidad de clientes clave para que el proyecto pueda ser viable
Externo	Oportunidades: La tecnología avanza y también lo hace la preocupación de las empresas por su seguridad tecnológica Algunas pequeñas y medianas empresas que requieren representación legal empiezan a tener necesidades de seguridad Un SGSI ayuda a cumplir normativas legales de seguridad de información. La sociedad empieza a ser consciente de la importancia de la seguridad de sus datos.	Amenazas: Ya existen bufetes especializados que ofrecen gran seguridad en la protección de sus datos Al ser una empresa pequeña se dispone de un presupuesto muy limitado

Figura 1. Análisis DAFO

Si nos fijamos en el cuadro de la Figura 1 vemos que tenemos los siguientes 4 puntos:

- Fortalezas: Como principal fortaleza cabe destacar que tenemos la implicación total de la dirección para abordar el proyecto, esto supone una gran ventaja, ya que no tendremos obstáculos a la hora de poder obtener información del funcionamiento actual de la empresa y obtendremos la total colaboración tanto de la directiva como de los trabajadores a la hora de solicitar actuaciones que deban realizar. Además, el interés tanto de la directiva como de los empleados por querer aumentar la seguridad de la información en el despacho hace que podamos contar proactivamente con ellos en todo momento del desarrollo del proyecto.

- Debilidades: Por otro lado, nos encontramos con ciertas deficiencias, ya que, aunque están muy implicados, el personal del despacho no tiene ninguna formación técnica en el campo que vamos a desarrollar. Además, el coste de análisis e implantación de un SGSI es bastante elevado y la certificación tiene todavía mayor coste. Por último, el despacho no dispone de clientes que ya tengan esa necesidad sobre los que poder repercutir estos gastos y que pueda suponer una rentabilidad al proyecto.

- Oportunidades: Los últimos avances tecnológicos han supuesto un verdadero problema para la seguridad y cada vez es mayor la preocupación de las empresas por la protección de sus datos. También las empresas pequeñas y medianas empiezan a preocuparse por la seguridad de sus datos y en la sociedad cada vez está más presente la preocupación por la protección de información. Además de que la implantación de un SGSI ayudaría a cumplir normativas como la LGPD y la de confidencialidad entre abogado-cliente que puede suponer sanciones importantes.

- Amenazas: Actualmente ya existen bufetes grandes con esta certificación y que están especializados en proteger convenientemente la información de sus clientes. Además de que las grandes empresas que tienen una mayor necesidad de proteger la información suelen tener su propio departamento legal y no depender de estos servicios subcontratados. Además, este bufete es pequeño y es la única fuente de ingresos familiar, con lo que una descapitalización tan grande podría exponer gravemente la situación del bufete.

Debido al análisis anterior, antes de llevar a cabo el proyecto del SGSI y la certificación deberíamos tener muy claros los costes económicos que supondrán y hacer un estudio de mercado para conocer los posibles clientes que pudieran estar interesados y atraídos por esta mejora en la seguridad del bufete y la capacidad económica de esos clientes para poder repercutir estos costes tan elevados.

3. Planificación

Para la presentación de este TFM se utilizará la convocatoria de septiembre. Debido a la imposibilidad de la compaginación del desarrollo del TFM con las asignaturas del máster, el trabajo y la conciliación familiar.

Por tanto, la planificación dará comienzo en junio cuando acaban las clases del máster y se pueda dedicar el tiempo de éstas al desarrollo del TFM. Así la planificación queda como sigue:

Contenidos	Tiempo total	Fecha límite fin
Motivación, justificación, objetivo general, Introducción Estado del arte	3 semanas	21 junio
Objetivos Metodología Análisis y especificación Presupuesto, estimaciones, planificación	3 semanas	12 julio
Elaboración del SGSI	1 mes	14 agosto
Análisis de la certificación	1 semana	21 agosto
Resultados Conclusiones y trabajo futuro Referencias, bibliografía y apéndices Agradecimientos, citas, índices	2 semanas	2 septiembre

Tabla 1. Planificación del TFM

En la fase de la certificación únicamente realizaremos un estudio en el que se muestren los pasos necesarios que hay que realizar para conseguir la certificación. No se obtendrá la certificación en sí misma ya que para su obtención se necesita haber implantado primero el SGSI, que tampoco se va a realizar en el tiempo en el que disponemos.

Lo que sí llevaremos a cabo es la realización del análisis del SGSI y el desarrollo del mismo, con el cual, si se llegase a implantar en el despacho, podría obtenerse la certificación ISO 27001.

4. Estado del arte

4.1. La protección de datos en los despachos de abogados

Los abogados por su profesión están obligados a cumplir un código deontológico [2] en el que en su artículo 5 se establece que existe un secreto profesional entre el abogado y su cliente, y el abogado tiene el derecho y la obligación de proteger este secreto.

Tal y como indica Pedro de la Torre Rodriguez en una serie de artículos sobre protección de datos personales en los bufetes de abogados [3], una de las responsabilidades activas y deber de secreto que tiene el abogado y más concretamente el despacho de abogados con todos sus trabajadores involucrados es:

> *"Que existen procedimientos de seguridad de la información encaminados a evitar en lo posible una comunicación de datos no autorizada, así como la destrucción o sustracción de datos de carácter personal."*

Parece claro que un Sistema de Gestión de la Seguridad de la Información en un despacho de abogados es algo más que optativo, llegando a convertirse en obligatorio. Y más cuando el incumplimiento de éste puede acarrear diversas sanciones, según indica el propio abogado Fernando Martínez Escurís en su blog [4]:

> *"El incumplimiento del secreto profesional podría traer consigo la aplicación del régimen sancionador previsto en el Estatuto General de la Abogacía, pudiendo dar lugar a sanciones muy graves (artículo 84.c), graves (artículo 85.g), o leves (artículo 86.d). Estas van desde la suspensión temporal del ejercicio de la abogacía, al mero apercibimiento al abogado infractor (todo un mal trago para un profesional). Y en los casos más graves, incluso está prevista la expulsión del Colegio de Abogados."*

Teniendo esto en cuenta, vamos a estudiar la situación en la que nos encontramos para poder aportar una solución óptima y cumplir con la responsabilidad y el deber de la protección del secreto y evitar incurrir en las sanciones mencionadas.

4.2. Antecedentes

El despacho CC-Abogados es un bufete de abogados fundado en 2010 por el propietario de la empresa y abogado Gonzalo Calderón Chao. Se dedica al asesoramiento legal (sobre derecho civil principalmente) a particulares y empresas. Además de a la representación y defensa ante los tribunales en el caso de citaciones o demandas en las que el cliente esté involucrado. Así como cualquier servicio que requiera de un representante legal.

Por temas legales, el bufete únicamente trabaja de cara al cliente (no hay venta de servicios online), aunque sí dispone de una página web publicitaria donde se informan de todos los servicios que se ofertan en el bufete y un formulario donde se pueden realizar consultas iniciales gratuitas para que si el cliente está conforme con la respuesta pueda ir a visitar el bufete en caso de asesoramiento más personalizado.

La página web está alojada en un servidor propiedad de una empresa de hosting de páginas web. El contenido de la página web está desarrollado por el propio abogado, pero el diseño y la maquetación de la página web se encarga una empresa especializada.

El bufete también cuenta con un pequeño programa de gestión de clientes y citas donde se guardan los datos de los clientes y se gestionan las próximas citas. Además, disponen de un NAS donde se almacenan todos los documentos (Word, Excel, pdf, etc…) sobre los que se trabajan con los clientes.

Los clientes saben que en el bufete existe la confidencialidad abogado-cliente y saben que todos los datos y documentos que aportan al bufete están protegidos por dicha confidencialidad

4.3. Estructura del despacho

El bufete está compuesto por el abogado y por su secretaria.

La empresa está organizada por dos empleados, el abogado realiza todos los documentos legales que se requieren para la defensa o asesoramiento de los clientes, realiza la representación en los juicios y responde al cuestionario de la página web, además de actualizarla con el contenido más novedoso en función del movimiento del mercado y de las consultas más recurrentes para atraer a nuevos posibles clientes

La secretaria se encarga de organizar las citas de los clientes, revisar el email del bufete y contestar con texto pre-escrito las consultas más recurrentes, además de traducir o ponerse en contacto con posibles clientes extranjeros.

El bufete cuenta con una conexión de internet a través del proveedor Movistar a través de fibra óptica. Una red interna donde se encuentra el equipo informático del abogado y otro equipo de la secretaria, sin ningún equipo que realice funciones de servidor. Estos equipos requieren de software con Office para gestionar tanto el correo como los documentos Word y Excel con los que deben trabajar a diario. Además de un navegador web para poder realizar consultas y trámites a través de las páginas del BOE, Notarios, Ministerio de justicia, etc… con los pertinentes certificados de identidad instalados. También poseen un equipo NAS donde se encuentran los documentos Word y Excel con los que trabajan. Una impresora multifunción en red con scanner para imprimir los documentos desde cualquier equipo o escanear a una carpeta de red local en la que los equipos de la red pueden acceder. Para la gestión de las citas y la recopilación de datos de clientes cuentan con un pequeño software (cliente – servidor) hecho a medida que instala una pequeña base de datos en mysql donde la parte servidor que está instalada en el equipo de la secretaria gestiona la base de datos y se comunica con los clientes que están instalados en ambos equipos. Además, en la misma red LAN está desplegada también una red WiFi securizada con WPA donde están conectados los dispositivos móviles de los trabajadores y los clientes que soliciten acceso para transmisión de documentos a la impresora y/o al scanner. Del NAS se realiza una copia de seguridad dos días a la semana en horario nocturno a través de FTP a otro NAS que está situado en el domicilio personal del abogado.

El servidor de correo electrónico está contratado por el mismo proveedor donde está alojada la página web.

El bufete tiene además un archivo donde se catalogan y almacenan todos los documentos impresos necesarios y derivados de todas las causas judiciales. Este archivo se encuentra en una habitación dentro del domicilio del bufete en la que únicamente se guarda dicho archivo y la habitación no es utilizada para ninguna otra función.

A los equipos informáticos se accede con usuarios y contraseñas locales en cada equipo. No existe un servidor de dominio centralizado que valide el acceso a los equipos.

4.4. Contexto

Lo que se pretende con la implantación del SGSI en la empresa es poder acreditar a sus clientes y a cualquier auditoría realizada por algún organismo competente (véase el colegio provincial de abogados de Alicante) un nivel de protección suficiente para todo lo referente a la seguridad de la información de los casos legales y judiciales en los que el bufete haya actuado representando a sus clientes, así como la protección del secreto profesional. Para una correcta implantación y ejecución del SGSI, tanto el abogado del bufete como la secretaria deberán recibir formación en los temas referentes a la seguridad de la información.

Ambas partes se encuentran identificadas y tienen claro los papeles que desempeñan. No existe documentación sobre los requerimientos de seguridad. Únicamente tienen subcontratada una empresa para la gestión de la LOPD que deberá ser actualizada a la nueva normativa europea RGPD.

Es necesario definir un SGSI, se debe realizar un plan de desarrollo y de mantenimiento y mejora una vez implantado.

Posteriormente, una vez implantado el SGSI haremos un estudio para realizar su certificación bajo la normativa ISO 27001.

4.5. Situación Actual del SGSI

No existe una política de seguridad de la información más allá de la LOPD que se contrató con una empresa externa pero que no se ha ido manteniendo, quedando obsoleta. No obstante, existen roles bien diferenciados entre el abogado y la secretaria en cuanto a responsabilidad sobre la seguridad de la información que se trata en el despacho.

En el bufete no existe ninguna política de seguridad con respecto a la información y a los datos almacenados en los distintos equipos del bufete. Deberemos realizar una política de seguridad para:

- Proteger la información sensible de los casos de los clientes que son representados legalmente por el bufete.
- Proteger las comunicaciones para asegurar la protección de los datos que viajan a través de ellas.

- Cumplir la norma de legislación europea RGPD para los datos almacenados de los clientes
- Asegurar el cumplimiento del secreto profesional ante una posible filtración de la información almacenada ya sea mediante un ataque dirigido o fortuito.

Basándonos en la normativa ISO27000 y en concreto en los puntos de la plantilla de la normativa ISO27001 estableceremos una situación inicial de la empresa, de la que partiremos para la realización del SGSI.

Para ello contamos con el compromiso total del propietario del bufete, que está concienciado con la realización e implantación de un SGSI sabiendo los posibles riesgos e impactos por el tratamiento de información sensible como son los datos legales y judiciales de sus clientes.

Así pues, la situación inicial de la que partimos es la siguiente:

Sección	Requerimientos ISO 27001	Estado
4	**Contexto de la organización**	
4,1	**Comprensión de la organización y de su contexto**	
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Repetible
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Inicial
4,3	**Determinación del alcance del SGSI**	
4,3	Determinar y documentar el alcande del SGSI	Inexistente
4,4	**SGSI**	
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Inexistente
5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Repetible
5,2	**Política**	
5,2	Documentar la Política de Seguridad de la Informacion	Inexistente

5,3	**Roles, responsabilidades y autoridades en la organización**	
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inicial
6	**Planificación**	
6,1	**Acciones para tratar los riesgos y oportunidades**	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Inexistente
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente
6,2	**Objetivos de seguridad de la información y planificación para su consecución**	
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inexistente
7	**Soporte**	
7,1	**Recursos**	
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Repetible
7,2	**Competencia**	
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Inexistente
7,3	**Concienciación**	
7,3	Implementar un programa de concianciación de seguridad	Inexistente
7,4	**Comunicación**	
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inicial
7,5	**Información documentada**	
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Inexistente
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inicial
7.5.3	Mantener un control adecuado de la documentación	Inicial
8	**Operación**	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Inexistente

8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios	Inexistente
8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inexistente
9,2	**Auditoría interna**	
9,2	Planificar y realizar una auditoría interna del SGSI	Inexistente
9,3	**Revisión por la dirección**	
9,3	La administración realiza una revisión periódica del SGSI	Inexistente
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

Figura 2. Situación actual de implantación de la normativa ISO 27001

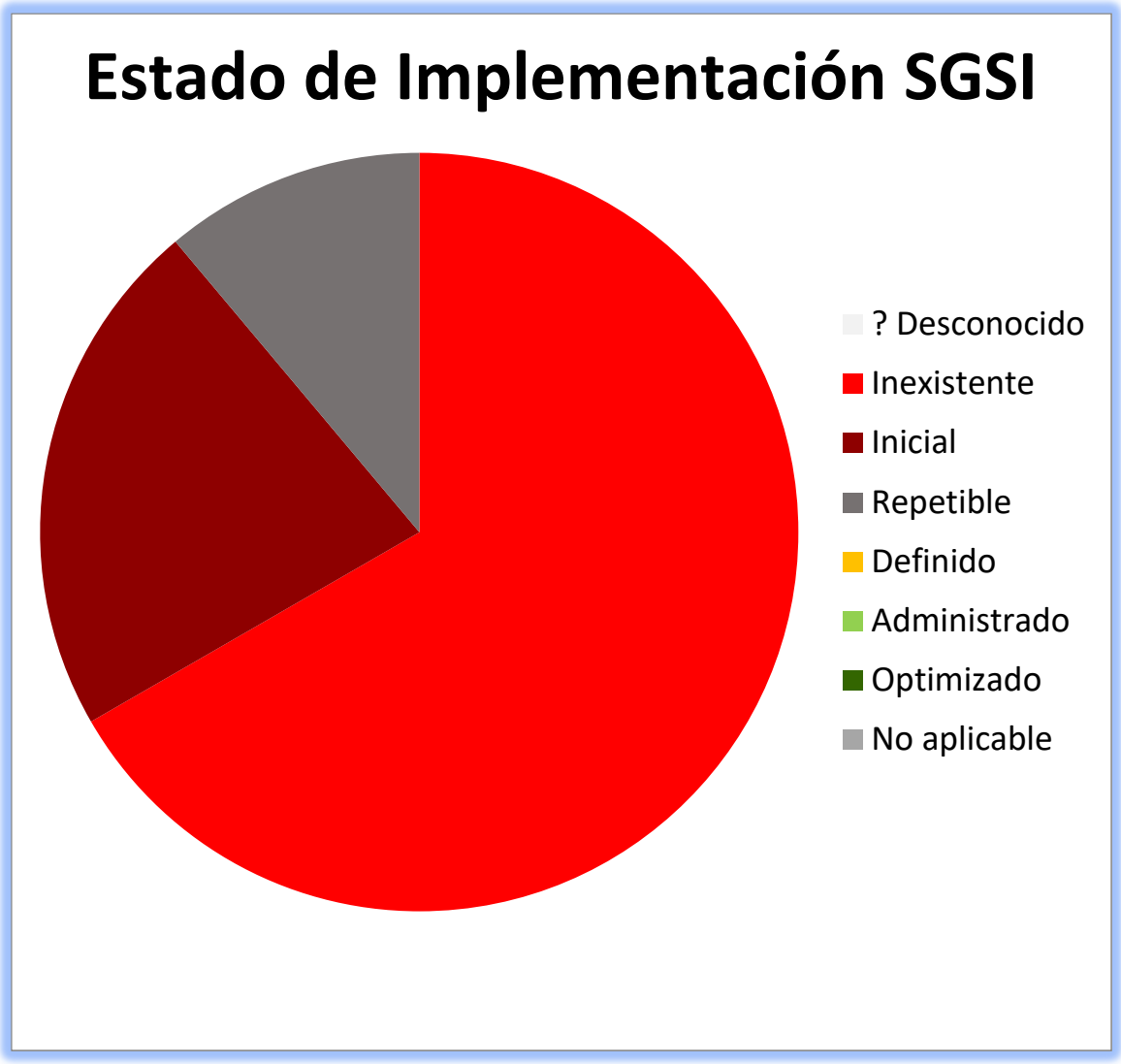

Figura 3. Esquema de situación actual de implantación del SGSI

Como se puede observar, el grado de implantación o calidad del SGSI es bajo o inexistente, debido a la falta de conocimiento de seguridad en datos automatizados y equipos informáticos. Una cosa es comprar unos equipos informáticos para poder realizar trabajos de ofimática y otra muy distinta es ponerlos en una red empresarial, configurar una red WiFi, contratar una conexión a internet y proteger toda la infraestructura frente a posibles amenazas a las que puede estar expuesto el bufete y que analizaremos en la sección “6.2 Amenazas”.

5. Objetivos

El objetivo del proyecto es el diseño e implantación de un Sistema de Gestión de la Seguridad de la Información en el despacho de abogados “CC-Abogados” que permita la protección de los datos y asegure el secreto profesional ante posibles amenazas. Posteriormente se realizará un análisis sobre la certificación del SGSI bajo la norma ISO 27001 para poder demostrar tanto a clientes que lo soliciten como a organismos que lo requieran, que el despacho posee un nivel de seguridad suficiente para proteger los datos personales de los clientes y cumplir eficazmente con el secreto profesional ante posibles amenazas que puedan surgir.

Para ello seguiremos los siguientes pasos:

- Estudio del despacho: Análisis del modelo de negocio, la infraestructura tecnológica y la información de los clientes que recopila y dónde se recopilan.

- Elaboración del catálogo de activos: Un listado con todos los elementos de la infraestructura tecnológica y su valoración

- Elaboración de un listado de amenazas: Para identificar de todas ellas cuáles afectan más o menos a los activos que tiene el despacho.

- Análisis de riesgos: Calcular qué riesgo tiene cada uno de los activos en función de la probabilidad de que le ocurra alguna de las amenazas.

- Estudio de salvaguardas: Frente al riesgo de cada uno de los activos, establecer una serie de salvaguardas que permitan disminuirlo

- Diseño de un plan de seguridad: Elaborar un documento con el plan de seguridad para que los trabajadores del despacho lo puedan evaluar y conocer la situación en la que se encuentran y la posibilidad de mejora que tienen

- Implantación: Implantación de las medidas redactadas en el documento de seguridad.

- Estudio de certificación: Realizar un análisis del coste y las acciones necesarias para la certificación del plan de seguridad bajo la normativa ISO 27001

6. Metodología

Para la elaboración del SGSI en el despacho de abogados seguiremos la metodología MAGERIT (acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) [5]. Existen otras metodologías igualmente válidas, pero nos centraremos en MAGERIT por ser una metodología muy usada en España, está elaborado por la "Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica" que depende del Ministerio de Hacienda para ser una ayuda a las empresas que tengan necesidad de diseñar e implantar un SGSI y que no tengan experiencia en el sector o carezcan de personal especializado, como es el caso que nos ocupa. Además de obtener buenos resultados a la hora de definir el catálogo de activos, identificar las posibles amenazas a las que están expuestos, evaluar los riesgos y proponer salvaguardas para reducir los efectos en cada uno de los activos identificados.

Además de la metodología y la elaboración del SGSI será conveniente la formación en materia de seguridad de la información tanto al propietario del despacho como a la secretaria. En el caso de que haya rotación en el puesto de la secretaria será necesario realizar el mismo curso de formación al nuevo empleado.

No sabemos los posibles futuros clientes que tendrá el despacho, ni el interés que despierten a los ciberdelincuentes, pero la mayoría de los ataques en realidad se dan de forma accidental, debido a que normalmente las empresas son más bien víctimas de una mala praxis por parte de sus propios trabajadores o usuarios, muchas veces por falta de formación, desconocimiento de las normas o incluso dejación. Y es precisamente este punto el que más queremos solventar.

Lo que MAGERIT pretende realizar es un análisis de riesgos mediante una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados, como son:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Una vez que hemos alcanzado el segundo punto tenemos lo que MAGERIT define como “impacto y riesgos potenciales”, o lo que es lo mismo, valoraciones “teóricas” que se dan en el caso de que no hubiera ninguna salvaguarda aplicada. Sobre este escenario teórico se incorporan las salvaguardas del siguiente punto, llegando así a una estimación más realista del impacto y del riesgo.

Cabe destacar que llegados a este punto puede suceder que no hayamos alcanzado el nivel de riesgo que estamos dispuestos a aceptar y que debamos volver a realizar un análisis de riesgos hasta que lleguemos al nivel deseado.

6.1. Catálogo de activos

El primer paso que describe la metodología MAGERIT es realizar un catálogo de activos. Es importante antes de tomar ninguna decisión respecto de la seguridad tener claros los elementos que queremos proteger, a estos elementos los denominamos “activos de información”. Para saber exactamente qué debemos incluir dentro de estos activos y que no, podemos referirnos a la norma UNE 71504:2008 [6] que define un activo como:

> *“Todo componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Esto incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.”*

A partir de esta definición podemos determinar que en un sistema de información hay 2 tipos de activos:

- La información que maneja
- Los servicios que presta

Subordinados a estos dos se pueden identificar otros activos relevantes:

- Datos que materializan la información
- Servicios auxiliares que se necesitan para poder organizar el sistema
- Las aplicaciones informáticas (software) que permiten manejar los datos
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios
- Los soportes de información que son dispositivos de almacenamiento de datos

- El equipamiento auxiliar que complementa el material informático
- Las redes de comunicaciones que permiten intercambiar datos
- Las instalaciones que acogen equipos informáticos y de comunicaciones
- Las personas que explotan u operan todos los elementos anteriormente citados

Cada uno de estos activos tiene un cierto interés, al que denominaremos “valor”. El valor no es "lo que cuesta" un activo, sino la importancia que tiene para la empresa, por lo que en cierta forma expresa la necesidad de proteger el activo, ya que cuanto más valioso es un activo mayor necesidad de protección.

El valor de los activos puede calibrarse desde cada una de las dimensiones que definen la seguridad, de forma que se puede apreciar el valor en función de:

- La **confidencialidad** de un activo, es decir ¿qué daño causaría que lo conociera quien no debe?
- La **integridad** de un activo, ¿Qué daño causaría que estuviese dañado o corrupto?
- La **disponibilidad** de un activo, ¿Qué daño causaría no tenerlo no poder utilizarlo?

Además de estas dimensiones, en la provisión de servicios digitales también son considera dos dimensiones más relacionadas con el conocimiento de los actores relacionados:

- La **autenticidad** de los usuarios que hacen uso de los activos, ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho de cada cosa?
- La **trazabilidad** del uso del servicio, ¿Qué daño causaría no saber a quién se presta el servicio, quien hace qué y cuándo?, o del acceso a los datos ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Para valorar los activos cualquier escala de valores sería útil. Sin embargo, es muy importante que:

- Se use una escala común para todas las dimensiones, permitiendo comparar riesgos
- Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas
- Se use un criterio homogéneo que permita comparar análisis realizados por separado

MAGERIT propone dos escalas de valores, una más sencilla y otra más detallada. Teniendo en cuenta los activos del despacho y la dimensión de la empresa se ha elegido una escala sencilla de diez valores, aunque agrupando algunos de ellos, dejando en valor 0 lo que sería un valor

despreciable (a efectos de riesgo) y 10 lo que sería un valor irremplazable, según el siguiente criterio:

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Tabla 2. Escala de valores de activos

Para una fácil, rápida y ordenada clasificación de activos MAGERIT en el apéndice 2 del "Libro II – Catálogo de elementos" propone unas fichas para identificación y valoración de activos que será la que utilicemos en el diseño del SGSI.

Ejemplo de ficha de activos:

[D] Datos / Información	
Código:	Nombre:
Descripción:	
Responsable:	
Tipo:	

Figura 4. Ficha de inventario de activos

Valoración		
Dimensión	Valor	Justificación
[D]		
[A]		
[T]		

Figura 5. Ficha de valoración de activos

6.2. Amenazas

El siguiente paso consiste en identificar las amenazas que pueden afectar a nuestros activos. Nuevamente nos referimos a la norma UNE 71504:2008 para definir una amenaza:

> *"Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización."*

MAGERIT clasifica las amenazas en 5 tipos:

- Naturales: como terremotos, inundaciones, incendios, etc. Aquí el sistema es víctima pasiva, pero debemos contemplarlos
- Del entorno: desastres que se dan por las mismas condiciones de la industria donde se desarrolla la actividad (fallo eléctrico, contaminación...)
- Defectos de las aplicaciones: ya sea software o hardware, son problemas del equipamiento que pueden generar consecuencias negativas, generalmente se conocen como vulnerabilidades
- Causadas por personas accidentalmente: problemas causados sin intención, por error u omisión
- Causados por personas deliberadamente: ataques deliberados con ánimo de beneficiarse indebidamente o causar daños y perjuicios a los propietarios.

Deberemos tener en cuenta que estas amenazas no afectan a nuestros activos por igual, sino que cuando una amenaza sucede afectará en mayor medida a ciertos activos y a otros activos puede no afectarles en absoluto. Como ejemplo, las instalaciones pueden incendiarse; pero las aplicaciones, no. Las personas pueden ser objeto de un ataque bacteriológico; pero los servicios, no. Sin embargo, los virus informáticos afectan a las aplicaciones, no a las personas

Tampoco afectan por igual a todas las dimensiones del activo (disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad). Es por ello por lo que se debe calcular el grado de degradación que una amenaza causa a un activo en cada una de sus dimensiones, pudiendo ser desde totalmente degradado hasta no sufrir afectación.

Además, también es necesario calcular el grado de probabilidad de ocurrencia de cada amenaza y para ello MAGERIT da la opción de usar una escala modelada numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Por ejemplo, para la probabilidad de ocurrencia de una amenaza usaremos la siguiente tabla:

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensual
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Tabla 3. Probabilidad de ocurrencia

Ahora, para cada una de las amenazas sobre cada una de las dimensiones a las que afecta, es necesario estimar el grado de degradación que provocaría. Si a un activo le impacta una amenaza puede verse afectado tan poco, que tal vez ni siquiera se note el efecto de la amenaza. Puede verse afectado de forma que, aunque se percibe que "algo" ocurre con el activo, se puede continuar trabajando casi con normalidad. O puede verse afectado de tal forma que dañe el funcionamiento, ya sea por completo o seriamente, normalmente en este estado ya carece de importancia si el daño es grave o muy grave por eso se tiende a marcar el activo como muy grave. Así, utilizaremos los siguientes valores para la determinación de la degradación de un activo:

Degradación	Descripción
1%	Inapreciable
10%	Perceptible
100%	Total o irrecuperable

Tabla 4. Valores de degradación

Para la identificación de amenazas recurriremos de nuevo las fichas que aparecen en el capítulo 5 del "Libro II – Catálogo de elementos" que será la que utilicemos en la realización del SGSI.

Ejemplo de ficha de amenazas:

[N.1] Fuego	
Tipos de activos: - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema	

Figura 6. Ficha de inventario de amenazas

6.3. Estimación de riesgos

Se denomina riesgo a la medida del daño probable sobre un sistema. Una vez que hemos determinado los activos que tenemos y las amenazas de las que los queremos proteger, ahora proporcionaremos el verdadero factor que determina las medidas de seguridad a aplicar y la generación de planes de seguridad, el riesgo.

El riesgo crece con el impacto y con la probabilidad. Por tanto, los verdaderos peligros y de los que tendremos que ocuparnos con más recursos serán aquellos en los que se provoque un gran impacto y, además, la probabilidad de que suceda sea muy alta.

Si utilizamos la escala de degradación que una amenaza puede realizar a un activo y tenemos el activo catalogado con un valor, podemos calcular el impacto potencial según la siguiente tabla:

Impacto		Degradación		
		1%	10%	100%
Valor del activo	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 5. Cálculo del impacto potencial

Conociendo el impacto y la probabilidad de una amenaza, el cálculo del riesgo es inmediato, utilizando de nuevo una tabla de doble entrada como la siguiente:

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 6. Matriz para el cálculo del riesgo

Con estas herramientas podemos calcular el riesgo y, además, evaluar el impacto de cada amenaza sobre cada dimensión de cada activo. Con esto obtendremos de forma muy clara sobre qué activos deberemos aplicar salvaguardas y cuántos recursos podremos dedicar a las salvaguardas de cada activo. Es evidente que un activo de menor valor que sufra un impacto bajo no dedicaremos los mismos recursos que a un activo de mayor valor y que pueda sufrir un gran impacto.

6.4. Salvaguardas

Las salvaguardas o también llamadas contramedidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se pueden evitar simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras requieren seguridad física y, por último, está la política de personal. Por lo que una contra medida no supone sólo la aplicación de un determinado software o la configuración de alguna característica concreta de este, sino también cualquier método que ayude a reducir el riesgo.

Teniendo en cuenta el cálculo de impacto y riesgos anteriores, se obtendría un resultado en una situación de completa desprotección. Aunque no es frecuente encontrar este tipo de situaciones. Lo más común es prever algún tipo de contramedida, aunque sea por precaución o

simplemente por sentido común, aunque esto no asegura que las salvaguardas aplicadas sea la más efectiva ni que todos los activos estén protegidos. En el siguiente punto veremos la manera de elegir las mejores salvaguardas para los distintos activos.

6.4.1. Elección de salvaguardas

Está claro que salvaguardas hay muchas, pero deberemos centrarnos principalmente en los activos que debemos proteger, para ello hemos realizado en el punto anterior un análisis de riesgo. Aquellos activos que corran un riesgo alto o muy alto deberán centrar nuestra atención. Una vez que ya tenemos claro lo que necesitamos proteger deberemos tener en cuenta los siguientes aspectos:

- Tipo de activo: Los diferentes tipos de activo tienen una forma distinta de protección.
- Dimensión a proteger: Para un activo podemos necesitar más protección para ciertas dimensiones que otras
- Amenazas de las que protegernos: Aquellas amenazas con más probabilidad de que sucedan será más prioritario protegernos
- Alternativas: Es posible que puedan existir salvaguardas alternativas o que al proteger el activo de cierta forma también se cumpla la protección en otra.

Es por ello que hay salvaguardas que se pueden excluir principalmente por dos justificaciones:

- No aplica: Como hemos visto antes, es posible que una salvaguarda no aplique al activo o a la protección de cierta dimensión del activo
- No se justifica: Cuando la salvaguarda si protege al activo pero es más costosa la protección que el valor del propio activo.

6.4.2. Cómo actúan las salvaguardas

Una salvaguarda ayuda a proteger el activo de dos formas:

- Reduciendo la probabilidad de que ocurra una amenaza: A estas salvaguardas se les denomina “preventivas” porque previenen la ocurrencia de la amenaza de forma que, en el mejor de los casos, se impida completamente que la amenaza se materialice. Como sabemos, en la estadística, es muy difícil bajar la probabilidad a cero, pero con una

probabilidad lo suficientemente baja para que no ocurra durante el periodo de tiempo en el que ese activo sea relevante, es más que suficiente.

- Reduciendo la degradación del activo: A veces no podemos impedir que una amenaza se materialice, es entonces cuando debemos proteger el activo para que, si esa amenaza le impacta, no dañe al activo de forma que lo inutilice. En este sentido, estas salvaguardas pueden limitar la degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

Así, resumiendo en una tabla podemos clasificar las salvaguardas según lo expuesto anteriormente, de la siguiente forma:

Efecto	Tipo
Preventivas: Reducen la probabilidad	[PR] Preventivas [DR] Disuasorias [EL] Eliminatorias
Acotan la degradación	[MI] Minimizadoras [CR] Correctivas [RC] Recuperadoras
Consolidan el efecto de las demás	[MN] de Monitorización [DC] de Detección [AW] de Concienciación [AD] Administrativas

Tabla 7. Tipos de salvaguardas

6.4.3. Eficacia de las salvaguardas

Además de elegir una salvaguarda para un activo, es posible que ésta no sea lo más eficaz posible. Para que una salvaguarda sea 100% eficaz debe combinar dos factores:

- Es técnicamente idónea para enfrentarse al riesgo que protege

- Se emplea siempre

Desde el punto de vista operacional:

- Está totalmente desplegada y configurada. Tiene un plan de mantenimiento
- Existen procedimientos de uso en caso de necesitar utilizarla
- Los usuarios tienen formación de la salvaguarda
- Existen controles que avisan de posibles fallos

6.4.4. Vulnerabilidades

Aun habiendo desplegado salvaguardas para protección de los activos, es posible que existan debilidades de los activos o de sus salvaguardas de protección. A estas debilidades se les llama vulnerabilidad. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

6.5. Tratamiento del riesgo

Con lo visto hasta ahora tenemos lo que se conoce por “Estudio de riesgos”. Que simplemente es un análisis que nos indica cuáles son los activos más valorados para protegerlos, de qué amenazas deberemos protegerlos y con qué salvaguardas los protegeremos. Un análisis sobre el que los responsables de la empresa deberán tomar decisiones, evaluando la situación y tratando los riesgos.

Aunque las decisiones las deban tomar los responsables de la empresa deberán estar bien asesorados por especialistas en seguridad.

La decisión que se debe realizar consiste principalmente en establecer unos niveles de riesgo aceptables y evaluar aquellos activos que tengan riesgo superior para ver qué acción llevaremos a cabo sobre ellos.

Las acciones a realizar sobre el riesgo de un activo pueden ser las siguientes:

6.5.1. Aceptación

Aceptar un riesgo implica aceptar la responsabilidad de la insuficiencia (o como vimos en el punto 6.4.4 también llamada vulnerabilidad) que ese activo posee. Esta decisión no es técnica y puede venir motivado por factores como legislación, por motivos políticos o compromisos contractuales con proveedores o usuarios.

Cualquier nivel de riesgo puede ser aceptable siempre que sea conocido y aceptado formalmente por la dirección, aunque en este caso se debería hacer una dotación de financiación para poder responder a las posibles consecuencias.

6.5.2. Eliminación

Esta opción implica eliminar la fuente de riesgo frente a un riesgo que no es aceptable. Seguramente en nuestro sistema podamos eliminar varias cosas, siempre que no afecte al modelo de negocio de la empresa. Evidentemente no se podrá prescindir de los activos esenciales de la empresa, ya que son la esencia de lo que es la empresa propiamente dicha, pero sí que se podría prescindir de otros componentes que ayudan a realizar el modelo de negocio pero que no son parte del mismo. En este aspecto se puede realizar de dos formas:

- Eliminar ciertos activos y emplear otros en su lugar (Cambiar un software por otro, o un fabricante por otro, etc…)
- Reordenar la arquitectura del sistema de forma que alejemos lo más valioso de lo más expuesto, por ejemplo: Segregando redes o desdoblando equipos.

Como hemos visto, eliminar una fuente de riesgo implica modificar el sistema, y por tanto, se deberá realizar un nuevo análisis de riesgo sobre el sistema modificado.

6.5.3. Mitigación

Como hemos visto en la sección “6.3 Estimación del riesgo”, un riesgo se compone fundamentalmente de dos factores: Impacto y probabilidad. Por tanto, para mitigar un riesgo sobre un activo deberemos actuar sobre uno o los dos factores que lo provocan:

- Reducir la degradación causada por una amenaza. El valor del activo es el que es, y eso no lo podemos cambiar (se podría compartir el riesgo cuantitativo como veremos más

adelante), pero para reducir el impacto podemos actuar sobre la degradación causada por la amenaza, consiguiendo el objetivo de disminuir el impacto y con ello el riesgo.

- Reducir la probabilidad de que la amenaza se materialice. Si conseguimos que una amenaza que puede suceder 1 vez al año suceda 1 vez cada 50 años, es muy posible que ya no tengamos que preocuparnos por esa amenaza en la vida útil del activo, y con ello reducimos igualmente el riesgo.

En los dos casos se trata de mejorar las salvaguardas que protegen al activo. Esto, a veces, como sucede en las salvaguardas de tipo técnico, se traduce en la inclusión de nuevo hardware o software que se convierten en un nuevo activo del sistema. Por tanto, estos activos tendrán su propio valor y habrá que calcularles el impacto y el riesgo nuevo que hemos introducido.

Lo que se pretende conseguir al final, es que el riesgo final del sistema con las salvaguardas desplegadas no supere al del sistema original y confirmar así que las salvaguardas disminuyen efectivamente el riesgo de la empresa.

6.5.4. Compartición

La compartición del riesgo, también llamada “transferencia del riesgo” pero como puede hacerse total o parcial es más correcto hablar de compartición. Se puede realizar de dos formas:

- Riesgo cualitativo: Compartir el riesgo se consigue externalizando componentes del sistema, así se dividen las responsabilidades técnicas para el operador del componente técnico y las legales según lo acordado en la prestación del servicio
- Riesgo cuantitativo: La compartición de riesgo cuantitativo se realiza mediante la contratación de seguros. Donde a cambio de la prima del seguro, el tomador reduce el impacto (reduciendo el coste de sustitución del activo) y el asegurador corre con el coste de esa sustitución. Este tipo de compartición es más bien útil cuando el valor del activo es más bien monetario y se puede cuantificar, ya que, si el valor del activo reside, por ejemplo, en los datos en sí mismos, o en que el activo es único y no se puede reemplazar, este tipo de compartición no sería tan eficaz.

Al igual que en el caso anterior, cuando se comparte un riesgo cambia el conjunto de los componentes del sistema, o su valoración. Por tanto, habrá que recalcular el impacto y riesgo nuevos mediante un nuevo análisis del sistema resultante.

6.6. Planes de seguridad

Cuando finaliza el análisis de riesgos es cuando se debe llevar a cabo un plan de seguridad. Que no es más que un conjunto de proyectos para materializar las decisiones adoptadas para tratar los riesgos.

En un plan de seguridad se identifican principalmente tres tareas que son:

- Identificación de los proyectos de seguridad
- Planificación para la ejecución de los proyectos
- Ejecución

6.6.1. Identificación de los proyectos de seguridad

Lo que se pretende con estos proyectos es plasmar las decisiones tomadas en el tratamiento de riesgos en acciones concretas. Es decir, dada una amenaza y un tratamiento de riesgo, indicar las tareas a realizar para implantar sus salvaguardas.

Un proyecto de seguridad consistirá en una agrupación de varias de estas tareas. La agrupación se hace por diversos criterios: Conveniencia, tareas que por sí mismas carecerían de eficacia, porque combaten un objetivo común o simplemente porque competen a una única unidad de acción.

Las tareas deben estar estructuradas para detallar los siguientes apartados:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
    - Costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas

    - Costes de implantación inicial y mantenimiento en el tiempo
    - Costes de formación, tanto de los operadores como de los usuarios, según convenga al caso
    - costes de explotación
    - Impacto en la productividad de la Organización
- Una relación de subtareas a afrontar, teniendo en cuenta:
    - Cambios en la normativa y desarrollo de procedimientos
    - Solución técnica: programas, equipos, comunicaciones e instalaciones
    - Plan de despliegue
    - Plan de formación
- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

Si el proyecto de seguridad es muy complejo, quizá todos estos puntos sean difíciles de concretar, en tal caso bastaría con proponer unas indicaciones orientativas.

6.6.2. Planificación para la ejecución de los proyectos

Una vez que se han desarrollado los proyectos de seguridad, se deben ordenar en el tiempo teniendo en cuenta diversos factores:

- La criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas
- El coste del programa
- La disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas
- Otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual, etc…

Los planes de seguridad se planifican con 3 niveles de detalle:

- Plan director (un único plan): También llamado “plan de actuación”, trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.
- Plan anual (uno o varios planes anuales): Trabaja sobre un periodo de entre 1 y 2 años, estableciendo la planificación de los programas en cada uno de ellos.
- Plan de proyecto (varios proyectos con su planificación): Trabaja en un plazo de más o menos 1 año, estableciendo el plan detallado de ejecución de cada programa.

La forma de actuación es desarrollar un plan director único, para dar visión amplia de conjunto y establecerá objetivos de acciones más puntuales. Este plan permitirá desarrollar planes anuales para poder gestionar la asignación de recursos que ejecutarán las tareas. Por último, los proyectos serán los que implantarán los programas de seguridad.

6.6.3. Ejecución

En esta fase se seguirán los planes de proyecto que componen el plan director con el objetivo de implantar las salvaguardas, redactar documentos de normativas internas, realizar cursos de formación del personal, etc… Que conseguirá llevar al sistema a un estado de riesgo aceptable.

6.7. Certificación ISO27001

Una vez implantado el plan director de seguridad que hemos obtenido con la metodología anterior, podemos solicitar a una entidad externa, independiente y acreditada, que nos realice una auditoría del sistema de información con respecto a la norma ISO/IEC 27001 y haga una medición del grado de implantación real y su eficacia. Si el resultado es positivo emitirían el correspondiente certificado.

Existen varias entidades que pueden llevar a cabo esta actuación. Cada entidad puede realzarlo de distintas formas, si por ejemplo nos basamos en la empresa bsigroup [7], el proceso se realizaría en tres fases.

- Fase de análisis: En esta fase se realiza una evaluación previa en la que se estudia el Sistema de Gestión de Seguridad de la Información existente para compararlo con los requisitos de la normativa ISO/IEC 27001. En este análisis la entidad certificadora puede realizar algunos comentarios sobre posibles incumplimientos o mejoras que debería tener el SGSI para que se puedan corregir antes de la realización de una auditoría formal.

- Auditoría formal: En esta fase se realiza una revisión del sistema comprobando si se han desarrollado los procedimientos y controles necesarios establecidos en la norma ISO/IEC 27001. Si todos los requisitos se cumplen, entonces se pasa a la comprobación de la implantación de los procedimientos y los controles en la organización, para asegurar que funcionen de forma eficaz.
- Certificación: Después de haber aprobado la auditoría formal la entidad emitirá un certificado ISO/IEC27001 que tendrá una validez de tres años.

Durante ese periodo de tiempo la organización obtiene el certificado, pasado ese periodo deberá volver a recertificar si desea seguir ostentando el certificado. Aunque pasar una recertificación es algo más complejo, ya que la entidad deberá asegurarse de que el sistema va mejorando y evolucionando, sin quedar anclado en la conformidad.

7. Resultados

El resultado de lo expuesto en los puntos anteriores queda reflejado en el capítulo Anexo I, donde se ha realizado un análisis de riesgos del despacho de abogados y se ha obtenido una serie de fichas donde queda reflejados aquellos activos que tenían el riesgo más elevado.

Posteriormente con una toma de decisiones consensuada con el responsable del despacho se decide actuar sobre los activos con mayor riesgo eliminando, compartiendo o mitigándolo, esto último proponiendo una serie de salvaguardas, que deberán disminuir el nivel de riesgo de los activos hasta niveles aceptables por la dirección del despacho.

Con esto se ha elaborado un plan de seguridad que consta de una serie de proyectos ordenados de mayor a menor prioridad en los que se trata de contener el riesgo del sistema a niveles aceptables.

Según lo visto en los capítulos “6.6 Planes de seguridad” y “6.7 Certificación ISO 27001”, al realizar la implantación de este plan de seguridad, se podría realizar el estudio de la certificación con una entidad certificadora en la que, con unas mínimas correcciones o indicaciones en la fase de análisis, se podría conseguir una certificación bajo la normativa ISO/IEC 27001.

8. Conclusiones y trabajo futuro

Como se puede comprobar, el diseño de un Sistema de Gestión de Seguridad de la Información no es algo trivial y necesita de recursos con formación y experiencia en este campo.

Además, posteriormente a la implantación se necesita una revisión continua y constante para que el plan de seguridad diseñado no quede obsoleto o estancado y esté constantemente incluyendo los nuevos elementos que se incorporen al sistema y eliminando los obsoletos. Es por tanto un sistema "vivo" que requiere de revisiones periódicas.

Para una pequeña empresa, como es el caso que nos ocupa, será necesario externalizar el proceso y subcontratar a alguna empresa especializada en el sector, el mantenimiento del mismo, ya que, aunque aquí hayamos diseñado un plan director adecuado para poder asegurar la infraestructura del despacho, no es suficiente con esto y deberán realizarse controles periódicos que permitan asegurar la actualización del mismo.

Revisando los objetivos marcados en este proyecto vemos que hemos podido cumplir la realización del análisis actual de la empresa en la que hemos obtenido un informe clarificador sobre los activos más esenciales del despacho y el riesgo a los que están expuestos, pudiendo establecer una serie de decisiones para tratar el riesgo ya sea eliminándolo, compartiéndolo o mitigándolo.

También hemos conseguido el objetivo de diseñar un plan director de seguridad que consta de una serie de proyectos identificados por criticidad y dirigidos a la protección de esos activos, de forma que abordando primero los más críticos se consigan mayores resultados en el menor tiempo posible.

Quedaría pendiente para un trabajo futuro y a discreción del despacho la implantación del plan director de seguridad aquí desarrollado. Dada mi relación con el responsable del despacho estoy comprometido en la colaboración para la implantación de los proyectos de seguridad aquí presentados y el asesoramiento para una certificación posterior si el estudio del mercado así lo indicase.

Referencias

1. Puntos 4 a 10 de la normativa ISO 27001: https://normaiso27001.es/fase-2-analisis-del-contexto-de-la-organizacion-y-determinacion-del-alcance/
2. Código deontológico adaptado al Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio: http://www.abogacia.es/wp-content/uploads/2012/06/codigo_deontologico1.pdf
3. Tercera entrega de la serie de artículos sobre protección de datos personales en los bufetes de abogados, por Pedro de la Torre Rodríguez, perito informático judicial certificado por el CPITIA, especialista en defensa penal y contra pericia: https://elderecho.com/deber-de-secreto-respecto-a-los-datos-personales
4. Artículo del blog del abogado Fernando Martínez Escurís que habla sobre el secreto profesional del abogado y de las posibles causas de su incumplimiento: https://www.escurisabogado.es/el-secreto-profesional-del-abogado_fb18270cb6761.html
5. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
6. Noma UNE 71504:2008: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430
7. Empresa bsigroup que se dedica a emitir certificaciones, entre otras la ISO/IEC 27001 https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/Certificacion-para-ISO-27001/

Anexo I – Análisis y desarrollo del SGSI en el despacho de abogados

En una empresa, la creación de un plan de seguridad puede ser algo optativo, es evidente que hoy en día todas las empresas se preocupan por la seguridad de sus datos, pero no todas tienen la capacidad, los recursos o el personal adecuado para llevar a cabo un buen plan de seguridad. Esto no es un gran problema para empresas que puedan decidir no manejar datos confidenciales o subcontratar empresas que se hagan cargo del cumplimiento de la nueva RGPD. Pero ¿Qué ocurre cuando una empresa no sólo maneja datos personales de clientes, sino que además, por motivos de su negocio obtiene también datos muy confidenciales de sus clientes?

La implantación de un Sistema de Gestión de Seguridad de la Información en un despacho de abogados, además de proteger los datos y la infraestructura de los elementos tecnológicos del despacho ayuda también a proteger el secreto profesional que el despacho debe cumplir con sus clientes. Que en caso de incumplimiento puede derivar en sanciones hasta muy graves e incluso la expulsión del colegio de abogados.

En este documento vamos a analizar los activos de los que consta el despacho, valorar las amenazas a los que están expuestos y realizar una valoración de riesgo para posteriormente proponer una serie de medidas o salvaguardas que permitan reducir estos riesgos. Además, este Plan de Seguridad servirá, junto con otras medidas de formación y otras, para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) según lo establecido en la normativa ISO 27001 y poder realizar una certificación en dicha norma para poder mostrar a los clientes que lo soliciten o a los organismos que lo requieran, que el despacho posee un nivel de seguridad suficiente para proteger los datos personales de los clientes y cumplir eficazmente con el secreto profesional ante posibles amenazas que puedan surgir.

Gráficos de la situación actual

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	67%	66%
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.	26%	15%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	7%	4%
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.	0%	2%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	0%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
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.	0%	14%

Figura 7. Estado actual del SGSI y Controles de la seguridad de la información

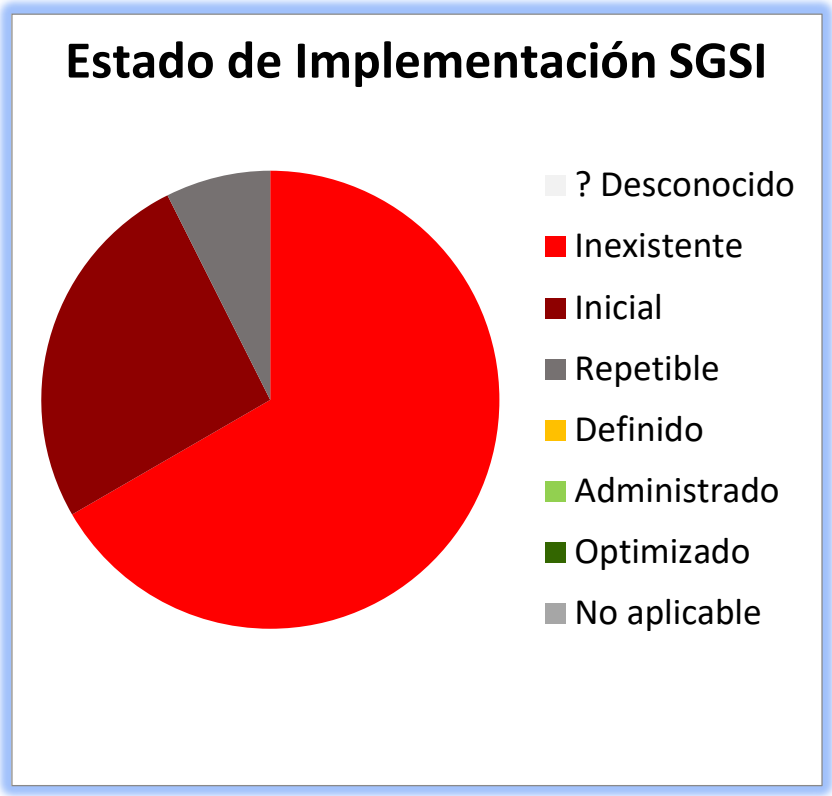

Figura 8. Diagrama del estado actual del SGSI

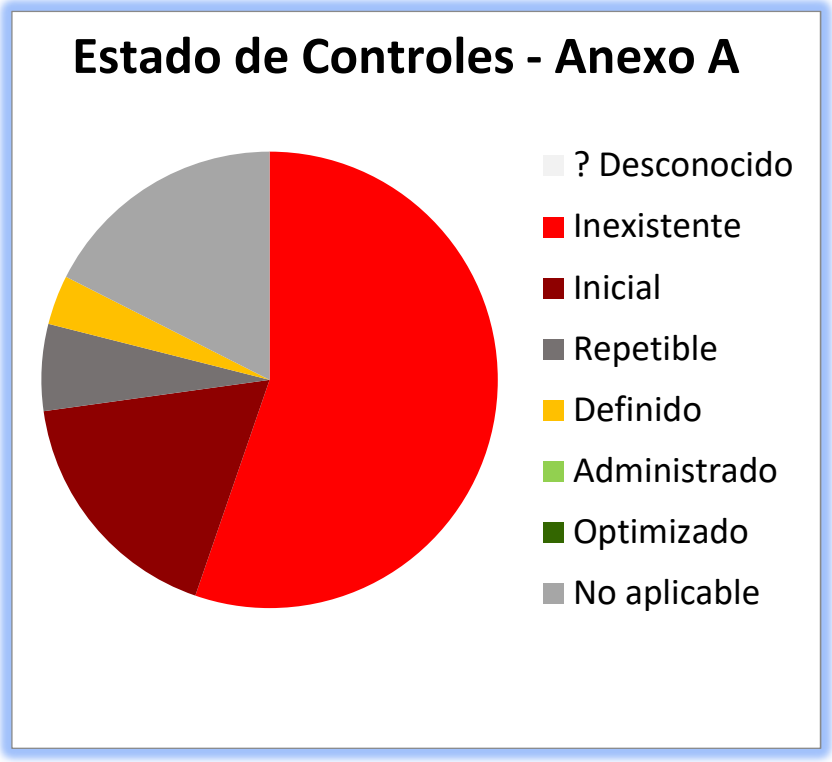

Figura 9. Diagrama actual del estado actual de los controles de seguridad

Identificación de activos

Para la creación del catálogo de activos del despacho de abogados vamos a utilizar herramientas que están especialmente diseñadas para ello y que han demostrado sobradamente su validez. En este caso utilizaremos Magerit v3. Siguiendo el apartado "2. Tipos de activos", vamos a realizar una lista de los activos del despacho y clasificarlos según la siguiente metodología:

- [info]: Activos esenciales de información
- [service]: Activos esenciales Servicio
- [arch]: Arquitectura del sistema
- [D]: Datos o información
- [K]: Claves criptográficas
- [S]: Servicios
- [SW]: Software
- [HW]: HardWare
- [COM]: Redes y comunicaciones
- [Media]: Soportes de información
- [Aux]: Equipamiento auxiliar
- [L]: Instalaciones
- [P]: Personal

También les daremos un código y un nombre, y además, un valor para cada dimensión según el siguiente baremo:

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Tabla 8. Baremo para valoración de activos

Así, el inventario de activos es el siguiente:

Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho

[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho
[P]	PR.001	Abogado
[P]	PR.002	Secretaria

Tabla 9. Inventario de activos

Y detalladamente las fichas de los activos quedarían como sigue:

[essential] Activos esenciales	
Código: ES.001	**Nombre:** Base de datos del programa ADA
Descripción: El programa ADA es un programa desarrollado a medida para el almacenamiento de los datos de los clientes, pequeño resumen del caso que se ocupa con el cliente en cuestión y programación y gestión de citas.	
Responsable: Propietario del despacho	
Ubicación: HW.002	
Número: 1	
Tipo: [per][M]	

Tabla 10. Ficha del activo ES.001

Valoración		
Dimensión	Valor	Justificación
[I]	10	Se utilizan en el trabajo y planificación del día a día
[C]	10	Datos sensibles protegidos por la RGPD
[A]	10	Datos sensibles protegidos por la RGPD
[T]	10	Datos sensibles protegidos por la RGPD

Tabla 11. Valoración del activo ES.001

[essential] Activos esenciales	
Código: ES.002	**Nombre:** Fichero Outlook con los emails de clientes
Descripción: Los emails de los clientes es la principal herramienta de trabajo que tiene el despacho. Contiene información detallada de los casos y datos personales de los clientes.	
Responsable: Propietario del despacho	
Ubicación: HW.001 y HW.002	
Número: 2	
Tipo: [classified][C]	

Tabla 12. Ficha del activo ES.002

Valoración		
Dimensión	Valor	Justificación
[I]	10	Son la base del trabajo del día a día
[C]	10	Datos sensibles protegidos por la RGPD
[A]	10	Datos sensibles protegidos por la RGPD
[T]	10	Datos sensibles protegidos por la RGPD

Tabla 13. Valoración del activo ES.002

[essential] Activos esenciales	
Código: ES.003	**Nombre:** Ficheros ofimáticos de los casos del despacho

Descripción: Documentos que contienen las demandas presentadas por el despacho en representación de sus clientes, así como otros datos de pruebas de juicios y documentos con información privada necesaria para el desarrollo de los casos de los clientes
Responsable: Propietario del despacho
Ubicación: HW.003
Número: 1
Tipo: [classified][C]

Tabla 14: Ficha del activo ES.003

Valoración		
Dimensión	Valor	Justificación
[I]	10	Documentos con los que se trabaja a diario
[C]	10	Datos sensibles protegidos por la RGPD
[A]	10	Datos sensibles protegidos por la RGPD
[T]	10	Datos sensibles protegidos por la RGPD

Tabla 15. Valoración del activo ES.003

[service] Activos esenciales	
Código: ES.004	**Nombre:** Página web del despacho
Descripción: Página web del despacho donde se publicitan los servicios ofertados y se pueden realizar consultas online gratuitas, además de solicitar cita previa y obtener los datos de contacto y ubicación del despacho.	
Responsable: Propietario del despacho	
Ubicación: Servicio subcontratado	

Número: 1
Tipo: [service]

Tabla 16. Ficha del activo ES.004

Valoración		
Dimensión	Valor	Justificación
[I]	4	Si no funcionan se puede seguir realizando el trabajo del despacho con cierta normalidad
[C]	6	Comprometer este servicio no da acceso a información sensible, pero puede dañar la imagen del despacho
[D]	4	Si no funcionan se puede seguir realizando el trabajo del despacho con cierta normalidad
[A]	6	Comprometer este servicio no da acceso a información sensible, pero puede dañar la imagen del despacho

Tabla 17. Valoración del activo ES.004

[HW] Equipamiento informático (hardware)	
Código: HW.001 y HW.002	**Nombre:** Ordenador abogado y secretaria
Descripción: Ordenadores de sobremesa donde el abogado realiza sus trabajos de ofimática y revisa los mails que la secretaria debe responder a los clientes, también se utiliza para el acceso con identificación a las páginas del Ministerio de Justicia, BOE, Colegio de abogados, Notarios, etc… Ordenador de sobremesa donde la secretaria realiza su trabajo de revisión y respuesta de mails y organización de citas, así como otros trabajos ofimáticos, también se utiliza para el acceso con identificación a las mismas páginas que el ordenador del abogado	
Responsable: Propietario del despacho	

Ubicación: Despacho principal y Secretaría
Número: 2
Tipo: [pc]

Tabla 18. Ficha de los activos HW.001 y HW.002

Valoración		
Dimensión	Valor	Justificación
[C]	6	A través de los equipos se podría acceder a información sensible
[D]	9	Si no funcionan no se puede realizar el trabajo del despacho
[I]	9	Si está dañado no se puede realizar el trabajo del despacho

Tabla 19. Valoración de los activos HW.001 y HW.002

[HW] Equipamiento informático (hardware)	
Código: HW.003	**Nombre:** NAS
Descripción: Servidor de ficheros NAS donde se encuentran ubicados los documentos ofimáticos de trabajo del despacho (casos, sentencias, documentos notariales, etc…)	
Responsable: Propietario del despacho	
Ubicación: Secretaría	
Número: 1	
Tipo: [nas]	

Tabla 20. Ficha del activo HW.003

Valoración		
Dimensión	Valor	Justificación

[C]	10	Contiene información importante y sensible
[D]	10	Si no funciona no se puede realizar el trabajo del despacho
[I]	10	Si está dañado no se puede realizar el trabajo del despacho

Tabla 21. Valoración del activo HW.003

[HW] Equipamiento informático (hardware)	
Código: HW.004	**Nombre:** Router
Descripción: Router de conexión a internet a través de fibra óptica	
Responsable: Propietario del despacho	
Ubicación: Secretaría	
Número: 1	
Tipo: [network] [router]	

Tabla 22. Ficha del activo HW.004

Valoración		
Dimensión	Valor	Justificación
[C]	10	A través del router se puede acceder a la red del despacho
[D]	8	Si no funciona se limita el trabajo que se puede realizar en el despacho
[I]	8	Si no funciona se limita el trabajo que se puede realizar en el despacho

Tabla 23. Valoración del activo HW.004

[HW] Equipamiento informático (hardware)	
Código: HW.005 HW.006	**Nombre:** Impresora y Scanner

Descripción: Equipo multifunción compuesto por impresora y scanner con conexión a red LAN
Responsable: Propietario del despacho
Ubicación: Secretaría
Número: 1
Tipo: [peripheral] [print] [scan]

Tabla 24 Ficha de los activos HW.005 y HW.006

Valoración		
Dimensión	Valor	Justificación
[C]	1	Estos dispositivos no almacenan ningún dato
[D]	2	Si no funciona se limita muy poco el trabajo que se puede realizar en el despacho
[I]	2	Si no funciona se limita muy poco el trabajo que se puede realizar en el despacho

Tabla 25. Valoración de los activos HW.005 y HW.006

[COM] Redes de comunicaciones	
Código: CO.001	**Nombre:** Servicio de internet por fibra óptica
Descripción: Servicio de internet contratado con un ISP que provee de conexión a internet al despacho.	
Responsable: Propietario del despacho	
Ubicación: HW.004	
Número: 1	
Tipo: [Internet]	

Tabla 26. Ficha del activo CO.001

Valoración		
Dimensión	Valor	Justificación
[C]	9	A través de este servicio circula información sensible
[D]	5	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[I]	5	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[A]	9	A través de este servicio circula información sensible

Tabla 27. Valoración del activo CO.001

[COM] Redes de comunicaciones	
Código: CO.002 y CO.003	**Nombre:** Red LAN Ethernet y WiFi
Descripción: Red LAN y WiFi del despacho.	
Responsable: Propietario del despacho	
Ubicación: HW.004	
Número: 1	
Tipo: [LAN] [WiFi]	

Tabla 28. Ficha de los activos CO.002 y CO.003

Valoración		
Dimensión	Valor	Justificación
[C]	9	A través de este servicio circula información sensible
[D]	4	Si no funciona se limita el trabajo que se puede realizar en el despacho

[I]	4	Si no funciona se limita el trabajo que se puede realizar en el despacho
[A]	9	A través de este servicio circula información sensible

Tabla 29. Valoración de los activos CO.002 y CO.003

[COM] Redes de comunicaciones	
Código: CO.004	**Nombre:** Centralita telefónica
Descripción: Centralita telefónica del despacho.	
Responsable: Propietario del despacho	
Ubicación: Secretaría	
Número: 1	
Tipo: [PSTN]	

Tabla 30. Ficha del activo CO.004

Valoración		
Dimensión	Valor	Justificación
[C]	8	A través de este servicio circula información sensible
[D]	4	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[I]	4	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[A]	8	A través de este servicio circula información sensible

Tabla 31. Valoración del activo CO.004

[SW] Aplicaciones (software)

Código: SW.001	**Nombre:** Outlook
Descripción: Programa para la gestión de mails del despacho.	
Responsable: Propietario del despacho	
Ubicación: HW.001 y HW.002	
Número: 2	
Tipo: [email_client]	

Tabla 32. Ficha del activo SW.001

Valoración		
Dimensión	Valor	Justificación
[C]	10	Contiene información sensible
[D]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho
[I]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho
[A]	10	Contiene información sensible

Tabla 33. Valoración del activo SW.001

[SW] Aplicaciones (software)	
Código: SW.002, SW.003	**Nombre:** Word y Excel
Descripción: Programa ofimático para la generación y modificación de documentos.	
Responsable: Propietario del despacho	
Ubicación: HW.001 y HW.002	
Número: 2	
Tipo: [office]	

Tabla 34. Ficha de los activos SW.002 y SW.003

Valoración		
Dimensión	Valor	Justificación
[C]	10	Tiene acceso a documentos con información sensible
[D]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho
[I]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho
[A]	10	Tiene acceso a documentos con información sensible

Tabla 35. Valoración de los activos SW.002 y SW.003

[SW] Aplicaciones (software)	
Código: SW.004, SW.005	**Nombre:** Cliente y Servidor ADA
Descripción: Programa hecho a medida para la gestión de información de clientes y citas del despacho.	
Responsable: Propietario del despacho	
Ubicación: HW.001 y HW.002	
Número: 1	
Tipo: [sub]	

Tabla 36. Ficha de los activos SW.004 y SW.005

Valoración		
Dimensión	Valor	Justificación
[C]	10	Contiene información sensible
[D]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho

[I]	6	Si no funciona se limita el trabajo que se puede realizar en el despacho
[A]	10	Contiene información sensible

Tabla 37. Valoración de los activos SW.004 y SW.005

[K] Claves criptográficas	
Código: KE.001	**Nombre:** Certificado de identidad del abogado
Descripción: Certificado de identidad del abogado para acreditación ante organismos públicos, colegio de abogados y entidades que necesiten acreditación de identidad/profesión.	
Responsable: Propietario del despacho	
Ubicación: HW.001	
Número: 1	
Tipo: [info] [sign] [public_signature]; [info] [encrypt] [public_encryption]	

Tabla 38. Ficha del activo KE.001

Valoración		
Dimensión	Valor	Justificación
[C]	9	Con el certificado de identidad se puede acceder a información sensible
[D]	6	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[I]	6	Si no funciona se limita algo el trabajo que se puede realizar en el despacho
[A]	9	Con el certificado de identidad se puede acceder a información sensible

Tabla 39. Valoración del activo KE.001

[L] Instalaciones	
Código: LU.001	**Nombre:** Piso donde se ubica el despacho
Descripción: Piso donde se ofrecen los servicios presenciales del despacho.	
Responsable: Propietario del despacho	
Ubicación: Calle Alemania	
Número: 1	
Tipo: [building]	

Tabla 40. Ficha del activo LU.001

Valoración		
Dimensión	Valor	Justificación
[D]	8	Si el piso no está disponible se limita bastante el trabajo del despacho
[C]	10	Si consiguen entrar en el piso pueden acceder a información sensible
[I]	10	Si consiguen entrar en el piso pueden acceder a información sensible

Tabla 41. Valoración del activo LU.001

[AUX] Equipamiento auxiliar	
Código: AU.001	**Nombre:** Aire acondicionado
Descripción: Aparato de regulación de temperatura del despacho	
Responsable: Propietario del despacho	
Ubicación: LU.001	
Número: 1	
Tipo: [ac]	

Tabla 42. Ficha del activo AU.001

Valoración		
Dimensión	Valor	Justificación
[D]	4	Si no está disponible puede causar sobrecalentamiento en el hardware
[C]	6	Si se manipula indebidamente puede causar fallos en hardware
[I]	6	Si se manipula indebidamente puede causar fallos en hardware

Tabla 43. Valoración del activo AU.001

[P] Personal	
Código: PR.001	**Nombre:** Abogado
Descripción: Abogado propietario del despacho	
Responsable: N/A	
Número: 1	
Tipo: [ui] [op] [adm] [com] [dba] [sec]	

Tabla 44. Ficha del activo PR.001

Valoración		
Dimensión	Valor	Justificación
[D]	10	Persona propietaria y relevante en el trabajo del despacho
[C]	10	Persona que conoce todos los datos sensibles del despacho
[I]	10	Persona que conoce todos los datos sensibles del despacho

Tabla 45. Valoración del activo PR.001

[P] Personal	
Código: PR.002	**Nombre:** Secretaria
Descripción: Secretaria del despacho que realiza tareas administrativas	
Responsable: Propietario del despacho	
Número: 1	
Tipo: [ui]	

Tabla 46. Ficha del activo PR.002

Valoración		
Dimensión	Valor	Justificación
[D]	4	Si no está disponible se incrementa la carga de trabajo del abogado
[C]	8	Persona que conoce muchos datos sensibles del despacho
[I]	8	Persona que conoce muchos datos sensibles del despacho

Tabla 47. Valoración del activo PR.002

Identificación de amenazas

Esta sección trata de identificar todas las posibles amenazas que pueden afectar a nuestros activos y las dimensiones en las que puede afectar. Para cada una de las amenazas crearemos una ficha con la información de los tipos de activos, las dimensiones y listaremos de nuestro inventario de activos aquellos que cumplen las condiciones.

Desastres naturales

[N.1] Fuego		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 48. Ficha de la amenaza Fuego de origen natural

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[N.2] Daños por agua		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 49. Ficha de la amenaza Daños por agua de origen natural

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[N.*] Desastres naturales		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre

[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 50. Ficha de la amenaza de Desastres Naturales

Considero adecuado que estas amenazas actúen sobre los activos provocando indisponibilidad.

De origen industrial

[I.1] Fuego		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router

[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 51. Ficha de la amenaza Fuego de origen Industrial

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.2] Daños por agua		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 52. Ficha de la amenaza Daños por agua de origen industrial

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.*] Desastres industriales		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 53. Ficha de la amenaza Desastres Industriales

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.3] Contaminación mecánica	
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad

Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 54. Ficha de la amenaza Contaminación mecánica

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.4] Contaminación electromagnética		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora

[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 55. Ficha de la amenaza Contaminación electromagnética

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.5] Avería de origen físico o lógico		
Tipos de Activos: - [SW]: Aplicaciones (software) - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner

[Aux]	AU.001	Aire Acondicionado

Tabla 56. Ficha de la amenaza Avería de origen físico o lógico

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.6] Corte del suministro eléctrico		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 57. Ficha de la amenaza Corte de suministro eléctrico

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.7] Condiciones inadecuadas de temperatura y/o humedad

Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 58. Ficha de la amenaza Condiciones inadecuadas de temperatura y/o humedad

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.8] Fallo de servicios de comunicaciones		
Tipos de Activos: - [COM]: Redes de comunicaciones		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono

Tabla 59: Ficha de la amenaza Fallo de servicios de comunicaciones

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.9] Interrupción de otros servicios y suministros esenciales		
Tipos de Activos: - [AUX]: Equipamiento auxiliar		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre
[Aux]	AU.001	Aire Acondicionado

Tabla 60. Ficha de la amenaza Interrupción de otros servicios y suministros esenciales

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.10] Degradación de los soportes de almacenamiento de la información		
Tipos de Activos: - [Media]: Soportes de información		Dimensiones: 1. [D] disponibilidad
Tipo	Código	Nombre

Tabla 61. Ficha de la amenaza Degradación de los soportes de almacenamiento de la información

Considero adecuado que esta amenaza actúe sobre los activos provocando indisponibilidad.

[I.11] Emanaciones electromagnéticas		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [Aux]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [C] confidencialidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 62. Ficha de la amenaza Emanaciones electromagnéticas

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

Errores y fallos no intencionados

[E.1] Errores de los usuarios	
Tipos de Activos: - [D]: datos / información - [K]: claves criptográficas - [service]: Servicios - [SW]: Aplicaciones (software) - [Media]: Soportes de información	Dimensiones: 1. [I] Integridad 2. [C] confidencialidad 3. [D] Disponibilidad

Tipo	Código	Nombre
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 63. Ficha de la amenaza Errores de los usuarios

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[E.2] Errores del administrador		
Tipos de Activos: - [D]: datos / información - [K]: claves criptográficas - [service]: Servicios - [SW]: Aplicaciones (software) - [HW]: Equipos informáticos (hardware) - [COM]: Redes de comunicaciones - [Media]: Soportes de información		Dimensiones: 1. [I] Integridad 2. [C] confidencialidad 3. [D] Disponibilidad
Tipo	Código	Nombre

[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono

Tabla 64. Ficha de la amenaza Errores del administrador

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[E.3] Errores de monitorización (log)		
Tipos de Activos: - [D.log]: registros de actividad		Dimensiones: 1. [I] Integridad (trazabilidad)
Tipo	Código	Nombre

Tabla 65. Ficha de la amenaza Errores de monitorización (logs)

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[E.4] Errores de configuración		
Tipos de Activos: - [D.conf]: datos de configuración		Dimensiones: 1. [I] Integridad
Tipo	Código	Nombre

Tabla 66. Ficha de la amenaza Errores de configuración

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[E.7] Deficiencias en la organización	
Tipos de Activos: - [P]: Personal	Dimensiones: 1. [D] Disponibilidad

Tipo	Código	Nombre
[P]	PR.001	Abogado
[P]	PR.002	Secretaria

Tabla 67. Ficha de la amenaza Deficiencias en la organización

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[E.8] Difusión del software dañino		
Tipos de Activos: - [SW]: Aplicaciones (software)		Dimensiones: 1. [D] Disponibilidad 2. [I] Integridad 3. [C] Confidencialidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 68. Ficha de la amenaza Difusión de software dañino

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[E.9] Errores de [re-]encaminamiento		
Tipos de Activos: - [service]: Servicios - [SW]: Aplicaciones (software) - [COM]: Comunicaciones		Dimensiones: 1. [C] Confidencialidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 69. Ficha de la amenaza Errores de [re-]encaminamiento

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[E.10] Errores de secuencia	
Tipos de Activos: - [service]: Servicios - [SW]: Aplicaciones (software)	Dimensiones: 1. [I] Integridad

- [COM]: Comunicaciones		
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 70. Ficha de la amenaza Errores de secuencia

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[E.15] Alteración accidental de la información		
Tipos de Activos: - [D]: Datos / Información - [K]: Claves criptográficas - [service]: Servicios - [SW]: Aplicaciones (software) - [COM]: Comunicaciones - [media]: soportes de información - [L]: Instalaciones		Dimensiones: 1. [I] Integridad
Tipo	Código	Nombre

[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 71. Ficha de la amenaza Alteración accidental de la información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[E.18] Destrucción de información	
Tipos de Activos: - [D]: Datos / Información - [K]: Claves criptográficas	Dimensiones: 1. [D] Disponibilidad

- [service]: Servicios - [SW]: Aplicaciones (software) - [COM]: Comunicaciones - [media]: soportes de información - [L]: Instalaciones	

Tipo	Código	Nombre
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 72. Ficha de la amenaza Destrucción de la información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[E.19] Fugas de información	
Tipos de Activos: - [D]: Datos / Información - [K]: Claves criptográficas - [service]: Servicios - [SW]: Aplicaciones (software) - [COM]: Comunicaciones - [media]: soportes de información - [L]: Instalaciones - [P]: Personal	Dimensiones: 1. [C] Confidencialidad

Tipo	Código	Nombre
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 73. Ficha de la amenaza Fugas de información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidenciallidad.

[E.20] Vulnerabilidades de los programas (software)		
Tipos de Activos: - [SW]: Aplicaciones (software)		Dimensiones: 1. [I] Integridad 2. [D] Disponibilidad 3. [C] Confidencialidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 74. Ficha de la amenaza Vulnerabilidades de los programas

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, disponibilidad y confidencialidad.

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de Activos: - [SW]: Aplicaciones (software)	Dimensiones: 1. [I] Integridad 2. [D] Disponibilidad

Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 75. Ficha de la amenaza Errores de actualización / mantenimiento de programas

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad y disponibilidad.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [media]: Soportes electrónicos - [AUX]: Equipamiento auxiliar		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 76. Ficha de la amenaza Errores de actualización / mantenimiento de equipos

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[E.24] Caída del sistema por agotamiento de recursos		
Tipos de Activos: - [service]: Servicios - [HW]: Equipos informáticos (hardware) - [COM]: Comunicaciones		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 77. Ficha de la amenaza Caída del sistema por agotamiento de recursos

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[E.25] Robo		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [media]: Soportes de información - [AUX]: Equipamiento auxiliar		Dimensiones: 1. [D] Disponibilidad 2. [C] Confidencialidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 78. Ficha de la amenaza Robo

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad y confidencialidad.

[E.28] Indisponibilidad del personal		
Tipos de Activos: - [P]: Personal interno		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[P]	PR.001	Abogado

[P]	PR.002	Secretaria

Tabla 79. Ficha de la amenaza Indisponibilidad del personal

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

Ataques intencionados

[A.3] Manipulación de los registros de actividad (log)		
Tipos de Activos: - [D.log]: Registros de actividad		Dimensiones: 1. [I] Integridad (trazabilidad)
Tipo	Código	Nombre

Tabla 80. Ficha de la amenaza Manipulación de los registros de actividad

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[A.4] Manipulación de la configuración		
Tipos de Activos: - [D.conf]: Registros de configuración		Dimensiones: 1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Tipo	Código	Nombre

Tabla 81. Ficha de la amenaza Manipulación de la configuración

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[A.5] Suplantación de la identidad del usuario		
Tipos de Activos: - [D]: datos / información - [K]: Claves criptográficas - [service]: Servicios - [SW]: Aplicaciones (software) - [COM]: Redes de comunicaciones		Dimensiones: 1. [I] Integridad 2. [C] Confidencialidad 3. [A] Autenticidad
Tipo	Código	Nombre
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho

Tabla 82. Ficha de la amenaza Suplantación de la identidad del usuario

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y autenticidad.

[A.6] Abuso de privilegios de acceso		
Tipos de Activos: - [D]: Datos / Información - [K]: Claves criptográficas - [services]: Servicos - [SW]: Aplicaciones (software) - [HW]: Equipos informáticos (hardware) - [COM]: Redes de comunicaciones		Dimensiones: 1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Tipo	Código	Nombre
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel

[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router

Tabla 83. Ficha de la amenaza Abuso de privilegios de acceso

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[A.7] Uso no previsto		
Tipos de Activos: - [services]: Servicos - [SW]: Aplicaciones (software) - [HW]: Equipos informáticos (hardware) - [COM]: Redes de comunicaciones - [media]: Soportes de información - [AUX]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Tipo	Código	Nombre
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi

[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[service]	ES.004	Página web del despacho
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 84. Ficha de la amenaza Uso no previsto

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[A.8] Difusión software dañino

Tipos de Activos: - [SW]: Aplicaciones (software)		Dimensiones: 1. [I] Integridad 2. [C] Confidencialidad 3. [D] Disponibilidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 85. Ficha de la amenaza Difusión software dañino

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad, confidencialidad y disponibilidad.

[A.9] [Re-]encaminamiento de mensajes		
Tipos de Activos: - [service]: servicios - [SW]: Aplicaciones (software) - [COM]: Redes de comunicaciones		Dimensiones: 1. [C] Confidencialidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)

[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 86. Ficha de la amenaza [re-]encaminamiento de mensajes

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[A.10] Alteración de secuencia		
Tipos de Activos: - [service]: servicios - [SW]: Aplicaciones (software) - [COM]: Redes de comunicaciones		Dimensiones: 1. [I] Integridad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet

[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 87. Ficha de la amenaza Alteración de secuencia

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[A.11] Acceso no autorizado	
Tipos de Activos: - [D]: Datos / Información - [K]: Claves criptográficas - [service]: servicios - [SW]: Aplicaciones (software) - [HW]: Equipos informáticos (hardware) - [COM]: Redes de comunicaciones - [Media]: Soportes de información - [AUX]: Equipamiento auxiliar - [L]: Instalaciones	Dimensiones: 1. [C] Confidencialidad 2. [I] Integridad

Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[COM]	CO.001	Fibra óptica

[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 88. Ficha de la amenaza Acceso no autorizado

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad e integridad.

[A.12] Análisis de tráfico		
Tipos de Activos: - [COM]: Redes de comunicaciones		Dimensiones: 1. [C] Confidencialidad
Tipo	Código	Nombre

[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono

Tabla 89. Ficha de la amenaza Análisis de tráfico

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[A.13] Repudio		
Tipos de Activos: - [services]: Servicios - [D.log]: Registros de actividad		Dimensiones: 1. [I] Integridad (trazabilidad)
Tipo	Código	Nombre
[service]	ES.004	Página web del despacho

Tabla 90. Ficha de la amenaza Repudio

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[A.14] Interceptación de información (escucha)		
Tipos de Activos: - [COM]: Redes de comunicaciones		Dimensiones: 1. [C] Confidencialidad
Tipo	Código	Nombre

[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono

Tabla 91. Ficha de la amenaza Interceptación de información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[A.15] Modificación deliberada de la información		
Tipos de Activos: - [D]: Datos / información - [K]: Claves criptográficas - [services]: Servicios (acceso) - [SW]: Aplicaciones (software) - [COM]: Redes de comunicaciones - [media]: Soportes de información - [L]: Instalaciones		Dimensiones: 1. [I] Integridad
Tipo	Código	Nombre
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel

[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 92. Ficha de la amenaza Modificación deliberada de información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de integridad.

[A.18] Destrucción de la información		
Tipos de Activos: - [D]: Datos / información - [K]: Claves criptográficas - [services]: Servicios (acceso) - [SW]: Aplicaciones (software) - [media]: Soportes de información - [L]: Instalaciones		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)

[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 93. Ficha de la amenaza Destrucción de la información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[A.19] Revelación de la información		
Tipos de Activos: - [D]: Datos / información - [K]: Claves criptográficas - [services]: Servicios (acceso) - [SW]: Aplicaciones (software) - [COM]: Redes de comunicaciones - [media]: Soportes de información - [L]: Instalaciones		Dimensiones: 1. [C] Confidencialidad
Tipo	Código	Nombre
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono

[SW]	SW.001	Outlook
[SW]	SW.002	Word
[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)
[K]	KE.001	Certificado de identidad del abogado
[info]	ES.001	Base de datos del programa ADA
[info]	ES.002	Fichero de Outlook con los emails de los clientes
[info]	ES.003	Documentos ofimáticos de los casos del despacho
[service]	ES.004	Página web del despacho
[L]	LU.001	Piso donde se ubica el despacho

Tabla 94. Ficha de la amenaza Revelación de la información

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[A.22] Manipulación de programas		
Tipos de Activos: - [SW]: Aplicaciones (software)		Dimensiones: 1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad
Tipo	Código	Nombre
[SW]	SW.001	Outlook
[SW]	SW.002	Word

[SW]	SW.003	Excel
[SW]	SW.004	Servidor ADA (Programa hecho a medida)
[SW]	SW.005	Cliente ADA (Programa hecho a medida)

Tabla 95. Ficha de la amenaza Manipulación de programas

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad.

[A.23] Manipulación de los equipos		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [Media]: Soportes de información - [AUX]: Equipamiento auxiliar		Dimensiones: 1. [C] Confidencialidad 2. [D] Disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 96. Ficha de la amenaza Manipulación de los equipos

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad y disponibilidad.

[A.24] Denegación de servicio		
Tipos de Activos: - [services]: Servicios - [HW]: Equipos informáticos (hardware) - [COM]: Redes de comunicaciones		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[COM]	CO.001	Fibra óptica
[COM]	CO.002	Red Ethernet
[COM]	CO.003	WiFi
[COM]	CO.004	Centralita Teléfono
[service]	ES.004	Página web del despacho

Tabla 97. Ficha de la amenaza Denegación de servicio

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[A.25] Robo	
Tipos de Activos:	Dimensiones:

- [HW]: Equipos informáticos (hardware) - [media]: Soportes de información - [AUX]: Equipamiento auxiliar		1. [D] Disponibilidad 2. [C] Confidencialidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS
[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado

Tabla 98. Ficha de la amenaza Robo

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad y confidencialidad.

[A.26] Ataque destructivo		
Tipos de Activos: - [HW]: Equipos informáticos (hardware) - [media]: Soportes de información - [AUX]: Equipamiento auxiliar - [L]: Instalaciones		Dimensiones: 1. [D] Disponibilidad
Tipo	Código	Nombre
[HW]	HW.001	Ordenador principal abogado
[HW]	HW.002	Ordenador secretaria
[HW]	HW.003	NAS

[HW]	HW.004	Router
[HW]	HW.005	Impresora
[HW]	HW.006	Escáner
[Aux]	AU.001	Aire Acondicionado
[L]	LU.001	Piso donde se ubica el despacho

Tabla 99. Ficha de la amenaza Ataque destructivo

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[A.27] Ocupación enemiga		
Tipos de Activos: - [L]: Instalaciones		Dimensiones: 1. [D] Disponibilidad 2. [C] Confidencialidad
Tipo	Código	Nombre
[L]	LU.001	Piso donde se ubica el despacho

Tabla 100. Ficha de la amenaza Ocupación enemiga

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad y confidencialidad.

[A.28] Indisponibilidad del personal	
Tipos de Activos:	Dimensiones:

- [P]: Personal interno		1. [D] Disponibilidad
Tipo	Código	Nombre
[P]	PR.001	Abogado
[P]	PR.002	Secretaria

Tabla 101. Ficha de la amenaza Indisponibilidad del personal

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de disponibilidad.

[A.29] Extorsión		
Tipos de Activos: - [P]: Personal interno		Dimensiones: 1. [C] Confidencialidad 2. [I] Integridad 3. [D] Disponibilidad
Tipo	Código	Nombre
[P]	PR.001	Abogado
[P]	PR.002	Secretaria

Tabla 102. Ficha de la amenaza Extorsión

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad, integridad y disponibilidad.

[A.30] Ingeniería social	
Tipos de Activos: - [P]: Personal interno	Dimensiones: 4. [C] Confidencialidad

		5. [I] Integridad 6. [D] Disponibilidad
Tipo	Código	Nombre
[P]	PR.001	Abogado
[P]	PR.002	Secretaria

Tabla 103. Ficha de la amenaza Ingeniería social

Considero adecuado que esta amenaza actúe sobre los activos provocando fallo de confidencialidad, integridad y disponibilidad.

Cálculo del impacto

Para el cálculo del impacto, listaremos para cada activo todas las amenazas y las dimensiones en las que puede estar afectado según el inventario de amenazas del punto anterior. Luego completaremos el valor del activo para esa dimensión según la tabla de activos que tenemos y asignaremos una degradación que provoca la amenaza para ese activo. Una vez tenemos todos los datos calcularemos el impacto de acuerdo con la siguiente tabla:

Impacto		Degradación		
		1%	10%	100%
Valor del activo	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 104. Tabla del cálculo del Impacto

Para valorar el activo utilizaremos la “Tabla 8: Baremo para valoración de activos” del apartado “Identificación de activos”

Y mediremos la degradación según si no afecta nada, le afecta algo pero el activo seguiría funcional, o le afecta totalmente:

Degradación	Descripción
1%	Inapreciable
10%	Perceptible
100%	Total o irrecuperable

Tabla 105. Tabla de degradación de activos

ID: ES.001	Nombre: Base de datos ADA		Tipo de activo: [info] Datos / información esencial		
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto

E.1	Errores de los usuarios	[I]	10	10	A
E.1	Errores de los usuarios	[C]	10	10	A
E.1	Errores de los usuarios	[D]	10	100	MA
E.2	Errores del administrador	[I]	10	10	A
E.2	Errores del administrador	[C]	10	10	A
E.2	Errores del administrador	[D]	10	100	MA
E.15	Alteración accidental de la inf.	[I]	10	10	A
E.18	Destrucción de la información	[D]	10	100	MA
E.19	Fugas de información	[C]	10	10	A
A.5	Suplantación identidad usuario	[C]	10	10	A
A.5	Suplantación identidad usuario	[A]	10	10	A
A.5	Suplantación identidad usuario	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[C]	10	10	A
A.6	Abuso de privilegios de acceso	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[D]	10	100	MA
A.11	Acceso no autorizado	[C]	10	10	A
A.11	Acceso no autorizado	[I]	10	10	A
A.15	Modificación deliberada de inf.	[I]	10	10	A
A.18	Destrucción de la información	[D]	10	100	MA
A.19	Revelación de información	[C]	10	10	A

Tabla 106. Ficha del cálculo del impacto del activo ES.001

ID: ES.002	Nombre: Fichero Outlook	Tipo de activo: [info] Datos / información esencial			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.1	Errores de los usuarios	[I]	10	10	A
E.1	Errores de los usuarios	[C]	10	10	A
E.1	Errores de los usuarios	[D]	10	100	MA
E.2	Errores del administrador	[I]	10	10	A
E.2	Errores del administrador	[C]	10	10	A
E.2	Errores del administrador	[D]	10	100	MA
E.15	Alteración accidental de la inf.	[I]	10	10	A
E.18	Destrucción de la información	[D]	10	100	MA
E.19	Fugas de información	[C]	10	10	A
A.5	Suplantación identidad usuario	[C]	10	10	A
A.5	Suplantación identidad usuario	[A]	10	10	A
A.5	Suplantación identidad usuario	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[C]	10	10	A
A.6	Abuso de privilegios de acceso	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[D]	10	100	MA
A.11	Acceso no autorizado	[C]	10	10	A
A.11	Acceso no autorizado	[I]	10	10	A
A.15	Modificación deliberada de inf.	[I]	10	10	A
A.18	Destrucción de la información	[D]	10	100	MA

A.19	Revelación de información	[C]	10	10	A

Tabla 107. Ficha del cálculo del impacto del activo ES.002

ID: ES.003	Nombre: Doc. ofi. casos desp	Tipo de activo: [info] Datos / información esencial			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.1	Errores de los usuarios	[I]	10	10	A
E.1	Errores de los usuarios	[C]	10	10	A
E.1	Errores de los usuarios	[D]	10	100	MA
E.2	Errores del administrador	[I]	10	10	A
E.2	Errores del administrador	[C]	10	10	A
E.2	Errores del administrador	[D]	10	100	MA
E.15	Alteración accidental de la inf.	[I]	10	10	A
E.18	Destrucción de la información	[D]	10	100	MA
E.19	Fugas de información	[C]	10	10	A
A.5	Suplantación identidad usuario	[C]	10	10	A
A.5	Suplantación identidad usuario	[A]	10	10	A
A.5	Suplantación identidad usuario	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[C]	10	10	A
A.6	Abuso de privilegios de acceso	[I]	10	10	A
A.6	Abuso de privilegios de acceso	[D]	10	100	MA
A.11	Acceso no autorizado	[C]	10	10	A
A.11	Acceso no autorizado	[I]	10	10	A
A.15	Modificación deliberada de inf.	[I]	10	10	A

A.18	Destrucción de la información	[D]	10	100	MA
A.19	Revelación de información	[C]	10	10	A

Tabla 108. Ficha del cálculo del impacto del activo ES.003

ID: ES.004	Nombre: Pag. Web	Tipo de activo: [service] Activos esenciales: Servicio			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.1	Errores de los usuarios	[I]	4	10	B
E.1	Errores de los usuarios	[C]	6	10	M
E.1	Errores de los usuarios	[D]	4	100	M
E.2	Errores del administrador	[I]	4	10	B
E.2	Errores del administrador	[C]	6	10	M
E.2	Errores del administrador	[D]	4	100	M
E.15	Alteración accidental de la inf.	[I]	4	10	B
E.18	Destrucción de la información	[D]	4	100	M
E.19	Fugas de información	[C]	6	10	M
A.5	Suplantación identidad usuario	[C]	6	10	M
A.5	Suplantación identidad usuario	[A]	6	10	M
A.5	Suplantación identidad usuario	[I]	4	10	B
A.6	Abuso de privilegios de acceso	[C]	6	10	M
A.6	Abuso de privilegios de acceso	[I]	4	10	B

A.6	Abuso de privilegios de acceso	[D]	4	100	M
A.11	Acceso no autorizado	[C]	6	10	M
A.11	Acceso no autorizado	[I]	4	10	B
A.15	Modificación deliberada de inf.	[I]	4	10	B
A.18	Destrucción de la información	[D]	4	100	M
A.19	Revelación de información	[C]	6	10	M

Tabla 109. Ficha del cálculo del impacto del activo ES.004

ID: HW.001 HW.002	Nombre: Ordenadores	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
N.1	Fuego	[D]	9	100	A
N.2	Daños por agua	[D]	9	100	A
N.*	Desastres naturales	[D]	9	100	A
I.1	Fuego	[D]	9	100	A
I.2	Daños por agua	[D]	9	100	A
I.*	Desastres industriales	[D]	9	100	A
I.3	Contaminación mecánica	[D]	9	10	M
I.4	Contaminación electromagnética	[D]	9	100	A
I.5	Avería de origen físico o lógico	[D]	9	10	M
I.6	Corte de suministro eléctrico	[D]	9	1	B

I.7	Condiciones inadecuadas temp.	[D]	9	100	A
I.11	Emanaciones electromagnéticas	[D]	9	1	B
E.2	Errores del administrador	[D]	9	1	B
E.2	Errores del administrador	[C]	6	100	M
E.2	Errores del administrador	[I]	9	1	B
E.23	Errores de mantenimiento	[D]	9	10	M
E.24	Caída por agotamiento	[D]	9	10	M
E.25	Robo	[D]	9	100	A
E.25	Robo	[C]	6	100	M
A.6	Abuso de privilegios de acceso	[C]	6	100	M
A.6	Abuso de privilegios de acceso	[D]	9	10	M
A.6	Abuso de privilegios de acceso	[I]	9	100	A
A.7	Uso no previsto	[C]	6	100	M
A.7	Uso no previsto	[D]	9	1	B
A.7	Uso no previsto	[I]	9	10	M
A.11	Acceso no autorizado	[C]	6	100	M
A.11	Acceso no autorizado	[I]	9	100	A
A.23	Manipulación de los equipos	[C]	6	100	M
A.23	Manipulación de los equipos	[D]	9	10	M
A.24	Denegación de servicio	[D]	9	10	M
A.25	Robo	[D]	9	100	A
A.25	Robo	[C]	6	100	M

A.26	Ataque destructivo	[D]	9	100	A

Tabla 110. Ficha del cálculo del impacto del activo HW.001 y HW.002

ID: HW.003	Nombre: NAS	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
N.1	Fuego	[D]	10	100	MA
N.2	Daños por agua	[D]	10	100	MA
N.*	Desastres naturales	[D]	10	100	MA
I.1	Fuego	[D]	10	100	MA
I.2	Daños por agua	[D]	10	100	MA
I.*	Desastres industriales	[D]	10	100	MA
I.3	Contaminación mecánica	[D]	10	10	A
I.4	Contaminación electromagnética	[D]	10	100	MA
I.5	Avería de origen físico o lógico	[D]	10	10	A
I.6	Corte de suministro eléctrico	[D]	10	1	M
I.7	Condiciones inadecuadas temp.	[D]	10	100	MA
I.11	Emanaciones electromagnéticas	[D]	10	1	M
E.2	Errores del administrador	[D]	10	1	M
E.2	Errores del administrador	[C]	10	100	MA
E.2	Errores del administrador	[I]	10	10	A
E.23	Errores de mantenimiento	[D]	10	10	A
E.24	Caída por agotamiento	[D]	10	10	A

E.25	Robo	[D]	10	100	MA
E.25	Robo	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[D]	10	10	A
A.6	Abuso de privilegios de acceso	[I]	10	100	MA
A.7	Uso no previsto	[C]	10	100	MA
A.7	Uso no previsto	[D]	10	1	M
A.7	Uso no previsto	[I]	10	100	MA
A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	10	100	MA
A.23	Manipulación de los equipos	[C]	10	100	MA
A.23	Manipulación de los equipos	[D]	10	10	A
A.24	Denegación de servicio	[D]	10	10	A
A.25	Robo	[D]	10	100	MA
A.25	Robo	[C]	10	100	MA
A.26	Ataque destructivo	[D]	10	100	MA

Tabla 111. Ficha del cálculo del impacto del activo HW.003

ID: HW.004	Nombre: Router	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
N.1	Fuego	[D]	8	100	A
N.2	Daños por agua	[D]	8	100	A
N.*	Desastres naturales	[D]	8	100	A

I.1	Fuego	[D]	8	100	A
I.2	Daños por agua	[D]	8	100	A
I.*	Desastres industriales	[D]	8	100	A
I.3	Contaminación mecánica	[D]	8	10	M
I.4	Contaminación electromagnética	[D]	8	10	M
I.5	Avería de origen físico o lógico	[D]	8	10	M
I.6	Corte de suministro eléctrico	[D]	8	1	B
I.7	Condiciones inadecuadas temp.	[D]	8	100	A
I.11	Emanaciones electromagnéticas	[D]	8	100	A
E.2	Errores del administrador	[D]	8	100	A
E.2	Errores del administrador	[C]	10	100	MA
E.2	Errores del administrador	[I]	8	100	A
E.23	Errores de mantenimiento	[D]	8	10	M
E.24	Caída por agotamiento	[D]	8	1	B
E.25	Robo	[D]	8	100	A
E.25	Robo	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[D]	8	10	M
A.6	Abuso de privilegios de acceso	[I]	8	100	A
A.7	Uso no previsto	[C]	10	100	MA
A.7	Uso no previsto	[D]	8	100	A
A.7	Uso no previsto	[I]	8	100	A

A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	8	100	A
A.23	Manipulación de los equipos	[C]	10	100	MA
A.23	Manipulación de los equipos	[D]	8	100	A
A.24	Denegación de servicio	[D]	8	100	A
A.25	Robo	[D]	8	100	A
A.25	Robo	[C]	10	100	MA
A.26	Ataque destructivo	[D]	8	100	A

Tabla 112. Ficha del cálculo del impacto del activo HW.004

ID: HW.005 HW.006	Nombre: Impresora y escáner	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
N.1	Fuego	[D]	2	100	B
N.2	Daños por agua	[D]	2	100	B
N.*	Desastres naturales	[D]	2	100	B
I.1	Fuego	[D]	2	100	B
I.2	Daños por agua	[D]	2	100	B
I.*	Desastres industriales	[D]	2	100	B
I.3	Contaminación mecánica	[D]	2	10	MB
I.4	Contaminación electromagnética	[D]	2	10	MB
I.5	Avería de origen físico o lógico	[D]	2	10	MB
I.6	Corte de suministro eléctrico	[D]	2	1	MB

I.7	Condiciones inadecuadas temp.	[D]	2	10	MB
I.11	Emanaciones electromagnéticas	[D]	2	10	MB
E.2	Errores del administrador	[D]	2	100	B
E.2	Errores del administrador	[C]	1	10	MB
E.2	Errores del administrador	[I]	2	10	MB
E.23	Errores de mantenimiento	[D]	2	1	MB
E.24	Caída por agotamiento	[D]	2	1	MB
E.25	Robo	[D]	2	100	B
E.25	Robo	[C]	1	100	B
A.6	Abuso de privilegios de acceso	[C]	1	1	MB
A.6	Abuso de privilegios de acceso	[D]	2	100	B
A.6	Abuso de privilegios de acceso	[I]	2	1	MB
A.7	Uso no previsto	[C]	1	1	MB
A.7	Uso no previsto	[D]	2	100	B
A.7	Uso no previsto	[I]	2	1	MB
A.11	Acceso no autorizado	[C]	1	1	MB
A.11	Acceso no autorizado	[I]	2	1	MB
A.23	Manipulación de los equipos	[C]	1	1	MB
A.23	Manipulación de los equipos	[D]	2	10	MB
A.24	Denegación de servicio	[D]	2	10	MB
A.25	Robo	[D]	2	100	B
A.25	Robo	[C]	1	100	B

A.26	Ataque destructivo	[D]	2	100	B

Tabla 113. Ficha del cálculo del impacto del activo HW.005 y HW.006

ID: CO.001	Nombre: Internet Fibra	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.8	Fallo servicio de comunicaciones	[D]	5	10	B
E.2	Errores del administrador	[D]	5	10	B
E.2	Errores del administrador	[C]	9	100	A
E.2	Errores del administrador	[I]	5	10	B
E.9	Errores de [re-]encaminamiento	[C]	9	100	A
E.10	Errores de secuencia	[I]	5	10	B
E.15	Alteración accidental de inform.	[I]	5	1	MB
E.18	Destrucción de información	[I]	5	1	MB
E.19	Fugas de información	[C]	9	100	A
E.24	Caída por agotamiento	[D]	5	1	MB
A.5	Suplantación identidad usuario	[C]	9	100	A
A.5	Suplantación identidad usuario	[A]	9	100	A
A.5	Suplantación identidad usuario	[I]	5	10	B
A.6	Abuso de privilegios de acceso	[C]	9	100	A
A.6	Abuso de privilegios de acceso	[I]	5	1	MB
A.6	Abuso de privilegios de acceso	[D]	5	1	MB
A.7	Uso no previsto	[C]	9	100	A

A.7	Uso no previsto	[I]	5	1	MB
A.7	Uso no previsto	[D]	5	1	MB
A.9	[Re-]encaminamiento mensajes	[C]	9	100	A
A.10	Alteración de secuencia	[I]	5	1	MB
A.11	Acceso no autorizado	[C]	9	100	A
A.11	Acceso no autorizado	[I]	5	1	MB
A.12	Análisis de tráfico	[C]	9	100	A
A.14	Interceptación de información	[C]	9	100	A
A.15	Modificación deliberada inform.	[I]	5	10	B
A.19	Revelación de información	[C]	9	100	A
A.24	Denegación de servicio	[D]	5	1	MB

Tabla 114. Ficha del cálculo del impacto del activo CO.001

ID: CO.002 CO.003	Nombre: LAN, WiFi	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.8	Fallo servicio de comunicaciones	[D]	4	100	M
E.2	Errores del administrador	[D]	4	10	B
E.2	Errores del administrador	[C]	9	100	MA
E.2	Errores del administrador	[I]	4	10	B
E.9	Errores de [re-]encaminamiento	[C]	9	100	MA

E.10	Errores de secuencia	[I]	4	10	B
E.15	Alteración accidental de inform.	[I]	4	10	B
E.18	Destrucción de información	[I]	4	10	B
E.19	Fugas de información	[C]	9	100	MA
E.24	Caída por agotamiento	[D]	4	1	MB
A.5	Suplantación identidad usuario	[C]	9	100	MA
A.5	Suplantación identidad usuario	[A]	9	100	MA
A.5	Suplantación identidad usuario	[I]	4	10	B
A.6	Abuso de privilegios de acceso	[C]	9	100	MA
A.6	Abuso de privilegios de acceso	[I]	4	10	B
A.6	Abuso de privilegios de acceso	[D]	4	10	B
A.7	Uso no previsto	[C]	9	100	MA
A.7	Uso no previsto	[I]	4	10	B
A.7	Uso no previsto	[D]	4	1	MB
A.9	[Re-]encaminamiento mensajes	[C]	9	100	MA
A.10	Alteración de secuencia	[I]	4	10	B
A.11	Acceso no autorizado	[C]	9	100	MA
A.11	Acceso no autorizado	[I]	4	10	B
A.12	Análisis de tráfico	[C]	9	100	MA
A.14	Interceptación de información	[C]	9	100	MA
A.15	Modificación deliberada inform.	[I]	4	100	M
A.19	Revelación de información	[C]	9	100	MA

A.24	Denegación de servicio	[D]	4	1	MB

Tabla 115. Ficha del cálculo del impacto del activo CO.002 y CO.003

ID: CO.004	Nombre: Centralita	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.8	Fallo servicio de comunicaciones	[D]	4	100	M
E.2	Errores del administrador	[D]	4	10	B
E.2	Errores del administrador	[C]	8	100	A
E.2	Errores del administrador	[I]	4	10	B
E.9	Errores de [re-]encaminamiento	[C]	8	100	A
E.10	Errores de secuencia	[I]	4	10	B
E.15	Alteración accidental de inform.	[I]	4	10	B
E.18	Destrucción de información	[I]	4	10	B
E.19	Fugas de información	[C]	8	100	A
E.24	Caída por agotamiento	[D]	4	1	MB
A.5	Suplantación identidad usuario	[C]	8	100	A
A.5	Suplantación identidad usuario	[A]	8	100	A
A.5	Suplantación identidad usuario	[I]	4	10	B
A.6	Abuso de privilegios de acceso	[C]	8	100	A
A.6	Abuso de privilegios de acceso	[I]	4	10	B
A.6	Abuso de privilegios de acceso	[D]	4	10	B
A.7	Uso no previsto	[C]	8	100	A
A.7	Uso no previsto	[I]	4	10	B

A.7	Uso no previsto	[D]	4	1	MB
A.9	[Re-]encaminamiento mensajes	[C]	8	100	A
A.10	Alteración de secuencia	[I]	4	10	B
A.11	Acceso no autorizado	[C]	8	100	A
A.11	Acceso no autorizado	[I]	4	10	B
A.12	Análisis de tráfico	[C]	8	100	A
A.14	Interceptación de información	[C]	8	100	A
A.15	Modificación deliberada inform.	[I]	4	100	M
A.19	Revelación de información	[C]	8	100	A
A.24	Denegación de servicio	[D]	4	1	MB

Tabla 116. Ficha del cálculo del impacto del activo CO.004

ID: SW.001	Nombre: Outlook	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.5	Avería de origen físico o lógico	[D]	6	10	M
E.1	Errores de los usuarios	[D]	6	10	M
E.1	Errores de los usuarios	[I]	6	10	M
E.1	Errores de los usuarios	[C]	10	100	MA
E.2	Errores del administrador	[D]	6	10	M
E.2	Errores del administrador	[I]	6	10	M
E.2	Errores del administrador	[C]	10	100	MA
E.8	Difusión de software dañino	[D]	6	10	M

E.8	Difusión de software dañino	[I]	6	10	M
E.8	Difusión de software dañino	[C]	10	100	MA
E.9	Errores de [re-]encaminamiento	[C]	10	100	MA
E.10	Errores de secuencia	[I]	6	1	B
E.15	Alteración accidental inform.	[I]	6	1	B
E.18	Destrucción de información	[D]	6	100	A
E.19	Fugas de información	[C]	10	100	MA
E.20	Vulnerabilidades (software)	[I]	6	1	B
E.20	Vulnerabilidades (software)	[D]	6	1	B
E.20	Vulnerabilidades (software)	[C]	10	100	MA
E.21	Errores de mantenimiento	[I]	6	1	B
E.21	Errores de mantenimiento	[D]	6	1	B
A.5	Suplantación de la identidad	[C]	10	100	MA
A.5	Suplantación de la identidad	[A]	10	100	MA
A.5	Suplantación de la identidad	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[D]	6	10	M
A.7	Uso no previsto	[D]	6	10	M
A.7	Uso no previsto	[C]	10	100	MA
A.7	Uso no previsto	[I]	6	10	M
A.8	Difusión de software dañino	[D]	6	1	B

A.8	Difusión de software dañino	[I]	6	1	B
A.8	Difusión de software dañino	[C]	10	100	MA
A.9	[Re-]encaminamiento mensajes	[C]	10	100	MA
A.10	Alteración de secuencia	[I]	6	1	B
A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	6	10	M
A.15	Modificación deliberada Inform.	[I]	6	10	M
A.18	Destrucción de información	[D]	6	100	A
A.19	Revelación de información	[C]	10	100	MA
A.22	Manipulación de programas	[C]	10	100	MA
A.22	Manipulación de programas	[I]	6	10	M
A.22	Manipulación de programas	[D]	6	10	M

Tabla 117. Ficha del cálculo del impacto del activo SW.001

ID: SW.002 SW.003	Nombre: Word y Excel	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.5	Avería de origen físico o lógico	[D]	6	10	M
E.1	Errores de los usuarios	[D]	6	10	M
E.1	Errores de los usuarios	[I]	6	10	M
E.1	Errores de los usuarios	[C]	10	100	MA
E.2	Errores del administrador	[D]	6	10	M
E.2	Errores del administrador	[I]	6	10	M

E.2	Errores del administrador	[C]	10	100	MA
E.8	Difusión de software dañino	[D]	6	10	M
E.8	Difusión de software dañino	[I]	6	10	M
E.8	Difusión de software dañino	[C]	10	100	MA
E.9	Errores de [re-]encaminamiento	[C]	10	100	MA
E.10	Errores de secuencia	[I]	6	1	B
E.15	Alteración accidental inform.	[I]	6	1	B
E.18	Destrucción de información	[D]	6	100	A
E.19	Fugas de información	[C]	10	100	MA
E.20	Vulnerabilidades (software)	[I]	6	1	B
E.20	Vulnerabilidades (software)	[D]	6	1	B
E.20	Vulnerabilidades (software)	[C]	10	100	MA
E.21	Errores de mantenimiento	[I]	6	1	B
E.21	Errores de mantenimiento	[D]	6	1	B
A.5	Suplantación de la identidad	[C]	10	100	MA
A.5	Suplantación de la identidad	[A]	10	100	MA
A.5	Suplantación de la identidad	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[D]	6	10	M
A.7	Uso no previsto	[D]	6	10	M
A.7	Uso no previsto	[C]	10	100	MA

A.7	Uso no previsto	[I]	6	10	M
A.8	Difusión de software dañino	[D]	6	1	B
A.8	Difusión de software dañino	[I]	6	1	B
A.8	Difusión de software dañino	[C]	10	100	MA
A.9	[Re-]encaminamiento mensajes	[C]	10	100	MA
A.10	Alteración de secuencia	[I]	6	1	B
A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	6	10	M
A.15	Modificación deliberada Inform.	[I]	6	10	M
A.18	Destrucción de información	[D]	6	100	A
A.19	Revelación de información	[C]	10	100	MA
A.22	Manipulación de programas	[C]	10	100	MA
A.22	Manipulación de programas	[I]	6	10	M
A.22	Manipulación de programas	[D]	6	10	M

Tabla 118. Ficha del cálculo del impacto del activo SW.002 y SW.003

ID: SW.004 SW.005	Nombre: Cliente y Servidor ADA	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
I.5	Avería de origen físico o lógico	[D]	6	10	M
E.1	Errores de los usuarios	[D]	6	10	M
E.1	Errores de los usuarios	[I]	6	10	M
E.1	Errores de los usuarios	[C]	10	100	MA

E.2	Errores del administrador	[D]	6	10	M
E.2	Errores del administrador	[I]	6	10	M
E.2	Errores del administrador	[C]	10	100	MA
E.8	Difusión de software dañino	[D]	6	10	M
E.8	Difusión de software dañino	[I]	6	10	M
E.8	Difusión de software dañino	[C]	10	100	MA
E.9	Errores de [re-]encaminamiento	[C]	10	100	MA
E.10	Errores de secuencia	[I]	6	1	B
E.15	Alteración accidental inform.	[I]	6	1	B
E.18	Destrucción de información	[D]	6	100	A
E.19	Fugas de información	[C]	10	100	MA
E.20	Vulnerabilidades (software)	[I]	6	1	B
E.20	Vulnerabilidades (software)	[D]	6	1	B
E.20	Vulnerabilidades (software)	[C]	10	100	MA
E.21	Errores de mantenimiento	[I]	6	1	B
E.21	Errores de mantenimiento	[D]	6	1	B
A.5	Suplantación de la identidad	[C]	10	100	MA
A.5	Suplantación de la identidad	[A]	10	100	MA
A.5	Suplantación de la identidad	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[C]	10	100	MA
A.6	Abuso de privilegios de acceso	[I]	6	10	M
A.6	Abuso de privilegios de acceso	[D]	6	10	M

A.7	Uso no previsto	[D]	6	10	M
A.7	Uso no previsto	[C]	10	100	MA
A.7	Uso no previsto	[I]	6	10	M
A.8	Difusión de software dañino	[D]	6	1	B
A.8	Difusión de software dañino	[I]	6	1	B
A.8	Difusión de software dañino	[C]	10	100	MA
A.9	[Re-]encaminamiento mensajes	[C]	10	100	MA
A.10	Alteración de secuencia	[I]	6	1	B
A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	6	10	M
A.15	Modificación deliberada Inform.	[I]	6	10	M
A.18	Destrucción de información	[D]	6	100	A
A.19	Revelación de información	[C]	10	100	MA
A.22	Manipulación de programas	[C]	10	100	MA
A.22	Manipulación de programas	[I]	6	10	M
A.22	Manipulación de programas	[D]	6	10	M

Tabla 119. Ficha del cálculo del impacto del activo SW.004 y SW.005

ID: KE.001	Nombre: Certificado identidad abogado	Tipo de activo: [K] Claves criptográficas			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.1	Errores de los usuarios	[I]	6	100	A
E.1	Errores de los usuarios	[C]	9	100	MA

E.1	Errores de los usuarios	[D]	6	100	A
E.2	Errores del administrador	[D]	6	100	A
E.2	Errores del administrador	[I]	6	100	A
E.2	Errores del administrador	[C]	9	100	MA
E.15	Alteración accidental información	[I]	6	100	A
E.18	Destrucción de información	[D]	6	100	A
E.19	Fugas de información	[C]	9	100	MA
A.5	Suplantación identidad usuario	[C]	9	100	MA
A.5	Suplantación identidad usuario	[A]	9	100	MA
A.5	Suplantación identidad usuario	[I]	6	100	A
A.6	Abuso de privilegios de acceso	[C]	9	100	MA
A.6	Abuso de privilegios de acceso	[I]	6	100	A
A.6	Abuso de privilegios de acceso	[D]	6	100	A
A.11	Acceso no autorizado	[C]	9	100	MA
A.11	Acceso no autorizado	[I]	6	100	A
A.15	Modificación deliberada inform.	[I]	6	100	A
A.18	Destrucción de información	[D]	6	100	A
A.19	Revelación de información	[C]	9	100	MA

Tabla 120. Ficha del cálculo del impacto del activo KE.001

ID: LU.001	Nombre: Piso donde se ubica el despacho	Tipo de activo: [L] Instalaciones			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto

N.1	Fuego	[D]	8	100	A
N.2	Daños por agua	[D]	8	10	M
N.*	Desastres naturales	[D]	8	10	M
I.1	Fuego	[D]	8	100	A
I.2	Daños por agua	[D]	8	10	M
I.*	Desastres industriales	[D]	8	10	M
I.11	Emanaciones electromagnéticas	[C]	10	10	A
I.15	Alteración accidental información	[I]	10	10	A
E.18	Destrucción de información	[D]	8	100	A
E.19	Fugas de información	[C]	10	100	MA
A.7	Uso no previsto	[D]	8	10	M
A.7	Uso no previsto	[C]	10	100	MA
A.7	Uso no previsto	[I]	10	10	A
A.11	Acceso no autorizado	[C]	10	100	MA
A.11	Acceso no autorizado	[I]	10	10	A
A.15	Modificación deliberada inform.	[I]	10	100	MA
A.18	Destrucción de información	[D]	8	100	A
A.19	Revelación de información	[C]	10	100	MA
A.26	Ataque destructivo	[D]	8	100	A
A.27	Ocupación enemiga	[D]	8	100	A
A.27	Ocupación enemiga	[C]	10	100	MA

Tabla 121. Ficha del cálculo del impacto del activo LU.001

ID: PR.001	Nombre: Abogado	Tipo de activo: [P] Personal			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.7	Deficiencias en la organización	[D]	10	1	M
E.19	Fugas de información	[C]	10	100	MA
E.28	Indisponibilidad del personal	[D]	10	100	MA
A.28	Indisponibilidad del personal	[D]	10	100	MA
A.29	Extorsión	[C]	10	100	MA
A.29	Extorsión	[I]	10	100	MA
A.29	Extorsión	[D]	10	100	MA
A.30	Ingeniería social	[C]	10	100	MA
A.30	Ingeniería social	[I]	10	100	MA
A.30	Ingeniería social	[D]	10	100	MA

Tabla 122. Ficha del cálculo del impacto del activo PR.001

ID: PR.002	Nombre: Secretaria	Tipo de activo: [P] Personal			
Tipo	Amenaza	Dimensión	Valor	Degradación	Impacto
E.7	Deficiencias en la organización	[D]	4	1	MB
E.19	Fugas de información	[C]	8	10	M
E.28	Indisponibilidad del personal	[D]	4	100	M
A.28	Indisponibilidad del personal	[D]	4	100	M
A.29	Extorsión	[C]	8	10	M
A.29	Extorsión	[I]	8	10	M
A.29	Extorsión	[D]	4	10	B

A.30	Ingeniería social	[C]	8	100	A
A.30	Ingeniería social	[I]	8	100	A
A.30	Ingeniería social	[D]	4	100	M

Tabla 123. Ficha del cálculo del impacto del activo PR.002

Cálculo del riesgo

Es el momento ahora de calcular el riesgo para cada activo. El riesgo se traduce como la probabilidad de que una amenaza impacte a un activo. Así para el cálculo del riesgo estimaremos la probabilidad de que ocurra cada una de las amenazas anteriores y calcularemos el riesgo en base a la siguiente tabla:

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 124. Tabla para el Cálculo del riesgo

ID: ES.001	Nombre: Base de datos ADA	Tipo de activo: [info] Datos / información esencial			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.1	Errores de los usuarios	[I]	A	B	A
E.1	Errores de los usuarios	[C]	A	B	A
E.1	Errores de los usuarios	[D]	MA	B	MA
E.2	Errores del administrador	[I]	A	B	A
E.2	Errores del administrador	[C]	A	B	A
E.2	Errores del administrador	[D]	MA	B	MA
E.15	Alteración accidental de la inf.	[I]	A	MB	M
E.18	Destrucción de la información	[D]	MA	MB	A
E.19	Fugas de información	[C]	A	MB	M

A.5	Suplantación identidad usuario	[C]	A	MB	M
A.5	Suplantación identidad usuario	[A]	A	MB	M
A.5	Suplantación identidad usuario	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[C]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[D]	MA	MB	A
A.11	Acceso no autorizado	[C]	A	MB	M
A.11	Acceso no autorizado	[I]	A	MB	M
A.15	Modificación deliberada de inf.	[I]	A	MB	M
A.18	Destrucción de la información	[D]	MA	MB	A
A.19	Revelación de información	[C]	A	MB	M

Tabla 125. Cálculo del riesgo para el activo ES.001

ID: ES.002	Nombre: Fichero Outlook	Tipo de activo: [info] Datos / información esencial			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.1	Errores de los usuarios	[I]	A	B	A
E.1	Errores de los usuarios	[C]	A	B	A
E.1	Errores de los usuarios	[D]	MA	B	MA
E.2	Errores del administrador	[I]	A	B	A
E.2	Errores del administrador	[C]	A	B	A
E.2	Errores del administrador	[D]	MA	B	MA
E.15	Alteración accidental de la inf.	[I]	A	MB	M
E.18	Destrucción de la información	[D]	MA	MB	A

E.19	Fugas de información	[C]	A	MB	M
A.5	Suplantación identidad usuario	[C]	A	MB	M
A.5	Suplantación identidad usuario	[A]	A	MB	M
A.5	Suplantación identidad usuario	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[C]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[D]	MA	MB	A
A.11	Acceso no autorizado	[C]	A	MB	M
A.11	Acceso no autorizado	[I]	A	MB	M
A.15	Modificación deliberada de inf.	[I]	A	MB	M
A.18	Destrucción de la información	[D]	MA	MB	A
A.19	Revelación de información	[C]	A	MB	M

Tabla 126. Cálculo del riesgo para el activo ES.002

ID: ES.003	Nombre: Doc. ofi. casos desp	Tipo de activo: [info] Datos / información esencial			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.1	Errores de los usuarios	[I]	A	B	A
E.1	Errores de los usuarios	[C]	A	B	A
E.1	Errores de los usuarios	[D]	MA	B	MA
E.2	Errores del administrador	[I]	A	B	A
E.2	Errores del administrador	[C]	A	B	A
E.2	Errores del administrador	[D]	MA	B	MA
E.15	Alteración accidental de la inf.	[I]	A	MB	M

E.18	Destrucción de la información	[D]	MA	MB	A
E.19	Fugas de información	[C]	A	MB	M
A.5	Suplantación identidad usuario	[C]	A	MB	M
A.5	Suplantación identidad usuario	[A]	A	MB	M
A.5	Suplantación identidad usuario	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[C]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[D]	MA	MB	A
A.11	Acceso no autorizado	[C]	A	MB	M
A.11	Acceso no autorizado	[I]	A	MB	M
A.15	Modificación deliberada de inf.	[I]	A	MB	M
A.18	Destrucción de la información	[D]	MA	MB	A
A.19	Revelación de información	[C]	A	MB	M

Tabla 127. Cálculo del riesgo para el activo ES.003

ID: ES.004	Nombre: Página Web	Tipo de activo: [service] Activos esenciales: Servicio			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.1	Errores de los usuarios	[I]	B	MB	MB
E.1	Errores de los usuarios	[C]	M	MB	B
E.1	Errores de los usuarios	[D]	M	MB	B
E.2	Errores del administrador	[I]	B	MB	MB
E.2	Errores del administrador	[C]	M	MB	B
E.2	Errores del administrador	[D]	M	MB	B

E.15	Alteración accidental de la inf.	[I]	B	B	B
E.18	Destrucción de la información	[D]	M	MB	B
E.19	Fugas de información	[C]	M	MB	B
A.5	Suplantación identidad usuario	[C]	M	B	M
A.5	Suplantación identidad usuario	[A]	M	B	M
A.5	Suplantación identidad usuario	[I]	B	B	B
A.6	Abuso de privilegios de acceso	[C]	M	B	M
A.6	Abuso de privilegios de acceso	[I]	B	B	B
A.6	Abuso de privilegios de acceso	[D]	M	B	M
A.11	Acceso no autorizado	[C]	M	B	M
A.11	Acceso no autorizado	[I]	B	B	B
A.15	Modificación deliberada de inf.	[I]	B	MB	MB
A.18	Destrucción de la información	[D]	M	MB	B
A.19	Revelación de información	[C]	M	MB	B

Tabla 128. Cálculo del riesgo para el activo ES.004

ID: HW.001 HW.002	Nombre: PCs Despacho	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
N.1	Fuego	[D]	A	MB	M
N.2	Daños por agua	[D]	A	MB	M
N.*	Desastres naturales	[D]	A	MB	M
I.1	Fuego	[D]	A	B	A

I.2	Daños por agua	[D]	A	B	A
I.*	Desastres industriales	[D]	A	MB	M
I.3	Contaminación mecánica	[D]	M	M	M
I.4	Contaminación electromagnética	[D]	A	MB	M
I.5	Avería de origen físico o lógico	[D]	M	B	M
I.6	Corte de suministro eléctrico	[D]	B	B	B
I.7	Condiciones inadecuadas temp.	[D]	A	MB	M
I.11	Emanaciones electromagnéticas	[D]	B	MB	MB
E.2	Errores del administrador	[D]	B	B	B
E.2	Errores del administrador	[C]	M	B	M
E.2	Errores del administrador	[I]	B	B	B
E.23	Errores de mantenimiento	[D]	M	MB	B
E.24	Caída por agotamiento	[D]	M	MB	B
E.25	Robo	[D]	A	MB	M
E.25	Robo	[C]	M	MB	B
A.6	Abuso de privilegios de acceso	[C]	M	MB	B
A.6	Abuso de privilegios de acceso	[D]	M	MB	B
A.6	Abuso de privilegios de acceso	[I]	A	MB	M
A.7	Uso no previsto	[C]	M	B	M
A.7	Uso no previsto	[D]	B	B	B
A.7	Uso no previsto	[I]	M	B	M
A.11	Acceso no autorizado	[C]	M	MB	B

A.11	Acceso no autorizado	[I]	A	MB	M
A.23	Manipulación de los equipos	[C]	M	MB	B
A.23	Manipulación de los equipos	[D]	M	MB	B
A.24	Denegación de servicio	[D]	M	MB	B
A.25	Robo	[D]	A	MB	M
A.25	Robo	[C]	M	MB	B
A.26	Ataque destructivo	[D]	A	MB	M

Tabla 129. Cálculo del riesgo para el activo HW.001 y HW.002

ID: HW.003	Nombre: NAS	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
N.1	Fuego	[D]	MA	MB	A
N.2	Daños por agua	[D]	MA	MB	A
N.*	Desastres naturales	[D]	MA	MB	A
I.1	Fuego	[D]	MA	B	MA
I.2	Daños por agua	[D]	MA	B	MA
I.*	Desastres industriales	[D]	MA	MB	A
I.3	Contaminación mecánica	[D]	A	M	A
I.4	Contaminación electromagnética	[D]	MA	MB	A
I.5	Avería de origen físico o lógico	[D]	A	B	A
I.6	Corte de suministro eléctrico	[D]	M	B	M
I.7	Condiciones inadecuadas temp.	[D]	MA	MB	A
I.11	Emanaciones electromagnéticas	[D]	M	MB	B

E.2	Errores del administrador	[D]	M	B	M
E.2	Errores del administrador	[C]	MA	B	MA
E.2	Errores del administrador	[I]	A	B	A
E.23	Errores de mantenimiento	[D]	A	MB	M
E.24	Caída por agotamiento	[D]	A	MB	M
E.25	Robo	[D]	MA	B	MA
E.25	Robo	[C]	MA	B	MA
A.6	Abuso de privilegios de acceso	[C]	MA	MB	A
A.6	Abuso de privilegios de acceso	[D]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	MA	MB	A
A.7	Uso no previsto	[C]	MA	MB	A
A.7	Uso no previsto	[D]	M	MB	B
A.7	Uso no previsto	[I]	MA	MB	A
A.11	Acceso no autorizado	[C]	MA	B	MA
A.11	Acceso no autorizado	[I]	MA	B	MA
A.23	Manipulación de los equipos	[C]	MA	MB	A
A.23	Manipulación de los equipos	[D]	A	MB	M
A.24	Denegación de servicio	[D]	A	MB	M
A.25	Robo	[D]	MA	B	MA
A.25	Robo	[C]	MA	B	MA
A.26	Ataque destructivo	[D]	MA	MB	A

Tabla 130. Cálculo del riesgo para el activo HW.003

ID: HW.004	Nombre: Router	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
N.1	Fuego	[D]	A	MB	M
N.2	Daños por agua	[D]	A	MB	M
N.*	Desastres naturales	[D]	A	MB	M
I.1	Fuego	[D]	A	B	A
I.2	Daños por agua	[D]	A	B	A
I.*	Desastres industriales	[D]	A	MB	M
I.3	Contaminación mecánica	[D]	M	B	M
I.4	Contaminación electromagnética	[D]	M	B	M
I.5	Avería de origen físico o lógico	[D]	M	B	M
I.6	Corte de suministro eléctrico	[D]	B	B	B
I.7	Condiciones inadecuadas temp.	[D]	A	MB	M
I.11	Emanaciones electromagnéticas	[D]	A	MB	M
E.2	Errores del administrador	[D]	A	B	A
E.2	Errores del administrador	[C]	MA	B	MA
E.2	Errores del administrador	[I]	A	B	A
E.23	Errores de mantenimiento	[D]	M	MB	B
E.24	Caída por agotamiento	[D]	B	MB	MB
E.25	Robo	[D]	A	B	A
E.25	Robo	[C]	MA	B	MA
A.6	Abuso de privilegios de acceso	[C]	MA	B	MA

A.6	Abuso de privilegios de acceso	[D]	M	B	M
A.6	Abuso de privilegios de acceso	[I]	A	B	A
A.7	Uso no previsto	[C]	MA	B	MA
A.7	Uso no previsto	[D]	A	B	A
A.7	Uso no previsto	[I]	A	B	A
A.11	Acceso no autorizado	[C]	MA	B	MA
A.11	Acceso no autorizado	[I]	A	B	A
A.23	Manipulación de los equipos	[C]	MA	MB	A
A.23	Manipulación de los equipos	[D]	A	MB	M
A.24	Denegación de servicio	[D]	A	MB	M
A.25	Robo	[D]	A	B	A
A.25	Robo	[C]	MA	B	MA
A.26	Ataque destructivo	[D]	A	MB	M

Tabla 131. Cálculo del riesgo para el activo HW.004

ID: HW.005 HW.006	Nombre: Impresora y Scanner	Tipo de activo: [HW] Equipos informáticos (hardware)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
N.1	Fuego	[D]	B	MB	MB
N.2	Daños por agua	[D]	B	MB	MB
N.*	Desastres naturales	[D]	B	MB	MB
I.1	Fuego	[D]	B	B	B

I.2	Daños por agua	[D]	B	B	B
I.*	Desastres industriales	[D]	B	MB	MB
I.3	Contaminación mecánica	[D]	MB	B	MB
I.4	Contaminación electromagnética	[D]	MB	B	MB
I.5	Avería de origen físico o lógico	[D]	MB	B	MB
I.6	Corte de suministro eléctrico	[D]	MB	B	MB
I.7	Condiciones inadecuadas temp.	[D]	MB	MB	MB
I.11	Emanaciones electromagnéticas	[D]	MB	MB	MB
E.2	Errores del administrador	[D]	B	B	B
E.2	Errores del administrador	[C]	MB	B	MB
E.2	Errores del administrador	[I]	MB	B	MB
E.23	Errores de mantenimiento	[D]	MB	MB	MB
E.24	Caída por agotamiento	[D]	MB	MB	MB
E.25	Robo	[D]	B	B	B
E.25	Robo	[C]	B	B	B
A.6	Abuso de privilegios de acceso	[C]	MB	B	MB
A.6	Abuso de privilegios de acceso	[D]	B	B	B
A.6	Abuso de privilegios de acceso	[I]	MB	B	MB
A.7	Uso no previsto	[C]	MB	B	MB
A.7	Uso no previsto	[D]	B	B	B
A.7	Uso no previsto	[I]	MB	B	MB
A.11	Acceso no autorizado	[C]	MB	B	MB

A.11	Acceso no autorizado	[I]	MB	B	MB
A.23	Manipulación de los equipos	[C]	MB	MB	MB
A.23	Manipulación de los equipos	[D]	MB	MB	MB
A.24	Denegación de servicio	[D]	MB	MB	MB
A.25	Robo	[D]	B	B	B
A.25	Robo	[C]	B	B	B
A.26	Ataque destructivo	[D]	B	MB	MB

Tabla 132. Cálculo del riesgo para el activo HW.005 y HW.006

ID: CO.001	Nombre: Internet fibra	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
I.8	Fallo servicio de comunicaciones	[D]	B	MB	MB
E.2	Errores del administrador	[D]	B	MB	MB
E.2	Errores del administrador	[C]	A	MB	M
E.2	Errores del administrador	[I]	B	MB	MB
E.9	Errores de [re-]encaminamiento	[C]	A	MB	M
E.10	Errores de secuencia	[I]	B	MB	MB
E.15	Alteración accidental de inform.	[I]	MB	MB	MB
E.18	Destrucción de información	[I]	MB	MB	MB
E.19	Fugas de información	[C]	A	MB	M
E.24	Caída por agotamiento	[D]	MB	MB	MB
A.5	Suplantación identidad usuario	[C]	A	MB	M

A.5	Suplantación identidad usuario	[A]	A	MB	M
A.5	Suplantación identidad usuario	[I]	B	MB	MB
A.6	Abuso de privilegios de acceso	[C]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	MB	MB	MB
A.6	Abuso de privilegios de acceso	[D]	MB	MB	MB
A.7	Uso no previsto	[C]	A	B	A
A.7	Uso no previsto	[I]	MB	B	MB
A.7	Uso no previsto	[D]	MB	B	MB
A.9	[Re-]encaminamiento mensajes	[C]	A	B	A
A.10	Alteración de secuencia	[I]	MB	B	MB
A.11	Acceso no autorizado	[C]	A	B	A
A.11	Acceso no autorizado	[I]	MB	B	MB
A.12	Análisis de tráfico	[C]	A	MB	M
A.14	Interceptación de información	[C]	A	MB	M
A.15	Modificación deliberada inform.	[I]	B	MB	MB
A.19	Revelación de información	[C]	A	MB	M
A.24	Denegación de servicio	[D]	MB	B	MB

Tabla 133. Cálculo del riesgo para el activo CO.001

ID: CO.002 CO.003	Nombre: LAN, WiFi	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
I.8	Fallo servicio de comunicaciones	[D]	M	MB	B

E.2	Errores del administrador	[D]	B	B	B
E.2	Errores del administrador	[C]	MA	B	MA
E.2	Errores del administrador	[I]	B	B	B
E.9	Errores de [re-]encaminamiento	[C]	MA	MB	A
E.10	Errores de secuencia	[I]	B	MB	MB
E.15	Alteración accidental de inform.	[I]	B	MB	MB
E.18	Destrucción de información	[I]	B	MB	MB
E.19	Fugas de información	[C]	MA	MB	A
E.24	Caída por agotamiento	[D]	MB	MB	MB
A.5	Suplantación identidad usuario	[C]	MA	M	MA
A.5	Suplantación identidad usuario	[A]	MA	M	MA
A.5	Suplantación identidad usuario	[I]	B	M	B
A.6	Abuso de privilegios de acceso	[C]	MA	M	MA
A.6	Abuso de privilegios de acceso	[I]	B	M	B
A.6	Abuso de privilegios de acceso	[D]	B	M	B
A.7	Uso no previsto	[C]	MA	B	MA
A.7	Uso no previsto	[I]	B	B	B
A.7	Uso no previsto	[D]	MB	B	MB
A.9	[Re-]encaminamiento mensajes	[C]	MA	B	MA
A.10	Alteración de secuencia	[I]	B	B	B
A.11	Acceso no autorizado	[C]	MA	M	MA
A.11	Acceso no autorizado	[I]	B	M	B

A.12	Análisis de tráfico	[C]	MA	M	MA
A.14	Interceptación de información	[C]	MA	M	MA
A.15	Modificación deliberada inform.	[I]	M	M	M
A.19	Revelación de información	[C]	MA	M	MA
A.24	Denegación de servicio	[D]	MB	M	MB

Tabla 134. Cálculo del riesgo para el activo CO.002 y CO.003

ID: CO.004	Nombre: Centralita	Tipo de activo: [COM] Redes de comunicaciones			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
I.8	Fallo servicio de comunicaciones	[D]	M	MB	B
E.2	Errores del administrador	[D]	B	MB	MB
E.2	Errores del administrador	[C]	A	MB	M
E.2	Errores del administrador	[I]	B	MB	MB
E.9	Errores de [re-]encaminamiento	[C]	A	MB	M
E.10	Errores de secuencia	[I]	B	MB	MB
E.15	Alteración accidental de inform.	[I]	B	MB	MB
E.18	Destrucción de información	[I]	B	MB	MB
E.19	Fugas de información	[C]	A	MB	M
E.24	Caída por agotamiento	[D]	MB	MB	MB
A.5	Suplantación identidad usuario	[C]	A	MB	M
A.5	Suplantación identidad usuario	[A]	A	MB	M
A.5	Suplantación identidad usuario	[I]	B	MB	MB

A.6	Abuso de privilegios de acceso	[C]	A	MB	M
A.6	Abuso de privilegios de acceso	[I]	B	MB	MB
A.6	Abuso de privilegios de acceso	[D]	B	MB	MB
A.7	Uso no previsto	[C]	A	B	M
A.7	Uso no previsto	[I]	B	B	MB
A.7	Uso no previsto	[D]	MB	B	MB
A.9	[Re-]encaminamiento mensajes	[C]	A	MB	M
A.10	Alteración de secuencia	[I]	B	MB	MB
A.11	Acceso no autorizado	[C]	A	MB	M
A.11	Acceso no autorizado	[I]	B	MB	MB
A.12	Análisis de tráfico	[C]	A	MB	M
A.14	Interceptación de información	[C]	A	MB	M
A.15	Modificación deliberada inform.	[I]	M	MB	B
A.19	Revelación de información	[C]	A	MB	M
A.24	Denegación de servicio	[D]	MB	MB	MB

Tabla 135. Cálculo del riesgo para el activo CO.004

ID: SW.001	Nombre: Outlook	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
I.5	Avería de origen físico o lógico	[D]	M	MB	B
E.1	Errores de los usuarios	[D]	M	B	M
E.1	Errores de los usuarios	[I]	M	B	M
E.1	Errores de los usuarios	[C]	MA	B	MA

E.2	Errores del administrador	[D]	M	B	M
E.2	Errores del administrador	[I]	M	B	M
E.2	Errores del administrador	[C]	MA	B	MA
E.8	Difusión de software dañino	[D]	M	M	M
E.8	Difusión de software dañino	[I]	M	M	M
E.8	Difusión de software dañino	[C]	MA	M	MA
E.9	Errores de [re-]encaminamiento	[C]	MA	MB	A
E.10	Errores de secuencia	[I]	B	MB	MB
E.15	Alteración accidental inform.	[I]	B	MB	MB
E.18	Destrucción de información	[D]	A	MB	M
E.19	Fugas de información	[C]	MA	MB	A
E.20	Vulnerabilidades (software)	[I]	B	MB	MB
E.20	Vulnerabilidades (software)	[D]	B	MB	MB
E.20	Vulnerabilidades (software)	[C]	MA	MB	A
E.21	Errores de mantenimiento	[I]	B	MB	MB
E.21	Errores de mantenimiento	[D]	B	MB	MB
A.5	Suplantación de la identidad	[C]	MA	B	MA
A.5	Suplantación de la identidad	[A]	MA	B	MA
A.5	Suplantación de la identidad	[I]	M	B	M
A.6	Abuso de privilegios de acceso	[C]	MA	B	MA
A.6	Abuso de privilegios de acceso	[I]	M	B	M
A.6	Abuso de privilegios de acceso	[D]	M	B	M

A.7	Uso no previsto	[D]	M	B	M
A.7	Uso no previsto	[C]	MA	B	MA
A.7	Uso no previsto	[I]	M	B	M
A.8	Difusión de software dañino	[D]	B	M	B
A.8	Difusión de software dañino	[I]	B	M	B
A.8	Difusión de software dañino	[C]	MA	M	MA
A.9	[Re-]encaminamiento mensajes	[C]	MA	MB	A
A.10	Alteración de secuencia	[I]	B	MB	MB
A.11	Acceso no autorizado	[C]	MA	MB	A
A.11	Acceso no autorizado	[I]	M	MB	B
A.15	Modificación deliberada Inform.	[I]	M	B	M
A.18	Destrucción de información	[D]	A	MB	M
A.19	Revelación de información	[C]	MA	MB	A
A.22	Manipulación de programas	[C]	MA	MB	A
A.22	Manipulación de programas	[I]	M	MB	B
A.22	Manipulación de programas	[D]	M	MB	B

Tabla 136. Cálculo del riesgo para el activo SW.001

ID: SW.002 SW.003	Nombre: Word, Excel	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
I.5	Avería de origen físico o lógico	[D]	M	MB	B
E.1	Errores de los usuarios	[D]	M	B	M

E.1	Errores de los usuarios	[I]	M	B	M
E.1	Errores de los usuarios	[C]	MA	B	MA
E.2	Errores del administrador	[D]	M	B	M
E.2	Errores del administrador	[I]	M	B	M
E.2	Errores del administrador	[C]	MA	B	MA
E.8	Difusión de software dañino	[D]	M	M	M
E.8	Difusión de software dañino	[I]	M	M	M
E.8	Difusión de software dañino	[C]	MA	M	MA
E.9	Errores de [re-]encaminamiento	[C]	MA	MB	A
E.10	Errores de secuencia	[I]	B	MB	B
E.15	Alteración accidental inform.	[I]	B	MB	B
E.18	Destrucción de información	[D]	A	MB	M
E.19	Fugas de información	[C]	MA	MB	A
E.20	Vulnerabilidades (software)	[I]	B	MB	MB
E.20	Vulnerabilidades (software)	[D]	B	MB	MB
E.20	Vulnerabilidades (software)	[C]	MA	MB	A
E.21	Errores de mantenimiento	[I]	B	MB	MB
E.21	Errores de mantenimiento	[D]	B	MB	MB
A.5	Suplantación de la identidad	[C]	MA	B	MA
A.5	Suplantación de la identidad	[A]	MA	B	MA
A.5	Suplantación de la identidad	[I]	M	B	M
A.6	Abuso de privilegios de acceso	[C]	MA	B	MA

A.6	Abuso de privilegios de acceso	[I]	M	B	M
A.6	Abuso de privilegios de acceso	[D]	M	B	M
A.7	Uso no previsto	[D]	M	B	M
A.7	Uso no previsto	[C]	MA	B	MA
A.7	Uso no previsto	[I]	M	B	M
A.8	Difusión de software dañino	[D]	B	M	B
A.8	Difusión de software dañino	[I]	B	M	B
A.8	Difusión de software dañino	[C]	MA	M	MA
A.9	[Re-]encaminamiento mensajes	[C]	MA	MB	A
A.10	Alteración de secuencia	[I]	B	MB	MB
A.11	Acceso no autorizado	[C]	MA	MB	A
A.11	Acceso no autorizado	[I]	M	MB	B
A.15	Modificación deliberada Inform.	[I]	M	B	M
A.18	Destrucción de información	[D]	A	MB	M
A.19	Revelación de información	[C]	MA	MB	A
A.22	Manipulación de programas	[C]	MA	MB	A
A.22	Manipulación de programas	[I]	M	MB	B
A.22	Manipulación de programas	[D]	M	MB	B

Tabla 137. Cálculo del riesgo para el activo SW.002 y SW.003

ID: SW.004 SW.005	Nombre: Cliente y Servidor ADA	Tipo de activo: [SW] Aplicaciones (software)			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo

I.5	Avería de origen físico o lógico	[D]	M	MB	B
E.1	Errores de los usuarios	[D]	M	MB	B
E.1	Errores de los usuarios	[I]	M	MB	B
E.1	Errores de los usuarios	[C]	MA	MB	A
E.2	Errores del administrador	[D]	M	MB	B
E.2	Errores del administrador	[I]	M	MB	B
E.2	Errores del administrador	[C]	MA	MB	A
E.8	Difusión de software dañino	[D]	M	MB	B
E.8	Difusión de software dañino	[I]	M	MB	B
E.8	Difusión de software dañino	[C]	MA	MB	A
E.9	Errores de [re-]encaminamiento	[C]	MA	MB	A
E.10	Errores de secuencia	[I]	B	MB	MB
E.15	Alteración accidental inform.	[I]	B	MB	MB
E.18	Destrucción de información	[D]	A	MB	M
E.19	Fugas de información	[C]	MA	MB	A
E.20	Vulnerabilidades (software)	[I]	B	MB	MB
E.20	Vulnerabilidades (software)	[D]	B	MB	MB
E.20	Vulnerabilidades (software)	[C]	MA	MB	A
E.21	Errores de mantenimiento	[I]	B	MB	MB
E.21	Errores de mantenimiento	[D]	B	MB	MB
A.5	Suplantación de la identidad	[C]	MA	MB	A
A.5	Suplantación de la identidad	[A]	MA	MB	A

A.5	Suplantación de la identidad	[I]	M	MB	B
A.6	Abuso de privilegios de acceso	[C]	MA	MB	A
A.6	Abuso de privilegios de acceso	[I]	M	MB	B
A.6	Abuso de privilegios de acceso	[D]	M	MB	B
A.7	Uso no previsto	[D]	M	MB	B
A.7	Uso no previsto	[C]	MA	MB	A
A.7	Uso no previsto	[I]	M	MB	B
A.8	Difusión de software dañino	[D]	B	MB	MB
A.8	Difusión de software dañino	[I]	B	MB	MB
A.8	Difusión de software dañino	[C]	MA	MB	A
A.9	[Re-]encaminamiento mensajes	[C]	MA	MB	A
A.10	Alteración de secuencia	[I]	B	MB	MB
A.11	Acceso no autorizado	[C]	MA	MB	A
A.11	Acceso no autorizado	[I]	M	MB	B
A.15	Modificación deliberada Inform.	[I]	M	MB	B
A.18	Destrucción de información	[D]	A	MB	M
A.19	Revelación de información	[C]	MA	MB	A
A.22	Manipulación de programas	[C]	MA	MB	A
A.22	Manipulación de programas	[I]	M	MB	B
A.22	Manipulación de programas	[D]	M	MB	B

Tabla 138. Cálculo del riesgo para el activo SW.004 y SW.005

ID: KE.001	Nombre: Certificado identidad abogado	Tipo de activo: [K] Claves criptográficas			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.1	Errores de los usuarios	[I]	A	MB	M
E.1	Errores de los usuarios	[C]	MA	MB	A
E.1	Errores de los usuarios	[D]	A	MB	M
E.2	Errores del administrador	[D]	A	MB	M
E.2	Errores del administrador	[I]	A	MB	M
E.2	Errores del administrador	[C]	MA	MB	A
E.15	Alteración accidental información	[I]	A	MB	M
E.18	Destrucción de información	[D]	A	MB	M
E.19	Fugas de información	[C]	MA	MB	A
A.5	Suplantación identidad usuario	[C]	MA	MB	A
A.5	Suplantación identidad usuario	[A]	MA	MB	A
A.5	Suplantación identidad usuario	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[C]	MA	MB	A
A.6	Abuso de privilegios de acceso	[I]	A	MB	M
A.6	Abuso de privilegios de acceso	[D]	A	MB	M
A.11	Acceso no autorizado	[C]	MA	MB	A
A.11	Acceso no autorizado	[I]	A	MB	M
A.15	Modificación deliberada inform.	[I]	A	MB	M
A.18	Destrucción de información	[D]	A	MB	M
A.19	Revelación de información	[C]	MA	MB	A

Tabla 139. Cálculo del riesgo para el activo KE.001

ID: LU.001	Nombre: Piso donde se ubica el despacho	Tipo de activo: [L] Instalaciones			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
N.1	Fuego	[D]	A	MB	M
N.2	Daños por agua	[D]	M	MB	B
N.*	Desastres naturales	[D]	M	MB	B
I.1	Fuego	[D]	A	MB	M
I.2	Daños por agua	[D]	M	MB	B
I.*	Desastres industriales	[D]	M	MB	B
I.11	Emanaciones electromagnéticas	[C]	A	MB	M
I.15	Alteración accidental información	[I]	A	MB	M
E.18	Destrucción de información	[D]	A	MB	M
E.19	Fugas de información	[C]	MA	MB	A
A.7	Uso no previsto	[D]	M	MB	B
A.7	Uso no previsto	[C]	MA	MB	A
A.7	Uso no previsto	[I]	A	MB	M
A.11	Acceso no autorizado	[C]	MA	MB	A
A.11	Acceso no autorizado	[I]	A	MB	M
A.15	Modificación deliberada inform.	[I]	MA	MB	A
A.18	Destrucción de información	[D]	A	MB	M
A.19	Revelación de información	[C]	MA	MB	A

A.26	Ataque destructivo	[D]	A	MB	M
A.27	Ocupación enemiga	[D]	A	MB	M
A.27	Ocupación enemiga	[C]	MA	MB	A

Tabla 140. Cálculo del riesgo para el activo LU.001

ID: PR.001	Nombre: Abogado	Tipo de activo: [P] Personal			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.7	Deficiencias en la organización	[D]	M	MB	B
E.19	Fugas de información	[C]	MA	MB	A
E.28	Indisponibilidad del personal	[D]	MA	MB	A
A.28	Indisponibilidad del personal	[D]	MA	MB	A
A.29	Extorsión	[C]	MA	MB	A
A.29	Extorsión	[I]	MA	MB	A
A.29	Extorsión	[D]	MA	MB	A
A.30	Ingeniería social	[C]	MA	MB	A
A.30	Ingeniería social	[I]	MA	MB	A
A.30	Ingeniería social	[D]	MA	MB	A

Tabla 141. Cálculo del riesgo para el activo PR.001

ID: PR.002	Nombre: Secretaria	Tipo de activo: [P] Personal			
Tipo	Amenaza	Dimensión	Impacto	Prob.	Riesgo
E.7	Deficiencias en la organización	[D]	MB	MB	MB
E.19	Fugas de información	[C]	M	B	M

E.28	Indisponibilidad del personal	[D]	M	B	M
A.28	Indisponibilidad del personal	[D]	M	B	M
A.29	Extorsión	[C]	M	MB	B
A.29	Extorsión	[I]	M	MB	B
A.29	Extorsión	[D]	B	MB	MB
A.30	Ingeniería social	[C]	A	B	A
A.30	Ingeniería social	[I]	A	B	A
A.30	Ingeniería social	[D]	M	MB	B

Tabla 142. Cálculo del riesgo para el activo PR.002

Aplicación de Salvaguardas y Calculo del Impacto y Riesgo residuales

Una vez calculado el riesgo de cada activo e identificado aquellos que están expuestos a riesgos más elevados, es el momento de actuar sobre ellos para aplicar salvaguardas que puedan protegerlos reduciendo el impacto de la amenaza o la probabilidad de que ésta suceda. Así, para cada uno de los activos esenciales aplicaremos las salvaguardas adecuadas y con el nuevo valor obtenido calcularemos el riesgo residual que queda sobre ese activo.

ID: ES.001	Nombre: Base de datos ADA							Tipo de activo: [info] Datos / información esencial				
Tipo	Amenaza	Dim.	Valor	Deg.	Imp.	Prob.	Ries.	Tipo	Salvaguarda	Reduce	Valor res.	Riesgo Res.
E.1	Errores de los usuarios	[I]	10	10	A	B	A	D.I	Aseguramiento Integridad	Deg.	1	M
E.1	Errores de los usuarios	[C]	10	10	A	B	A	D.C	Cifrado de la información	Deg.	1	M
E.1	Errores de los usuarios	[D]	10	100	MA	B	MA	D.A	Copias de seguridad (Backup)	Deg.	1	M
E.2	Errores del administrador	[I]	10	10	A	B	A	D.I	Aseguramiento Integridad	Deg.	1	M
E.2	Errores del administrador	[C]	10	10	A	B	A	D.C	Cifrado de la información	Deg.	1	M
E.2	Errores del administrador	[D]	10	100	MA	B	MA	D.A	Copias de seguridad (Backup)	Deg.	1	M
E.15	Alteración accidental de la inf.	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B

E.18	Destrucción de la información	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
E.19	Fugas de información	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.5	Suplantación identidad usuario	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.5	Suplantación identidad usuario	[A]	10	10	A	MB	M					M
A.5	Suplantación identidad usuario	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.6	Abuso de privilegios de acceso	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.6	Abuso de privilegios de acceso	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.6	Abuso de privilegios de acceso	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
A.11	Acceso no autorizado	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.11	Acceso no autorizado	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.15	Modificación deliberada de inf.	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.18	Destrucción de la información	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
A.19	Revelación de información	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B

Tabla 143. Cálculo del riesgo residual para el activo ES.001

ID: ES.003	Nombre: Documentos ofimáticos casos despacho							Tipo de activo: [info] Datos / información esencial				
Tipo	Amenaza	Dim.	Valor	Deg.	Imp.	Prob.	Ries.	Tipo	Salvaguarda	Reduce	Valor res.	Riesgo Res.
E.1	Errores de los usuarios	[I]	10	10	A	B	A	D.I	Aseguramiento Integridad	Deg.	1	M
E.1	Errores de los usuarios	[C]	10	10	A	B	A	D.C	Cifrado de la información	Deg.	1	M
E.1	Errores de los usuarios	[D]	10	100	MA	B	MA	D.A	Copias de seguridad (Backup)	Deg.	1	M
E.2	Errores del administrador	[I]	10	10	A	B	A	D.I	Aseguramiento Integridad	Deg.	1	M
E.2	Errores del administrador	[C]	10	10	A	B	A	D.C	Cifrado de la información	Deg.	1	M
E.2	Errores del administrador	[D]	10	100	MA	B	MA	D.A	Copias de seguridad (Backup)	Deg.	1	M
E.15	Alteración accidental de la inf.	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
E.18	Destrucción de la información	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
E.19	Fugas de información	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.5	Suplantación identidad usuario	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B

A.5	Suplantación identidad usuario	[A]	10	10	A	MB	M					M
A.5	Suplantación identidad usuario	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.6	Abuso de privilegios de acceso	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.6	Abuso de privilegios de acceso	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.6	Abuso de privilegios de acceso	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
A.11	Acceso no autorizado	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B
A.11	Acceso no autorizado	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.15	Modificación deliberada de inf.	[I]	10	10	A	MB	M	D.I	Aseguramiento Integridad	Deg.	1	B
A.18	Destrucción de la información	[D]	10	100	MA	MB	A	D.A	Copias de seguridad (Backup)	Deg.	1	B
A.19	Revelación de información	[C]	10	10	A	MB	M	D.C	Cifrado de la información	Deg.	1	B

Tabla 144. Cálculo del riesgo residual para el activo ES.003

ID: HW.003	Nombre: NAS	Tipo de activo: [HW] Equipos informáticos (hardware)

Tipo	Amenaza	Dim.	Valor	Deg.	Imp.	Prob.	Ries.	Tipo	Salvaguarda	Reduce	Valor res.	Riesgo Res.
N.1	Fuego	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B
N.2	Daños por agua	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B
N.*	Desastres naturales	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B
I.1	Fuego	[D]	10	100	MA	B	MA	H	Duplicacion / Respaldo	Deg.	1	M
I.2	Daños por agua	[D]	10	100	MA	B	MA	H	Duplicacion / Respaldo	Deg.	1	M
I.*	Desastres industriales	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B
I.3	Contaminación mecánica	[D]	10	10	A	M	A	H	Duplicacion / Respaldo	Deg.	1	M
I.4	Contaminación electromagnética	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B
I.5	Avería de origen físico o lógico	[D]	10	10	A	B	A	H	Duplicacion / Respaldo	Deg.	1	M
I.6	Corte de suministro eléctrico	[D]	10	1	M	B	M					M
I.7	Condiciones inadecuadas temp.	[D]	10	100	MA	B	MA	H	Duplicacion / Respaldo	Deg.	1	M
I.11	Emanaciones electromagnéticas	[D]	10	1	M	MB	B					B

E.2	Errores del administrador	[D]	10	1	M	B	M					M
E.2	Errores del administrador	[C]	10	100	MA	B	MA	D.C	Cifrado del disco	Prob	MB	A
E.23	Errores de mantenimiento	[D]	10	10	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	B
E.24	Caída por agotamiento	[D]	10	10	A	B	A	H	Duplicacion / Respaldo	Deg.	1	M
E.25	Robo	[D]	10	100	MA	B	MA	H	Duplicacion / Respaldo	Deg.	1	M
E.25	Robo	[C]	10	100	MA	B	MA	D.C	Cifrado del disco	Prob	MB	A
A.6	Abuso de privilegios de acceso	[C]	10	100	MA	MB	A	D.C	Cifrado del disco	Prob.	MB	A
A.6	Abuso de privilegios de acceso	[D]	10	10	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	M
A.7	Uso no previsto	[C]	10	100	MA	MB	A	D.C	Cifrado del disco	Prob	MB	A
A.7	Uso no previsto	[D]	10	1	M	MB	B					B
A.11	Acceso no autorizado	[C]	10	100	MA	MB	A	D.C	Cifrado del disco	Prob	MB	A
A.23	Manipulación de los equipos	[C]	10	100	MA	MB	A	D.C	Cifrado del disco	Prob	MB	A
A.23	Manipulación de los equipos	[D]	10	10	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	B

A.24	Denegación de servicio	[D]	10	10	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	B
A.25	Robo	[D]	10	100	MA	B	MA	H	Duplicacion / Respaldo	Deg.	1	M
A.25	Robo	[C]	10	100	MA	B	MA	D.C	Cifrado del disco	Prob.	MB	A
A.26	Ataque destructivo	[D]	10	100	MA	MB	A	H	Duplicacion / Respaldo	Deg.	1	B

Tabla 145. Cálculo del riesgo residual para el activo HW.003

ID: HW.004	Nombre: Router							Tipo de activo: [HW] Equipos informáticos (hardware)				
Tipo	Amenaza	Dim.	Valor	Deg.	Imp.	Prob.	Ries.	Tipo	Salvaguarda	Reduce	Valor res.	Riesgo Res.
N.1	Fuego	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
N.2	Daños por agua	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
N.*	Desastres naturales	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
I.1	Fuego	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
I.2	Daños por agua	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
I.*	Desastres industriales	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB

I.3	Contaminación mecánica	[D]	8	10	M	B	M	H	Duplicacion / Respaldo	Deg.	1	B
I.4	Contaminación electromagnética	[D]	8	10	M	B	M	H	Duplicacion / Respaldo	Deg.	1	MB
I.5	Avería de origen físico o lógico	[D]	8	10	M	B	M	H	Duplicacion / Respaldo	Deg.	1	B
I.6	Corte de suministro eléctrico	[D]	8	1	B	B	B					B
I.7	Condiciones inadecuadas temp.	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
I.11	Emanaciones electromagnéticas	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
E.2	Errores del administrador	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
E.2	Errores del administrador	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A
E.2	Errores del administrador	[I]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
E.23	Errores de mantenimiento	[D]	8	10	M	MB	B	H	Duplicacion / Respaldo	Deg.	1	MB
E.24	Caída por agotamiento	[D]	8	1	B	MB	MB					MB
E.25	Robo	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
E.25	Robo	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A

A.6	Abuso de privilegios de acceso	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A
A.6	Abuso de privilegios de acceso	[D]	8	10	M	B	M	H	Duplicacion / Respaldo	Deg.	1	B
A.6	Abuso de privilegios de acceso	[I]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
A.7	Uso no previsto	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A
A.7	Uso no previsto	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	B
A.7	Uso no previsto	[I]	8	100	A	B	A	H.IA	Identif. Y autenticación	Prob.	MB	M
A.11	Acceso no autorizado	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A
A.11	Acceso no autorizado	[I]	8	100	A	B	A	H.IA	Identif. Y autenticación	Prob.	MB	M
A.23	Manipulación de los equipos	[C]	10	100	MA	MB	A	H.IA	Identif. Y autenticación	Prob.	MB	A
A.23	Manipulación de los equipos	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
A.24	Denegación de servicio	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB
A.25	Robo	[D]	8	100	A	B	A	H	Duplicacion / Respaldo	Deg.	1	MB
A.25	Robo	[C]	10	100	MA	B	MA	H.IA	Identif. Y autenticación	Prob.	MB	A

A.26	Ataque destructivo	[D]	8	100	A	MB	M	H	Duplicacion / Respaldo	Deg.	1	MB

Tabla 146. Cálculo del riesgo residual para el activo HW.004

Tratamiento del Riesgo, Proyectos y Plan de Seguridad

Es evidente que por la forma de trabajar del despacho lo más importante y que tiene que estar disponible para el trabajo del día a día es la información esencial compuesta por los documentos ofimáticos, emails y base de datos ADA y el hardware donde están alojados. En este aspecto diseñaremos varios proyectos de seguridad destinados a proteger estos activos de los riesgos y amenazas identificadas. Además, permitirán a los miembros del despacho la implantación de acuerdo con sus niveles y conocimientos técnicos.

Para ello realizaremos los proyectos con la información necesaria y los pasos adecuados para que se puedan poner en marcha y estarán estructurados de la siguiente forma:

- ID y nombre del proyecto
- Activos que protegen
- Objetivo del proyecto de seguridad
- Prioridad
- Ubicación temporal
- Salvaguardas involucradas
- Unidad responsable de su ejecución
- Estimación de costes financieros y de recursos
- Descripción de tareas a realizar

Estos proyectos ayudarán a la persona responsable del despacho para identificar la formación que es necesaria para abordar cada uno de ellos, adquirirla y poner en marcha las medidas a adoptar. O evaluar la contratación de un personal experto en la materia para la puesta en marcha.

Teniendo en cuenta que el responsable del despacho es una única persona que llevará a cabo la mayoría o prácticamente la totalidad de todos los proyectos de seguridad, los estructuraremos de forma que se puedan realizar secuencialmente para poder ir realizando una implantación lineal a medida que se vayan acometiendo cada uno de los proyectos.

Proyecto de Seguridad PS1 – Duplicación, Encriptación y Backup de activos esenciales

Activos que protegen:

- HW.003, NAS
- ES.001, Base de datos del programa ADA
- ES.002, Fichero de datos Outlook
- ES.003, Documentos ofimáticos del despacho

Objetivo: Ahora mismo el despacho dispone de un único NAS modelo Sinology DS119j. Este modelo únicamente tiene capacidad para 1 solo disco duro, por tanto, no podremos hacer duplicación en modo RAID 1, por ejemplo. La estrategia será utilizar la capacidad de encriptación AES que tiene este modelo para encriptar las carpetas de los documentos y de la base de datosy posteriormente se añadirá un sistema de Backup en la nube a través de la herramienta Google Drive que también posee este modelo.

Prioridad: 10, este proyecto tiene la prioridad máxima y es el primero que se deberá abordar.

Ubicación temporal: Con una dedicación de 2h/día se estima una duración de 3 semanas.

Salvaguardas:

- D.C Cifrado de disco
- D.A Backup
- D.I Aseguramiento de Integridad

Unidad responsable de ejecución: Responsable del despacho

Costes: 30h responsable

Descripción de tareas:

- Creación de los usuarios en el NAS a los que se les permitirá el acceso seguro a las carpetas de documentos ofimáticos, base de datos del programa ADA y fichero de Outlook de mails archivados.
- Encriptación de la carpeta de los documentos en el NAS mediante la herramienta de encriptación que posee este modelo.
- Contratación de espacio adicional en la nube con el proveedor Google Drive.
- Configuración en el NAS de la herramienta de sincronización Google Drive incluida en el dispositivo para realizar una copia de las carpetas en el espacio contratado en la nube.

- Configuración de Outlook para que exporte a la carpeta de mails archivados los mails anteriores a dos años de antigüedad.
- Elaboración de un documento con el plan de contingencia en caso de fallo/destrucción del NAS en el que se detalle paso por paso: La adquisición de un nuevo NAS, su configuración, la sincronización con Google Drive y el cifrado de las carpetas.

Proyecto de Seguridad PS2 – Segmentación de red y protección WiFi

Activos que se protegen:

- CO.002, Red Ethernet
- CO.003, Red WiFi
- HW.004, Router

Objetivo: Ahora mismo en el despacho la red WiFi y la red Ethernet están en el mismo segmento. Y aunque la red WiFi está protegida mediante WPA, si es cierto que si un cliente solicita acceso WiFi para transmitir algún documento en el despacho o alguna otra necesidad puntual se le facilita la clave. Crearemos una red WiFi para invitados que estará segmentada de la red Ethernet y de la red WiFi del despacho.

Prioridad: 8, este proyecto es prioritario y se abordará en cuanto se tenga oportunidad.

Ubicación temporal: Con una dedicación de 2h/día se estima una duración de 2 semanas

Salvaguardas:

- COM Protección de las Comunicaciones
- COM.DS Segregación de las redes
- COM.wifi Seguridad Wireless

Unidad responsable de ejecución: Responsable del despacho

Costes: 20h responsable

Descripción de tareas:

- Establecer una contraseña segura para acceso al router
- Crear una SSID para invitados con protección WPA
- Crear VLANs y separar la red Ethernet y WiFi de la red WiFi de invitados
- Ocultar el SSID de la red WiFi del despacho
- Elaboración de un documento con el plan de contingencia en caso de fallo/destrucción del router que detalle paso por paso: La adquisición de un nuevo rotuter, la segmentación de las redes en VLANs y ocultar el SSID de la red WiFi del despacho

Proyecto de seguridad PS3 – Protección de Software

Activos que protegen:

- SW.001
- SW.002
- SW.003
- SW.004
- SW.005

Objetivo: Actualmente los ordenadores del despacho tienen instalado únicamente el antivirus que viene por defecto con el sistema operativo Windows10, aunque esto puede proteger de la mayoría de las amenazas, es recomendable poder tener algo más de protección pagando la licencia de un software antivirus, además del soporte que pueden brindarnos ante software que todavía no haya sido catalogado.

Prioridad: 5, este proyecto es muy aconsejable, aunque existe cierta protección con el antivirus instalado por defecto en el Sistema Operativo.

Ubicación temporal: Se estima una duración de 1 semana.

Salvaguardas:

- SW Protección de las aplicaciones informáticas

Unidad responsable de ejecución: Responsable del despacho

Costes: 140 € / año

Descripción de tareas:

- Comprar licencia de antivirus para 5 ordenadores
- Instalar el antivirus con licencia en los ordenadores del despacho

Proyecto de seguridad PS4 – Alta disponibilidad del servicio Internet

Activos que protegen:

- CO.001

Objetivo: Internet es una de las herramientas fundamentales del despacho, ya que en su mayoría para la captación de clientes se realizan mediante las respuestas a las consultas generadas en la página web y el seguimiento de los casos y actualización de documentos se realiza vía mail. Es vital para la continuidad de negocio que este servicio esté disponible la mayor parte del tiempo

Prioridad: 5, el proyecto es aconsejable, pero una caída del servicio es algo poco frecuente hoy día.

Ubicación temporal: se estima una duración de 1 semana.

Salvaguardas:

- COM.A Aseguramiento de la disponibilidad

Unidad responsable de ejecución: Responsable del despacho

Costes: 10 - 15€ / mes

Descripción de tareas:

- Contratación con el proveedor actual de internet (movistar) de un SLA máximo de 2 horas para la respuesta y reparación del servicio en caso de caída de la red.

Proyecto de seguridad PS5 – Formación del personal

Activos que protegen:

- PR.001
- PR.002

Objetivo: Una de las principales causas de fuga de información involuntaria son las técnicas de ingeniería social. Por otro lado, las buenas prácticas y el conocimiento en materia de seguridad son claves para la prevención de posibles amenazas.

Prioridad: 5, el proyecto es aconsejable.

Ubicación temporal: Curso de formación en seguridad de 4 semanas.

Salvaguardas:

- PS Gestión del Personal
- PS.AT Formación y concienciación

Unidad responsable de ejecución: Todo el personal del despacho

Costes: Curso de formación + h de asistencia responsable despacho + h de asistencia secretaria

Descripción de tareas:

- Concertación con un centro especializado de formación para la impartición de cursos de seguridad.

Plan Director de Seguridad

Para implantar los proyectos de seguridad anteriores definiremos un plan de seguridad o plan director.

El objetivo del plan director se centra en establecer el momento y la duración de cada uno de los proyectos de seguridad, ordenándolos de la forma más conveniente. En este caso utilizaremos el criterio de la criticidad de los proyectos para abordar antes los más críticos por ser éstos los que protegen a los activos de mayor riesgo.

Además, teniendo en cuenta que el despacho no cuenta con recursos especializados para la implantación de estos proyectos realizaremos la planificación de forma que se aborde cada proyecto secuencialmente y abordar antes los que no requieran de personal cualificado. Dejando al final los proyectos que son menos críticos y que pueden suponer un coste por la contratación de servicios o personal cualificado, teniendo margen así para poder dotar de presupuesto a esos proyectos.

Por último, en la ejecución de los proyectos de seguridad que lo especifique se crearán unos documentos de contingencia que formarán parte del plan de seguridad y que deberán estar almacenados junto con el mismo.

Así el orden de los proyectos quedaría como sigue:

- PS1 – Duplicación, Encriptación y Backup de activos esenciales
- PS2 – Segmentación de red y protección WiFi
- PS3 – Protección de Software
- PS4 – Alta disponibilidad del servicio Internet
- PS5 – Formación del personal

Así estableceremos el siguiente cronograma:

		Noviembre 2019				Diciembre 2019				Enero 2020			
Proyecto de seguridad	Duración	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
PS1 – Duplicación, Encriptación y Backup de activos esenciales	3 semanas												
PS2 – Segmentación de red y protección WiFi	2 semanas												
PS3 – Protección de Software	1 semana												
PS4 – Alta disponibilidad del servicio Internet	1 semana												
PS5 – Formación del personal	4 semanas												

Tabla 147. Cronograma del Plan Director de Seguridad