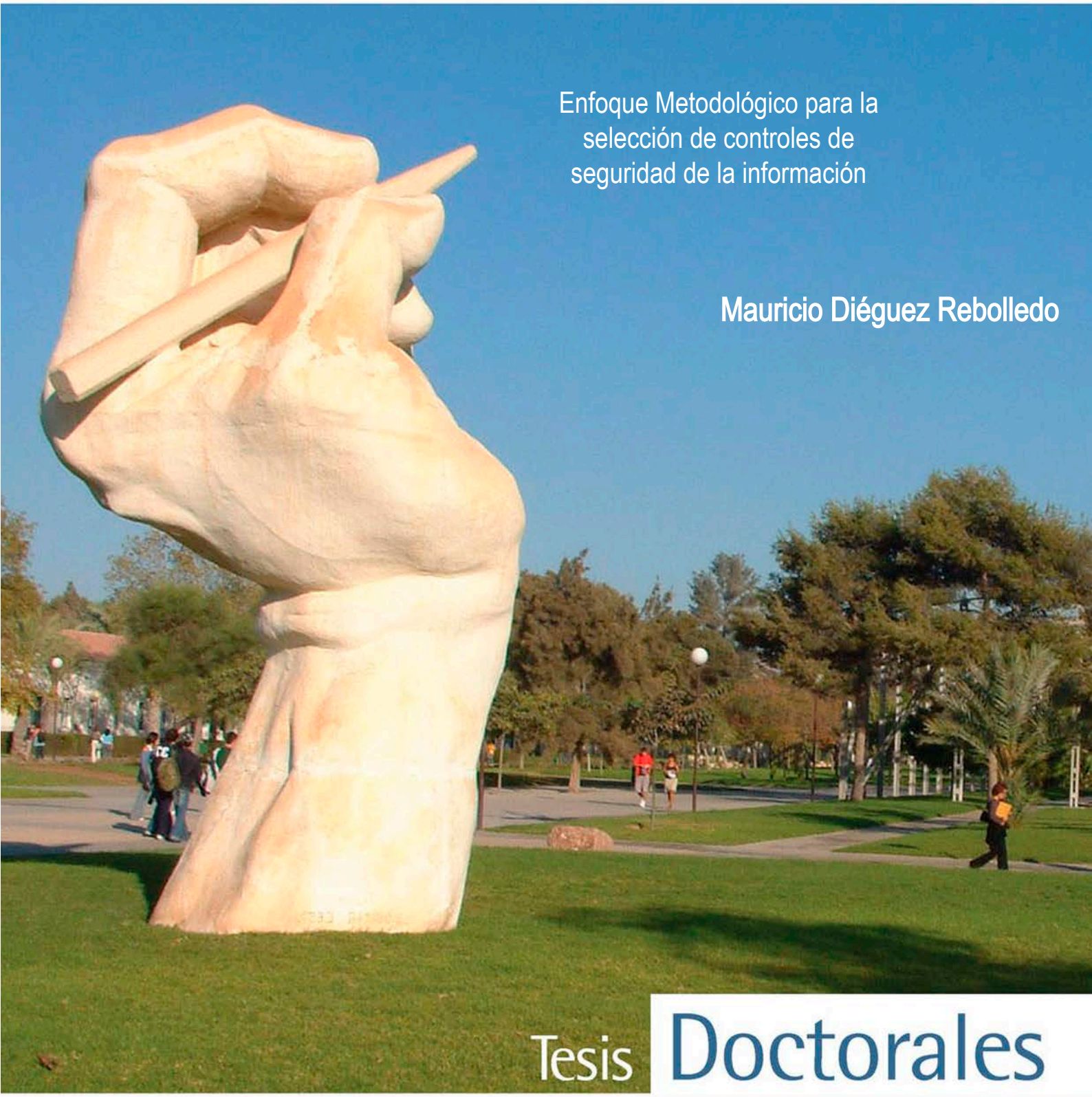
Universitat d'Alacant
Universidad de Alicante

Enfoque Metodológico para la selección de controles de seguridad de la información

Mauricio Diéguez Rebolledo



Tesis Doctorales
UNIVERSIDAD de ALICANTE

Unitat de Digitalització UA
Unidad de Digitalización UA

UNIVERSIDAD DE ALICANTE
Departamento de Lenguajes
y Sistemas Informáticos

Enfoque Metodológico para la selección de controles de seguridad de la información

Mauricio Rubén Diéguez Rebolledo

Tesis doctoral

Directores:
Dra. Cristina Cachero Castro
Dr. Carlos Cares Gallardo

Diciembre 2021

TESIS DOCTORAL

Enfoque Metodológico para la selección de controles de seguridad de la información

Este documento muestra el trabajo realizado por Mauricio Diéguez Rebolledo, bajo la dirección de los doctores Cristina Cachero Castro y Carlos Cares Gallardo, para optar por el grado de Doctor en Informática. Se presenta en la Universidad de Alicante y se estructura según la normativa establecida para la presentación de tesis doctorales.

Enero 2022

Índice general

Índice de figuras

Índice de tablas

Agradecimientos

En primer lugar, a Dios por su infinito amor y misericordia. Aunque no pueda verlo, doy Fe de su presencia en cada área de mi vida.

A mi esposa Karen e hijos, Gabriel y Gustavo, que han sacrificado invaluables momentos de juegos y compañía. Gracias por su apoyo y amor incondicional.

A mis directores de Tesis: Dra. Cristina Cachero y Dr. Carlos Cares, quienes no solo han compartido conmigo sus conocimientos, sino que han sido enormemente generosos al disponer de su tiempo, compartir sus ideas y extremar su paciencia. ¡Muchas gracias! han sido maravillosos.

Al Dr. Jaime Bustos, de la Universidad de La Frontera, por su apoyo, conocimientos y direccionamiento en un área que no es trivial para un informático.

Gracias a mis colegas con los que inicié este desafío, Samuel Sepúlveda y Jorge Hochstetter. Es el cierre de una etapa, no solo a nivel personal, si no que también a nivel departamental. Gracias por su apoyo y consejos.

A colegas y amigos que de una u otra forma apoyaron este desafío. Gracias en particular a Gamaliel Zapata, Ruth Novoa y Mario Guzmán.

Por último, quiero agradecer a la Universidad de Alicante y al

equipo responsables de la gestión del programa de doctorado en Informática, por su guía y apoyo en este proceso.

¡Gracias a todos y que DIOS les Bendiga!

Resumen

La gestión de la seguridad de la información es un desafío que ha ido cobrando cada vez más importancia. A medida que el número y gravedad de los ataques informáticos han crecido en el mundo, las empresas han comenzado a tomar conciencia de cuán importante es estar protegidos frente a acciones maliciosas que buscan vulnerar sus sistemas y acceder a sus activos de información.

En particular, la automatización de los procesos y la digitalización de la información han expuesto a las organizaciones a ataques que buscan robar información o dañar sus sistemas. Cada vez es menos extraño escuchar noticias sobre un secuestro de información a través de los ransomware, o sobre ataques de denegación de servicio (DoS) para bloquear los accesos a dichos servicios. Estos ataques provocan cientos de millones de dólares en pérdidas en el mundo entero e incluso pueden llegar a detener la continuidad operacional de una organización.

Frente a este escenario, es primordial que las organizaciones realicen una correcta gestión de la seguridad de la información, con el objetivo de proteger sus activos de información. Para ello, las organizaciones deben adoptar una actitud proactiva en lo referente a la seguridad, e implementar un conjunto de buenas prácticas en el quehacer de la organización que les permitan disminuir el riesgo de ser afectados por ataques informáticos.

Con el fin de lograr este objetivo, existen estándares de seguri-

dad en los que las organizaciones pueden apoyarse. Un estándar de seguridad de la información es una guía de implementación de buenas prácticas de seguridad, desde una perspectiva holística e integrada, que busca disminuir las vulnerabilidades de la organización a través de la implementación de un sistema de gestión de la seguridad de la información. Por tanto, a simple vista, la acción de protegerse es sencilla, ya que en teoría debería bastar con implementar el estándar para considerarse protegido.

Sin embargo, la situación es algo más compleja, ya que se debe considerar que cada organización es un mundo aparte, con condiciones de operación y disponibilidad de recursos distintas. Lamentablemente el problema no consiste solo en implementar el estándar, sino que radica en determinar cuál es la mejor ruta de avance que puede tener una organización, considerando sus objetivos y condiciones particulares, así como su disponibilidad de recursos. Esto implica que cada definición de ruta es propia para cada organización. Desafortunadamente, hasta el momento no existe un modelo estándar que haya sistematizado el proceso de la definición de una ruta de avance de manera que pueda ser aplicada por cualquier organización. Actualmente la definición de una ruta de avance se traduce en la selección y planificación de la implementación de controles de un estándar de seguridad, y se basa principalmente en el juicio experto. Sin embargo, este proceder es subjetivo, ya que depende de la experiencia y visión del asesor, que no siempre considera las condiciones propias de la organización. Además, es un proceso que puede tomar bastante tiempo, ya que son múltiples las variables que se deben considerar. Otro problema es que este modo de definir la ruta de avance no asegura que la respuesta sea la óptima para la organización en base a sus condiciones, ya que, si bien se utilizan algunas técnicas como la gestión de riesgos, estas mayormente son de índole cualitativa. Por último, dado que el proceso de recomendación de la selección e implementación de controles de seguridad no

está estandarizado ni es sistemático y dependen del asesor de seguridad, éste no es replicable, es decir, nada asegura que, de realizarse nuevamente, se obtendrían los mismos resultados.

Esta tesis pretende paliar estos problemas, para lo cual plantea un enfoque metodológico para la selección y planificación de la implementación de controles de seguridad que estandarice y sistematice dicho proceso a través de la aplicación de modelos y técnicas de optimización. Estos modelos y técnicas permiten modelar la situación particular de la organización (Objetivos y restricciones) y aseguran una solución óptima para las condiciones representadas.

La principal contribución de este trabajo es por tanto la propuesta de un proceso estándar y sistemático, pero que puede ser aplicado a cualquier organización, ajustándose a sus condiciones particulares, y que entrega la mejor solución para dichas condiciones. Este proceso se presenta como un apoyo útil para el asesor de seguridad a la hora de que éste realice sus recomendaciones de seguridad respecto de los controles que cada organización debe implementar para avanzar en el logro de un estándar de seguridad.

Como contribuciones secundarias, se ha definido un marco conceptual de seguridad de la información que integra diversas visiones de las variables y relaciones que involucra la seguridad de la información. Es este marco conceptual el que apoya la modelación de los problemas de optimización que genera nuestra propuesta.

Otro aporte es la identificación y categorización de los diversos problemas o escenarios que podrían considerarse para la modelación, es decir, basada en los diversos tipos de situaciones que una organización podría querer resolver. Esta categorización va más allá de los casos particulares de la industria que se suelen reportar en la literatura, y

ha permitido identificar casos de las categorías más complejas que las que suelen encontrarse en dicha literatura. En esta línea, hemos desarrollado un ejemplo con una situación de una categoría compleja, lo que representa una contribución en sí misma.

Un cuarto aporte es la generación de una herramienta informática que soporta el enfoque propuesto y apoya al asesor de seguridad en la aplicación de nuestra propuesta. La herramienta facilita, principalmente, la modelación y la resolución de dichos modelos, por lo que el asesor solo debe preocuparse del análisis de las respuestas. No hemos encontrado en otras propuestas descritas en la literatura herramientas que apoyen sus propuestas.

Por último, el trabajo presenta una evaluación de la propuesta, a través de un estudio de adopción de métodos, con estudiantes de pregrado en un curso de auditoría informática. Este estudio evidenció una tendencia de los sujetos en estudio hacia la adopción de la propuesta, percibiéndola como un elemento útil y que se ajusta a su manera de trabajar. La principal debilidad de la propuesta se centró en la facilidad de uso, ya que la modelación y resolución del problema requiere de conocimientos avanzados de técnicas de optimización.

En definitiva, la propuesta de este trabajo provee a la comunidad de la gestión de la seguridad de la información de un enfoque metodológico que permite sistematizar un proceso que hasta el momento solo se sustentaba en propuestas sobre casos particulares, por lo que no había sido estandarizado y su alcance era bastante limitado. Esto representa un avance en un ámbito que se encuentra en desarrollo y que aún no logra abarcar y solucionar todas las complejidades que presenta este problema.

Abstract

Information security management is a challenge that has become increasingly important. As cyber-attacks grow in the world, companies have begun to realize how important it is to be protected against malicious actions that seek to breach their systems and access their information assets.

The automation of processes and the digitization of information have exposed organizations to attacks that seek to steal information or damage their systems. It is becoming less and less strange to hear of information hijacking, through ransomware, or denial of service (DoS) attacks, to block access to said services. These attacks cause hundreds of millions of dollars in losses worldwide and can even stop the operational continuity of an organization.

Faced with this scenario, it is essential that organizations carry out correct information security management, to protect their information assets. For this, organizations must adopt a proactive attitude when it comes to security, implementing solutions that allow them to reduce the risk of being affected by computer attacks. One way to protect themselves is by implementing preventive actions or implementing a set of good practices in the work of the organization.

Information security standards can help in this endeavour. An information security standard is a guide for the implementation of good security practices, from a holistic and integrated perspective, which seeks to reduce the vulnerabilities of the organization through the im-

plementation of a security management system of the information in which the set of good practices are defined. At first glance, the action of protecting oneself seems simple, since, in theory, it would be enough to implement the standard to be considered protected.

However, the situation is somewhat more complex, since it must be considered that each organization is a separate world, with different operating conditions and availability of resources. Unfortunately, the problem does not consist only in implementing the standard, but in determining what is the best route of advance that an organization can have, considering its objectives and particular conditions, as well as its availability of resources. This implies that each route definition needs to be specific to each organization.

To the best of our knowledge, there is no standard model that has systematized the process of defining a route of advance, which can be applied by any organization. The definition of a path forward, which translates into the selection and planning of the implementation of controls of a security standard, is mainly based on expert judgment. However, this procedure is subjective, since it depends on the experience and vision of the advisor, and it does not always consider the conditions of the organization. Also, it is a process that can take a long time, since multiple variables must be considered, and it does not ensure that the response is optimal for the organization based on its conditions, since, although some techniques such as risk management are used, these are mostly qualitative in nature. Finally, given that the recommendation process for the selection and implementation of security controls is not standardized or systematic and depends on the security advisor, it is not replicable, so the same results would not necessarily be obtained when performing it again.

This work proposes a methodological approach for the selection

and planning of the implementation of security controls. It standardizes and systematizes said process through the application of optimization models and techniques, which allow modeling the particular situation of the organization (Objectives and restrictions) and ensure an optimum solution for the conditions represented.

The main contribution of this work is to propose a standard and systematic process that can be applied to any organization, adjusting to its particular conditions, and that provides the best solution for those conditions. This process is a useful support to the security advisor, so that he can make his security recommendations regarding the controls that each organization must implement to advance in the achievement of a security standard.

As secondary contributions, there is the definition of a conceptual information security framework, which integrates diverse views of the variables and relationships that information security involves. This conceptual framework supports the modeling of the optimization problems generated by our proposal.

Another contribution is related to the identification and categorization of the various problems or scenarios that can be considered for modeling. A systematic literature search showed how this classification was missing in the literature, where only particular cases of the industry were analyzed. In our work, we have proposed a categorization of the various types of situations that an organization might want to resolve. This categorization has also allowed to analyze the level of complexity of the cases of study presented in the literature, and to develop a new example that increases this complexity, and therefore is closer to the security challenges daily faced by organizations. This represents a contribution in itself.

A fourth contribution is the development of a computer tool that implements the proposed approach, supporting the security advisor in the application of the proposal, mainly by facilitating the modeling and resolution of said models, so the advisor should only worry of the analysis of the responses. We have not found this tool support in other proposals described in the literature.

Finally, the work presents an evaluation of the proposal, through a study of the adoption of methodologies with undergraduate students in a computer audit course. This study showed a tendency of the study subjects towards the adoption of the proposal, perceiving it as a useful element that adjusts to their way of working. The main weakness of the proposal focused on ease of use, since the modeling and resolution of the problem requires advanced knowledge of optimization techniques.

In short, the proposal presented in this Thesis provides the information security management community with a methodological approach that allows systematizing a process that until now was only addressed on a case by case basis, so it had not been standardized and its scope was quite limited. This represents progress in an area that is under development and that has not yet managed to cover and solve all the complexities that a problem like this presents.

Palabras clave

Palabras Clave: Seguridad de la información, Gestión de la Seguridad del información, Estándar de seguridad, Control de seguridad, Selección de controles de seguridad, Evaluación del riesgo, Enfoque metodológico, Intención de adopción, Utilidad, Facilidad de Uso, Compatibilidad, Norma Subjetiva, UMAM, Herramienta informática.

Keywords: Information Security, Information Security Management, Security Standard, Security Control, Selection of Security Controls, Risk Assessment, Methodological Approach, Intention to Adopt, Utility, Ease of Use, Compatibility, Subjective Norm, UMAM, IT Tool.

Listado de acrónimos

C	Compatibilidad
CIA	Confidencialidad, Integridad y Disponibilidad
DS83	Decreto Supremo 83
FU	Facilidad de Uso
GAMS	Sistema General de Modelado Algebraico - General Algebraic Modeling System
GUI	Guía metodológica del Gobierno de Chile
IC	Intención de Comportamiento
II	Ingeniería Informática
IO	Investigación de Operaciones
ISC	Controles de Seguridad de la Información - Information Security Controls
ISCM	Gestión de los Controles de Seguridad de la Información - Information Security Controls Management
ISO	International Organization for Standardization
NS	Norma Subjetiva
PDCA	Plan - Do - Check - Act

PCKP	problema de mochila con precedencia limitada
PSP	problema de programación de proyecto
RCPSP	problema de planificación de proyectos con recursos limitados
rc-mPSP	Programación de múltiples proyectos restringidos por recursos
SGSI	Sistema de Gestión de Seguridad de la Información
SI	Seguridad de la Información
TI	Tecnologías de Información
U	Utilidad
UMAM	Unified Method Adoption Model
UMAM-Q	Unified Method Adoption Model-Questionnaire
V	Voluntariedad

Parte I

Aspectos preliminares

1. Introducción

Este capítulo presenta una introducción a la temática del presente trabajo de investigación, destacando la problemática que se enfrenta y que se desea resolver, así como los objetivos que se esperan alcanzar con la investigación.

En la sección 1.1, se realiza una introducción sobre la seguridad de la información y la importancia de la gestión de ésta en las organizaciones.

En la sección 1.2 se ilustra la experiencia práctica del doctorando que hizo patente algunas de las carencias en el campo de investigación.

En la sección 1.3 se centra el problema que aborda esta tesis doctoral, que es la selección de controles de seguridad de la información como parte de la gestión de la seguridad en las organizaciones.

En la sección 1.4, se describe la solución propuesta al problema de la selección de controles de seguridad. Además, se presenta la hipótesis del trabajo y los objetivos que se esperan alcanzar durante este trabajo de investigación.

Por último, en la sección 1.5, se resume la estructura del presente documento.

1.1 La seguridad de la información en el contexto de las organizaciones

En las últimas décadas se ha producido una incorporación exponencial de Tecnologías de Información (TI) dentro de la habitualidad de la vida moderna. Tanto las personas como las organizaciones se han vuelto cada vez más dependientes de estas tecnologías en el desarrollo de sus actividades diarias.

El manejo de información sensible por parte de estos sistemas, así como la dependencia de la continuidad operacional de las organizaciones, han convertido a estos sistemas en activos críticos y estratégicos y, por ende, en blancos de posibles ataques o vulneraciones que buscan robar información o dañar el normal funcionamiento de éstos.

Además, la globalización de los servicios y los sistemas informáticos han aumentado drásticamente el riesgo de recibir ataques que pueden provenir no sólo de una fuente local sino de cualquier parte del mundo. Es más, estos ataques no necesariamente son efectuados por "lobos solitarios", expertos en informática, sino que se han registrado ataques por parte de grupos organizados o incluso por gobiernos antagónicos.

Se han reportado múltiples casos en que organizaciones o países han sufrido de este tipo de ataques. Uno de los que ha causado mayor impacto es el caso del virus Stuxnet [87], que afectó directamente un importante número de computadores de las instalaciones nucleares de Irán. El grave impacto potencial de este tipo de acciones, junto con la escalada de los ataques, ha causado la clasificación de los mismos como un acto de guerra cibernética hacia infraestructura crítica de un país [46].

Otro ejemplo de gran alcance mediático, aunque no afectó infraestructuras críticas, es el ataque del Ransomware denominado "WannaCry"que se registró a nivel mundial, afectando a más de 200.000 computadores en 150 países durante los primeros días del mes de mayo de 2017 [136]; un segundo caso es la intervención a la campaña presidencial de los Estados Unidos de América durante el año 2016 [135].

Este fenómeno ha abierto un nuevo y amplio frente de defensa tanto para las organizaciones privadas como para las organizaciones gubernamentales, ya que se ha visto cómo los ataques tienen un alcance global y buscan a menudo la desestabilización de las organizaciones e incluso de los gobiernos, lo que impacta directamente en la seguridad nacional de los países [106, 139]. Así, frente a este nuevo escenario, se han acuñado términos como Ciberespacio, Ciberguerra, Ciberamenazas, Ciberseguridad, Ciberataques o Ciberdefensa, para dar cuenta de este tipo no tradicional de conflicto, el cual no se produce en un ambiente físico sino virtual, y que busca afectar los activos de información y/o la continuidad operacional de organizaciones privadas o de unidades de gobierno.

Para dar respuesta a esta situación, las organizaciones se han visto obligadas a definir y aplicar un conjunto de contramedidas que, basadas en criterios de expertos, permiten asegurar sus activos de información frente a ataques casuales o deliberados. Sin embargo, estas medidas se están demostrando insuficientes ante el aumento de este tipo de ataques en el mundo, por lo cual se hace imprescindible, por parte de las organizaciones, la definición sistemática de políticas de seguridad que contemplen la gran variedad de ataques a los cuales se ven expuestos [119, 133].

Según Whitman y Mattord [146], la seguridad es "la calidad o

estado de mantenerse seguro o libre de daño". En términos organizacionales, se pueden considerar la seguridad en distintos ámbitos: seguridad física, seguridad personal, seguridad operacional, seguridad de las comunicaciones y SI. Esta tesis se centra en el ámbito de la SI, entendida como la protección de la información de una organización frente a ataques deliberados o casuales, ya sean internos o externos. Ésta se preocupa de proteger la confidencialidad, integridad y la disponibilidad de los activos de información de la organización, ya sea que se encuentre almacenada, se esté procesando o transmitiendo [96].

Una forma de gestionar la SI, es a través del control del riesgo asociado a las prácticas de la organización. Esto se puede lograr mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI define un conjunto de prácticas tendientes a regular el comportamiento de la organización, en sus diversos ámbitos, desde la mirada de la SI [131]. Su objetivo es por tanto la protección de los activos de información de una organización, que se consigue a través de la definición de un conjunto de políticas y/o acciones que sirven de directriz para establecer un comportamiento organizacional con respecto a la SI [2].

Para ayudar en la definición de estas políticas y acciones, expertos internacionales han desarrollado un conjunto estándares de SI, reconocidos e implementados a nivel mundial. Estos estándares son a menudo utilizados como base para la definición de un SGSI [12].

Se puede considerar un estándar como un conjunto de reglas o buenas prácticas que proporcionan un punto de referencia sobre el cual un SGSI puede compararse. Existe una gran cantidad de estándares de SI. De entre éstos, el más difundido es la familia ISO/IEC 27000 [72]. Esta norma propone 114 Controles de Seguridad de la Información - Information Security Controls (ISC) que se clasifican en 14 dominios

principales descritos en la norma ISO/IEC 27002:2013 [52]. El grado de cumplimiento de estos controles determina el nivel de seguridad de una organización y si califica para la certificación.

Como puede observarse en este estándar, los ISC pueden ser de distinto tipo: algunos de ellos pueden ser muy técnicos desde el punto de vista del software, otros están estrechamente relacionados con la infraestructura y otros se relacionan con diferentes aspectos de la gestión, como el control de recursos humanos o el acceso físico.

Esta diversidad de ámbitos de ISC está en consonancia con el objetivo principal de los estándares de seguridad de la información que, como ya se ha mencionado anteriormente, es guiar a todos los niveles la gobernanza de la seguridad de la información para asegurar la Confidencialidad, Integridad y Disponibilidad (CIA) de los activos de información. Por lo tanto, cumplir con un estándar de seguridad significa abarcar diferentes dimensiones organizacionales, que en algunos casos se encuentran más allá del foco de un administrador de seguridad. Como ejemplo, la familia ISO/IEC 27000 incluye prácticas tales como tener cláusulas de seguridad de la información en los contratos de los administradores o la capacitación continua de los equipos técnicos. Estar comprometido con algún estándar de seguridad de la información significa, por tanto, tener una estructura organizativa que soporte tanto los roles políticos y de alta gerencia como los roles técnicos.

Esta variedad de ámbitos involucra también tener que gestionar una amplia variedad de prácticas o controles de seguridad asociados a los estándares. Por ejemplo, como ya se mencionó, el estándar ISO 270002:2013 propone la implementación de 114 controles. Para aplicar correctamente estos controles, se debe realizar un permanente control y monitoreo del comportamiento de la organización respecto de dichos

controles. Estos procesos de evaluación y monitoreo son actividades relevantes para determinar el desempeño de un sistema de gestión dentro de las organizaciones, así como el grado de conformidad que se tiene respecto del estándar. Conocer el grado de conformidad, implica conocer que prácticas se han implementado, cuáles no se han implmentado y cuáles se han implementado erroneamente, para, a partir de esta información, poder planificar una línea de acción sobre aquellas situaciones que no se ajustan a lo indicado por el estándar, gestionando los recursos para corregir la diferencia que se presentan con dicho estándar.

Sin embargo, esta gestión no es trivial, ya que son muchas la variables que se deben considerar para tomar una decisión respecto del curso de acción a tomar para corregir las diferencias de conformidad de la organización respecto del estándar, como por ejemplo; los niveles de riesgo, costos y tiempos de implementación, limitaciones del recurso humano, políticas internas o externas, etc. Esto implica que las decisiones respecto de la selección o recomendación del grupo de controles que se deben implementar para disminuir la brecha que existe con la totalidad del estándar, bajo un escenario de múltiples objetivos y restricciones, se convierta en un problemna difícil de resolver. Este problema se hace aún más complejo si se pretende lograr la optimización de los recursos de la organización, en otras palabras, la mejor solución conforme a los recursos disponibles.

A pesar de esta dificultad, actualmente, la manera tradicional de atacar este problema es a través de métodos cualitativos, como es la opinión de expertos apoyados por algunas técnicas de priorización y selección. Como se mostrará en la sección 4.1, son pocos los trabajos que proponen la utilización de técnicas cuantitativas, como son las propuestas por el área de IO, para la resolución de la selección y programación de la implementación de los ISC. Además, estos trabajos

solo presentan soluciones a casos particulares y no proponen una solución integral al problema general de la selección de controles.

En este trabajo se presenta una solución a este problema, a través de la definición de enfoque metodológico que guía el proceso de selección de controles mediante el modelado de diferentes escenarios (diferentes objetivos y restricciones) y recomendado técnicas de optimización a aplicar para la modelación y resolución de dichos escenarios, de tal manera de asegurar la mejor solución dadas las condiciones de la organización.

1.2 Motivación práctica del trabajo de investigación

La situación descrita anteriormente se hizo evidente para el doctorando cuando, en el año 2012, participó de una auditoría de seguridad para una organización gubernamental regional. Las características particulares de este tipo de organizaciones hacen que las consideraciones políticas y de gestión tengan un gran impacto sobre la toma de decisiones, tanto o más que las consideraciones técnicas. Durante la realización de esta asesoría se vivió de primera mano la dificultad de realizar una propuesta de implementación de controles de seguridad dentro de un plan global de mejora de seguridad específico para esta organización. Fue durante este trabajo que se identificó la utilidad para el asesor de seguridad de disponer de un método sistemático para generar una recomendación de controles que maximice el avance en las metas de logro respecto de las normas de seguridad, pero que considere las particularidades de una organización de gobierno y las restricciones presupuestarias de la unidad.

1.3 Definición del problema

En base a todo lo comentado anteriormente, este trabajo busca definir una metodología que, basada en la aplicación de técnicas cuantitativas, permita solucionar el problema de la recomendación de avance y logro de una norma o estándar de seguridad de la información basada en controles o en la implementación de buenas prácticas de seguridad. Esta recomendación busca apoyar el proceso de toma de decisiones para la definición de un plan de inversión en seguridad informática, que permita avanzar en el cumplimiento de una norma o estándar de seguridad.

Tal como se presenta en la figura 1.1, una organización se puede encontrar en un estado ("Estado Actual") en el cual no tiene implementados todos los controles definidos por una norma o estándar de seguridad, pero desea lograr en el futuro, para llegar así a un estado ("Estado Deseado") en el cual haya avanzado en la implementación de controles. El cambio de estado se produce al implementar aquellos controles que aún no se han implementado dentro de la organización. Sin embargo, existen muchos caminos posibles para pasar desde el "Estado Actual" a un "Estado Deseado". En muchas ocasiones, las organizaciones no tienen los recursos para implementar la totalidad de los controles no implementados, por lo que debe seleccionar un conjunto de controles que le permita avanzar hacia el "Estado Deseado", considerando los recursos que posee. Por tanto, el problema consiste en determinar la ruta o secuencia óptima de cumplimiento de controles para llegar al nivel deseado dentro de la norma, entendiendo como óptima aquella ruta que minimice o maximice los parámetros propios de la organización.

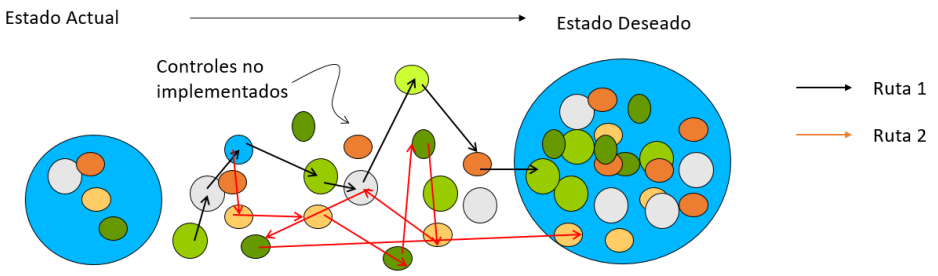


Figura 1.1: Problema - Ruta de cumplimiento

1.4 Proyecto de investigación

Todo lo argumentado anteriormente ilustra la necesidad que tienen las organizaciones de contar con un método sistemático para la selección de controles de seguridad de la información, basada en métodos cuantitativos, que apoye el proceso de toma de decisiones de un asesor de seguridad en las recomendaciones que realiza respecto del avance en el cumplimiento de un estándar de seguridad de la información.

1.4.1 Propuesta de solución

Para determinar un modelo cuantitativo para la selección de controles de seguridad, se propone estudiar la problemática como un problema de optimización, entendido como una situación en la que se requiere determinar la mejor solución para un problema dado, sujeto a un conjunto de diferentes limitaciones o restricciones [117]. La representación de este tipo de problema requiere que la situación sea modelada

matemáticamente a través de una función multidimensional, conocida como función objetivo -la que se debe minimizar o maximizar- y por un conjunto de restricciones, modeladas por ecuaciones e inecuaciones, tales como el tiempo, costo, espacio, etc.

En el caso de la selección de controles, lo que se busca es el conjunto óptimo de controles que minimice riesgos y considere las restricciones propias de la organización, tales como costos, tiempos, prioridades, políticas organizacionales, etc.

Para la resolución del problema planteado, esta tesis propone la aplicación de técnicas y métodos provenientes de la IO. La IO es un enfoque científico para la toma de decisiones que busca definir la mejor manera de diseñar y operar un sistema [93]. La IO es una disciplina que durante muchas décadas se ha dedicado a investigar las técnicas y métodos cuantitativos para la resolución de problemas de optimización. Su historia se remonta a los primeros intentos de aplicar enfoques científicos a la producción industrial y la gestión de las organizaciones. En estos ámbitos de aplicación, ha desarrollado modelos matemáticos, estadísticos y algoritmos para resolver problemas complejos con el fin de apoyar los procesos de toma de decisiones. Por lo general, la IO se aplica bajo condiciones que requieren la asignación de recursos limitados. En base a este entendido, la IO se ha convertido en una disciplina consolidada, con su propio conjunto de conocimientos y un tipo característico de investigación [149].

Desde esta tesis se postula que el conjunto de técnicas y métodos de resolución de problemas de optimización ofertado por la IO son valiosas de cara a resolver el problema de selección del conjunto óptimo de controles.

1.4.2 Hipótesis de trabajo

La hipótesis de este proyecto es que la incorporación de un método para la selección de controles de seguridad, basada en técnicas y métodos cuantitativos, genera un impacto positivo y un cambio de práctica en los asesores de seguridad de la información.

1.4.3 Objetivo general

En función de la hipótesis planteada, el objetivo principal del proyecto es definir una metodología de selección de controles de seguridad de la información que ayude a los asesores de seguridad a realizar sus recomendaciones con mayor eficiencia, eficacia y satisfacción de la que obtendrían utilizando sus métodos habituales. Para ello, se propone que la metodología se base en un modelo cuantitativo para la selección de controles de seguridad de la información, y que se vea apoyada por herramientas informáticas que automaticen parcialmente el proceso.

1.4.4 Objetivos específicos

Los objetivos específicos son:

OE1: Establecer cuáles son las prácticas actuales de un asesor de seguridad.

OE2: Identificar los procesos en donde se presenta una oportunidad de mejora.

OE3: Identificar los modelos cuantitativos apropiados para la selección óptima de controles de seguridad.

OE4: Definir la metodología para la selección de controles de seguridad, considerando los modelos, las herramientas, los procesos y las personas que se involucrarán con ella.

OE5: Implementar una herramienta, a nivel de prototipo funcional, que dé soporte a la metodología y avance en el grado de automatización del proceso.

OE6: Aplicar el marco metodológico en un ambiente controlado.

OE7: Realizar un estudio piloto de adopción de metodologías para evidenciar el posible impacto que esta propuesta tendría sobre los asesores de seguridad.

1.5 Estructura del documento de tesis

El presente trabajo se estructura de la siguiente manera:

Capítulo 2: Método de Investigación.

En este capítulo se describe el paradigma Design Science propuesto por Hevner en [68] y se justifica por qué este paradigma es el más idóneo para el desarrollo de este trabajo de investigación. Se describen las diversas etapas que propone y como éstas se relacionan con las fases del método de investigación seguido para el desarrollo de esta tesis.

Además, por cada una de las fases, se describen las técnicas particulares aplicadas, los resultados esperados y su relación con los objetivos planteados en el presente trabajo de investigación.

Capítulo 3: Contexto de la Investigación.

Este capítulo presenta el contexto teórico que sustenta esta investigación. Aquí se describen los dos campos de conocimiento que abarca este trabajo, tanto lo relacionado a SI como a IO, y cómo la aplicación de la IO sobre el campo de SI permite resolver el problema de la

selección de controles.

En primer lugar, se describe la importancia de la Gestión de los Controles de Seguridad de la Información - Information Security Controls Management (ISCM) dentro de las organizaciones para el control del riesgo de los activos de información pertenecientes a una organización. Aquí se describe el porqué del problema de la selección de controles de seguridad como parte de la gestión de la seguridad.

En segundo lugar, se describe el campo de la IO, como un área de conocimiento consolidada, en el contexto de la resolución de problemas de toma de decisiones, en base a modelos y técnicas matemáticas.

Por último, se describe cómo la aplicación de las técnicas de IO pueden ayudar a resolver el problema de la selección de controles de seguridad.

Capítulo 4: Mapeo Sistemático de la Literatura.

En este capítulo se presenta el desarrollo de un Mapeo Sistemático, basado en el protocolo de [115], que ha permitido identificar las respuestas que, desde la comunidad científica, se han dado al problema planteado, lo que a su vez ha permitido identificar un conjunto de oportunidades de investigación.

Para ello, este capítulo comienza con la presentación del protocolo que se aplicó para el desarrollo del mapeo sistemático, describiendo por cada fase los resultados obtenidos. Además, se resumen los trabajos encontrados y se identifican aquellos que se encuentran en el ámbito de nuestra propuesta. Sobre ellos, se analiza cómo definen el problema y cómo desarrollan sus propuestas de solución.

En segundo lugar, y a partir de los resultados del Mapeo Sistemático, se identifican las oportunidades de investigación, proponiendo una estructura de enfoque metodológico que delinea nuestra propuesta de solución al problema de la recomendación de ISC.

El capítulo finaliza con la descripción de esta estructura metodológica.

Capítulo 5: Propuesta de Solución

En este capítulo se detalla la propuesta de solución al problema de la selección de ISC. En primer lugar se detalla el problema que se quiere resolver y, a partir de él, se describe la estructura del enfoque metodológico propuesto y su flujo de aplicación, detallando por cada etapa las características y los resultados de cada una de ellas.

Por otra parte, en este capítulo también se presenta una propuesta de modelo conceptual que describe los conceptos y relaciones que forman parte del contexto del problema, y sobre el cual se sustenta la modelación del problema de optimización.

Además, aquí se definen un conjunto de escenarios o tipos de problemas de optimización y se relaciona cada escenario con las técnicas o modelos de optimización que son atingentes para su resolución.

Por último, el capítulo describe un ejemplo de aplicación de la propuesta, en el cual se muestra la modelación y resolución de un caso particular de selección de controles, además de un analisis de los resultados obtenidos.

Capítulo 6: Evaluación Empírica de la Propuesta

Este capítulo presenta la evaluación de la solución propuesta, a través de la aplicación del enfoque metodológico en un contexto académico. Se aplicó la propuesta a un grupo de estudiantes de un curso de grado, quienes tuvieron que utilizarla para proponer un plan de mejora sobre los resultados de una auditoría realizada a una organización real.

La evaluación se realizó utilizando el modelo UMAM [38], el cual permite estimar el grado de adopción, de una metodología por parte de los sujetos de estudio. En este estudio se aplicó el cuestionario UMAM-Q para obtener las apreciaciones de los estudiantes respecto de la aplicación del enfoque metodológico. Por último, se muestran los análisis de las respuestas de los estudiantes y las conclusiones y limitaciones del estudio realizado.

Capítulo 7: Soporte Software

En este capítulo se presenta el diseño de una herramienta informática de apoyo a la aplicación del enfoque metodológico propuesto. Se detallan las características de la herramienta y como ésta puede apoyar en cada fase de la propuesta metodológica.

Capítulo 8: Contribuciones, Conclusiones y Trabajos Futuros

En este capítulo se resumen los aportes más relevantes de la investigación, junto con la descripción de los principales trabajos realizados y las líneas de trabajos futuros que se abren como consecuencia de los resultados obtenidos. Por último, se incluye un resumen de las principales publicaciones obtenidas como resultado del trabajo en esta tesis doctoral.

2. Método de Investigación

En este capítulo se presenta el proceso y las actividades realizadas para el logro de los objetivos de este trabajo de investigación.

En la sección 2.1 se presenta una visión general del paradigma de investigación Design Science, que ha guiado el método de investigación seguido para el desarrollo de este trabajo de investigación.

En la sección 2.2 se profundiza en las distintas etapas del método y cómo se han aplicado para cubrir los objetivos planteados para esta investigación.

2.1 Introducción

Para enfrentar la investigación y lograr los objetivos del trabajo, se definió un método de investigación dividido en cuatro fases, consistentes con las propuestas por el paradigma de investigación Design Science [68]. Este paradigma plantea la resolución de problemas prácticos a través del desarrollo de nuevos artefactos que innoven los procesos estudiados [147].

Según este enfoque, la situación en estudio siempre deriva de un problema práctico presente en la realidad, y, a través de un enfoque cíclico, busca la solución de dicho problema. El ciclo de investigación de Design Science, propone el desarrollo de la investigación a través de 6 fases: (1) identificación del problema; (2) definición de objetivos; (3) diseño y desarrollo; (4) demostración; (5) evaluación y (6) comunicación, tal y como se ilustra en la figura 2.1

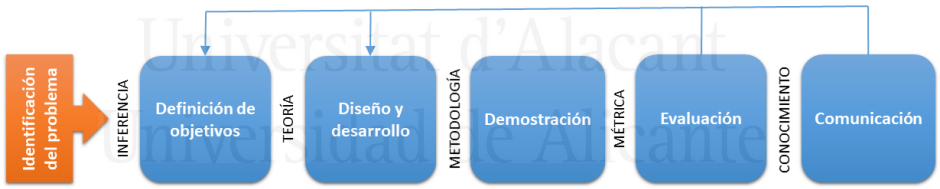


Figura 2.1: Ciclo de Investigación - Design Science, [68]

Una de las características importantes a tener en cuenta en este paradigma es que éste permite desarrollar las diferentes fases que propone a través de la aplicación de otros métodos de investigación que sean atingentes tanto a la fase como al contexto donde se aplica. Esto dota al paradigma de una gran flexibilidad, ya que por cada fase es posible aplicar un marco metodológico distinto, de acuerdo a las ne-

cesidades del problema que se esté enfrentando.

Las razones que justifican la elección de este paradigma para el desarrollo de este trabajo se resumen de la siguiente manera:

- Permite llegar a soluciones de un problema práctic, a través de la aplicación de un proceso sistemático.
- Permite trabajar en diversos contextos, considerando las limitaciones particulares de cada problema práctico y su ámbito de aplicación.
- Presenta un alto potencial de generalización de los resultados alcanzados.
- Permite la aplicación de distintos métodos de investigación de acuerdo al contexto y la fase en que se encuentre.

Como ya hemos comentado, en el contexto de este trabajo, el problema práctico que sustenta la investigación se refiere a las dificultades que enfrentan los asesores de seguridad para generar recomendaciones de implementación de controles de seguridad a través de un proceso objetivo y sistemático, de manera que se optimicen los recursos de la organización.

A partir de esta situación y dado el alcance de la investigación, para el desarrollo de este trabajo se han agrupado las etapas del paradigma Design Science en cuatro fases: (i) Investigación del problema, donde se encuentran las etapas de “Identificación del problema” y “Definición de objetivos”; (ii) Diseño de la propuesta, donde se define el diseño de la solución, así como las técnicas y herramientas utilizadas, abarcando las etapas de “Diseño y desarrollo” y “Demostración”; (iii) Evaluación de la propuesta, donde se detalla el marco de validación,

que incluye los instrumentos de medición y el proceso de validación aplicado, abarcando la etapa de "Evaluación" del método; (iv) la etapa de "Comunicación", centrada en la presentación de avances y resultados del trabajo de investigación, a través de publicaciones en revistas científicas y congresos de la especialidad.

2.2 Fases del método

A continuación, para cada una de estas fases, se describe en profundidad el trabajo a realizar y los objetivos específicos de la tesis con los que se asocia cada fase.

2.2.1 Fase 1: Investigación del Problema

En esta fase se requiere realizar gran parte de la investigación que dará sustento al diseño del marco metodológico para la selección de controles. En esta etapa se deben identificar las prácticas de los expertos en seguridad para realizar sus recomendaciones. Para esto se estudiará lo que indican los estándares respecto del proceso de recomendación de controles. Por una parte se revisará el estándar ISO27001 y por otra parte se estudiarán las Directrices para la auditoría de los sistemas de gestión - estándar ISO19011. Además, se revisará lo que indica la literatura a este respecto.

Por otro lado, se considera realizar una revisión del estado del arte en torno a los modelos cuantitativos para la selección de controles, propuestos por la comunidad, a través de una revisión bibliográfica basada en protocolos de Mapeos Sistemáticos de Literatura.

Por último, se realizará una búsqueda en la literatura en el área de la Investigación de Operaciones, para buscar aquellos métodos de optimización que se adecúen a los problemas de la selección de controles de seguridad.

Los objetivos específicos que se cubren con esta etapa de la investigación son: OE1 y OE2.

OE1: Establecer las prácticas actuales de un asesor de seguridad.

Para determinar la forma en que se realizan las recomendaciones, se estudiará el estándar ISO/IEC 19011:2018, el cual describe las Directrices para la auditoría de los sistemas de gestión, define los procesos que se deben llevar a cabo para la realización de un programa de auditoría en una organización, desde la planeación hasta la finalización del programa. De la misma forma se estudiará el estándar ISO/IEC 27001:2013, el cual contiene los requisitos para un SGSI, considerándose una guía para la implementación de un SGSI. En ambos casos, se estudiará lo que los estándares indican respecto a la definición de un plan de mejora del estado del SGSI que involucre la selección de controles de seguridad de una organización. Por otra parte, se analizará lo que la literatura indica respecto de las prácticas de los asesores de seguridad en lo concerniente a la ISCM. Se estudiarán los procesos involucrados en la ISCM y lo que estos proponen en lo que respecta a la recomendación de controles.

Este trabajo se complementará con la ejecución de un mapeo sistemático de la literatura para identificar las respuestas que se han dado a este problema desde la comunidad científica. Un mapeo sistemático, según [21], es un método robusto y repeti-

ble usado particularmente para responder de forma metódica, objetiva y libre de sesgo un conjunto de preguntas de investigación. Los mapeos permiten identificar los principales estudios que pueden contener información relevante, seleccionar los estudios pertinentes de mayor relevancia y, donde sea apropiado, realizar una evaluación de calidad de los estudios seleccionados.

OE2: Identificar los procesos en donde se presenta una oportunidad de mejora.
A partir de los estudios descritos en el punto anterior, se procederá a identificar los procesos que, por un lado, pueden ser mejorados y, por otro lado, aquellos procesos que no están cubiertos dentro de las recomendaciones de los estándares y de la literatura de la comunidad. Para lograr esto, se determinarán los procesos que deberían formar parte de la selección de controles de seguridad y el grado en que se encuentran descritos en el material revisado. A partir de aquí, se podrán realizar las propuestas de mejora y determinar la forma en que se incluirán los modelos de optimización en el problema de selección.

2.2.2 Fase 2: Diseño de la propuesta

Esta fase se dividirá en 2 etapas; la primera tiene relación con el diseño del marco metodológico, mientras que la segunda aborda el diseño y desarrollo de la herramienta informática que apoyará la operacionalización de la propuesta.

Los objetivos específicos que se cubren con esta etapa de la investigación son: OE3, OE4 y OE5.

OE3: Identificar los modelos cuantitativos apropiados para la selección óptima de controles de seguridad.
A partir de la identificación de las oportunidades de mejora, uno de las situaciones que se debe resolver es la aplicación de modelos cuantitativos para la selección de controles de seguridad, con el objetivo de disminuir la subjetividad de las recomendaciones de inversión por parte de los expertos. En este sentido, una de las propuestas nucleares de este trabajo es la aplicación de modelos de optimización para resolver esta problemática. Por lo tanto, se realizará una búsqueda bibliográfica en el cuerpo de conocimientos del área de la IO, con el objetivo de identificar aquellos métodos de optimización que son aplicables a la problemática de la selección de controles.

OE4: Definir la aproximación metodológica para la selección de controles de seguridad, considerando los modelos, las herramientas, los procesos y las personas que se involucrarán con ella.
Conforme a la información encontrada tanto en los estándares como en el mapeo sistemático y la revisión bibliográfica, se propondrá un marco metodológico que permita cubrir aquellas deficiencias encontradas y complementar la forma de trabajo actual (basada en la opinión experta, y por tanto sujeta a un alto grado de subjetividad) con métodos cuantitativos, de tal manera que se mejore la objetividad y trazabilidad de las decisiones. Para esto se identificarán e integrarán (a) los modelos cuantitativos que resuelven el problema de selección, (b) los procesos que definirán el marco metodológico, (c) las herramientas que permiten resolver el problema y (d) las personas que participan en la resolución. Para construir el marco metodológico se recurrirá al Análisis Conceptual [116] para determinar los conceptos claves que delimitan el ámbito de la investigación, así como las ideas

y teorías que se revisarán. El Análisis Conceptual contextualiza los conceptos dentro del área en que se definen.

OE5: Implementar una herramienta, a nivel de prototipo funcional, que dé soporte a la metodología y avance en el grado de automatización del proceso.
En esta etapa se diseñará y desarrollará un prototipo de herramienta informática que permita operacionalizar/aplicar el marco metodológico, de tal manera que apoye al experto en la captura y almacenamiento de la información, en la modelación y resolución del problema y, por último, en el resumen y visualización de los resultados. Para llevar a cabo esta etapa, se utilizará un proceso de desarrollo software iterativo e incremental [7]. Estas características del proceso permiten el crecimiento progresivo de la funcionalidad, de manera que el producto pueda ir evolucionando con cada una de las entregas previstas hasta que se amolde a lo requerido por el cliente. En este tipo de proyectos se define una serie finita de iteraciones del prototipo hasta que este cumpla con los requerimientos establecidos.

2.2.3 Fase 3: Evaluación de la propuesta

En esta etapa se realizará una evaluación del desempeño de la propuesta, a través de un estudio de la percepción de los usuarios del marco metodológico. Esta etapa se realizará para responder preguntas como: ¿Qué percepción tienen los actores relevantes respecto del método planteado? ¿El método planteado genera beneficios respecto de los métodos utilizados tradicionalmente?, etc. Para estudiar la percepción de los usuarios, se realizará un estudio de adopción de métodos software, de tal manera que sea posible determinar el grado en que los usuarios estarían dispuestos a un cambio de práctica y adoptar el mar-

co metodológico propuesto

Para esta evaluación se diseñará un quasi-experimento [40], el cual consiste en un método de investigación similar a los experimentos, pero en el cual los sujetos o grupos de sujetos de estudio no han sido asignados aleatoriamente. Con los resultados obtenidos se evaluarán las diferencias en cuanto a percepciones subjetivas de los estudiantes respecto a la utilización de la propuesta.

En esta etapa se abordarán los objetivos específicos OE6 y OE7.

OE6: Aplicar el marco metodológico en un ambiente controlado.
Para la evaluación de la propuesta, se diseñará un experiencia con estudiantes de una asignatura de Auditoría Informática, en la cual los estudiantes deberán aplicar el marco metodológico sobre un caso de auditoría, en un contexto real (una organización chilena), donde los estudiantes deberán realizar recomendaciones de selección de controles de acuerdo a las condiciones particulares de dicha organización.

OE7: Realizar un estudio de adopción de la propuesta para evidenciar el impacto que tendría sobre los asesores de seguridad.
A través de un estudio de intención de adopción, se estudiará la percepción de los estudiantes respecto de la aplicación del marco metodológico.

Para analizar la percepción de los participantes, se utilizará el modelo UMAM [38] el cual permite estudiar la adopción de un

nuevo método de trabajo por parte de los usuarios involucrados mediante la aplicación del cuestionario validado UMAM-Q.

2.2.4 Fase 4: Comunicación

Esta fase se relaciona con la documentación y comunicación de los avances y resultados del proyecto de investigación. En particular, se refiere a las publicaciones en revistas especializadas y trabajos en congresos del área.

Esta fase no está ligada explicitamente a ningún objetivo en particular, sino que es transversal, es decir, está relacionada con todos los objetivos trazados para este proyecto, ya que documenta y difunde los resultados obtenidos en el resto de fases del método.

Parte II

Desarrollo de la investigación

3. Contexto de la Investigación

Este capítulo define los conceptos básicos de IO y de ISCM, y cómo estos conceptos se pueden relacionar para dar solución al problema propuesto. Además, se presenta el estado de la investigación respecto de la utilización de IO en el problema de la selección de controles de seguridad.

En la sección 3.1, se describen los principales conceptos asociados a la gestión de la seguridad de la información y cómo, desde estos, se deriva la gestión de los controles de seguridad y el problema de selección que enfrenta este trabajo.

En la sección 3.2 se describe el área de la IO, sus principales conceptos y su campo de aplicación.

Por último, en la sección 3.3 se justifica la aplicación de las técnicas de IO para resolver el problema de la selección de controles de seguridad.

3.1 Gestión de la seguridad de la información

La gestión de la seguridad de la información se preocupa de definir, implementar y controlar un conjunto de acciones y políticas tendientes a asegurar los activos de información a través de la implementación de sistemas de gestión de seguridad, disminuyendo de este modo el riesgo de dicho activo.

Como se aprecia en la figura 3.1, el riesgo se determina en base al valor del activo, a las amenazas y las vulnerabilidades que afectan al activo. Mientras mayor sea el valor del activo, mayor es el riesgo de ataque, por lo que requiere de mayor protección. De la misma manera, las amenazas, que se puede entender como la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre un activo de información, aumentan el riesgo al aprovechar las vulnerabilidades que exponen a un activo. Por tanto, mientras más vulnerabilidades presenta un activo de información, mayor es la posibilidad de un ataque sobre el activo, lo que implica un aumento del riesgo.

La gestión de riesgos de seguridad de la información es un proceso que considera la identificación y el análisis de los riesgos a los que está expuesta la organización, la evaluación de los potenciales impactos y la decisión de las acciones a implementar para eliminar o reducir el riesgo a un nivel aceptable [107]. Según Bojanc y Jerman-Blažič [15], en el proceso de gestión de riesgos de seguridad se suelen identificar las siguientes etapas:

- identificación de los activos;
- identificación de amenazas y evaluación de daños de posibles

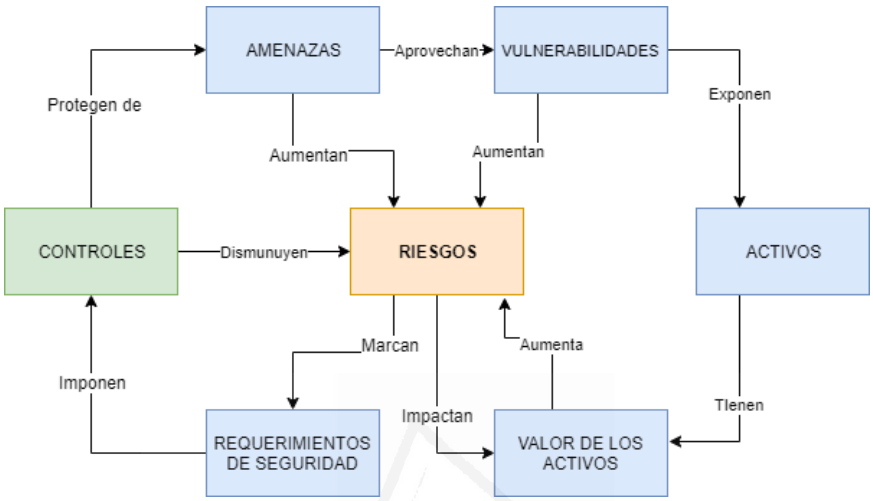


Figura 3.1: Factores en la gestión del riesgo de SI. Imagen tomada de `http://www.iso27000.es`

ataques;

- identificación de vulnerabilidades de seguridad de los sistemas que el ataque puede explotar;
- evaluación de riesgos de seguridad;
- puesta en marcha de medidas para minimizar el riesgo mediante la implementación de controles apropiados;
- monitorización de la efectividad de los controles implementados.

Dubois et al. [39] clasifican en 4 categorías las distintas propuestas de gestión de riesgos de seguridad de la información:

- Estándares de Gestión de Riesgos. Incluye estándares como ISO/IEC Guide 73 [50] y AS/NZs 4360 [82].

- Frameworks orientados a Requerimientos de Seguridad. Agrupa las propuestas para el manejo de los riesgos de seguridad de la información basadas en la determinación de los requisitos de seguridad. Existen múltiples propuestas en esta categoría, como son la de Mellado et al. [97] y la de Khan e Ikram [78], donde se mencionan un conjunto de frameworks que incluyen distintos métodos y técnicas destinadas a determinar de la mejor forma los requerimientos de seguridad. Entre estos métodos y técnicas destacan SecureUML [10][11], SIREN [140] y el i* Framework [44].

- Métodos de Gestión de Riesgos de Seguridad. Incluye métodos como EBIOS [33], OCTAVE [4] y CORAS [143], entre otros.

- Estándares de Seguridad de la Información. En esta categoría se clasifican los diversos estándares de seguridad existentes a la fecha, tales como ISO27001 [51], NIST [107] y COBIT [73], entre otros. Éstos buscan disminuir el riesgo de un evento de seguridad a través de la implementación de un sistema de gestión de seguridad que reuna un conjunto de buenas prácticas [71], denominados ISC [76].

La presente tesis doctoral se enmarca dentro de esta última forma de gestionar riesgos, al proponer un conjunto de modelos y técnicas cuyo propósito es apoyar la selección de controles de seguridad de un estándar de seguridad de forma que se minimice el riesgo y se maximice la utilización de los recursos de la organización. Es por ello que a continuación se profundiza en el área del uso de estándares de seguridad de la información.

3.1.1 Estándares de seguridad de la información

Un estándar para la seguridad de la información consiste en un conjunto de reglas que tiene como objetivo regular el funcionamiento de una empresa, con un énfasis especial en la gestión de la información y el aseguramiento de la información. En general, el cumplimiento de cualquier estándar de seguridad de la información significa lograr un conjunto de objetivos a través de la implementación de acciones o ISC, definidas por cada estándar [114].

En la actualidad, muchos estándares de seguridad de la información se basan en controles que guían el desarrollo, operación, monitoreo, revisión, mantenimiento y mejora de los SGSI [61, 137]. Algunos de los estándares más reconocidos a nivel mundial son la familia ISO/IEC 27000, BS17799, PCIDSS, ITIL, COBIT y estándares nacionales o regionales como la serie NIST SP 800 y GASSP [12, 132], los cuales se reconocen como un conjunto completo de mejores prácticas (controles) que pueden ayudar a las organizaciones a administrar de manera efectiva la seguridad de sus datos y activos de TI.

La International Organization for Standardization (ISO) [1], es una organización internacional que trabaja en el desarrollo de diversos estándares, reuniendo a expertos internacionales en distintas áreas, quienes definen un marco de referencia para medir un sistema de gestión particular, además de otorgar certificaciones a las organizaciones cuando cumplen con los estándares definidos por ellos. Los estándares propuestos por ISO son los más utilizados a nivel mundial.

Para efectos de este trabajo de investigación, se estudiarán dos estándares propuestos por ISO. El primero es la norma ISO/IEC 27001:2013, ya que es uno de los estándares más conocidos para la gestión de la

[1] https://www.iso.org/home.html

seguridad de la información [37]. El segundo estándar que se analizará es la norma ISO/IEC 19011:2018, que se presenta como una guía para el desarrollo de procesos de auditoría de sistemas de gestión. Esta norma propone diversos pasos para llevar a cabo una auditoría, dentro de los cuales se encuentra la definición de un plan de mejora, en el cual se detalla los controles a implementar para lograr el estándar sobre el cual se está auditando. Esta descripción de los controles a implementar lleva implícito el proceso de selección de controles en el que se centra esta tesis.

Estándar ISO/IEC 27001:2013

Como ya se ha mencionado, esta norma ha sido desarrollada por ISO con el objetivo de proponer requisitos para el diseño e implementación de un SGSI. Tal como se aprecia en figura 3.2, la norma se basa en un modelo de mejora continua (Plan - Do - Check - Act (PDCA)) [124], lo que implica que el modelo se desarrolle en base a un ciclo que se divide en un cuatro grandes etapas:

i Planificar (Plan), en esta etapa se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar.

ii Hacer (Do): Se realizan los cambios para implantar la mejora propuesta.

iii Verificar (Check): Periodo de prueba para verificar el correcto funcionamiento de la mejora implementada.

iv Actuar (Act): Estudio de los efectos de la mejora, comparándolos con la situación previa a la implementación.

En la figura 3.2, en la etapa de Planificación, se puede apreciar que uno de los puntos que trata es la selección de controles. Estos controles se refieren al conjunto de buenas prácticas para la seguridad de la información, que la norma, en su anexo A, recomienda implementar. En su versión del año 2013, la norma propone un conjunto de 114 controles distribuidos en 14 dominios y 35 objetivos de control.

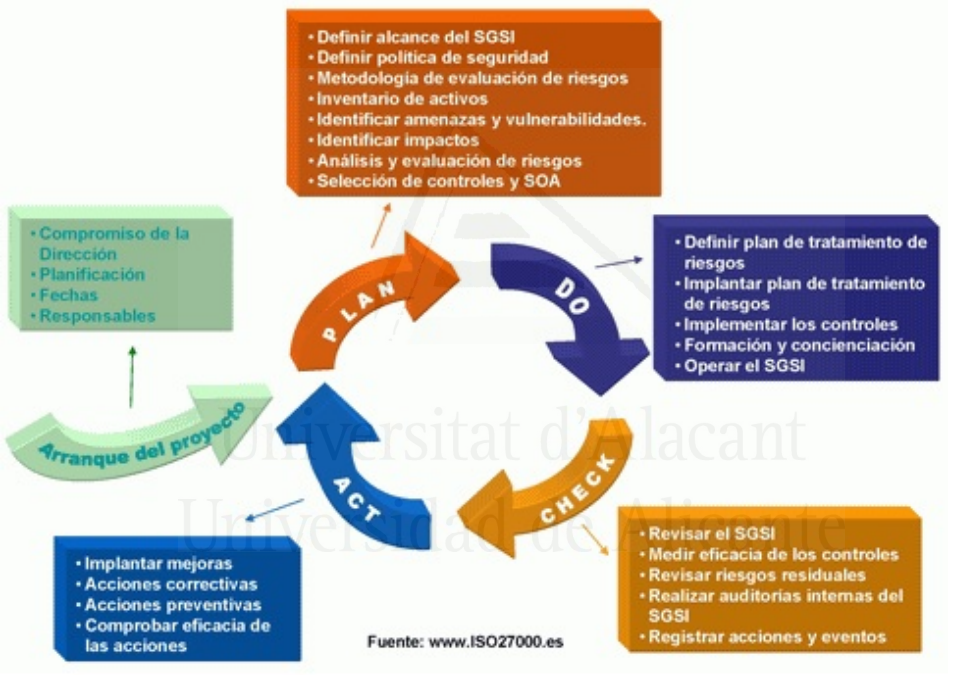


Figura 3.2: Modelo PDCA ISO27001 - Fuente: http://www.iso27000.es

De acuerdo a la norma, la sección "6.1.3 - Tratamiento de riesgo de la seguridad de la información", en el punto (b) indica que la organización debe *"determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de*

información escogida". Como se puede apreciar, en esta indicación no se detallan lineamientos respecto de cómo se debe realizar esta determinación; solo se da a entender que esta selección debe ser congruente con los niveles de riesgo identificados por la organización. Por tanto se deja al libre albedrío del asesor el decidir cómo discriminar, del conjunto total de controles que permiten mitigar el riesgo, aquellos que le permitan cumplir con las restricciones de recursos que sufren las organizaciones.

De la lectura de la norma se puede concluir que la selección de los controles adecuados para la mitigación del riesgo de la seguridad de la información es un paso relevante, a pesar de que ésta no detalle cuál debe ser el proceso para realizar dicha selección.

Estándar ISO/IEC 19011:2018

La norma ISO/IEC 19011:2018 es una norma internacional, no certificable, desarrollada por la ISO, que establece las directrices para la auditoría de cualquier sistema de gestión implementado por alguna organización. Esta norma define un marco metodológico, basado en un modelo de mejora continua, que apoya un programa de auditorías sobre un sistema de gestión. Esta norma no establece requisitos, sino que se presenta como una guía que orienta la gestión de un programa de auditoría, considerando la planificación y realización de una auditoría sobre un sistema de gestión, así como la definición de las competencias de un equipo auditor.

Como se muestra en el figura 3.3, esta norma se basa en el concepto de mejora continua de los sistemas de gestión de una organización, en otras palabras, su objetivo es establecer un programa de auditoría que permita la mejora del sistema de gestión implementado, bajo la

perspectiva de un modelo PDCA. Esta visión, enfocada en la mejora, implica que esta guía estimula la incorporación de prácticas, asociadas al sistema de gestión evaluado, que permitan un mejor desempeño de este. Así, el programa de auditoría se utiliza como una herramienta de control de la evolución del sistema de gestión evaluado.

Para llevar adelante este control, la auditoría contrasta la realidad de la organización con un norma objetiva asociada al sistema de gestión que se está evaluando. En otras palabras, la auditoría determina el grado de conformidad que posee la implementación de un sistema de gestión respecto de la norma elegida. Así, la información proporcionada por la auditoría permite a la organización actuar para mejorar su desempeño. A partir de este diagnóstico y en base a la visión de la mejora del sistema de gestión, La guía indica que, dependiendo de los objetivos de la auditoría, las conclusiones de ésta pueden indicar la necesidad de implementar acciones correctivas y/o acciones preventivas para la mejora.

De acuerdo a la Nota 2 del punto 3.4 de la norma, se indica que "Los hallazgos de auditoría pueden llevar a la identificación de oportunidades de mejora o al registro de mejores prácticas". De la misma forma, en el punto 6.4.8, se indica que "Si el plan de auditoría así lo especifica, las conclusiones de la auditoría pueden llevar a recomendaciones para la mejora o futuras actividades de auditoría". De estos puntos se desprende que la guía establece que el equipo auditor, como parte del informe de auditoría, puede recomendar una serie de acciones que puede realizar la organización en pos de la mejora del sistema de gestión.

Sin embargo, dada la generalidad de la norma, ésta no establece un procedimiento o metodología que guíe al equipo auditor, a partir del diagnóstico proporcionado por la auditoría, respecto de cómo determi-

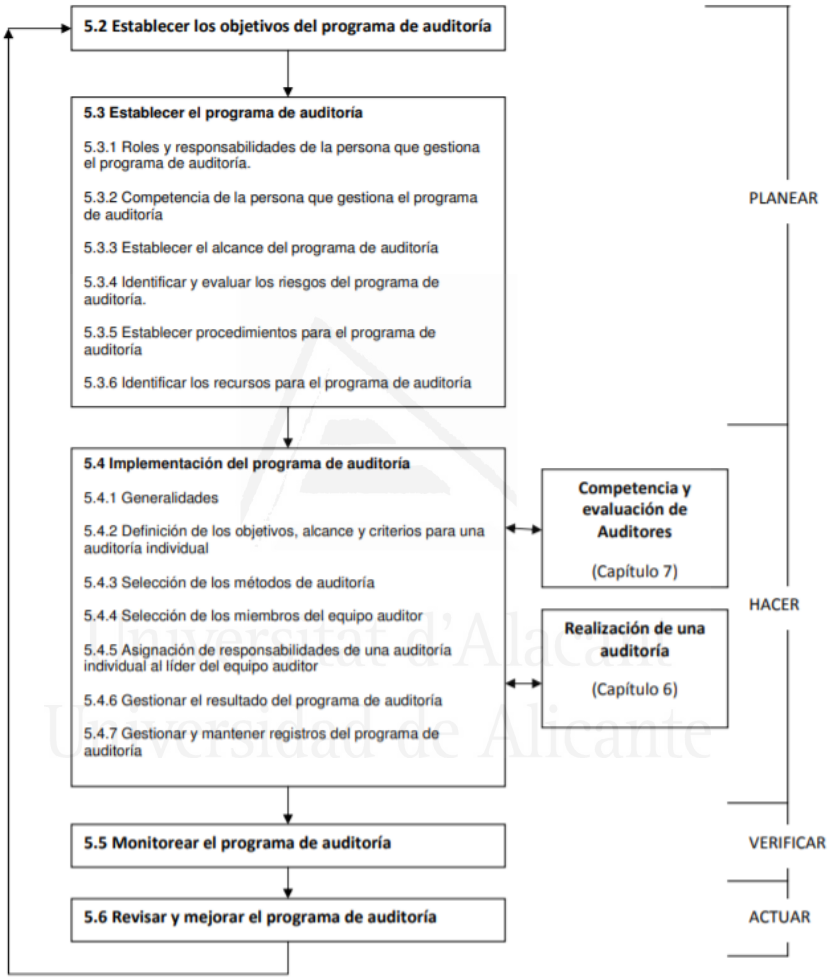


Figura 3.3: Esquema PDCA. Fuente: ISO/IEC 19011:2018 [53]

nar o seleccionar el conjunto de mejoras o acciones que la organización debería implementar en sus sistema de gestión. Así, este proceso queda a criterio y experiencia del equipo auditor.

Como se ha visto, ni la norma general para la auditoría de sistemas de gestión (ISO/IEC 19011:2018), ni la norma específica para la implementación de un SGSI (ISO/IEC 27001:2013) proveen directrices respecto de cómo proceder para realizar la propuesta de acciones para la mejoras a través de la recomendación de implementación de controles de seguridad. En otras palabras, aunque ambas normas reconocen la necesidad de avanzar hacia la mejora, implementado buenas prácticas en el quehacer del SGSI, ninguna provee lineamientos formales respecto de cómo seleccionar las mejores acciones a implementar, por lo que este proceso se deja al juicio experto.

Si bien es cierto que existen algunas técnicas en la literatura que pueden ser aplicadas por los expertos, éstas no conforman un método sistemático que permitan proponer las mejores acciones a implementar por las organizaciones, dadas sus condiciones particulares.

3.1.2 Gestión del cumplimiento de un estándar de seguridad

Como parte del gobierno organizacional de la seguridad, es esencial hacer cumplir y medir el grado de cumplimiento de las normas o políticas relacionadas a la seguridad de la información [142]. Para ello, los procesos de auditoría son una herramienta relevante para la mejora continua de dicha seguridad [51]. Con el fin de implantar estos procesos, las organizaciones deben definir un programa de auditoría, que consiste en un conjunto sucesivo de auditorías para medir cada mejora

y, finalmente, lograr el pleno cumplimiento de los estándares elegidos.

Un diagnóstico de seguridad de la información dentro de un proceso de auditoría basado en estándares se basa en una lista de chequeo de controles realizados y no realizados. Esto implica que el mapa de controles implementados / no implementados es una herramienta de gestión para lograr avances en la seguridad de la información respecto de una o más guías a las que se hace referencia.

Cada control a implementar, en el sentido de ponerlo en práctica, implica recursos para asignar y una mejora correspondiente en la seguridad de la información. Bajo esta perspectiva, cumplir con algún estándar de seguridad basado en procesos también se traduce en un problema de implementar un conjunto de controles de seguridad de la información. La complejidad de este problema difiere en función de las diferentes variables que se necesitan modelar, tales como recursos (personas, presupuestos, tiempo) o variables para evaluar las mejoras de seguridad de la información (mitigación de riesgos, reducciones de vulnerabilidades, cumplimiento del estándar).

3.1.3 Gestión de los controles de Seguridad

Como se mencionó anteriormente, la gestión del riesgo involucra la determinación de aquellas acciones que permitan mitigar el riesgo sobre el activo. Desde la perspectiva de los estándares de seguridad de la información, como la ISO/IEC 27001:2013, estas acciones se traducen en un conjunto de buenas prácticas de seguridad (los ISC), recomendadas por el estándar. Esto implica que debe existir un proceso de gestión de los ISC para asegurar la efectividad de la aplicación del estándar.

Si bien es cierto que, como ya hemos visto, la norma ISO/IEC 27001:2013 no propone explicitamente un modelo de gestión de controles, sí plantea que el tratamiento del riesgo se puede realizar a través de la implementación de los controles propuestos. Como se aprecia en la figura 3.4, en el modelo de gestión de riesgo propuesto por esta norma se propone realizar la mitigación del riesgo a través de un proceso que se centra sobre los ISC. Este proceso implica la selección de los controles a implementar, la declaración de aplicabilidad de los mismos y, por último, la implantación de los controles seleccionados y que son elegibles de aplicar. Sin embargo, no proporciona mayores detalles respecto de la metodología con que se deben seleccionar o decidir su aplicabilidad. En otras palabras, la definición de este proceso proporciona una vista general, y debe refinarse en función de las características y objetivos de cada organización, así como en función del equipo de expertos que realiza los análisis y recomendaciones.

Este carácter generalista del proceso ha generado cierto grado de escepticismo respecto de la efectividad de un estándar en la mitigación del riesgo. De acuerdo a Diesch et al. [36], los expertos declaran que los estándares ayudan a guiar el cumplimiento, pero no siempre ayudan a reducir el riesgo o mejorar la seguridad. En este contexto, estos mismos autores compilaron una lista de razones que explican este fenómeno, que se listan a continuación:

- Los estándares tienen un alcance muy genérico y tienden a ser muy abstractos.
- Los estándares consisten en una gran cantidad de información, lo que los vuelve demasiado complejos y conduce a un retroceso hacia las implementaciones ad-hoc.
- Los controles y las contramedidas a menudo se implementan sin

Figura 3.4: Gestión de riesgo, propuesto por la Norma ISO/IEC 27001:2013. Fuente: `http://www.iso27000.es`

una adecuada consideración de su necesidad o esfuerzo de implementación.

- No existen suficientes estudios empíricos que validen los estándares y las mejores prácticas propuestas por éstos.

- Existen diferencias regionales en el uso y los contextos de los estándares.

Por otro lado, la visión desde la práctica de la industria tampoco es más esclarecedora a este respecto. En un trabajo de investigación

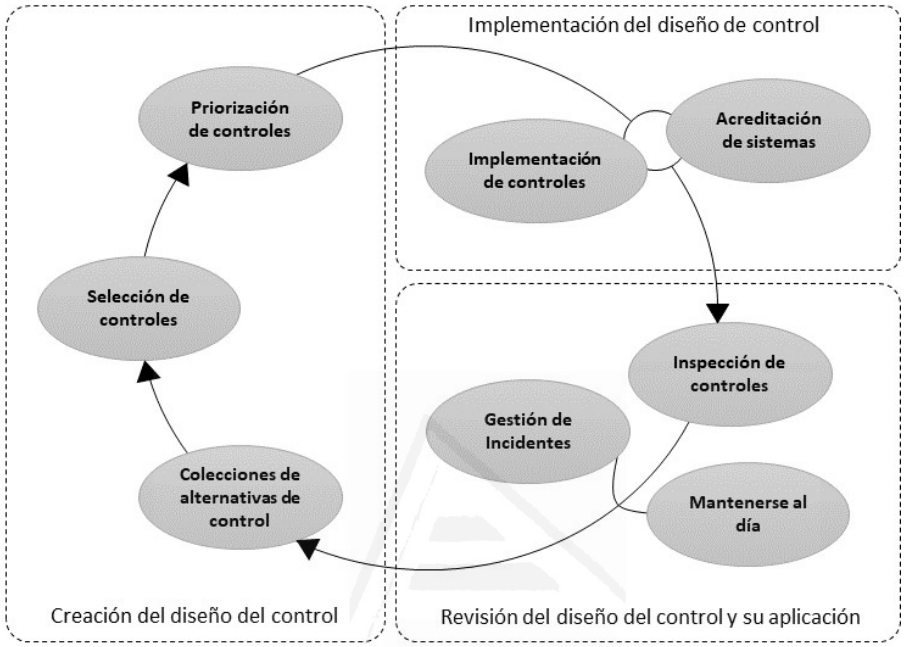


Figura 3.5: Ciclo de gestión de controles de seguridad de Bachlechner et al. [8]

que recogió el quehacer de profesionales de la seguridad de la información, pertenecientes a grandes y medianas organizaciones de Europa, Bachlechner et al. [8] construyeron un modelo para la ISCM. Este modelo formaliza y sistematiza las actividades que los expertos en seguridad de las organizaciones llevan a cabo para gestionar los controles de seguridad. En la figura 3.5, se muestran las etapas del proceso definido por Bachlechner et al. [8].

De la misma manera que en el caso del modelo propuesto por la Norma ISO/IEC 27001:2013, este modelo no provee de mayor detalle respecto de cómo se debe llevar a cabo la selección y priorización de

los ISC. En ambos casos no se define una metodología para la selección de controles, de lo que se deduce que este proceso depende del experto de seguridad, quien se basa principalmente en su experiencia.

Por tanto, una manera de disminuir la subjetividad del proceso de selección de controles es sistematizar el proceso a través de la definición de una metodología aplicable en la diversidad de casos que podrían sucederse y que considere métodos cuantitativos para la selección de controles. Esta sistematización se convertiría así en una herramienta de apoyo a la toma de decisiones del experto en seguridad.

3.1.4 Selección de controles de seguridad de la información

Los estándares de seguridad de la información basados en la implementación de controles se focalizan en disminuir las vulnerabilidades y los riesgos, internos y externos, que afectan los activos de información, a través de la implementación de las acciones o controles que ellos mismos definen [72]. Por lo tanto, para cumplir con uno o más de estos estándares, se deben implementar y lograr la totalidad de estos controles. La diferencia que existe entre los controles alcanzados y los que aún no se han logrado representa la brecha que la organización debe cubrir para dar cumplimiento con el estándar y optar a una certificación.

La consecución del objetivo final por parte de la organización (el cumplimiento de algún estándar basado en controles) se suele realizar en base a avances parciales en un plan de seguridad de la información. En este proceso, si bien es cierto que los controles asociados a cada nor-

ma están claramente establecidos, la manera en que las organizaciones deben ir realizando estos avances para disminuir la brecha y lograr así la certificación no es estándar, sino que depende de las condiciones propias de cada organización. En otras palabras, la selección de los controles, así como la definición de un programa de implementación de éstos, implica determinar, dadas las características propias de la organización, cuál es el mejor subconjunto de controles a implementar [111], cuál es la forma más eficiente de cumplirlos y cómo realizar un seguimiento de dichos controles [9]. Por lo tanto, como se plantea en [9], el foco no está en la cantidad de controles que se debe implementar para alcanzar un determinado nivel de seguridad, sino que se debe considerar la "calidad" del conjunto de controles que logre una mayor disminución del riesgo con el menor costo posible.

Desde la perspectiva de la gestión de la seguridad de la información, determinar el conjunto idóneo de controles que deben ser implementados en una organización no es una situación simple de resolver para los asesores de seguridad [138], ya que, como ya hemos comentado, los estándares o los modelos de madurez asociados a éstos [120] son demasiado generales y no se ajustan a las características propias de una organización [129], por lo que no explicitan una manera formal de realizar estas recomendaciones. Además los estándares no proporcionan un método formal y cuantitativo que permita asegurar resultados óptimos en la selección y programación de los controles de seguridad, sino que se basan en modelos cualitativos apoyados por el juicio experto [8]. Es por ello que, al intentar determinar cuál es el mejor conjunto de controles a implementar por una organización, solo se obtienen aproximaciones y no un conjunto que optimice los recursos de la organización para el logro de sus objetivos, acorde a su realidad, de tal manera que, por ejemplo, se minimice el riesgo o se minimice el presupuesto necesario para alcanzar un cierto nivel de seguridad.

Dada la importancia de una adecuada gestión de los controles dentro de la organización y, por ende, la importancia de poseer un modelo formal de gestión de controles de seguridad que se corresponda con las prácticas de las organizaciones [128], es necesario apoyar a las organizaciones con técnicas que permitan responder a la problemática respecto de cuál es la mejor combinación de avance, o cuáles deben ser los controles que se deben implementar y en qué orden hacerlo. Esta tesis se ocupa de avanzar en este camino.

3.2 Investigación de Operaciones

La investigación de operaciones se define como un enfoque científico para la toma de decisiones que busca definir la mejor manera de diseñar y operar un sistema [149].

Como ya se ha comentado anteriormente, IO es una disciplina que durante muchas décadas ha definido técnicas y métodos cuantitativos para resolver problemas de decisiones. IO plantea que las soluciones alcanzadas mediante el uso de un modelo obtenido a través de estas técnicas, son significativamente mas eficientes en comparación a aquellas que se podrían obtener a través de la intuición o experiencia del tomador de decisiones [54]. Esto es particularmente evidente en problemas que presentan un alto grado de complejidad, donde se identifican una gran cantidad de variables y condiciones.

Su historia se remonta a los primeros intentos de aplicar enfoques científicos, primero a la producción industrial, y más tarde a la gestión de la organización. Para estos campos de aplicación, la IO ha desarrollado modelos matemáticos, estadísticos y algoritmos que permiten resolver problemas complejos con el fin de apoyar los procesos de toma

de decisiones [108]. Se trata por tanto de una disciplina consolidada, con su propio cuerpo de conocimiento y líneas de investigación características [93].

Por lo general, la IO tiene sentido en condiciones que requieren la asignación óptima de recursos limitados. Para resumir, un problema de optimización puede entenderse como una situación que requiere determinar la mejor solución para un problema dado. El problema se representa como una función para minimizar o maximizar, sujeto a un conjunto de restricciones [117]. Para formular este tipo de problema, la situación debe modelarse matemáticamente mediante una métrica multidimensional, su función objetivo y un conjunto de restricciones modeladas como ecuaciones y/o inecuaciones. Las restricciones representan limitaciones, tales como secuencias de costos, tiempo y espacio, entre otras. Tanto las restricciones como la función objetivo deben estar compuestas por diferentes variables y relaciones del sistema en estudio.

La complejidad de los problemas de optimización depende de varios factores. En primer lugar hay que considerar los tipos de variables, que pueden ser todas continuas, todas discretas o de ambos tipos. Además, en función del grado de certeza con el cuál se conocen los parámetros del modelo matemático, podemos encontrarnos ante un modelo determinístico (cuando se tiene certeza de los valores de los parámetros), o estocástico (cuando los parámetros usados para caracterizar el modelo son variables aleatorias).

El tipo de modelo resultante (ecuaciones) podría ser lineal, cuadrático, polinómico o incluso diferencial. Estas categorías pueden aplicarse tanto a funciones objetivas como a restricciones.

Además, la complejidad del problema también cambia en función

de la cantidad de funciones objetivo y restricciones, así como en función del tipo específico de problema: clasificación, selección, programación, empaquetado o, una combinación de ellos. Es importante destacar que todas las características anteriores pueden estar presentes en la misma formulación.

La IO, como disciplina, ha desarrollado técnicas de optimización específicas en función de las características del problema mencionadas [117]. Así, ofrece técnicas de programación lineal y no lineal para problemas con variables continuas, y métodos de asignación ortogonal para problemas con variables discretas [24].

Además, se han desarrollado nuevos métodos, como programación matemática, simulación, teoría de juegos, teoría de colas, análisis de redes, análisis de decisiones o análisis multicriterio, entre otros [108]. Las formulaciones de problemas complejos, en el sentido de la cantidad de variables consideradas, pueden resolverse mediante métodos exactos o enfoques basados en heurísticas [101].

3.3 Utilización de IO en el problema de la selección de controles de seguridad

En el ámbito particular de este trabajo, es posible considerar el problema de decisión de la selección de ISC, como un problema de optimización, en el cual se busca el conjunto óptimo de controles que minimice riesgos y considere las restricciones propias de la organización, tales como costos, tiempos, prioridades, políticas organizacionales, etc.

Para la resolución del problema planteado, la Investigación de Operaciones proporciona distintas técnicas enfocadas a enfrentar problemas de optimización [22], que pueden aportar en la resolución del problema de selección del conjunto óptimo de controles. La incorporación de técnicas y metodologías provenientes de la disciplina de Investigación de operaciones puede resolver la problemática planteada, entregando resultados óptimos.

4. Mapeo Sistemático de la Literatura

En esta sección se presenta un análisis del problema de selección desde la revisión de lo que se presenta en la literatura del área.

En la sección 4.1, se presentan los resultados de una revisión bibliográfica basada en un protocolo de mapeo sistemático. Se muestran los artículos que presentan propuestas cuantitaivas similares a la presentada en este trabajo.

En la sección 4.2, se presentan las oportunidades de investigación que se derivan de los trabajos encontrados en la revisión bibliográfica, se define una estructura de solución y se describen las etapas generales que conforman esta propuesta.

4.1 Selección de controles de SI: Mapeo Sistemático de la literatura

Como ya se indicó en el capítulo 3 cuando se discutieron los principales estándares de seguridad de la Información [48], se puede observar que éstos no establecen claramente un modelo formal para la etapa de la gestión de los controles de seguridad en las organizaciones [8].

Para solventar en parte este problema, diversos autores han propuesto frameworks para medir el nivel de cumplimiento de un estándar [16, 18, 23, 100, 132]. Sin embargo, medir un nivel de logro no resuelve el problema de seleccionar y programar el siguiente conjunto de controles a implementar. Solo en los casos de enfoques de madurez [120] se puede encontrar una guía general para la implementación de los controles de seguridad.

Estos enfoques de madurez a menudo dividen el estándar en diferentes grupos de prácticas de seguridad (diferentes grupos de controles). Estos grupos constituyen diferentes "niveles de madurez". De esta manera, se debe progresar a través de la implementación de estos grupos de controles, avanzando de un nivel al siguiente. Sin embargo, se ha establecido que estos modelos son demasiado generales y no consideran las características particulares de cada organización [123, 129]. Además, los estándares basados en la implementación de buenas prácticas no definen guías o lineamientos respecto al desarrollo de un plan para la implementación de dichas prácticas (su programación), a pesar de que es un hecho reconocido que diferentes escenarios internos y externos (distintas restricciones en función de la organización) requieren rutas de implementación distintas [79, 111].

Otro tipo de enfoques aborda el problema del cumplimiento de la

seguridad desde el punto de vista del comportamiento humano, es decir, se centra en las prácticas de seguridad de la organización y en las guías para fomentarlas [66, 84, 92, 105]. Sin embargo, ninguno de estos enfoques resuelve los problemas formulados de selección, planificación o programación de los controles de seguridad de la información. Por otro lado, parecen muy adecuados como complemento para considerar las variables relacionadas con las personas en una implementación exitosa de los controles de seguridad.

Para poner en contexto la contribución de esta propuesta, se ha realizado una búsqueda bibliográfica basada en un protocolo de mapeo sistemático [115], con el objeto de determinar las contribuciones que existen referentes a esta problemática. En particular, el objetivo fue identificar qué métodos o técnicas se han propuesto para seleccionar y programar el conjunto óptimo de controles de seguridad de la información a implementar. Para evaluar los logros de esta búsqueda, se definió como pregunta de investigación:

RQ1:"¿Qué métodos o técnicas se han propuesto para resolver el problema de la selección y programación de un conjunto de controles de un estándar de seguridad de la información que permite la evaluación del riesgo o la seguridad de una organización?".

Sobre la base de la pregunta de investigación y los conceptos principales que se derivan de ella, se obtuvo la siguiente cadena de búsqueda:

" ("Security Evaluation" OR "Controls Selection" OR "Security Solutions") AND "Information Security Compliance" ".

Para ejecutar la cadena de búsqueda, se seleccionaron los principales repositorios digitales de informática y disciplinas relacionadas: IEEEXplore, Biblioteca Digital ACM, Springer Link y Science Direct.

Además, se revisaron las principales conferencias en el área de seguridad de la información, como son la Conferencia Internacional sobre Disponibilidad, Confiabilidad y Seguridad (ARES), la Conferencia Internacional sobre Inteligencia y Seguridad Computacional (CIS) y la Revista Internacional de Tecnología de la Información y Toma de Decisiones (CISIS).

Como criterio de inclusión se consideró:

- Estudios que presenten propuestas, modelos teóricos, ejemplos teóricos o estudios de casos, relacionados con la selección y/o programación de controles de una norma de seguridad de la información o que aborden el problema de selección de medidas de seguridad de la información.

Además, se consideró el siguiente conjunto de criterios de exclusión:

- Estudios que no incluyen propuestas, modelos teóricos, ejemplos teóricos o estudios de casos relacionados con la selección y/o programación de controles de una norma de seguridad de la información o no abordan el problema de selección de medidas de seguridad de la información.
- Libros o reportes técnicos.
- Documentos de tesis.
- Trabajos duplicados del mismo estudio en diferentes fuentes.
- Documentos de discusión o revisiones bibliográficas.
- Artículos que no son accesibles.
- Artículos que no están escritos en inglés.

De esta revisión, se seleccionaron 35 artículos. En la tabla 4.1, se presentan una lista de los trabajos encontrados.

Tabla 4.1: Resumen de enfoques para la selección de controles de seguridad de la información.

Año	Título	Ref.
2007	Using CP-nets as a guide for countermeasure selection.	[13]
2008	Pareto-optimal situation analysis for selection of security measures.	[109]
2009	A Vikor-based multiple criteria decision method for improving information security risk.	[152]
	Security Evaluation Method Based on Host Resource Availability.	[56]
	An information system security evaluation model based on AHP and GRAP.	[31]
	Information security solution decision-making based on Entropy Weight and Gray Situation Decision.	[27]
	Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking.	[103]
2010	A multi-criteria evaluation of information security controls using Boolean features.	[111]
	A ranking method for information security risk management based on AHP and PROMETHEE.	[90]
2011	Evaluation of information security controls in organizations by grey relational analysis.	[110]
	AHP-GRAP based security evaluation method for mils system within cc framework.	[151]

Continúa en siguiente página

Tabla 4.1 – continuación pagina anterior

Año	Título	Ref.
	A multi-criteria evaluation method of information security controls.	[91]
	Decision support for Cybersecurity risk planning.	[118]
2012	A fuzzy logic-based information security control assessment for organizations.	[112]
	A Multi-attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory.	[43]
	New approach in information system security evaluation.	[18]
	A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem.	[141]
	A multi-objective decision support framework for simulation-based security control selection.	[79]
2013	Simulation-based optimization of it security controls: Initial experiences with meta-heuristic solution procedures.	[80]
	Simulation-based optimization of information security controls: An adversary-centric approach.	[81]
	A vikor technique based on DEMATEL and ANP for information security risk control assessment.	[153]
	Selection of optimal countermeasure portfolio in IT security planning.	[126]
	On identifying proper security mechanisms.	[19]
	On selecting critical security controls.	[20]
2014	Security evaluation model based on the score of security mechanisms.	[17]

Continúa en siguiente página

Tabla 4.1 – continuación pagina anterior

Año	Título	Ref.
	Selection of information security controls based on AHP and GRA.	[29]
	A multiple attribute decision making for improving information security control assessment.	[3]
	Proposal of a model supporting decision-making on information security risk treatment.	[75]
2015	The Application Research of Information Security Risk Assessment Model Based on AHP Method.	[98]
	A comprehensive security control selection model for inter-dependent organizational assets structure.	[127]
	Selecting optimal subset of security controls.	[154]
2016	Optimal selection of security countermeasures for effective information security.	[125]
2017	Ranking information security controls by using fuzzy analytic hierarchy process.	[77]
2018	Decision support for selecting information security controls.	[6]
	Decision support for the optimal allocation of security controls.	[156]

En la tabla 4.2 se han clasificado las propuestas según la complejidad del problema abordado: (i) Priorización, como una lista ordenada de acuerdo a algún criterio, de los controles de seguridad pero sin seleccionar un subconjunto de estos, (ii) Selección de controles, donde los modelos recomiendan un conjunto específico de controles a implementar, (iii) Programación, donde además de seleccionar controles, el modelo propone un plan para la implementación de dichos controles

de acuerdo con las necesidades de la organización. A medida que la categoría se eleva a un nivel superior, existe una mayor complejidad de modelado y solución de los problemas de optimización correspondientes. Un segundo eje de clasificación ha sido el tipo de solución. Aquí hemos distinguido entre (a) soluciones IO, es decir, modelos matemáticos donde al menos existe una función objetivo y se ejecuta algún algoritmo de IO conocido, y (b) soluciones no IO . Estas soluciones, a veces multidimensionales, pueden combinar variables cualitativas y cuantitativas, pero, bajo las variables consideradas, no hay forma de estar seguros de que la recomendación corresponda a un comportamiento óptimo.

Tabla 4.2: Clasificación de propuestas en función de complejidad del problema y uso de técnicas IO

Categoría	Dominio de Seguridad de la Información	
	Soluciones IO	Soluciones no IO
Priorización		[13, 77, 90, 103, 110, 111]
Selección	[6, 75, 126, 127, 154, 156]	[3, 17–20, 27, 29, 31, 43, 56, 79–81, 91, 98, 109, 112, 118, 125, 141, 151–153]
Programación		

A partir del análisis de los resultados de la búsqueda (ver tabla 4.2) se observa cómo no hay propuestas a nivel de programación de controles; alrededor de un 83 % de las propuestas se encuentra en el nivel de selección, mientras que el 17 % restante se encuentra en el nivel de priorización.

Además, se observa que los modelos propuestos sin IO se basan en múltiples técnicas para distintas etapas de la resolución del problema y/o se utilizan en combinación. En cuanto a los modelos de optimización cuantitativos, solo seis de los 35 artículos encontrados [6, 75, 126, 127, 154, 156], se refieren a investigaciones que incluyen explícitamente modelos de optimización. En casi todos estos enfoques se propone una función objetivo para mitigar los riesgos. Una excepción es Almeida et al. [6], donde utilizan la implementación de salvaguardas como una función objetivo. Además, solo [126] y [154] agregan el valor de los activos amenazados como parte de la función objetivo. Casi todos ellos usan los recursos involucrados en las unidades organizativas como restricciones; sin embargo, solo [127] utiliza estos recursos como elementos para optimizar.

Del estudio de la literatura relacionada se puede concluir que, actualmente, el problema de proponer el conjunto de controles que una organización debe implementar de acuerdo a sus características (presupuesto, estructura, prioridades, etc.), depende exclusivamente del juicio experto del asesor de seguridad. Por lo tanto, en la práctica, no se utilizan métodos cuantitativos que apoyen la toma de decisión respecto del conjunto de controles de seguridad a implementar en una organización.

4.2 Identificación de oportunidades de mejora del proceso de recomendación de controles

A partir de todo lo comentado hasta ahora se deduce que la recomendación de acciones de mejora es una etapa deseable dentro de la

Figura 4.1: Principales etapas identificadas

operación y evaluación de un SGSI. Sin embargo, tanto los diferentes estándares que regulan la implementación y funcionamiento del sistema de gestión como las prácticas identificadas en la industria no proveen de un marco metodológico que apoye el proceso de identificación y selección de mejoras.

Aún así, a partir de la literatura revisada, es posible describir un proceso general, tal como se presenta en la figura 4.1, que refleja los principales pasos a seguir para realizar recomendaciones. Este proceso se puede resumir en tres grandes etapas: (i) Diagnóstico, (ii) Recomendación y (iii) Comunicación

4.2.1 Etapa de Diagnóstico

Antes de realizar cualquier recomendación de mejora, es necesario conocer el estado actual de la organización. En esta etapa se considera el proceso que permite levantar la información que refleje el estado actual del desempeño del SGSI. Esta etapa provee de la información que

revela las condiciones de operación del sistema de gestión, indicando cuales son las prácticas que la organización ha implementado. De este diagnóstico se desprenden cuáles son las debilidades del sistema y se determina cual es la brecha que la organización de cubrir para mejorar el desempeño de su SGSI.

Esta etapa está bien cubierta por los estándares revisados anteriormente, ISO/IEC 19011:2018 e ISO/IEC 27001:2013, ya que ellos proporcionan un marco metodológico claro respecto de las acciones que se deben llevar a cabo para levantar la información de diagnóstico.

En el caso de la norma ISO/IEC 19011:2018, ésta establece claramente cuáles deben ser los pasos a seguir para aplicar una auditoría a un sistema de gestión. La misma norma define auditoría como un proceso sistemático, independiente y documentado para obtener evidencias del desempeño de un sistema de gestión y evaluarlas de manera objetiva, con el fin de determinar el grado en que éste cumple los criterios de auditoría [53]. En otras palabras, una auditoría determina el grado en que un sistema de gestión está en conformidad con criterios objetivos que definen su desempeño.

Como se observa en las figuras 3.3 y 4.2, la norma es clara en definir los pasos y etapas necesarias para realizar la auditoría. Como resultado de este proceso, se obtiene un documento con los hallazgos de la auditoría y la evidencia de éstos. Los hallazgos informan respecto del grado de conformidad del sistema de gestión respecto de los criterios de la auditoría. En otras palabras, es en este informe en donde se comunica el diagnóstico de la organización, desde el punto de vista de la conformidad del sistema de gestión, respecto de un grupo de políticas, procedimientos o requisitos que se utilizan como referencia [53], como puede ser la norma ISO/IEC 27001:2013. Por lo tanto, está última provee de los criterios objetivos sobre los cuales se aplica

la auditoría y se obtiene el diagnóstico de conformidad del sistema de gestión, indicando en detalle qué controles o criterios de la norma cumple y cuáles no. Con esta información, es posible determinar la brecha de la organización y cuáles son las oportunidades de mejora del sistema de gestión, traducido en la identificación del conjunto de buenas prácticas en la que la organización puede avanzar.

4.2.2 Etapa de Recomendación

Al llegar a este punto ya se conoce la brecha que la empresa debe cubrir si quiere alcanzar la totalidad del estándar. Sin embargo, las organizaciones no siempre pueden avanzar en la implementación de la totalidad de la brecha en una sola etapa, sino que, debido a los recursos que posee, se ve en la obligación de definir un proyecto de múltiples etapas que le permita alcanzar la totalidad de los criterios paulatinamente.

En estos casos, es necesario definir cuáles serán los criterios que se deben implementar en cada etapa y en qué orden hacerlo. Como se ha revisado en las secciones anteriores, donde se estudiaron los estándares y se revisó la bibliografía relevante, no existe un proceso o marco metodológico que cubra esta necesidad, sino que solo se han propuesto técnicas o métodos de apoyo al proceso.

Dada esta situación, en esta etapa visualizamos un oportunidad de investigación que permita proponer un marco metodológico que defina los procedimientos, técnicas y herramientas que apoyen la definición de un plan de implementación que cubra la totalidad de los criterios de la norma, en un tiempo determinado y de acuerdo a las metas, estrategias y condiciones de recursos propias de cada organización.

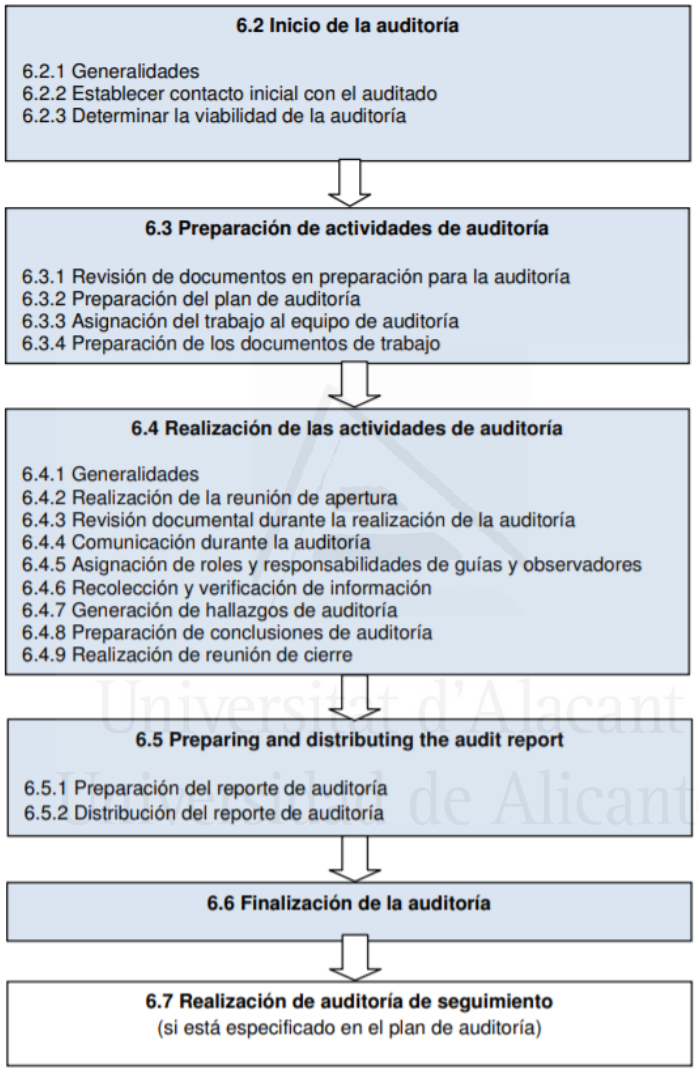


Figura 4.2: Proceso de ejecución de una Auditoría - ISO/IEC 19011:2018

En el capítulo 5 se presenta en detalle la propuesta metodológica para la selección de controles de seguridad.

4.2.3 Etapa de Comunicación

En esta etapa se considera la comunicación de las recomendaciones respecto de la selección de controles. Como se ha observado en los estándares, esta etapa está propuesta una vez finalizada la auditoría o revisión del SGSI. No existe un formato estándar respecto del contenido y de la forma en que se presentan los resultados, sin embargo, existen recomendaciones a la hora de comunicarlos.

De acuerdo a lo establecido en la norma ISO/IEC 19011:2018, el reporte de auditoría debe contener como mínimo:

1. los objetivos de la auditoría;
2. el alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados;
3. identificación del cliente de auditoría;
4. identificación del equipo auditor y los participantes del auditado en la auditoría;
5. las fechas y los lugares donde se realizaron las actividades de auditoría;
6. los criterios de auditoría;
7. los hallazgos de la auditoría y la evidencia relacionada;
8. las conclusiones de la auditoría;

9. una declaración sobre el grado en el cual se han cumplido los criterios de la auditoría.

Además, opcionalmente, dependiendo de las condiciones de la auditoría, se puede incluir en el informe, entre otros puntos:

- oportunidades de mejora, si está especificado en el plan de auditoría;
- planes de acción acordados, si los hubiese.

Como se puede apreciar, la comunicación de las recomendaciones, representadas en este caso por el plan de mejora, no está estipulada como parte del informe de auditoría, a menos que se haya establecido previamente con el auditado, por lo que no se ha planteado como un proceso obligatorio. No obstante, es posible establecer un formato para la comunicación de estos resultados que facilite su comprensión por parte de la organización.

5. Propuesta de Solución

Este capítulo presenta la propuesta para enfrentar el problema de la selección y programación de controles de seguridad a través de la aplicacion de técnicas y modelos de optimización propuestos por IO.

En la sección 5.1, se presenta de manera general el flujo de ejecución y las etapas del enfoque metodológico propuesto en esta tesis.

En la sección 5.2, se detalla la primera etapa del enfoque metodológico (etapa de diagnóstico), y se describen las técnicas y artefactos involucrados.

En la sección 5.3, se describe la etapa de recomendación de la propuesta. Esta etapa incluye la identificación del problema de optimización involucrado, la modelación del problema y la resolución del modelo.

En la sección 5.4, se presenta la fase de resolución del modelo de optimización.

Por último, en la sección 5.5, se presenta un caso práctico de aplicación de la propuesta en un entorno real. El contexto de aplicación fue una asesoría de seguridad realizada por el autor de esta tesis a una organización gubernamental.

5.1 Presentación general de la propuesta

Como ya se ha mencionado, la propuesta se centra en la provisión de un marco metodológico o framework para la recomendación de la implementación de un grupo de controles de seguridad de la información, como parte de un plan de mejora que permita a la organización pasar de un estado actual de conformidad con la norma hacia un estado deseado de conformidad, de acuerdo a las condiciones y restricciones propias de la organización.

Tal y como se muestra en la figura 5.1, la primera contribución de esta propuesta es un proceso sistemático que, a partir de información de diagnóstico y las condiciones particulares de la organización, permite la generación de un modelo que representa la intención de mejora basada en las restricciones de la organización. Este modelo se construye como un problema de optimización, ya que busca la mejor solución a la problemática de avance definida por la organización. De esta forma, el modelo debe ser resuelto por la técnica de optimización que mejor se adapte a la situación. La resolución de este modelo proveerá del mejor conjunto de controles de seguridad que se adhieren a las restricciones impuestas por la organización.

Dado que lo que se busca es optimizar la selección de controles dado un conjunto de objetivos y condiciones que pueden variar de una organización a otra, la propuesta define que, como parte del proceso de selección, deben considerarse: procesos dedicados a la recopilación de las necesidades de la organización (etapa de diagnóstico), procesos que permitan reconocer la problemática, modelar la situación y resolver el modelo de optimización (etapa de recomendación) y por último, la definición de procesos y formatos que permitan divulgar los resultados del estudio (etapa de comunicación).

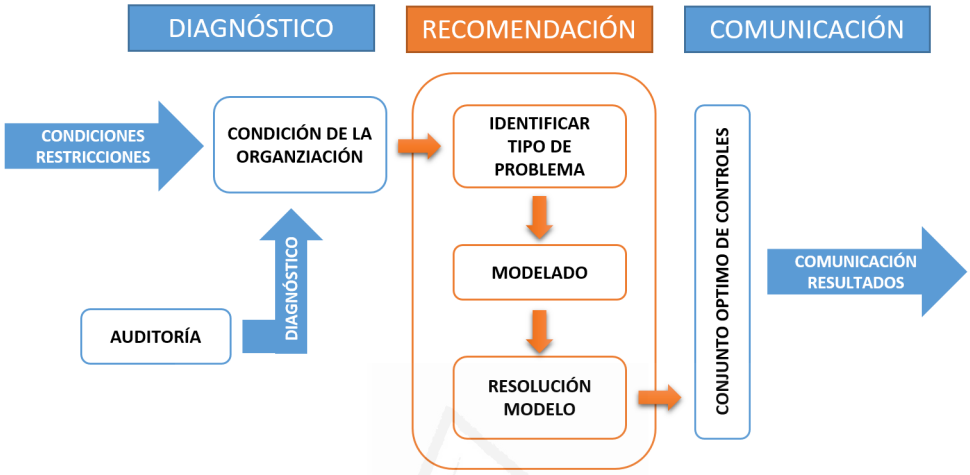


Figura 5.1: Visión general de la propuesta

En las siguientes secciones se detallan los aportes de la propuesta en cada una de las etapas del proceso de recomendación de controles de seguridad. Es importante destacar que los principales aportes de la propuesta se concentran en la etapa de "Recomendación", aunque, como se verá a continuación, esta tesis también ha generado algunos aportes en las otras dos etapas.

5.2 Etapa de Diagnóstico

Como ya se ha comentado, esta etapa se encuentra bien definida en los estándares ISO/IEC 27001:2013 e ISO/IEC 19011:2018. En estas normas se establecen los procesos y técnicas para, por un lado, la implementación de un SGSI y, por otro, la evaluación de su desempeño. Con esta base, es posible realizar un diagnóstico de la organización res-

pecto de la conformidad con las prácticas propuestas por el estándar. A partir de este diagnóstico, se puede determinar el conjunto de controles o buenas prácticas que la organización no tiene implementadas en su SGSI. A su vez, con esta información es posible determinar el estado actual de la organización respecto de la brecha que se debe cubrir. Esto es particularmente importante para el proceso de selección de controles, ya que define el universo de controles sobre los cuales realizar el modelamiento y selección.

Como una forma de apoyar el proceso de diagnóstico y levantamiento de información, la propuesta presentada en esta tesis incluye como aporte un artefacto de entrada al proceso, en forma de cuestionario, que permite al asesor de seguridad recolectar la información del estado actual de la organización respecto de normas o estándares de seguridad de la información. El cuestionario permite, en primer lugar, determinar el grado de conformidad de la organización con el estándar. Este cuestionario fue creado ad-hoc para una auditoría de seguridad y contiene más de 400 preguntas que, hasta este momento, abarcan 3 estándares o normas de seguridad de la información: (i) ISO/IEC 27001:2013, (ii) Decreto Supremo 83 del Gobierno de Chile [62] y (iii) la Guía Metodológica para la seguridad de la información del Gobierno de Chile [63]). En segundo lugar, el cuestionario permite el ingreso de los parámetros para la modelación para aquellas preguntas que tienen una pregunta negativa.

En la figura 5.2 se puede ver parte de este cuestionario. Con este instrumento se puede recoger la información necesaria para la modelación de la situación particular de la organización, que permitirá realizar la recomendación de los controles de seguridad. El cuestionario completo se encuentra disponible en el Anexo A de este documento.

Figura 5.2: Formulario para el diagnóstico

5.3 Etapa de Recomendación

Como ya hemos mencionado, es en esta etapa donde se concentra el mayor número de aportes de la propuesta. Ésta define un marco metodológico para incorporar técnicas de optimización para la resolución del problema de selección de controles. Esto implica considerar la recomendación de un plan de mejora para el avance en la conformidad respecto de un estándar como un problema de optimización, en el cual se debe definir un objetivo e identificar las restricciones de la organización.

Como se muestra en la figura 5.3, esta etapa se ha divido en tres

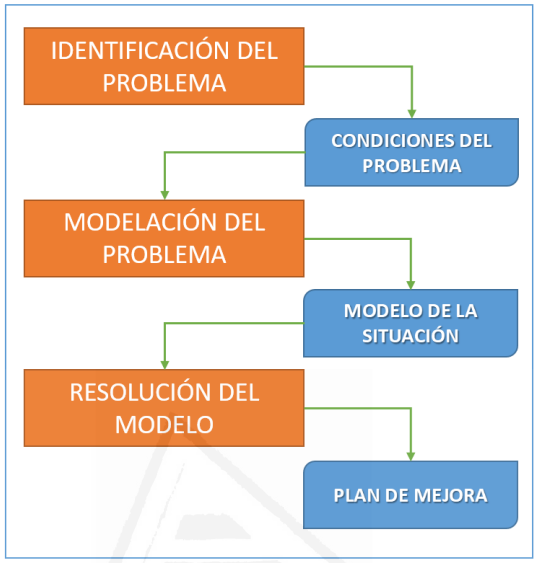


Figura 5.3: Procesos generales de la etapa de Recomendación

grandes procesos. El primero se refiere a la identificación del problema de optimización que se requiere solucionar. El resultado de esta etapa es el detalle del problema que se está enfrentando, en el cual se explicita: (i) el objetivo a lograr, (ii) las restricciones a considerar y (iii) los parámetros de las variables que definen el objetivo, así como las restricciones propias de la organización. El segundo proceso se refiere a la modelación de la situación como un problema de optimización. El resultado de esta etapa es el modelo matemático que se deriva de los formatos que se encuentran en el campo de la IO. Por último, el tercer proceso se refiere a la solución del modelo propuesto a través de las diversas técnicas de resolución de problemas de optimización propuestas en la IO. El resultado de esta etapa es el conjunto de controles que forman parte del plan de mejora recomendado.

En las siguientes subsecciones se profundiza en cada etapa.

5.3.1 Identificación del problema

Antes de realizar la modelación del problema, es necesario definir el problema de optimización que se desea resolver. Dadas las características de las organizaciones y la naturaleza del problema de la selección de controles de seguridad, se pueden presentar diversas situaciones.

En la tabla 5.1 se presenta un resumen de las siete situaciones posibles que se han identificado en la propuesta, clasificadas de acuerdo a su objetivo, en orden de complejidad creciente: problemas de priorización, selección o programación. La priorización de controles se refiere a ordenar los controles respecto de algún criterio, por ejemplo el riesgo. En este caso se prioriza el conjunto posible de controles a implementar. En el caso de la selección, existe una recomendación de un subconjunto de controles respecto del conjunto total, basado en los objetivos y restricciones de la organización. En el caso de la programación, además de seleccionar el subconjunto de controles a implementar, se determina una secuencia de implementación de los controles seleccionados.

Estas situaciones (tipos de problema a los que se puede enfrentar el asesor de seguridad) se detallan en profundidad en la sección 5.3.3 del presente documento. Esta definición de situaciones categorizadas por objetivo facilita la modelación posterior, ya que, tal como se presenta en la sección 5.3.3, cada una de estas situaciones requiere una modelación distinta, así como el uso de técnicas de IO distintas para su resolución. De este modo se apoya a los asesores de seguridad en el proceso de selección de estas técnicas de modelación y resolución de la situación planteada.

Tabla 5.1: Categorización de situaciones identificadas en la propuesta

Categoría	Situación
Priorización	Ranking multidimensional de controles
	Secuenciación de controles independientes
Selección	Selección de controles con restricciones
	Selección de controles con restricciones y dependencias entre controles
Programación	Secuenciamiento de dimensiones y programación de controles con anidamiento
	Selección y programación de controles considerando anidamiento
	Programación multicriterio de controles con restricciones

Además del tipo de problema que se debe resolver, en esta etapa es necesario determinar las condiciones y/o restricciones que se deben considerar para realizar la modelación. En este sentido, la propuesta plantea la necesidad de establecer tres aspectos:

- los objetivos del plan de mejora,
- las restricciones de la organización y
- los parámetros relevantes para la modelación.

Con respecto al objetivo que busca la organización, se espera que esta establezca qué es lo que espera alcanzar o satisfacer con el proceso de selección. Algunos ejemplos de objetivos válidos son:

- maximizar la cantidad de controles a implementar,
- maximizar el beneficio que reporta la implementación del grupo de controles,
- minimizar el riesgo de la no implementación de los controles, o
- minimizar el tiempo de implementación del grupo de controles.

Conforme a un problema de optimización, estos objetivos se traducirán en el modelo como una función o ecuación que dirigirá la resolución del problema. Por tanto, es importante definir claramente lo que la organización busca con la definición del grupo de controles a implementar. Cabe destacar que la situación a representar puede estar conformada por uno o más objetivos.

Por otro lado, también es necesario establecer, previamente a la modelación y resolución del problema, las condiciones o restricciones propias de la organización que deben ser consideradas al momento de realizar la recomendación. Usualmente, estas restricciones están asociadas a la disponibilidad de los recursos con los que la organización cuenta para implementar un posible plan de mejora. Algunos ejemplos de restricciones podrían ser:

- un determinado nivel de presupuesto,
- un tiempo específico para realizar el proyecto de implementación,
- un determinado nivel de riesgo que la organización requiere disminuir,

- la dependencia entre controles de seguridad.

Por último para realizar la modelación de las restricciones y de los objetivos, es necesario establecer algunos parámetros relevantes para la modelación, como son:

- costo de implementación por control,
- tiempo de implementación de cada control,
- beneficio asociado a la implementación del control,
- riesgo asociado a cada control.

Una vez definido todo esto, llega el momento de definir las ecuaciones y los parámetros de las variables que se utilizarán en la modelación del problema. Para ello, es necesario determinar cuáles son las variables que, en el contexto de la SI, permiten modelar la situación como un problema de optimización. Para lograr esto, se ha propuesto, en base al conocimiento recopilado durante la fase de Design Science de investigación del problema (ver capítulo 3), un modelo integrado de los principales conceptos y variables que se pueden encontrar en un problema de SI. A continuación se presenta este modelo junto con el proceso que se siguió para diseñarlo.

5.3.2 Conceptos y variaciones en la implementación de controles de seguridad de la información

Desde la perspectiva de IO, los problemas de optimización se formulan como un modelo matemático que tiene una función (o varias) para maximizar (o minimizar) bajo un conjunto de restricciones (ecuaciones). Los modelos IO siempre tienen suposiciones sobre sus variables

contenidas y sus relaciones [108].

Sin embargo, el reconocimiento de variables, restricciones y objetivos a optimizar dependen, más que de las percepciones del analista, del marco conceptual subyacente que el analista (el modelador) aplica al modelo de optimización propuesto. Esto complica la modelación, ya que en seguridad existen distintos marcos conceptuales de referencia.

Las variables, particularmente en un modelo de IO, corresponden a construcciones humanas que agrupan objetos y situaciones observables, y posiblemente medibles, que se consideran relevantes para comprender este dominio específico. Por lo tanto, para proponer un mapa general de las técnicas de optimización aplicadas a los controles de seguridad de la información se requiere un marco conceptual común para las variables involucradas en los modelos de optimización correspondientes. Esto requiere un conocimiento de cómo empaquetar y elegir el marco conceptual subyacente en el mapa propuesto.

Para este fin es posible aplicar una técnica proviniente de la Ingeniería del Conocimiento, que consiste en empaquetar estos marcos conceptuales en forma de ontologías [130]. En particular, el desafío de desarrollar una ontología de seguridad de la información completa fue formulado por [102]. Sin embargo, una ontología completa de seguridad de la información, como referencia, ha demostrado ser un enfoque complejo y poco pragmático, debido a la gran variedad de variables existentes.

Una revisión de diferentes enfoques ontológicos en seguridad de la información especialmente relevante para este trabajo es la que aparece en [14]. Este estudio revisa 31 propuestas principales relacionadas tanto con con ontologías de seguridad de propósito general como con ontologías de seguridad de dominio específico.

De ellas, tres se refieren de manera explícita a los estándares asociados a la gestión de la SI, incluida la familia ISO/IEC 27000:2013, y consideran los controles de seguridad de la información asociados, por lo que son especialmente relevantes desde el punto de vista de esta tesis. La primera de estas propuestas es la de [88]. En esta propuesta se incluyen fórmulas para valores de activos, cálculos de riesgo y posibles impactos de amenaza. Por otro lado, en la propuesta de [47] se refinan diferentes conceptos de seguridad (por ejemplo, vulnerabilidad, activo y función), y se reconocen relaciones específicas (por ejemplo, que una amenaza puede surgir o ser el resultado de otra amenaza). En esta propuesta, los autores incluyen además conceptos relevantes y cuantificables, como las calificaciones de implementación de control para medir la efectividad de las combinaciones de activos / control y las probabilidades de amenaza a priori para establecer valores de riesgo iniciales. Finalmente, la propuesta de [113] añade la perspectiva del comportamiento humano, que supone la inclusión variables adicionales para representar las implicaciones del comportamiento humano en las decisiones de gestión de SI.

En esta tesis, para representar los conceptos asociados a la SI y las relaciones entre estos, se ha creado una fusión de estas tres propuestas, guiada por el marco conceptual presentado en [14].

De acuerdo a este marco, es posible realizar una integración de ontologías estudiando las ontologías originales y realizando un proceso en dos pasos, que son:

1. Ordenación: las ontologías que se van a integrar tienen que ser ordenadas usando algún criterio, por ejemplo, la cantidad de conceptos.

2. Integración: una vez ordenadas, se selecciona la primera onto-

> logía como base y se le integra la segunda ontología. La ontología resultante se integra luego con la tercera ontología y así sucesivamente. Para el proceso de integración recursivo, se sugiere realizar tres pasos: (i) encontrar áreas superpuestas dentro de las ontologías, para evitar redundancias, (ii) relacionar los conceptos que se agregan en cada iteración y (iii) verificar la consistencia, coherencia y no redundancia del resultado.

Además, a la hora de realizar esta integración, es necesario prestar atención a posibles conflictos entre ontologías. Algunos ejemplos de estos conflictos, descritos en [14], son:

- El mismo concepto se define con diferentes términos.
- El mismo término se usa para representar diferentes conceptos.
- Un mismo concepto se define utilizando diferentes atributos.

El resultado de la aplicación de este proceso a las tres propuestas seleccionadas [47, 88, 113] ha sido una vista integrada que contiene referencias documentadas de variables en el modelo de optimización, y que permite navegar a través del modelo para producir diferentes escenarios de optimización. Una forma aceptada de representar esta perspectiva integrada en forma de ontología son los diagramas de clase UML [64]. En la figura 5.4 utilizamos uno de estos diagramas para ilustrar dicha ontología.

En términos generales, cada clase en UML representa un conjunto de objetos. Cada asociación representa productos cartesianos entre clases relacionadas. Los atributos en una clase representan propiedades particulares de los objetos (elementos) de esta clase (conjunto). Por lo tanto, se pueden formular diferentes problemas de optimización en función de los elementos UML (clases, atributos, asociaciones), que

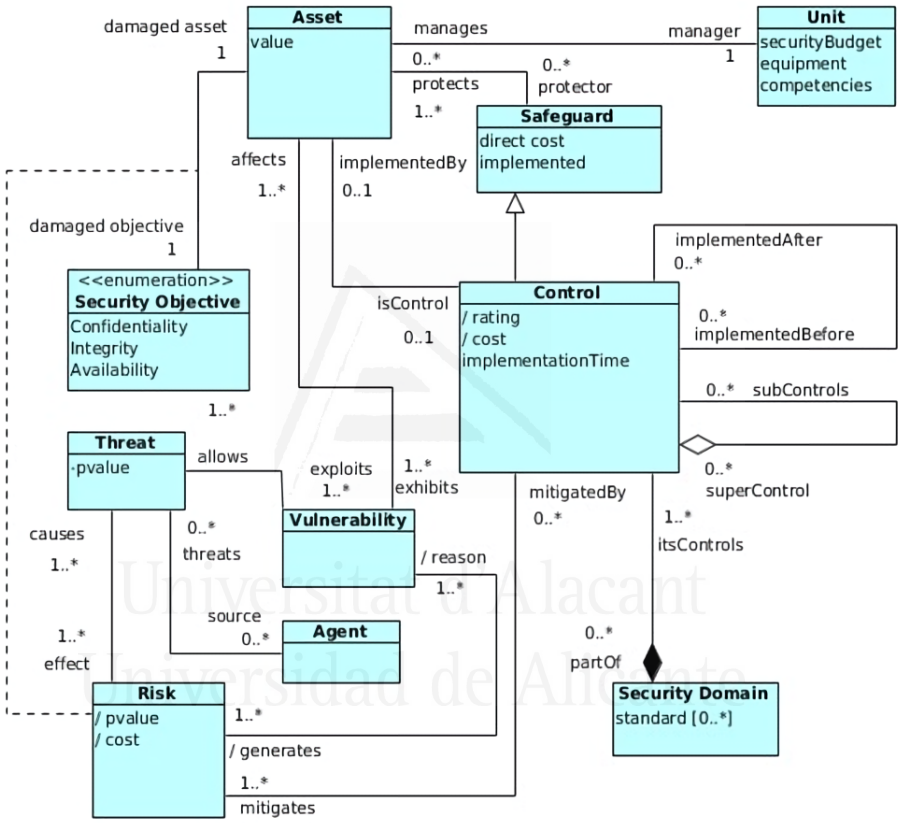


Figura 5.4: Vista integrada de los principales conceptos y variables de seguridad

se elige considerar.

El elemento del que parte la vista integrada de la figura 5.4 es el concepto de Riesgo tal y como sen entiende en la Ingeniería de Sistemas. Desde este punto de vista, un riesgo es un evento "negativo"potencial, y puede medirse, por ejemplo, por la probabilidad de que ocurra este evento [57]. Bajo esta perspectiva, consideramos un riesgo de SI como el daño potencial a un activo de información ante el fallo en un objetivo de seguridad. El riesgo se modela usando la probabilidad de ocurrencia y el costo de enfrentar los daños correspondientes. La probabilidad y el costo del riesgo se expresan como variables derivadas (barra diagonal antes del nombre del atributo), es decir, sus valores se calculan en función de otras variables del modelo.

Para mitigar los riesgos, se pueden seleccionar un conjunto de controles, representados por la clase Control. Un control está asociado a uno o más dominios del estándar de seguridad (Security Domain Standard). El modelo además mantiene el concepto de salvaguarda (Safeguard) como la generalización de los controles del estándar. Las salvaguardas tienen asociado un costo de implementar una salvaguarda (costo directo), y permiten proteger al activo de información (Asset), el cual posee un valor organizacional y que es gestionado a través de alguna unidad de la organización, a la cual se le asocian diversos recursos (Presupuesto, equipos y competencias), para su gestión. Sobre el activo de información existe un objetivo de seguridad (niveles de confidencialidad, integridad y disponibilidad deseados). El activo además puede presentar una o más vulnerabilidades que generan riesgos, los cuales pueden ser representados a través de un valor o costos. Estos riesgos se asocian con las amenazas que buscan explotar las vulnerabilidades de los activos. Estas amenazas pueden provenir tanto de un agente interno como de uno externo.

También se reconoce una estructura de controles potencialmente anidada, es decir, la posibilidad de que existan relaciones de dependencia en la implementación de dichos controles (por ejemplo, procedimientos organizativos de un centro de datos que puede contener barreras de acceso físico). Esto quiere decir que existen controles que dependen de que otros controles se implementen primero. Esta es una situación que no está representada en las propuestas estudiadas.

Por último, para considerar el modelado de la solución en términos de secuencias de implementaciones de controles, se ha agregado una asociación recursiva sobre la clase Control.

5.3.3 Modelación del problema de optimización.

Como se ha señalado, formular el problema de optimizar la selección de controles de seguridad que se deben implementar puede dar lugar a un gran número de alternativas. Por ejemplo, una organización podría querer cumplir completamente con algún estándar de seguridad de la información, mientras que otra podría desear lograr solo un cumplimiento parcial considerando su progreso actual, y otra podría desear lograr múltiples objetivos de seguridad al mismo tiempo. El conjunto de opciones resultante para la toma de decisiones es un universo demasiado amplio, debido a su naturaleza combinatoria, como para ser resuelto de manera cualitativa, en base en la experiencia del analista.

Para ayudar a resolver el problema de forma cuantitativa, existen distintas aproximaciones dependiendo de lo que se quiera considerar. Algunas posibilidades son:

- Considerar solo el costo heredado de los controles, y realizar una clasificación de costos bajos, medios y altos. Esta situación

puede ser relevante para una oficina pública, porque los procesos de compra pública tienen diferentes procedimientos, es decir, diferentes esfuerzos organizativos, dependiendo de los montos disponibles para gastar.

- Considerar la asociación supercontrol-subcontrol como una asociación facilitadora-dependiente, para considerar algún conjunto de controles como clases equivalentes (sentido algebraico); por lo tanto, hay conjuntos separados de controles para implementar.
- Considerar la priorización de los activos de información (clase Asset) de acuerdo a su valor organizativo (atributo de Asset) y, según el valor, navegar hasta sus protectores (asociación protects-protector) que serán los controles a implementar (clase Control).

En términos generales, cualquiera de los conceptos en el diagrama puede ser parte de una función objetivo, y las diferentes rutas definidas por su navegabilidad son las consideraciones potenciales de las restricciones. Incluso debería ser posible dejar salir los controles asociados y obtener otros análisis; por ejemplo, un ranking de las unidades organizativas más riesgosas. Las opciones de navegación y sus variables involucradas (determinadas por los subconjuntos de objetos) están especificadas en el lenguaje de especificación de restricciones Object Constraint Language (OCL), que es una herramienta de análisis común para los diagramas UML [25].

En la tabla 5.2, se resumen las clases y asociaciones que se pueden utilizar en el modelado del problema.

Para abordar mejor estos casos, otra contribución de esta tesis ha sido la identificación y categorización del conjunto de escenarios posibles, de tal manera que sea posible proponer, a partir del cuerpo de

Tabla 5.2: Elementos relevantes para la modelación del problema de selección, presentes en el modelo conceptual

Clases	Asociaciones
Security Objective	damaged asset - damaged obj
Risk	affects – exhibits
Vulnerability	reason - generates
Asset	effect - caused by
Threat	exploits – allows
Safeguard	arises - caused by
Control	threats – source
Unit	is asset - is control
Security Domain	protects - protector
Agent	manages - manager
	participates in - requires
	superControl - subControls
	implementedAfter - iBefore
	mitigatedBy - mitigates
	itsControls

conocimientos de IO, los modelos y las técnicas más adecuadas para resolver los diferentes problemas de seguridad de la información identificados. Se debe tener en cuenta que la mayoría de los escenarios resultantes pertenecen a la clase NP-Hard [138], o incluyen este tipo de problema, lo que los hace mucho más difíciles de resolver.

Como ya se ha comentado, la propuesta de clasificación de problemas de selección de controles de seguridad incluye siete categorías, o tipos de problemas, según el tipo de implementación que se desea realizar (total o parcial), y según sus requisitos de planificación temporal (sin planificación de tiempo o construcción de programas reales).

Además, dentro de una categoría, se diferencia el objetivo deseado (cumplimiento más temprano, satisfacción de la fecha de vencimiento u otro). La razón detrás de estas categorías se basa en el número de funciones objetivas, considerando los controles anidados y los costos asociados, y el tipo de restricciones; por ejemplo, solo una priorización (ordenamiento de los controles), controles planificados en un período, controles que no excedan un presupuesto determinado o una combinación de estas consideraciones. Las categorías resultantes no implican necesariamente distintos niveles de complejidad de cómputo; más bien, la complejidad ascendente se refiere a la cantidad de variables consideradas que participan en restricciones y funciones objetivo. Estas diferentes variables forman parte del marco conceptual de seguridad de la información y las más relevantes ya se han considerado en la ontología de seguridad de la información presentada en la sección 5.3.2.

En la tabla 5.3, se presentan los siete tipos de problemas identificados (columnas), y las clases y asociaciones de la ontología que intervienen en cada uno de ellos (filas). En esta tabla se han omitido atributos en el nivel de clases y asociaciones, ya que su objetivo es representar las áreas macro de variación entre los diferentes tipos de problema. Además, no hay grandes diferencias al considerar un atributo u otro (en la complejidad de un problema) para una determinada clase de objetos (conjunto). La tabla 5.3 refleja además la forma en que estos elementos de la ontología están involucrados en el modelo. Se han realizado las siguientes distinciones: "R"significa que el elemento de la ontología se utiliza para obtener una priorización (un ordenamiento), es decir, no hay una función objetivo para optimizar. "C"significa que el elemento de la ontología se puede usar como parte de una restricción en el modelo de optimización. Finalmente, "O"significa que el elemento de ontología se utiliza en la función objetivo a optimizar. Hemos utilizado signos adicionales para expresar algunas subvariaciones; así, "+" significa que la inclusión del elemento es una forma alterna-

tiva de formular el problema, y "*" significa que los elementos pueden combinarse, principalmente en el sentido de una función objetivo que hace que el problema de decisión sea un problema multiobjetivo. Finalmente, "!"significa que el elemento de ontología es obligatorio en esas variaciones. Aquí, la semántica del elemento puede provocar un problema de optimización muy diferente, ya que diferentes elementos de la ontología pueden tener una representación similar (por ejemplo, una asociación); sin embargo, debido a que algunos de los elementos pueden implicar una dependencia temporal o un consumo de un recurso, la consideración del elemento implicará un problema de optimización diferente.

Existen relaciones que no se consideran en la función objetivo o en las restricciones, ya que solo tienen un propósito de navegación en el modelo; es decir, no hay atributos asociados, y el número de elementos involucrados en la navegación no constituye una variable considerada en el problema.

Tipo de problema 1: Ranking multidimensional de controles

En esta categoría, se asume que no existen restricciones ni dependencias entre los controles (anidamiento); los controles tienen la misma importancia y no se agrupan en dimensiones. En este caso, el costo de implementación y los beneficios son las sumas de todos los componentes individuales, ignorando las interferencias o las sinergias entre ellos. El problema es clasificar adecuadamente los controles según sus características para ayudar al tomador de decisiones a elegir los que desea implementar, utilizando el orden de clasificación como una recomendación de programación.

El problema de clasificación es multidimensional porque cada con-

Tabla 5.3: Tipos de problemas de decisión de seguridad de la información según las variables involucradas

Ontología	Tipo de Problema						
Clases	1	2	3	4	5	6	7
Security Objective			O^+	O^+	O^+	O^+	O^*
Risk			O^+ C^+	O^+ C^+	O^+ C^+	O^+ C^+	O^*
Vulnerability			O^+ C^+	O^+ C^+	O^+ C^+	O^+ C^+	O^* C^+
Asset			C^+	C^+	C^+	C^+	C^+
Threat			C^+	C^+	C^+	C^+	C^+
Safeguard			O^+	O^+	O^+	O^+	O^*
Control	R	R	O^+ C^+	O^+ C^+	O^+ C^+	O^+ C^+	O^* C^+
Unit			C^+	C^+	C^+	C^+	C^+
Security Domain			C^+	C^+	C!	C^+	C^+
Agent							
Asociaciones	1	2	3	4	5	6	7
damaged asset - damaged obj			O^+ C^+	O^+ C^+	O^+ C^+	O^+ C^+	O^* C^+
affects – exhibits							
reason - generates							
effect - caused by			C^+	C^+	C^+	C^+	C^+
exploits – allows			C^+	C^+	C^+	C^+	C^+
arises - caused by							
threats – source							
is asset - is control			C^+	C^+	C^+	C^+	C^+
protects - protector			C^+	C^+	C^+	C^+	C^+
manages - manager			C^+	C^+	C^+	C^+	C^+
participates in - requires							
superControl - subControls				C!	C!	C!	C!
implementedAfter - iBefore		C!				C!	C!
mitigatedBy - mitigates			O^+	O^+	O^+	O^+	O^*
itsControls							

trol tiene varias características asociadas, como la inversión, el costo operacional, la duración y dificultad de la implementación y los beneficios resultantes (reducción del riesgo, etc.). El caso improbable de encontrar solo una característica relevante en cada control es trivial, y corresponde al ordenamiento en el dominio de los números reales.

En el caso de múltiples dimensiones, el problema es establecer so-

luciones de Pareto no denominadas, donde es posible usar estrategias como las sumas ponderadas [58] o lograr una función escalar [148]. Recientemente, este problema ha sido abordado por [111] utilizando las funciones de deseabilidad para cuantificar la conveniencia de cada control de seguridad de la información, considerando los beneficios y sanciones (restricciones) asociadas con la implementación del control.

Tipo de problema 2: Secuenciación de controles independientes

Al igual que con los problemas de Tipo 1, se supone que los controles son totalmente independientes y no se agrupan en dimensiones. El objetivo es programar la implementación de todos los controles.

Se supone que el proceso es secuencial, trabajando en la implementación de un control a la vez. El problema asociado es el conocido "problema de programación de una máquina/recurso"discutido por [59]. El menor tiempo de finalización no es relevante en este caso, ya que no depende de una secuencia de implementación. Sin embargo, si se consideran plazos, el escenario se convierte en un problema de "planificación de un recurso/máquina con retraso", que es revisado por [86]. Si el objetivo es asegurar un mayor número de controles dentro de un plazo, el problema se resuelve de manera óptima utilizando la regla simple de tiempo de procesamiento más corto (SPT). Si hay preferencias, o una importancia relativa entre los controles, los problemas consideran sus contrapartes ponderadas, como ocurre en [28].

Por otro lado, si se trabaja con varios controles simultáneamente (por ejemplo, teniendo varios equipos de implementación), el problema se enfrenta como un "problema de secuenciación de máquinas paralelas", con máquinas idénticas o diferentes [41].

Por último, en el caso de equipos únicos o múltiples, es posible considerar los costos asociados con la secuencia de implementaciones de los controles, lo que resulta en un problema del tipo "problemas de programación dependientes de la secuencia"[5].

Tipo de problema 3: Selección de controles con restricciones

Esta categoría es una extensión del Tipo de problema 2, teniendo en cuenta la existencia de recursos limitados para la implementación de controles (presupuesto, recursos humanos, competencias, equipos, otros recursos, etc.). Suponemos que cada control está totalmente especificado por una o más características asociadas con el uso de recursos escasos. En este caso, no se presta atención a la programación de la implementación de los controles ni a la cantidad de controles que se pueden implementar en paralelo. El objetivo es no abusar de los recursos disponibles.

Si se considera un solo recurso limitado (por ejemplo, presupuesto o recurso humano), y el deseo es seleccionar los controles que optimizan una única medida de rendimiento, como el "beneficio"(seguridad total, robustez, etc.), el problema corresponde al conocido "problema de la mochila"(knapsack), que ha sido ampliamente discutido en la documentación de problemas de empaquetado. Se puede encontrar una tipología de problemas en [150].

Por el contrario, si se consideran dos o más recursos simultáneos, el problema se convierte en un "problema de múltiples paquetes", tratado en [42, 49, 60, 144].

Este tipo de problema de selección de controles con restricciones incluye el caso de controles agrupados en dimensiones independientes, cuyo cumplimiento se planificará a lo largo del tiempo. Las dimensio-

nes deben tener pleno cumplimiento antes de avanzar a la siguiente. Se supone independencia entre dimensiones y controles.

Tipo de problema 4: Selección de controles considerando restricciones y dependencias entre controles

Este caso extiende el problema del Tipo 3, considerando las dependencias entre controles (anidadas en la misma dimensión o dependencias generales entre las dimensiones). En otras palabras, en esta situación se consideran aquellos casos en los que para seleccionar un control (Ci), primero debe seleccionar un grupo de controles (Cij). Por ejemplo, implementar un cortafuegos puede ayudar a lograr alguna restricción en un protocolo de autenticación al mismo tiempo que evita algunos ataques de disponibilidad. La solución a este tipo de situación se realiza de la misma manera que en el caso anterior, agregando restricciones de dependencia de control temporal.

Tipo de problema 5: Secuenciamiento de dimensiones y programación de controles con anidamiento (restricciones de precedencia)

Al igual que con el problema de Tipo 3, se supone que todos los controles que pertenecen a una dimensión deben implementarse antes de abordar otra dimensión, agregando la condición de anidación de control (dentro de la misma dimensión). En otras palabras, antes de implementar un control dado, se debe cumplir un grupo particular de controles de requisitos previos. Se supone que los requisitos previos son conocidos y correctos (es decir, no hay anidación cíclica).

El problema se puede dividir en dos niveles de decisión: el primero (nivel de dimensión) consiste en secuenciar las dimensiones (determinar su orden de implementación), y el segundo (nivel de control)

requiere determinar el itinerario de implementación de los controles dentro de una dimensión.

Se consideran los dos niveles como independientes, cuando se busca determinar la secuencia de dimensiones y el plan de controles que minimice el tiempo total de implementación, sin tener en cuenta restricciones de recursos. EEn este caso, el primer nivel (secuencia de dimensiones) corresponde al tipo de problema 2, mientras que el segundo es la "planificación del proyecto con recursos ilimitados"(problema de programación de proyecto (PSP))", que se resuelve de manera eficiente utilizando el método de ruta crítica.

Si se tienen recursos limitados, el problema de primer nivel sigue siendo un Tipo de problema 2, mientras que el problema de segundo nivel se corresponderá al "problema de planificación de proyectos con recursos limitados (RCPSP)", para el cual existen múltiples enfoques de solución [65].

Además, se pueden incluir fechas límite (hitos) y penalidades por incumplimiento; por lo tanto, el problema puede verse, en términos de dimensiones, como un "problema de secuenciación de múltiples proyectos". Esto da lugar a una variación revisada explicada en la Sección 3.3 de [65]. El problema de segundo nivel es un PSP, una extensión del trabajo de [134], para el cual los análisis se denominan "Programación de múltiples proyectos restringidos por recursos (rc-mPSP)". En este caso, el PSP de segundo nivel solo considera un número limitado de opciones de realización factibles y busca determinar la secuencia de programación de diferentes proyectos (en este caso, las dimensiones), que pueden ejecutarse de acuerdo con una de las realizaciones. El objetivo es determinar el cronograma con un tiempo de finalización total mínimo para todos los proyectos; por lo tanto, es posible minimizar las penalizaciones generadas por el retraso en el tiempo de finalización. El

método de solución utilizado es un algoritmo de decisión de múltiples etapas basado en metaheurística evolutiva (mdGA).

Si se utiliza otra medida de rendimiento, por ejemplo, en cumplimiento con los plazos establecidos para controles específicos, los niveles de dimensión ya no se pueden separar de los problemas de los controles, porque la secuencia de nivel superior establece algunas condiciones para programar actividades. Este tipo de problema ha sido abordado por varios autores, tal como se presenta en la Sección 6.2 de [65].

En este tipo de problemas se puede incluir o no la selección de controles, pero de todas maneras deben establecerse hitos o plazos de cumplimiento de los controles, como restricciones para el cumplimiento del progreso en el estándar. En este caso, el PSP añade restricciones blandas para el cumplimiento de los plazos establecidos, como se ve en la Sección 3.3. de [134].

Tipo de problema 6: Selección y programación de controles considerando anidamiento (restricciones de precedencia)

El objetivo es seleccionar controles de seguridad y planificar su implementación para maximizar el rendimiento (beneficio) en el menor tiempo posible, de acuerdo con la disponibilidad de recursos.

En este caso, se incluye la posibilidad de anidar controles dentro de una dimensión (similar al Tipo de problema 3), o la dependencia de los controles entre diferentes dimensiones. A diferencia del problema Tipo 3, es posible abordar diferentes dimensiones simultáneamente.

El anidamiento de los controles puede ser explícito (y fijo) o parcial. En el primer caso, asumimos controles anidados conocidos durante la etapa de planificación (son factibles, sin ciclos) que deben res-

petarse por completo. Por tanto, el problema se puede dividir en un primer nivel de "selección con restricciones de precedencia y máximo beneficio" ("problema de mochila con precedencia limitada (PCKP)") [45, 121, 122], donde un control solo puede ser direccionado si sus predecesores han sido seleccionados. El segundo nivel de "programación" correspondería al establecimiento del calendario de implementación para los controles seleccionados. En [155] se presenta un esquema para resolver un PCKP de una dimensión. El aspecto de la programación es un problema de planificación de proyecto (PSP o RCPSP), como se discute en la Sección 4.2.4 de [155].

En este tipo de problema (anidamiento fijo), los niveles de selección y programación no son independientes. Normalmente, el problema apunta a elegir y programar los controles que optimizan una (o más) medidas de rendimiento. [26] y [83] analizan el problema de seleccionar y programar simultáneamente múltiples proyectos independientes. Sin embargo, en este caso, no es posible seleccionar un subconjunto de actividades dentro de un proyecto. Otra vista podría provenir de la "programación en el problema de mochila parcialmente ordenado" [85].

En el caso de anidamiento parcial, entre los controles (dentro de las mismas o diferentes dimensiones) se especifican relaciones de "preferencia de orden parcial". De este modo se definen secuencias de implementación alternativas. Por ejemplo, los controles A.1, B.1 y C.1 de las dimensiones A, B y C podrían ordenarse de izquierda a derecha o de derecha a izquierda, o cualquier otro orden aún por especificar, aunque una vez que se decida el orden no se puede cambiar. En este caso, no es posible dividir el problema en dos niveles independientes porque la determinación de una secuencia explícita, basada en la precedencia parcial entre controles, interfiere con la solución óptima para el tiempo de implementación más corto posible para los controles

seleccionados. El problema resultante es muy complejo, considerado como un problema del tipo NP-Hard. Consiste en una versión modificada y mixta del problema de programación, problema de mochila y problema de planificación de proyecto. No se ha encontrado ninguna referencia a este problema en la literatura.

Debido a la alta complejidad de ambos problemas en la "selección y planificación de controles con anidación", parece aconsejable abordarlos utilizando métodos de aproximación, como las metaheurísticas.

Tipo de problema 7: Programación multicriterio de controles con restricciones.

En este caso, las restricciones prácticas aparecen como objetivos multicriterio, buscando, por ejemplo, maximizar el progreso y minimizar los costos. En [65] se revisa este tipo de problema en las Secciones 5.8 y 3.3. Corresponde a extensiones de problemas del tipo 1 al 5 mencionados anteriormente. Los problemas de planificación multicriterio se pueden encontrar en [69] y [95]. En [49], describen un enfoque metaheurístico para problemas de selección de múltiples etaoas con múltiples criterios, relacionados con los problemas de anidación.

En la tabla 5.4 se muestra un resumen de los distintos tipos de problemas presentados, incluyendo las soluciones propuestas y un clasificación respecto del tipo de solución.

5.3.4 Otras características de interés.

Además de las características descritas en los Tipos de problema 1-7, puede haber otros elementos relevantes en el problema de la programación de la implementación de los controles de seguridad. Es importante

Tabla 5.4: Resumen de los tipos de problemas y los métodos de solución en IO

Categoría	Método IO	Priorización	Secuencia	Selección	Programación	Función Objetivo	Amidamiento
Tipo 1	[58, 148]	✓					
Tipo 2	[28, 41, 86]		✓			Single	
Tipo 3	[42, 49, 60, 144, 150]			✓		Single	
Tipo 4	[42, 49, 60, 144, 150]			✓		Single	✓
Tipo 5	[65, 134]		✓	✓	✓	Single	✓
Tipo 6	[45, 49, 69, 121, 122]			✓	✓	Single	✓
Tipo 7	[49, 69, 95]			✓	✓	Multi	✓

mencionar que estas situaciones no se consideran categorías independientes de los 7 tipos de problemas identificados, sino que son situaciones especiales que pueden ocurrir dentro de cada tipo de problema y, por lo tanto, deben tener un tratamiento específico. A continuación se muestran algunos ejemplos.

- Problemas de planificación con costos dependientes de la secuencia. Una consideración adicional para todos los problemas de planificación anteriores podría ser el impacto de una secuencia de implementación determinada en los beneficios (o costos). En este caso, los problemas de programación pertenecen a la categoría general de "programación con tiempos de configuración dependientes de la secuencia". Una caracterización de estos problemas se puede encontrar en [5].

- Planificación de la implementación de controles con duración o costo variable. Los controles pueden implementarse de varias maneras, lo que desemboca en diferentes requisitos de recursos para la duración de la implementación (intercambio de tiempo y costo). Esto corresponde a problemas relacionados con la "planificación de proyectos con alternativas tecnológicas o modos de ejecución alternativos". Una revisión de estos problemas se puede encontrar en [145]. Si bien estas condiciones agregan características realistas al proceso de toma de decisiones, también agregan complejidad a problemas ya difíciles. No se han encontrado referencias para manejar simultáneamente las características mencionadas anteriormente.

- Planificación bajo incertidumbre. Los sistemas reales con frecuencia están sujetos a incertidumbre en la duración de la actividad, el costo, la disponibilidad de recursos, etc. Por lo tanto, algunas características de los sistemas generalmente se modelan como variables estocásticas o difusas. Aparecen características importantes de las soluciones, como la robustez y la estabilidad. Estos tipos de problemas de selección y programación se describen en [67, 74, 94].

5.4 Resolución del modelo

Una vez realizada la modelación de la situación, se debe resolver el modelo obtenido. El problema de la resolución del modelo es relativamente simple. En primer lugar, el modelo desarrollado en la etapa anterior se debe escribir en algún lenguaje de modelación de problemas de optimización. Tras este paso, la resolución se puede realizar de manera manual, utilizando las diversas técnicas de resolución de este tipo de problemas, o utilizar alguna herramienta o aplicación in-

formática que soporte estas técnicas.

Existen diversos programas o aplicaciones que apoyan este proceso y que soportan diversos lenguajes de modelación de problemas de optimización. Los programas más conocidos o utilizados en este contexto se resumen en la tabla 5.5. Como se observa, existen variadas opciones, gratuitas o de pago, ambiente Web o para equipos de trabajo y que soportan diversos lenguajes de modelación de este tipo de problemas.

Para efectos de este trabajo de tesis, se ha decidido trabajar con el Sistema General de Modelado Algebraico - General Algebraic Modeling System (GAMS) [55] como lenguaje de modelación, ya que es soportado por una gran cantidad de herramientas. Este lenguaje de modelado posee su propia herramienta de resolución. Sin embargo ésta no es gratuita, por lo que, para resolver el modelo, se optó por trabajar con la plataforma web NEOS-SERVER [104], que sí es gratuita, es de acceso Web y soporta una gran cantidad de tipos de problemas y lenguajes de modelación.

5.5 Caso de estudio: aplicación de la propuesta

Para ilustrar la formulación propuesta y evaluar algunos de los escenarios no contemplados en la literatura, se ha aplicado el modelo a dos situaciones que hacen referencia a dos tipos de problemas descritos en la sección anterior. Para esto, se han utilizado los datos de una auditoría real a una organización pública del estado chileno. Para su ejecución, se consideraron los controles de seguridad de este estudio y se aplicó el modelo para observar su desempeño. Se trata por tanto de un entorno real en el que se tuvieron que evaluar más de 400 controles

Tabla 5.5: Resumen de lenguajes de modelación de problemas de optimización.

Hojas de cálculo con Solver asociado	
Se consideran todas aquellas formulaciones matemáticas que pueden ser resueltas a través de las propiedades de un programa de hojas de cálculo. En general, se aplican para la resolución de problemas simples, que no requieren una modelación muy compleja, como un problema de programación lineal.	Solver MsExcel
Entornos de cálculo matemático y/o simbólico	
Aplicaciones dedicadas a la resolución de problemas matemáticos que poseen su propio Solver. Estos programas tienen capacidad de resolver problemas de optimización más complejos, ya que poseen funcionalidades dedicadas a estos tipos de problemas.	MatLab Maple Mathematica NEOS-SERVER
Lenguajes algebráicos de modelado	
Este tipo de lenguajes y herramientas asociadas, poseen capacidades específicas para la resolución de este tipo de problemas, con una sintaxis que permite construir un modelo muy cercano a la expresión matemática que representa la situación.	GAMS AMPL AIMMS XPRESS-MP

de tres estándares de seguridad diferentes, donde el objetivo era poder generar los resultados con la máxima velocidad y el mínimo esfuerzo posibles.

En términos de las variables de seguridad referenciadas en el modelo conceptual (tabla 5.4), se han incluido: controles, dependencias de controles, presupuesto y costos de implementación de los controles. La tabla 5.6 resume esta inclusión (última columna), y compara las características de estos dos casos con respecto al resto de casos encontrados en la revisión de la literatura presentada en el capítulo 4.

Como se muestra en la tabla 5.4, los casos de estudio son similares en estructura, variando la fución objetivo a optimizar y los elementos de las restricciones. Además, algunos casos tienen más de una función objetivo (multicriterio). Como contribución al conjunto de casos de la literatura, el caso de estudio de esta tesis aportan como novedad la consideración de la relación "superControl - subControls", es decir, la adición de una restricción que evidencia el anidamiento de los controles.

El objetivo de la auditoría realizada fue averiguar el grado de cumplimiento de la organización analizada respecto de los tres conjuntos de normas de seguridad de la información a las que ésta está suscrita, ya sea voluntariamente o como requisito. La norma a la que se suscribe voluntariamente es la norma internacional ISO 27001 en la versión 2005. Además, el conjunto de reglas que la organización está obligada a cumplir como organización perteneciente al estado chileno es (i) el Decreto Supremo 83 (Decreto Supremo 83 (DS83)) [62], que corresponde a una norma técnica para las organizaciones estatales sobre la seguridad y confidencialidad de los documentos electrónicos y (ii) la guía metodológica para la seguridad de la información (Guía metodológica del Gobierno de Chile (GUI)) [63], en el marco del programa

Tabla 5.6: Características de los casos de la literatura vs. caso de esta tesis en función de elementos de la ontología.

Ontología	Casos						
Clases	[126]	[75]	[154]	[127]	[6]	[156]	Tesis
Security Objective							
Risk	C O	C O	O	O			
Vulnerability					C		
Asset							
Threat	C						
Safeguard					O		
Control	O		O C	O C			O
Unit	C	C	C	O			C
Security Domain							O
Agent							
Asociaciones	[126]	[75]	[154]	[127]	[6]	[156]	Tesis
damaged asset - damaged obj	O		O				
affects – exhibits							
reason - generates							
effect - caused by							
exploits – allows							
arises - caused by							
threats – source							
is asset - is control							
protects - protector							
manages - manager							
participates in - requires							
superControl - subControls							C
implementedAfter - iBefore							
mitigatedBy - mitigates							
itsControls							

de mejora del gobierno de Chile, que describe los requisitos técnicos asociados con el diagnóstico, la planificación y la implementación de un sistema de seguridad de la información.

Para determinar si la organización cumplió con los controles de los tres conjuntos descritos anteriormente, los controles de cada estándar

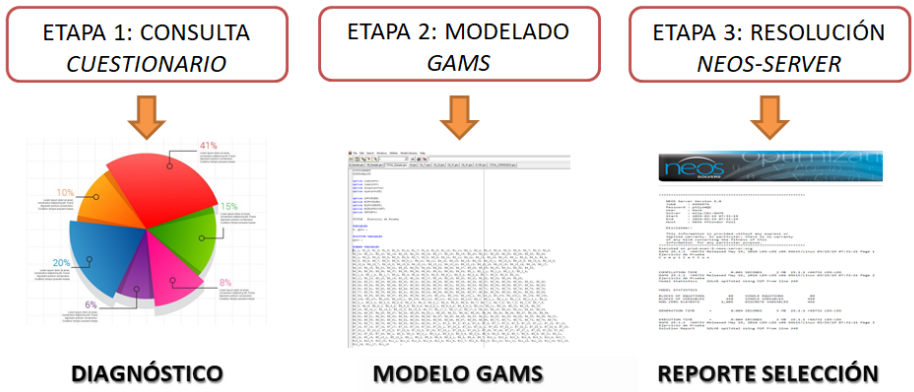


Figura 5.5: Secuencia de aplicación ejemplo.

se agruparon por dominios de aplicación, en función de los dominios dados en la ISO 27002; Se identificaron los controles comunes y las interdependencias y anidación entre ellos. Para obtener el diagnóstico inicial de la organización respecto del cumplimiento de cada estándar, se construyó y aplicó un cuestionario que preguntaba por el estado de implementación de cada control de seguridad. Este cuestionario fue presentado en la sección 5.2 y se encuentra disponible en el Anexo A de este documento.

Tal y como se ha comentado en la sección anterior, la situación se formuló matemáticamente y se resolvió utilizando el portal web de NEOS Server [104], que es un sitio web gratuito para resolver problemas de optimización. Para formular el problema, se utilizó el lenguaje GAMS [55], que es un sistema de modelado de alto nivel para programación y optimización matemática. La secuencia de aplicación del ejemplo se realizó de acuerdo a los pasos descritos en la figura 5.5.

5.5.1 Caso de estudio: modelado de un problema de Tipo 4 - centrado en el costo-beneficio

En este caso de estudio, el objetivo es obtener un conjunto de controles para optimizar un presupuesto dado en función del costo de implementación de cada control y el "beneficio" que cada control informa. Se considera como un "beneficio" el número de estándares en los que el control está presente, dado que el objetivo de la organización es avanzar lo más posible en el cumplimiento de los tres estándares. En otras palabras, se espera obtener un conjunto de controles que permita cubrir la mayor cantidad posible de controles de cada estándar, en base a un presupuesto limitado. Esta situación se corresponde con un problema del Tipo 4.

La formulación del modelo incluyó las siguientes condiciones: (i) los controles se clasificaron de acuerdo con las dimensiones de la norma ISO 27002; (ii) se utilizaron controles anidados, es decir, hay controles que no pueden implementarse hasta que se haya implementado el conjunto de controles de los que dependen; (iii) en la función objetivo, la cobertura de cada control se consideró con respecto a los estándares que se están evaluando y (iv) se aplicaron dos variables de restricción: el costo individual de la implementación del control y el presupuesto total disponible para la implementación.

Para modelar la situación, la función objetivo (ecuación 5.1) se construyó como la sumatoria de los controles que pertenecen a una dimensión de la norma, considerando los controles anidados en el control anterior (hasta dos niveles), y el "beneficio" de cada control. Como restricciones se consideraron: (i) ecuación 5.2, que representa la restricción del costo de implementación en base al presupuesto disponible, donde la suma de estos costos, incluidos los costos de los controles anidados, no puede exceder el presupuesto disponible para

la implementación; (ii) ecuaciones 5.3, que representan las restricciones asociadas al anidamiento de primer nivel y (iii) ecuaciones 5.4, que representan las restricciones asociadas al anidamiento de segundo nivel.

$$MAX\left(\sum_{i,j>0} PX_{ij} + \sum_{i,j>0,k\in A_{ij}} PX_{ijk} + \sum_{i,j>0,k\in A_{ij},l\in A_{ijk}} PX_{ijkl}\right) \quad (5.1)$$

s.t.

$$\sum_{i,j>0} C_{ij}X_{ij} + \sum_{i,j>0,k\in A_{ij}} C_{ijk}X_{ijk} + \sum_{i,j>0,k\in A_{ij},l\in A_{ijk}} C_{ijkl}X_{ijkl} - B \leq 0 \quad (5.2)$$

$$\begin{gathered} X_{ij} - X_{ijk} \leq 0 \\ i,j > 0, k \in A_{ij}, A_{ij} \neq \Phi \end{gathered} \quad (5.3)$$

$$\begin{gathered} X_{ijk} - X_{ijkl} \leq 0 \\ i,j > 0, k \in A_{ij}, l \in A_{ijk}, A_{ij} \neq \Phi, A_{ijk} \neq \Phi \end{gathered} \quad (5.4)$$

donde,

P Beneficio de implementar cada control.

i Dimensión de un estándar de seguridad.

j Controles pertenecientes a la dimensión.

k Primer nivel de anidamiento para el j^{th} control.

l Segundo nivel de anidamiento para el jk^{th} control.

B Presupuesto disponible.

A_{ij} conjunto de i^{th} controles anidados.

A_{ijk} conjunto de ij^{th} controles anidados.

Para explicar cómo se realiza la formulación y la resolución de los modelos para este tipo de problemas, se utilizará la situación representada en la figura 5.6 como ejemplo. En ella, se identifican 10 controles de seguridad con sus correspondientes costos de implementación y su beneficio, representados por una tupla con el formato (control - costo - beneficio). Las dependencias entre controles están graficadas a través de las llaves. Por ejemplo, el control C10 se puede seleccionar solo si también se seleccionan los controles C7 y C8.

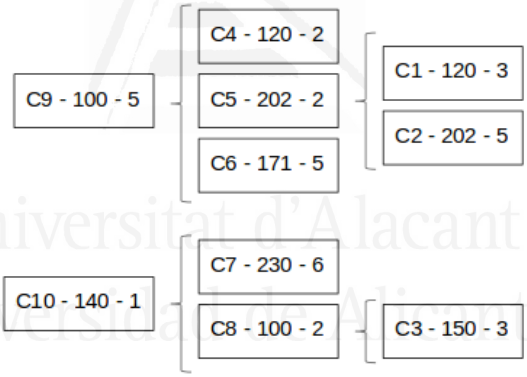


Figura 5.6: Controles candidatos a implementar, sus costos, beneficios y dependencias.

Dado que puede haber múltiples combinaciones de controles que cumplan con un presupuesto determinado, se esperaría que los modelos presentados pudieran determinar el conjunto de controles que optimizara el presupuesto de una organización.

La formulación matemática de este modelo de optimización se presenta a continuación, donde (i) la ecuación 5.5 presenta la función objetivo del modelo, que busca maximizar el número de controles a implementar, (ii) la ecuación 5.6 presenta la restricción asociada a los costos de implementación y el presupuesto disponible, (iii) la ecuación 5.7 presenta las restricciones asociadas con el primer nivel de anidamiento y (iv) la ecuación 5.8 presenta las restricciones de anidación de segundo nivel.

$$MAX(5C9+C10+2C4+2C5+5C6+6C7+2C8+3C1+5C2) \quad (5.5)$$

s.t.

$$\begin{aligned} 100C9+140C10+120C4+202C5+171C6+230C7+ \\ 100C8+120C1+202C2+150C3-B \leq 0 \end{aligned} \quad (5.6)$$

$$\begin{aligned} C9-C4 \leq 0 \\ C9-C5 \leq 0 \\ C9-C6 \leq 0 \\ C10-C7 \leq 0 \\ C10-C8 \leq 0 \end{aligned} \quad (5.7)$$

$$\begin{aligned} C5-C1 \leq 0 \\ C5-C2 \leq 0 \\ C8-C3 \leq 0 \end{aligned} \quad (5.8)$$

En las siguientes imágenes, se muestra la modelación de la situación en el lenguaje de modelado GAMS, que incluye la configuración

de las variables (ver figura 5.7), y la definición de las ecuaciones (función objetivo y restricciones, ver figura 5.8). Estas ecuaciones incluyen los beneficios de implementar cada control, las ecuaciones de restricciones presupuestarias y las restricciones que definen las dependencias entre controles.

```
$OFFSYMXREF
$OFFSYMLIST

option limrow=0;
option limcol=0;
option solprint=on;
option sysout=off;

option LP=CPLEX;
option MIP=CPLEX;
option NLP=CONOPT;
option MINLP=DICOPT;
option OPTCR=0;

$TITLE   Ejercicio de Prueba

VARIABLES

F, ppto, B ;

POSITIVE VARIABLES

ppto, B ;

BINARY VARIABLES

C1, C2, C3, C4, C5, C6, C7, C8, C9, C10;
```


Figura 5.7: Configuración y definición de variables del modelo en GAMS.

Una vez obtenido el modelo, se procedió a resolver el problema de optimización en el portal NEOS Server para problemas de optimización. En la figura 5.9, se muestra la portada del sitio web de NEOS Server. El problema se configuró como una Programación lineal de enteros mixtos, utilizando la entrada GAMS.

```
EQUATIONS

funcObj, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10;

funcObj.. F =E= 5*C9 + C10 + 2*C4 + 2*C5 + 5*C6 + 6*C7 +
                2*C8 + 3*C1 + 5*C2  ;

R1.. 100*C9 + 140*C10 + 120*C4 + 202*C5 + 171*C6 + 230*C7 +
      100*C8 + 120*C1 + 202*C2 + 150*C3 - B =L= 0 ;

R2.. B =L= 1000;
R3.. C9 - C4 =L= 0;
R4.. C9 - C5 =L= 0;
R5.. C9 - C6 =L= 0;
R6.. C10 - C7 =L= 0;
R7.. C10 - C8 =L= 0;
R8.. C5 - C1 =L= 0;
R9.. C5 - C2 =L= 0;
R10.. C8 - C3 =L= 0;

MODEL ejemplo /ALL/ ;

SOLVE ejemplo using MIP maximizing F ;
```

Figura 5.8: Formulación de ecuaciones del modelo en lenguaje GAMS.

En la figura 5.10, se muestra parte del reporte entregado por el portal.

Del reporte obtenido, se observa que los controles seleccionados fueron: C1, C2, C4, C5, C6, C9. El costo total de la propuesta fue de $ 915, para un presupuesto de $ 1.000.

Para el caso de estudio, la formulación con los datos obtenidos de la auditoría a la organización gubernamental Chilena se aplicó a un total de 456 controles, provenientes de los tres estándares de asociados a seguridad de la información, tal como se describió al inicio de la sección. Al considerar las dependencias, aproximadamente 40 controles mostraron dependencias jerárquicas.

El modelo se probó en cuatro escenarios posibles, considerando diferentes niveles de presupuesto, medidos como un porcentaje del costo

Figura 5.9: Portada del portal de optimización NEOS Server.

total de implementar todos los controles. La estimaci[on de los costos de implementaci[on de cada control se realizó por el equipo auditor y se redondeó a un monto de $ 310.000.000 de pesos chilenos. En consecuencia, el primer escenario representó un presupuesto del 10 % del costo total de implementación, el segundo representó el 40 %, el tercero el 60 % y el último el 80 % del costo.

Como condiciones de los casos, se asumió que no había controles implementados y, para cada control, se estimó el costo de implementación y se consideró como beneficio su presencia en los tres estándares y su pertenencia a una regulación obligatoria o un estándar opcional. Esto quiere decir que, si el control se encontraba considerado en más de un estándar y pertenecía a una regulación obligatoria, se le asignaba un mayor valor (reporta un mayor beneficio). Con estos parámetros, se modeló el problema para obtener el conjunto de controles que op-

```
                           LOWER      LEVEL      UPPER     MARGINAL

---- VAR F                 -INF       22.000     +INF        .
---- VAR B                   .       915.000     +INF        .
---- VAR C1                  .         1.000     1.000      3.000
---- VAR C2                  .         1.000     1.000      5.000
---- VAR C3                  .           .       1.000       EPS
---- VAR C4                  .         1.000     1.000      2.000
---- VAR C5                  .         1.000     1.000      2.000
---- VAR C6                  .         1.000     1.000      5.000
---- VAR C7                  .           .       1.000      6.000
---- VAR C8                  .           .       1.000      2.000
---- VAR C9                  .         1.000     1.000      5.000
---- VAR C10                 .           .       1.000      1.000


**** REPORT SUMMARY :        0     NONOPT
                             0 INFEASIBLE
                             0  UNBOUNDED


EXECUTION TIME       =        0.000 SECONDS      2 MB  24.8.2 r59988 WEX-WEI


USER: GAMS Development Corporation, Washington, DC   G871201/0000CA-ANY
      Free Demo,  202-342-0180,  sales@gams.com,  www.gams.com   DC0000


**** FILE SUMMARY
```

Figura 5.10: Extracto del reporte entregado por NEOS Server.

timizase el presupuesto de cada uno de los cuatro escenarios definidos .

Las fórmulas de estos escenarios se especificaron en el software GAMS con los distintos valores de presupuesto. Los modelos y sus salidas correspondientes están disponibles en `https://bit.ly/2JZkfyi`.

La tabla 5.7 muestra un resumen de los avances en el cumplimiento de cada estándar de acuerdo con el nivel de presupuesto, así como la eficiencia en el uso del presupuesto disponible. Cabe señalar que tanto el presupuesto como el costo de cada escenario se encuentran en miles de pesos chilenos.

En la figura 5.11, la variación en los controles se muestra gráficamente de acuerdo con una variación del presupuesto.

Tabla 5.7: Resumen de cumplimiento por nivel de presupuesto

Cantidad de controles				Presupuesto	Costo	Eficencia
Total	GUI	ISO	DS83			
55,48 %	77,48 %	46,97 %	75,72 %	$ 62.000 (20 %)	$ 61.824	99,72 %
79,61 %	89,18 %	76,66 %	91,32 %	$ 124.000 (40 %)	$ 123.590	99,67 %
91,23 %	96,40 %	89,33 %	97,11 %	$ 186.000 (60 %)	$ 185.090	99,51 %
98,46 %	99,09 %	98,27 %	98,84 %	$ 248.000 (80 %)	$ 245.900	99,15 %

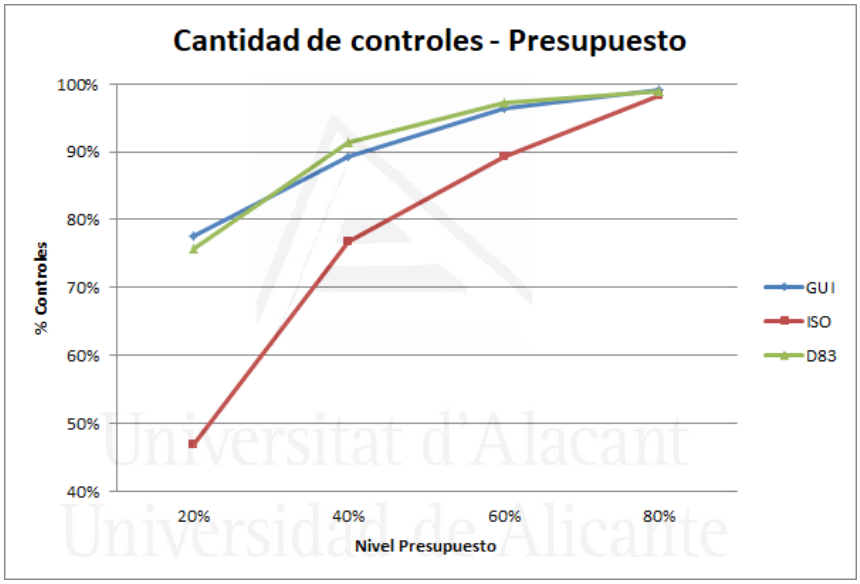


Figura 5.11: Gráfico presupuesto vs % controles

De los resultados obtenidos en el caso de estudio, se puede destacar lo siguiente:

- Con un bajo porcentaje del presupuesto (20 %), es posible seleccionar un grupo importante de controles, alcanzando aproximadamente el 50 % del número total de controles a implementar.

Es decir que con un bajo esfuerzo es posible lograr un avance significativo en el cumplimiento de los estándares.

- Tanto GUI como DS83 presentan un mayor avance, respecto de ISO, para la primera selección de controles (Escenario 1 - 20 % del presupuesto). Esto significa que el modelo prioriza aquellos controles que pertenecen a los estándares obligatorios.

- El modelo maximizó el presupuesto disponible, logrando una eficiencia en el uso de este de más del 99 % en todos los escenarios. En otras palabras, el método entrega la lista de controles que deben implementarse para utilizar el 99 % del presupuesto de la organización, lo que implica un alto grado de eficiencia en el uso de los recursos. Esto es muy significativo en el contexto de una organización gubernamental que debe rendir cuentas públicamente de su gestión

Finalmente, la tabla 5.8 muestra los procentajes de controles seleccionados de acuerdo a los estándares en los que se encuentran. En la primera columna se muestran los distintos niveles de presupuestos que se consideraron para cada caso. En la columna de "1 estándar", se muestran aquellos controles seleccionados que solo se encuentran en un estándar. En la columna de "2 estándares, se muestra el procentaje de controles seleccionados que se enceuntran en dos estándares. En la columna de "3 estándares", se muestra el porcentaje de selección de aquellos controles que son comunes a los tres estándares. Por último, en la columna del Total, se muestra el procentaje de selección, del total de controles evaluados. Como se observa, para todos los niveles de presupuesto, siempre presenta un mayor porcentaje de selección el grupo de controles que son comunes a los tres estándares, ya que estos, de acuerdo al modelo, tenían prioridad sobre aquellos controles que solo eran comunes a dos estándares o a un solo estándar.

Tabla 5.8: Cobertura de controles por grupo de estándares de acuerdo a cada nivel de presupuesto

Presupuesto	1 estándar	2 estandares	3 estándares	Total
20 %	48,6 %	67,0 %	83,3 %	55,5 %
40 %	74,3 %	90,4 %	93,3 %	79,6 %
60 %	88,7 %	96,5 %	96,7 %	91,2 %
80 %	98,4 %	98,3 %	100 %	98,5 %

Debe reconocerse que los costos no son datos sólidos, porque están bajo incertidumbre y deben ser estimados por los evaluadores. Una estrategia para reducir la incertidumbre de estos datos es la realización de un análisis de sensibilidad, con el fin de obtener una visión sobre el comportamiento del conjunto de controles seleccionados frente a las variaciones de este tipo de datos. Dado que los atributos de un modelo pueden ser independientes entre sí, estar interrelacionados o ser sinérgicos [32], una forma de abordar este problema es considerar la sinergia como un valor agregado al modelado, como ya se ha utilizado en [32, 89]. Si bien el enfoque de la mochila se considera una forma de tratar la sinergia, se pueden considerar los beneficios de la interacción entre los controles. Estas interdependencias que surgen de la interacción entre controles son parte de los modelos propuestos para futuras investigaciones.

6. Evaluación Empírica de la Propuesta

Este capítulo presenta el estudio empírico sobre la intención de adopción de la propuesta. El estudio está basado en el modelo unificado de adopción de métodos en Ingeniería del Software UMAM y analiza la intención de adopción de la propuesta en un contexto académico.

En la sección 6.1 se describe el contexto de la experiencia y se presentan los objetivos del estudio.

La sección 6.2 presenta el modelo UMAM y sus principales componentes.

La sección 6.3 detalla el proceso de ejecución del estudio empírico.

La sección 6.4 presenta el análisis de los resultados del estudio. Este análisis incluye tres vistas de los datos: (i) estadísticos descriptivos, (ii) análisis de opiniones cualitativas y (iii) análisis cuantitativo, a través de un modelo de regresión lineal múltiple.

Por último, en la sección 6.5 se resumen las conclusiones obtenidas a partir del análisis de datos realizado. Además, se presentan las amenazas a la validez del estudio.

6.1 Objetivos y contexto del estudio empírico

Con el fin de medir el desempeño de la propuesta y las percepciones que sobre ella tienen los futuros asesores de seguridad, se realizó un estudio empírico de selección de controles de seguridad en el curso de pregrado denominado "Auditoría Informática", que se dicta para estudiantes de los últimos años de las carreras de Ingeniería Informática de la Facultad de Ingeniería y Ciencias de la Universidad de La Frontera.

En este curso se revisan materias relacionadas con Gobernanza TI y los Frameworks y estándares asociados (entre ellos aquellos relacionados a SI), además de métodos para realizar una auditoría TI en las organizaciones. El curso se dicta todos los semestres, pero la aplicación del estudio se realizó en el segundo semestre del año 2020.

Cabe destacar que el estudio no se vio afectado por la pandemia, ya que para la realización de la auditoría se utilizaron técnicas remotas para el levantamiento de la información, como las propuestas en el estándar ISO/IEC 19.0011:2018. Por otra parte, tanto el entrenamiento de los estudiantes respecto del enfoque metodológico, como la aplicación de la propuesta en el trabajo semestral, también se desarrollaron remotamente, utilizando herramientas de trabajo colaborativo (por ejemplo, Zoom para las clases y reuniones), y las herramientas de Google para almacenamiento de archivos y trabajo en documentos de ofimática.

6.2 Modelo Unificado de Adopción de Métodos en Ingeniería del Software: UMAM

Dado que no se encontró ningún modelo teórico que sirviera para evaluar la intención de adopción de métodos en el campo de la Ingeniería Informática (II), el primer paso para el diseño del estudio consistió en proponer un Modelo Conceptual de Adopción de Métodos en Ingeniería del Software, que fue denominado Modelo Unificado de Adopción de Métodos (UMAM por sus siglas en Inglés), y que, junto con su cuestionario asociado UMAM-Q, fue publicado en [38].

El UMAM es un modelo de adopción de métodos que proporciona un marco de evaluación de la intención de uso de un método de trabajo relacionado con la Ingeniería del Software por parte de un grupo de profesionales. Si bien es cierto que el UMAM se desarrolló pensando en su aplicación para estudios respecto de la adopción de métodos de desarrollo software como es el Desarrollo Dirigido por Modelos, su estructura y fundamento teórico hace que pueda ser aplicado con cualquier tipo de método que implique un cambio en la forma de trabajar del profesional informático.

Este modelo surge de una revisión sistemática de las dimensiones más importantes consideradas en los modelos de adopción de tecnologías más populares, y que fueron analizados en [38]. Este análisis detectó varios problemas en las propuestas de modelos existentes, entre los que destacan [38]:

- Varios de ellos usaban nombres diferentes para el mismo concepto, por ejemplo Utilidad y Ventaja Relativa.

- Muchas definiciones de conceptos eran poco precisas, complicadas o, en algunos casos, incluso inexistentes.

- Varios constructos tenían significados que se solapaban parcialmente, por ejemplo Utilidad y Adecuación al trabajo.

- En algunos modelos los autores distinguían entre variables externas, primarias y de control, mientras que otros hablaban solo de variables primarias.

- Algunas variables eran consideradas primarias en algunas propuestas y externas o de control en otras, por ejemplo soporte organizacional.

- La mayoría de las escalas definidas para medir los constructos de los modelos tenían menos de cuatro ítems, lo que supone una amenaza a su fiabilidad.

Como se observa en la figura 6.1, el modelo propone que la adopción de nuevos métodos de trabajo se explique en base a 5 aspectos (dimensiones del modelo) que inciden sobre la Intención de Comportamiento (IC), entendida como el grado en que los posibles adoptantes expresan su intención explícita de adoptar el método evaluado en el futuro si tienen oportunidad. Estas cinco dimensiones o constructos son:

- Utilidad (U): El grado en que una persona cree que el uso de un método en particular aumentará su rendimiento en el trabajo [99].

- Facilidad de Uso (FU): Se refiere al grado en que una persona cree que el uso de un método o herramienta provoca un mayor o menor esfuerzo [99].

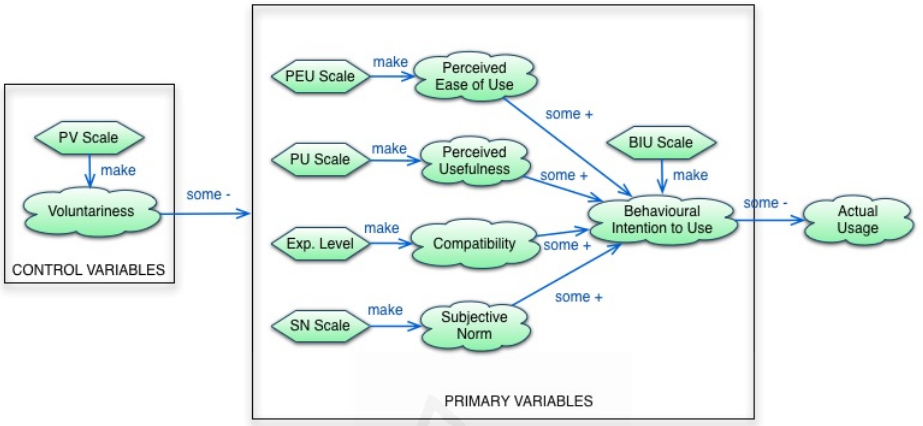


Figura 6.1: Modelo Unificado de Adopción de Métodos (UMAM).

- Norma Subjetiva (NS): Es el grado en que los desarrolladores piensan que otras personas, cuya opinión es importantes para ellos, creen que deberían utilizar un método [99].

- Compatibilidad (C): Es el grado en que se percibe un método como consistente con los valores existentes, los principios, las prácticas y la experiencia previa de los posibles adoptantes [99].

- Voluntariedad (V): es el grado en que los posibles adoptantes perciben la decisión de adopción como no obligatoria, y representa la presión del entorno social sobre el potencial adoptante [1].

6.2.1 Validación cualitativa del modelo

El grado de cobertura de los factores del modelo fue evauado de manera cualitativa dentro de un contexto de evaluación de métodos de desarrollo software. Como parte de un estudio más amplio, se pidió a un conjunto de sujetos, que habían estado expuestos a tres métodos diferentes de desarrollo software (uno dirigido por modelos, otro basado en modelos y un tercero tradicional, sin modelos) que indicaran los factores que consideraban que afectaban positivamente su intención de utilizar cada método, y cuáles eran percibidos como negativos para dicha intención de adopción. Los comentarios resultantes fueron sintetizados y clasificados en categorías. Por último, se estudió si esas categorías podían considerarse parte de los constructos del UMAM. El resultado fue que dos de las categorías se relacionaban con FU, tres se relacionaban con U y dos con C [38].

Acompañando a este modelo, se definió además un instrumento de medición, en forma de cuestionario, denominado UMAM-Q, que operacionaliza el modelo teórico. Para la creación del cuestionario se siguió un proceso sistemático que se detalla a continuación.

6.2.2 Cuestionario del Modelo Unificado de Adopción de Métodos: UMAM-Q

A partir de las dimensiones del modelo conceptual, el primer paso consistió en recopilar los ítems de las escalas publicadas en los distintos cuestionarios disponibles para cada una de las dimensiones seleccionadas. Estos ítems fueron seleccionados/adaptados de acuerdo a tres criterios:

- las escalas tenían que ser lo suficientemente genéricas como para ser aplicables a una amplia variedad de métodos y técnicas de

Ingeniería del Software.

- Los ítems debían seguir una estructura estándar (compartamiento específico hacia un objetivo específico dentro de un contexto específico)
- Al menos se debían seleccionar/definir 14 ítems por dimensión, con el fin de permitir la eliminación de los ítems que peor se adaptaran a cada contexto concreto.

Para la definición de los nuevos ítems en los casos necesarios, se utilizó como base el conjunto de comentarios realizados por los sujetos durante la etapa de validación cualitativa del modelo.

Por último, el conjunto completo de ítems se sometió a una ronda de clasificación por parte de dos expertos que no habían participado en la fase de selección/creación de los mismos. A estos jueces se les proporcionaron los seis constructos con sus definiciones, y se les pidió que clasificaran los ítems en cada categoría. Un análisis del grado de acuerdo inter-juez mostró un estadístico Kappa con un alto nivel de fiabilidad (K = 0,949 p ¡0,001). Este análisis, aunque simple, proporciona una primera intuición sobre la validez convergente y discriminante de las escalas.

El resultado de este esfuerzo es el cuestionario UMAM-Q. UMAM-Q está estructurado en seis escalas, que se corresponden a las seis dimensiones consideradas en el modelo UMAM (U, FU, NS, C, V y IC). Existen dos versiones de este cuestionario. En la versión extendida, el cuestionario incluye 14 preguntas por cada uno de los dominios, en una escala Likert de 7 niveles, desde “Totalmente en desacuerdo” hasta “Totalmente de acuerdo”. En la versión reducida, el número de ítems por dimensión se ha reducido a 7 en base a un Análisis de Componentes Principales sobre datos empíricos de un conjunto de estudios

de intención de adopción realizados para distintos métodos y técnicas de Ingeniería del Software.

Dado que el dominio de la SI era un dominio para el que no se disponía de datos previos (y que, por tanto, no había sido incluido en el Análisis de Componentes Principales), para la realización de la experiencia se utilizó la versión extendida del cuestionario UMAM-Q, que se encuentra disponible en el Anexo B de este documento.

6.3 Ejecución del estudio empírico

El estudio se realizó durante el segundo semestre del año 2020, con un total de 12 estudiantes. Para capacitar a los estudiantes en el uso de la propuesta, durante el desarrollo del curso los estudiantes debieron resolver un conjunto de casos teóricos, en los cuales debían identificar un conjunto de "no conformidades" y proponer un plan de mejora a través de la selección del conjunto óptimo de controles que cumpliera con una o más restricciones impuestas en cada caso, tales como costos, beneficios y riesgos. La mitad de los casos teóricos debían ser resueltos de manera tradicional, es decir, en base al estudio de los estándares y sus propios análisis de la situación, mientras que la otra mitad debía ser resuelta utilizando el modelo propuesto. A cada alumno se le asignó de manera aleatoria el conjunto de casos que debía resolver sin y con el modelo.

Dada la imposibilidad de desdoblar los grupos para controlar el posible efecto que el orden de los tratamientos (sin/con ayuda de la propuesta) pudiese tener en los resultados, y con el fin de evitar en lo posible el sesgo de propagación del efecto, los alumnos realizaron primero los casos de estudio donde no debían utilizar la propuesta.

Tras esta etapa, se les explicó la propuesta con 2 ejemplos descritos en los artículos [34, 35]. Por último, los alumnos trabajaron en los casos de estudio en donde les había tocado aplicar la propuesta. Los casos en los que trabajaron los alumnos y cuáles resolvieron sin la propuesta (SP) y de manera sistemática con la propuesta (CP) pueden ser vistos en la tabla C.1 del Anexo C. Al finalizar esta fase, podemos asumir que los alumnos disponían del mismo nivel de destreza con ambos tratamientos.

Tras aplicar la propuesta a este segundo conjunto de casos, los estudiantes realizaron un proyecto completo de auditoría. En este proyecto los estudiantes, agrupados en equipos de trabajo de 3 personas, debían realizar una auditoría TI, acotada al contexto de seguridad de la información, en una organización real elegida por el equipo. Nuevamente, se les pidió que aplicaran la propuesta para evaluar el nivel de idoneidad de esta para la resolución de casos reales.

Para este proyecto, los estudiantes tuvieron que seguir las fases definidas en la norma ISO/IEC 19011:2018 - "Guidelines for auditing management systems" [53], en base a los controles propuestos por la norma ISO/IEC 27002:2013 [52].

Estas fases son las siguientes: (i) Planificación de un programa de Auditoría, (ii) Planificación de una Auditoría, (iii) Realización de una Auditoría y (iv) Reporte de hallazgos y Plan de mejora. Es en estas últimas dos etapas (diagnóstico y plan de mejora) donde los equipos debían aplicar el proceso y los modelos propuestos en este trabajo. El modelado del problema de optimización que propone la propuesta se aplicó de manera manual, sin el soporte de ningún tipo de herramienta, por lo que los estudiantes debieron construir el modelo, a partir de los datos de la auditoría, utilizando el lenguaje GAMS. Para la resolución del sistema resultante se utilizó el portal web para la resolución

de modelos de optimización, NEOS-Server [104].

El último paso del estudio consistió en que los alumnos evaluaran, mediante el instrumento UMAM-Q, la utilidad, la facilidad de uso, la norma social y la compatibilidad percibidas de la propuesta de esta tesis, así como su intención de usarla en el futuro para el diagnóstico y la realización de recomendaciones de seguridad en su entorno laboral. El análisis de los resultados de esta evaluación se presenta a continuación.

6.4 Análisis de los resultados del estudio

A continuación se presentan los resultados de la aplicación de UMAM-Q a los estudiantes de la asignatura, una vez que utilizaron el modelo propuesto para la recomendación de controles tanto en casos acotados como en un entorno real. Cabe destacar que se ha dejado fuera del estudio el constructo de "Voluntariedad", ya que el contexto académico en el que se desarrolló el proyecto obligó a los estudiantes a utilizar el método, por lo que este dominio pierde sentido para el análisis.

Para el análisis de los datos recopilados a través del cuestionario, se ha realizado, en primer lugar, un análisis de los estadísticos descriptivos relacionados con las dimensiones del modelo UMAM. Además, se ha realizado un análisis cualitativo de las principales bondades e inconvenientes de la propuesta a través de la revisión de las respuestas a las preguntas abiertas del cuestionario, donde los estudiantes debían indicar las ventajas y dificultades que percibían con respecto a la aplicación de la propuesta. Por último, se presenta un análisis cuantitativo, a través de un modelo de regresión lineal múltiple, aplicado sobre las respuestas de los estudiantes.

6.4.1 Estadísticos descriptivos

Para la caracterización de las dimensiones del modelo UMAM a través de los estadísticos descriptivos se utilizó la herramienta para análisis estadístico SPSS. De acuerdo a la estructura del instrumento, las dimensiones de Utilidad (U), Facilidad de Uso (FU), Compatibilidad (C) y Norma Subjetiva (NS) presentan una escala de 14 ítems, cada una con puntuaciones de 1 a 7, donde 1 es la percepción más negativa (Totalmente en desacuerdo) y 7 la más positiva (Totalmente de acuerdo) con respecto a cada afirmación. Por tanto, el rango de puntuación de estas variables va desde 14 puntos hasta 98 puntos. Por otra parte, la dimensión de Intención de Comportamiento (IC) presenta una escala de 7 ítems, con un rango de puntuación desde 7 puntos hasta 49 puntos.

En la tabla 6.1, se presenta un resumen con los datos descriptivos de cada dimensión, mientras que en la figura 6.2 se presentan gráficos de caja para cada una de las dimensiones del modelo.

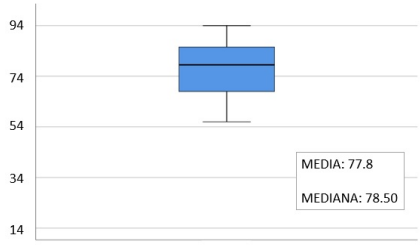
A la vista de los datos expuestos tanto en la tabla 6.1 como en los gráficos de la figura 6.2, se destaca el alto nivel de **Utilidad** percibida del método propuesto. Esta dimensión presenta una mediana de 78,5 puntos sobre un máximo de 98. Esto implica que los estudiantes perciben que el método es de gran utilidad a la hora de resolver el problema planteado.

La dimensión **Compatibilidad** también presenta una mediana alta, 71,5 puntos sobre un máximo de 98. Esto indica que los estudiantes también perciben que el método se ajusta a la forma en la que ven normal trabajar, es decir, el método es compatible con el estilo de trabajo que espera realizar un futuro ingeniero.

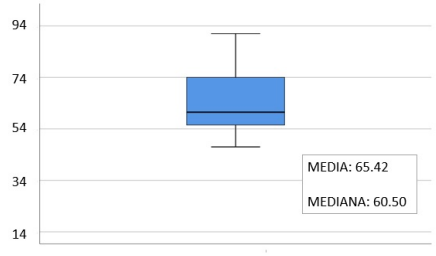
En el otro extremo se encuentra la dimensión **Norma Subjetiva**,

Tabla 6.1: Descriptivos de las dimensiones de UMAM

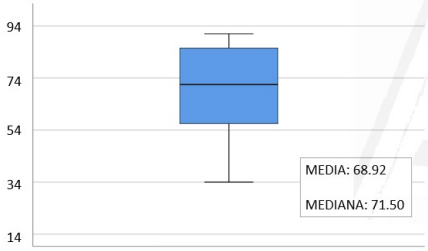
Utilidad	Media		77,8
	95 % Intervalo confianza para la media	Límite Inferior	69,31
		Límite Superior	84,86
	Mediana		78,50
	Mínimo		56
	Máximo		94
Facilidad de Uso	Media		65,42
	95 % Intervalo confianza para la media	Límite Inferior	56,49
		Límite Superior	74,45
	Mediana		60,50
	Mínimo		47
	Máximo		91
Compatibilidad	Media		68,92
	95 % Intervalo confianza para la media	Límite Inferior	57,02
		Límite Superior	80,81
	Mediana		71,50
	Mínimo		34
	Máximo		91
Norma Subjetiva	Media		58,67
	95 % Intervalo confianza para la media	Límite Inferior	50,15
		Límite Superior	67,18
	Mediana		57,50
	Mínimo		35
	Máximo		83
Intención de Adopción	Media		34,67
	95 % Intervalo confianza para la media	Límite Inferior	29,05
		Límite Superior	40,28
	Mediana		35,00
	Mínimo		17
	Máximo		49



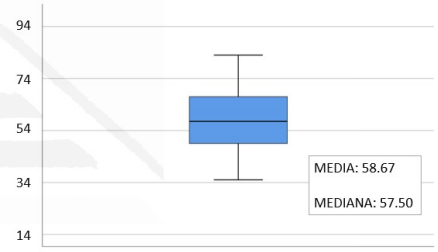
(a) Utilidad



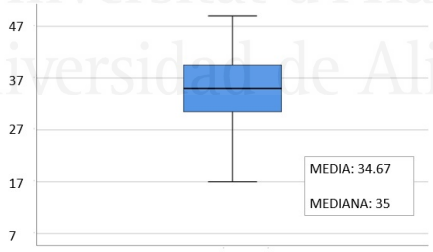
(b) Facilidad de Uso



(c) Compatibilidad



(d) Norma Subjetiva



(e) Intención de Adopción

Figura 6.2: Gráficos Estadísticos Descriptivos

cuya mediana se encuentra en 57,5 puntos sobre 98. Esto se explica porque los estudiantes saben que este método no es un método estándar de la industria, y por tanto no sienten ninguna presión externa a la hora de usarlo. Nuestra hipótesis es que, dado que no existe ninguna alternativa estandarizada en la industria, esta dimensión no tienen por qué impactar de manera significativa en la decisión del estudiante a la hora de adoptar este marco metodológico.

Este análisis también refleja cómo el principal punto débil de la propuesta es la dimensión **Facilidad de Uso**, que presenta una mediana de 60,98 puntos sobre un máximo de 98, lo que es bastante más bajo que las dimensiones de Utilidad y Compatibilidad. En principio parece que los estudiantes perciben que el método es difícil de asimilar y poco intuitivo. Esto convierte a esta dimensión en el aspecto de mejora prioritario de cara a futuras iteraciones de mejora de la propuesta.

Por último, por lo que respecta a la **Intención de Comportamiento**, la mediana se sitúa en 35 puntos sobre un máximo de 49, lo que implica una intención ligeramente positiva hacia su adopción.

6.4.2 Opiniones Cualitativas

Con el fin de obtener información cualitativa sobre las percepciones de los sujetos, en el instrumento de evaluación se definió una sección de preguntas abiertas, donde el estudiante podía exponer tres aspectos positivos y tres aspectos negativos que la propuesta presentaba. Estas opiniones fueron recogidas y analizadas para entender mejor la percepción de los estudiantes respecto de las bondades y dificultades de la propuesta, y dar o quitar razón a las primeras intuiciones obtenidas mediante los estadísticos descriptivos.

Para facilitar el análisis de las opiniones de los estudiantes, se clasifican las respuestas de éstos, respecto de las componentes del modelo UMAM, por lo que cada respuesta se asignó a alguna de estas componentes: U - Utilidad, FU - Facilidad de Uso, C - Compatibilidad y NS - Norma Subjetiva.

En la tabla 6.2 se presenta un resumen de las respuestas positivas de los estudiantes clasificadas en función de la dimensión con la que están relacionadas. A partir de esta tabla, en la tabla 6.3 se presenta un resumen cuantitativo del porcentaje de comentarios positivos asociados con cada una de las dimensiones del UMAM: un 47.6 % se refieren a aspectos de U, un 38.1 % a aspectos relacionados con la C y solo un 14.3 % a aspectos relacionados con la FU.

De estos porcentajes se desprende que los estudiantes perciben como principal fortaleza de la propuesta el contribuir a una mayor eficacia y eficiencia del trabajo del asesor de seguridad (U). Además, destacan sus cualidades de generalidad, estructuración y automatización, en el sentido de sistematización del proceso (C). Solo un 14 % de los comentarios apuntan a que la propuesta no es compleja de aprender y de utilizar (FU). Por último, la dimensión de NS no aparece reflejada en ninguno de los comentarios.

Por otro lado, en la tabla 6.4 se presentan las respuestas de los estudiantes respectos de los aspectos negativos que perciben del uso de la propuesta, y su clasificación en función de la dimensión principal con la que se relacionan.

A partir de esta tabla, en la tabla 6.5 se presenta un resumen del porcentaje de respuestas negativas relacionadas con cada dimensión del modelo. De estas opiniones negativas, solo el 18.75 % se pueden

Tabla 6.2: Respuestas abiertas - Aspectos Positivos

Aspectos Positivos - Opiniones de los estudiantes	
Es más estructurado al momento de realizar.	C
Genera documentación más limpia y entendible.	C
Aumenta el índice de productividad.	U
Es rápida al momento de resolver problemas grandes.	U
es procedimental.	C
Puede ser aplicada en cualquier contexto	C
Mejor eficiencia	U
Metodología simple	FU
Dada a la precisión que tiene	U
Permite restricciones lo cual es necesario y otras metodologías no la tienen	U
No es difícil de aprende a utilizar si es que ya se tiene conocimiento de código basado en matemáticas	FU
Eficiencia de tiempo	U
Automatización	C
Lenguaje estandarizado	C
Es rápida una vez que se entiende la sintaxis	U
Es certero el resultado que nos entrega	U
Son datos confiables que apoyan la toma de decisiones	U
Facilidad ante el requerimiento de un plan de mejora para un proyecto de gran envergadura	FU
Es completa	U
Segura	C
Formal	C

Tabla 6.3: Resumen de respuestas - Aspectos Positivos

Dimensión	**Respuestas**	**Porcentaje**
U	10	47.6 %
FU	3	14.3 %
C	8	38.1 %
NS	0	0 %

asociar a U, y solo un 6.25 % a C. Nuevamente, la NS no aparece en los comentarios, añadiendo peso a la hipótesis inicial de que, tratándose de un marco metodológico que trata un problema para el que no existen alternativas estandarizadas, no es un aspecto al que los sujetos den mayor importancia. Sin embargo, un 75 % de los comentarios apuntan directamente a la FU como principal problema de la propuesta.

De estos porcentajes se desprende que los estudiantes perciben que la propuesta es difícil de usar y aprender, que requiere de conocimientos previos, y, que en caso de no tenerlos, toma un tiempo apreciable obtenerlos. En menor medida piensan que la necesidad de modelar el problema puede ralentizar su trabajo en determinadas condiciones. Por último, una opinión se refiere a que no es la manera usual a la que acostumbran a programar, lo que les provoca algunas dificultades relacionadas con la C.

Frente a estos resultados, la hipótesis es que el alto porcentaje de respuestas negativas en el dominio de la Facilidad de Uso se debe principalmente a la deficiente formación de los estudiantes de Ingeniería Informática en lo que respecta a IO y a la modelación y resolución de problemas de optimización. Actualmente, el plan de estudios de estas carreras en Chile no profundiza en este dominio de la ingeniería, por

Tabla 6.4: Respuestas abiertas - Aspectos Negativos

Aspectos Negativos - Opiniones de los estudiantes	
Tiene una curva de aprendizaje algo inclinada en un inicio.	FU
Si no se tiene un contexto específico para ocupar lo puede llevar a entregar resultados erróneos.	U
Dificultad de tener que aprender otro lenguaje.	FU
Es lenta al momento de programar en código un problema grande.	U
No hay herramienta de desarrollo que ayude a escribir el código.	FU
Suele ser enredada al momento de usar tantas variables es vez de usar arreglos o listas.	FU
En algunos grupos de trabajo puede costar crear el hábito de utilizarla.	FU
En caso de no saber algún tipo de código matemático.	FU
La entrega de resultados no se puede traspasar a otro documento fácilmente.	FU
La sintaxis es un poco diferente a lo que se acostumbra a programar.	C
Requiere un entendimiento previo para poder ocuparla.	FU
Toma tiempo.	FU
Requiere varios conocimientos previos.	FU
Difícil de propagar a otras personas.	U
Dificultad de aprendizaje.	FU
tiempo de aprendizaje.	FU

Tabla 6.5: Resumen de respuestas - Aspectos Positivos

Dimensión	**Respuestas**	**Porcentaje**
U	3	18.75 %
FU	12	75 %
C	1	6.25 %
NS	0	0 %

lo que los estudiantes no poseen un fondo de conocimientos en estos temas, lo que obviamente dificulta la utilización de la propuesta.

Como se puede observar, las opiniones cualitativas de los estudiantes son consistentes con las puntuaciones obtenidas mediante el instrumento UMAM-Q. Por lo tanto, se puede afirmar que el marco metodológico propuesto se presenta como una herramienta útil para apoyar el proceso de toma de decisiones en la selección de controles para una propuesta de mejora en el avance del cumplimiento de un estándar. Además, es un instrumento compatible con las prácticas del asesor. Sin embargo, no es fácil de utilizar, ya que requiere de conocimientos previos en la modelación de problemas de optimización y presenta una marcada curva de aprendizaje.

Este último punto es la mayor debilidad de la propuesta e implica que un asesor de seguridad debe adquirir conocimientos en técnicas de IO para la modelación y resolución de problemas de optimización si desea beneficiarse de las ventajas de usar la propuesta. Esto convierte el desarrollo de técnicas, artefactos y herramientas para facilitar este modelado y resolución de problemas en el principal punto a mejorar.

6.4.3 Análisis cuantitativo: regresión lineal múltiple.

Por último, se ha realizado un análisis piloto de regresión lineal múltiple para reconocer el impacto de cada una de las variables independientes (U, FU, C, NS) sobre la IC (variable dependiente). Este análisis pretende cuantificar cuánto de la variación de la variable dependiente se explica por la variable independiente. Es importante hacer notar que, dado el pequeño número de observaciones, las conclusiones de este análisis deben ser tratadas con mucha precaución. Nuestro objetivo al realizarlo ha sido no tanto crear un modelo predictivo como añadir o quitar peso a las primeras intuiciones sobre cuál es el peso relativo de las variables independientes analizadas sobre la intención de adopción de este método. Esta información es importante de cara a planear cómo priorizar futuras mejoras del método.

Para lograr el objetivo del estudio, se requiere que se cumplan las siguientes asunciones:

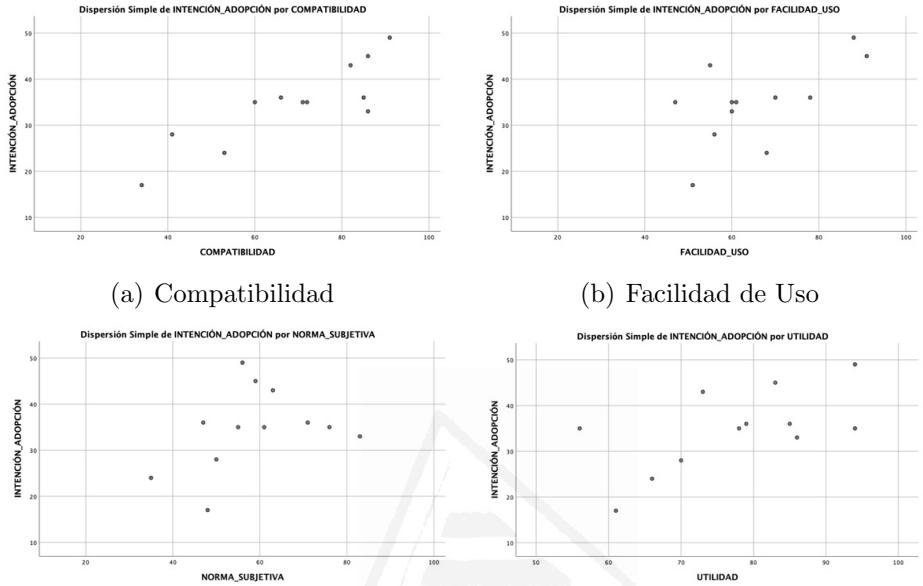
1. Variable dependiente de tipo ratio (continua).

   Dadas las características de la variable de IC, se puede decir que ésta cumple con esta condición.

2. Las variables independientes son de tipo ratio.

   De la misma manera que la variable dependiente, las variables independientes, U, FU, C, NS, también cumplen con esta condición.

3. Existe una relación lineal entre las variables dependientes e independientes, tanto individual como colectivamente.



(a) Compatibilidad (b) Facilidad de Uso

(c) Norma Subjetiva (d) Utilidad

Figura 6.3: Gráficos Regresión Lineal

Si se observa la figura 6.3, en donde se muestran cuatro gráficos de dispersión respecto de cada dimensión del modelo evaluada en este estudio, una inspección visual de los mismos demuestra cómo U, FU y C tienen una relación aproximadamente lineal con respecto a IC. No ocurre lo mismo con NS, donde a partir de cierto nivel no parece que se vea afectada la IC. Como además esta dimensión es la que menos interés tiene para nuestro análisis, al tratarse de algo que no tiene que ver directamente con posibilidades de mejora del método propuesto, en lo que queda de análisis la atención se centrará en U, figura 6.3(d), FU, figura 6.3(b) y C, figura 6.3(a).

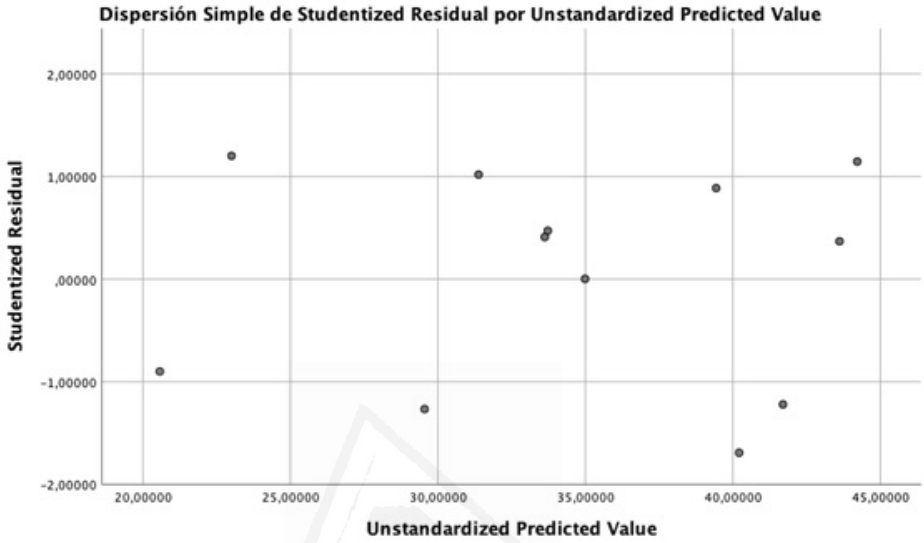


Figura 6.4: Diagrama de dispersión.

En cuanto a la relación lineal entre todas las variables consideradas en su conjunto y la variable dependiente, lo hemos comprobado mediante un diagrama de dispersión de los studentized residuals (SRE_1) contra los (unstandardized) predicted values (PRE_1), presentado en la figura 6.4.

A pesar de los pocos puntos (12 observaciones) se puede ver cómo los residuos forman aproximadamente una banda horizontal, por lo que se puede asumir que la relación entre la variable dependiente y las variables independientes es aproximadamente lineal.

4. Homoscedasticidad de varianzas

En el mismo diagrama de dispersión anterior, figura 6.4, además, se puede observar cómo los puntos del diagrama no muestran ningún patrón y están aproximadamente diseminados de manera constante, lo que sugiere que existe homoscedasticidad de varianza.

5. Independencia de observaciones

   El propio diseño del estudio asegura la independencia de observaciones: los sujetos cumplimentaron el cuestionario UMAM-Q en el mismo momento temporal, y sin interacción entre ellos. Esta independencia de residuos se comprobó también con el estadístico de Durbin-Watson, que arrojó un resultado de 2.227, lo que implica que no existe autocorrelación.

6. No hay multicolinearidad entre las variable independientes

   Las estadísticas de colinearidad, figura 6.5, muestran cómo la tolerancia de todas las variables independientes es mayor que 0.1, lo que indica que no hay multicolinearidad.

   Además, en la tabla de correlaciones se puede observar cómo la Compatibilidad está fuertemente relacionada (correlación > 0.7) con la Utilidad.

7. No hay puntos inusuales o que influyan de manera indebida.

   Un estudio de los residuos estandarizados demostró que todos los puntos se encontraban por debajo del valor umbral de +-3, lo que indica que no hay outliers significativos.

   Asimismo, un examen del valor de leverage de todos los casos mostró que ningún de ellos era peligroso (es decir, que el valor de

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.	95,0% intervalo de confianza para B		Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta			Límite inferior	Límite superior	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	7,914	10,326		,766	,465	-15,898	31,727					
	UTILIDAD	-,105	,201	-,145	-,521	,617	-,569	,359	,602	-,181	-,091	,395	2,532
	FACILIDAD_USO	,100	,148	,158	,675	,519	-,241	,440	,596	,232	,118	,557	1,796
	COMPATIBILIDAD	,411	,128	,870	3,206	,013	,115	,706	,859	,750	,561	,416	2,403

a. Variable dependiente: INTENCIÓN_ADOPCIÓN

Figura 6.5: Coeficientes de colinearidad.

leverage sea mayor que 0.5). Cabe recordar que, según [70], por regla general, se considera que si el valor de leverage es menor que 0.2, se consideran los casos como seguros, si esta entre 0.2 y 0.5, existe riego, y si es mayor o igual que 0.5, se considera peligroso. En nuestro caso no hay ningún caso con valores de leverage >= 0.5.

Por último, los valores de distancia de Cook para todos los casos, muestra que no hay ningún valor mayor que 1, lo que indica que no hay ningún caso que presente una influencia destacada.

8. Residuos de la línea de regresión siguen una distribución aproximadamente normal.

   Como se aprecia en la figura 6.7, la distribución de los puntos en el gráfico es aproximadamente una línea recta. Sin embargo, reconocemos que el bajo número de observaciones hace difícil conseguir una distribución normal para los residuos. No obstante el análisis de regresión es robusto con respecto a desviaciones de la normalidad, por lo que hemos decidido continuar con el análisis.

Interpretación de los resultados

Los resultados del análisis muestran cómo todas las variables son relevantes para calcular la IC. Como se muestra en la figura 6.7, el coeficiente de correlación múltiple muestra un valor de R de 0.869, (strong), con un coeficiente de determinación ajustado de 0.663, es decir, que el modelo explica un 66.3 % de la variabilidad en la IC, lo que, según Cohen [30], es un efecto de tamaño grande.

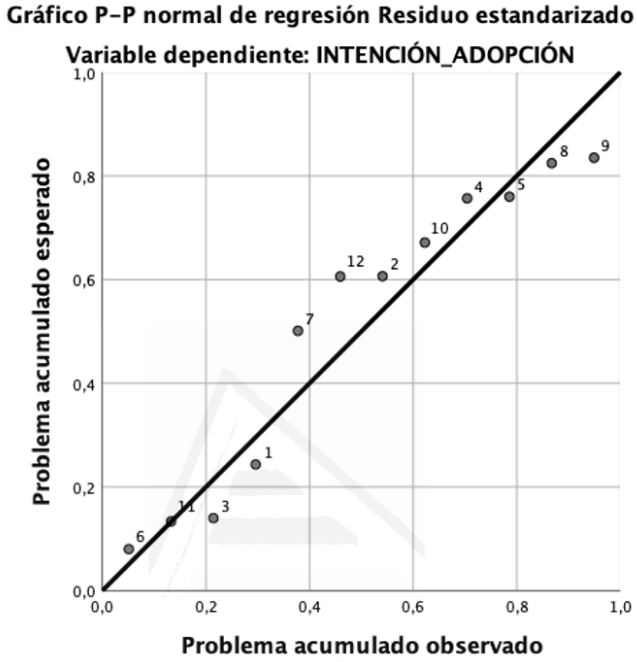


Figura 6.6: Gráfico de probabilidad normal

Resumen del modelo[b]

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Durbin-Watson
1	,869[a]	,755	,663	5,132	2,227

a. Predictores: (Constante), COMPATIBILIDAD, FACILIDAD_USO, UTILIDAD

b. Variable dependiente: INTENCIÓN_ADOPCIÓN

Figura 6.7: Resumen del modelo

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	647,965	3	215,988	8,201	,008[b]
	Residuo	210,702	8	26,338		
	Total	858,667	11			

a. Variable dependiente: INTENCIÓN_ADOPCIÓN

b. Predictores: (Constante), COMPATIBILIDAD, FACILIDAD_USO, UTILIDAD

Figura 6.8: Tabla ANOVA del modelo de regresión

El modelo propuesto es, además, altamente significativo ($F(3,8) = 8.201$, $p<0.05$), tal como se muestra en la figura 6.8, lo que indica que la adición de todas nuestras variables independientes conduce a un modelo que es significativamente mejor a la hora de predecir la IC que el modelo 'media'.

Por tanto, de acuerdo a la información presentada en la figura 6.9, el modelo de regresión da como resultado la ecuación 6.1:

$$IC = 7{,}914 - 0{,}105 * U + 0{,}1 * FU + 0{,}411 * C \tag{6.1}$$

Por otra parte, dado el pequeño número de observaciones, vemos que los intervalos de confianza para todas las variables son muy amplios. Esto hace que, con estos datos, C sea la única variable cuyo impacto en la IC es definitivamente positivo (podemos estar seguros a un 95 % de que C va a tener siempre un impacto positivo en la IC). Además, C es el único coeficiente estadísticamente significativo, lo que implica que C tiene una relación lineal con IC.

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.	95,0% intervalo de confianza para B		Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta			Límite inferior	Límite superior	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	7,914	10,326		,766	,465	-15,898	31,727					
	UTILIDAD	-,105	,201	-,145	-,521	,617	-,569	,359	,602	-,181	-,091	,395	2,532
	FACILIDAD_USO	,100	,148	,158	,675	,519	-,241	,440	,596	,232	,118	,557	1,796
	COMPATIBILIDAD	,411	,128	,870	3,206	,013	,115	,706	,859	,750	,561	,416	2,403

a. Variable dependiente: INTENCIÓN_ADOPCIÓN

Figura 6.9: Tabla con los coeficientes del modelo de regresión

De todo lo anterior, podemos concluir que, para impulsar la adopción del método propuesto entre los estudiantes de informática, tenemos que asegurar que lo perciban como un método altamente compatible con el modo en que creen que deben trabajar. Esta percepción tiene más impacto en su IC que otras tradicionalmente consideradas más importantes, como son la U y la FU percibidas.

6.5 Conclusiones del estudio de evaluación de la propuesta

La aplicación de la propuesta en un curso de pregrado de las carreras de Informática de la Universidad de la Frontera ha permitido visualizar el impacto de la utilización de este marco metodológico en un caso realista de una auditoría informática. Se capacitó a los estudiantes en la utilización de la propuesta, y a continuación se pidió que la utilizaran en el desarrollo de su proyecto semestral de auditoría. Posteriormente, a través de la aplicación del modelo UMAM, se obtuvieron datos que daban cuenta de la intención de adopción de la propuesta.

Como conclusiones de este estudio se puede mencionar lo siguiente:

1 **Los estudiantes reaccionaron favorablemente a la propuesta**.

El estudio de los resultados de la evaluación muestran que éstos son consistentes entre los tres tipos de análisis realizados. Estos resultados indican que los estudiantes perciben la propuesta metodológica como una herramienta útil para la selección del conjunto de controles de seguridad que mejor se ajusta a las

condiciones de la organización bajo estudio. Además, se percibe que la propuesta es compatible con la forma de trabajar de los sujetos, lo que indica que se ajusta al quehacer de un asesor de seguridad, por lo que se puede considerar como un aporte y no un estorbo para el asesor. Por otro lado, se percibe que la propuesta presenta cierto grado de dificultad en su aplicación, debido, principalmente, al desconocimiento que los estudiantes tienen de las técnicas de IO para resolver un problema de optimización.

Respecto de la IC de la propuesta metodológica, se pudo observar que ésta presenta una tendencia ligeramente positiva, lo que implica que existe buenas posibilidades que la propuesta sea adoptaba por los sujetos, pero esta posibilidad no es alta, por lo que existe espacio para la mejora. Además, si se considera que los estudiantes manifestaron como debilidad de la propuesta la FU, y que la IC está fuertemente relacionada con la percepción de la C del método, se puede deducir que las acciones de mejora que pueden aplicarse al modelo deberían estar enfocadas en estos dos aspectos de manera preferencial.

2 **El modelo propuesto es consistente**.

En análisis de los resultados de los tres estudios muestra la consistencia de la propuesta respecto de los factores que explican la IC. Esto se refleja en que las respuestas de los estudiantes, recogidas con el instrumento UMAM-Q, las percepciones cualitativas declaradas por los estudiantes y el estudio de Regresión Lineal aplicado apuntan todos en la misma dirección, es decir, reflejan que las fortalezas de la propuesta se encuentran tanto en

la C como en la U de ésta, mientras que la principal debilidad radica en su FU.

Además, a partir de los resultados del estudio de regresión, también se pudo evidenciar que el modelo es altamente significativo, lo que implica que el UMAM es un modelo confiable para la predicción de la IC. Esto, acompañado de los resultados del estudio cualitativo y del análisis de los estadísticos descriptivos, dotan de una gran significancia a las opiniones de los estudiantes, por lo que se puede confiar en los resultados que indican que la propuesta metodológica es una buena herramienta para apoyar el proceso de toma de decisiones respecto de la selección de controles de seguridad.

Amenazas a la validez del estudio

Dadas las características de la experiencia, se pueden mencionar como situaciones que amenazan la validez del estudio, lo siguiente:

1 **Tamaño del grupo de estudio**.

El principal problema que presenta el estudio es la baja cantidad de sujetos que formaron parte de él. Solo 12 estudiantes respondieron el instrumento de consulta. Si bien es cierto que esta cantidad representan el 100 % del universo de estudiantes sobre el cual se recogerían las observaciones, el grupo es claramente insuficiente, por lo que no es posible generalizar los resultados a la población general de auditores, ni siquiera de estudiantes de auditoría. Sin embargo, estos resultados permiten establecer una tendencia y una base sobre la que diseñar un futuro proceso de mejora a la propuesta antes de intentar expandirla a otros

ámbitos fuera de mi universidad y realizar un estudio empírico más ambicioso.

2 **Características del grupo de estudio**.

Otro factor importante a considerar, también relacionado con la validez externa del estudio, es la representatividad del grupo respecto del público objetivo de la propuesta. Reconocemos que los estudiantes incluidos en la muestra no son expertos asesores de seguridad, sino que poseen conocimientos básicos del área y de las prácticas de un asesor de seguridad. Sin embargo, cabe mencionar que la asignatura, dentro del programa de estudios, tiene justamente por objetivo proveer de estos conocimientos al estudiante, y que es la única asignatura dedicada a esta área, por lo que cualquier recién egresado va a contar con los mismos conocimientos que los estudiantes que han participado en el estudio. Por otra parte, previamente al estudio, se realizaron sesiones de capacitación en la propuesta de selección, la construcción de los modelos de optimización, la ejecución de los modelos y la interpretación de los resultados.

7. Soporte Software

Este capítulo presenta una herramienta infomática que apoya el enfoque metodológico, interviniendo en la mayoría de las etapas definidas en este trabajo.

En la sección 7.1, se detallan las características de la herramienta a través de los modelos de clases y de componentes que definen su estructura.

En la sección 7.2, se describe como la herramienta interviene en la mayor parte de las etapas del método y detalla, por cada etapa, sus funcionalidades.

En la sección 7.3, se detallan las limitaciones que la herramienta presenta en su aplicación y, a partir de éstas, las oportunidades de mejora en su desarrollo.

7.1 Características de la herramienta

Como ya se ha mostrado, el enfoque metodológico propuesto puede desarrollarse de manera manual en cada una de sus etapas, desde la recopilación de la información hasta la modelación y resolución del problema de optimización. Sin embargo, y tal como lo mostraron los resultados de la evaluación de la propuesta, existen algunas etapas del proceso que resultan complicadas de ejecutar, principalmente para personas que no poseen conocimientos referentes a la modelación y resolución de un problema de optimización.

En este sentido, para facilitar la implementación del proceso propuesto, se ha desarrollado una herramienta informática para asistir al experto en la determinación del mejor conjunto de controles que se ajuste al problema que se desea resolver. Como se muestra en la figura 7.1, esta herramienta automatiza gran parte de la propuesta, proporcionando un soporte informático para la recolección de datos, la generación automática del modelo de optimización y la resolución automática de este modelo, lo que permite obtener el conjunto óptimo de controles que satisface las condiciones del problema.

Cómo se observa en la figura 7.2, la arquitectura de la herramienta, concebida como un prototipo, es muy sencilla. Es una herramienta concebida para ir enriqueciéndose con el paso del tiempo a través de la inclusión permanente de los distintos casos que puedan identificarse a partir de cada una de los tipos de problemas que forman parte de esta propuesta y que están descritos en la sección 5.3.3. Cabe señalar que, dadas las diversas variables que pueden considerarse en la formulación del modelo (ver tabla 5.2), existe una gran cantidad de casos o ejemplos que pueden producirse. Actualmente, los casos totalmente cubiertos por la herramienta incluyen dos tipos de problemas:

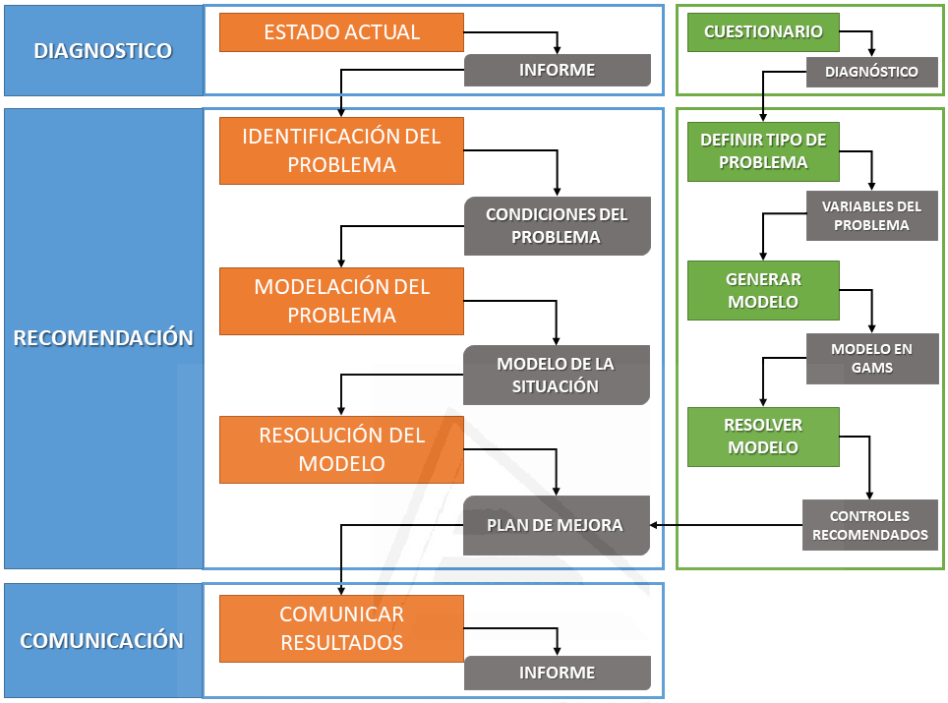


Figura 7.1: Etapas generales cubiertas por la herramienta

- Tipo de problema 3: Selección de controles con restricciones

- Tipo de problema 4: Selección de controles con restricciones y dependencia de controles

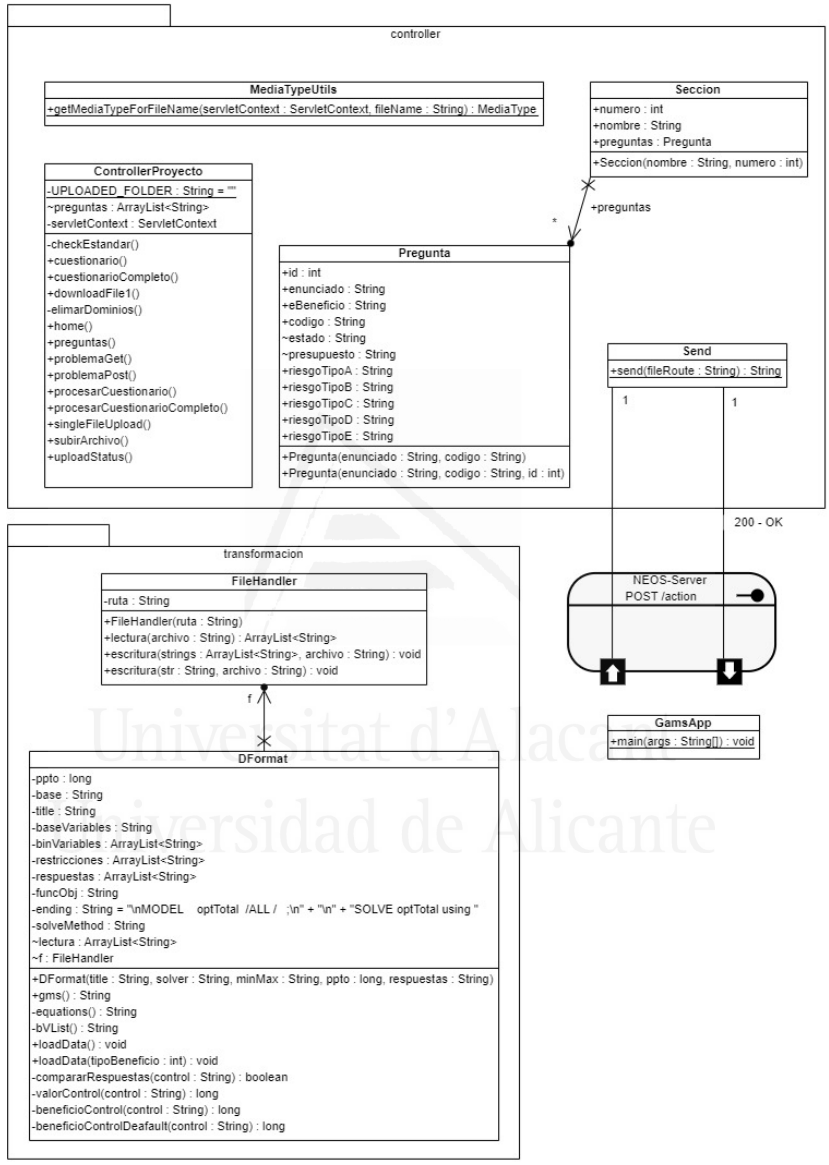


Figura 7.2: Diagrama de clases de la herramienta

7.2 Intervención de la Herramienta en las fases propuestas por enfoque metodológico propuesto

Tal como se muestra en la figura 7.1, la herramienta apoya prácticamente todas las fases propuestas por el enfoque metodológico. Es así que, por cada una de las fases que el enfoque describe, la herramienta tiene presencia y permite automatizar gran parte de los procesos involucrados. A continuación se detalla cómo.

7.2.1 Etapa I - Diagnóstico

En esta etapa, la herramienta apoya el proceso de captura y visualización de la información. A través de un cuestionario, construido a partir de los controles de la norma ISO27001, el usuario puede describir la situación de la organización respecto de dicha norma. Con estas respuestas, se puede determinar el grado de conformidad de la organización respecto de la norma ISO27001, lográndose un diagnóstico preliminar de la organización. En la actualidad, este cuestionario posee más de 400 preguntas, ya que además de los controles de la norma ISO27701, también incluye los requerimientos del DS83 y la GUI, para cubrir las necesidades de las organizaciones públicas chilenas, con las que el autor de esta tesis ha colaborado.

En primer lugar, la herramienta consulta por el tipo de problema que se desea resolver (ver figura 7.3). Esto está relacionado con los tipos de problemas de optimización que se han presentado en esta propuesta, y que fueron presentado en la sección 5.3.3.

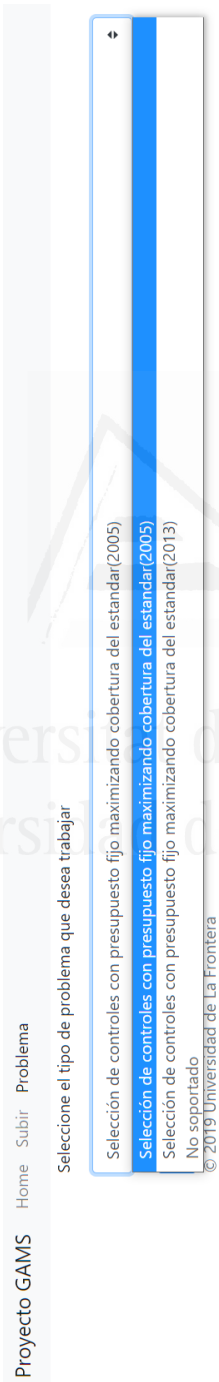


Figura 7.3: Selección del tipo de problema

De acuerdo a la respuesta proporcionada por el asesor de seguridad, la herramienta presenta la configuración del cuestionario (ver figura 7.4). En este cuestionario se pide al asesor que proceda a realizar las siguientes acciones:

- Seleccionar las normas que se desean considerar en el estudio: En este caso, el usuario puede seleccionar una o más de las normas que están disponibles hasta el momento, esto es, ISO27001, DS83 o GUI. Dependiendo de la selección del usuario, el cuestionario desplegará las preguntas asociadas a cada norma o estándar.

- Seleccionar la forma en que se desplegarán las preguntas en la pantalla. Hasta el momento la herramienta posee dos configuraciones: (a) una pregunta a la vez o (b) todas las preguntas en una página.

- Seleccionar la forma en que se considerará el beneficio reportado por cada control. La herramienta proporciona dos opciones: (a) el beneficio es el mismo para todos los controles o (b) el usuario define el beneficio de cada control.

- Seleccionar los dominios de la norma o estándar que se desea evaluar. La herramienta permite al usuario seleccionar los dominios de la norma que desea evaluar. Es posible evaluar la norma en su totalidad o solo algunos dominios de la misma. De acuerdo a la selección del usuario, la herramienta desplegará las preguntas asociadas a los dominios seleccionados. Cabe destacar que las preguntas están asociadas o clasificadas según los dominios que presenta el estándar ISO27001:2013.

Posteriormente, la herramienta despliega el cuestionario, con las preguntas agrupadas por dominio (ver figura 7.5). En esta ventana, la

Figura 7.4: Configuración del cuestionario

herramienta permite que el usuario responda las preguntas del cuestionario. Todas las preguntas tienen dos posible respuestas: "Sí" o "No". En el caso de que la situación esté cubierta por la organización, la respuesta será "Sí". En el caso contrario, la respuesta será "No". En este último caso, la herramienta permite que se ingrese el costo asociado a la implementación de la situación, además del beneficio, en caso que fuera necesario.

Para finalizar el proceso de responder al cuestionario, la herramienta solicita ingresar un título al proyecto y definir el presupuesto disponible (ver figura 7.6).

Con las respuestas al cuestionario, es posible determinar el grado de conformidad de la organización respecto del estándar. La herramienta entrega los porcentajes de conformidad o no conformidad respecto del estándar, con la posibilidad de visualizarlo por dominio y en su totalidad. Cabe señalar que las respuestas y las configuraciones entregadas por el usuario son guardadas en el sistema para el desarrollo posterior del modelo de optimización. A partir de las respuestas negativas, de la configuración del tipo de problema y de las variables involucradas, la herramienta es capaz de diseñar un modelo de optimización en la etapa de recomendación, tal y como se detalla a continuación.

7.2.2 Etapa II - Recomendación

En esta etapa, la herramienta automatiza los procesos de la definición del problema, la generación del modelo y la resolución del mismo.

La primera fase de esta etapa se refiere a la definición del tipo de problema a considerar y de las variables involucradas en la modelación (función objetivo y restricciones). Para la realización de este paso

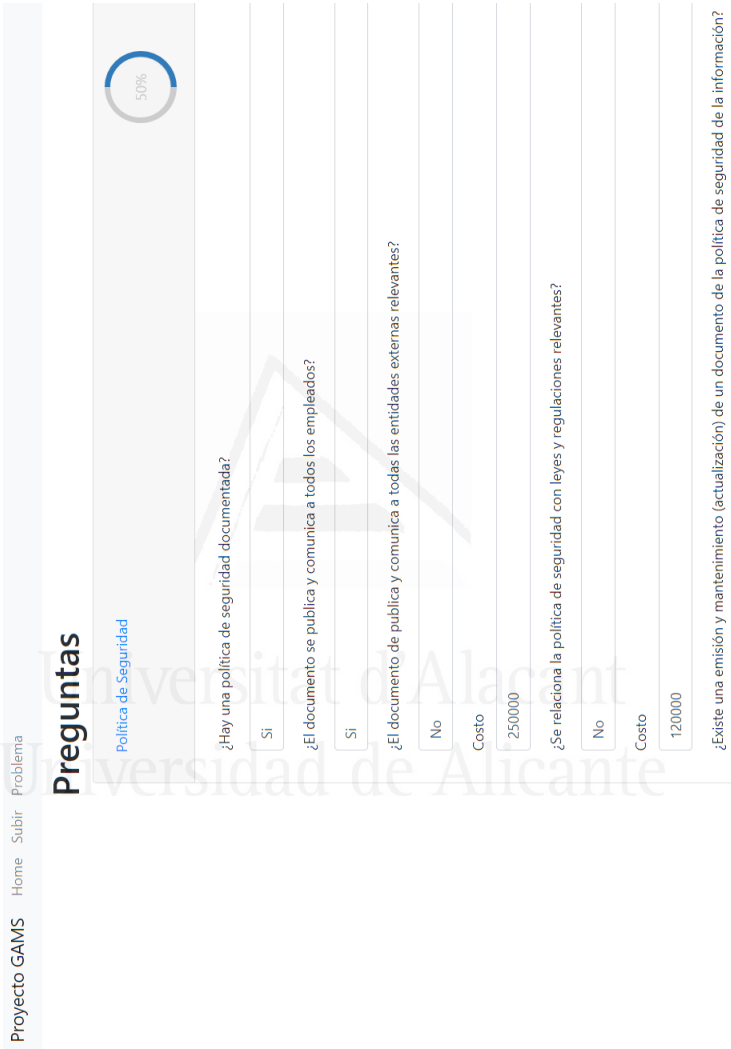


Figura 7.5: Ventana de respuesta del cuestionario

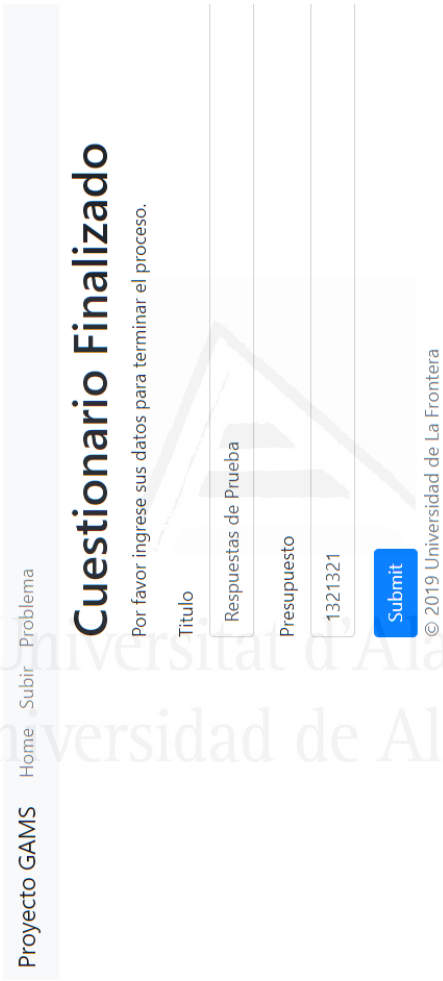


Figura 7.6: Ventana de cierre de cuestionario

basta con que el usuario/asesor haya seleccionado el tipo de problema que desea resolver (ver figura 7.3).

Otra forma en que la herramienta permite definir los parámetros del modelo es subiendo directamente el modelo en el lenguaje GAMS por medio de un archivo de texto (ver figura 7.7). En esta ventana se permite, (i) definir el tipo de problema, a través de la definición del Solver a utilizar, (ii) definir el presupuesto disponible y (iii) definir el tipo de optimización a realizar (maximizar o minimizar).

Con toda esta información, la herramienta tiene la capacidad de generar automáticamente el modelo de optimización en el lenguaje GAMS. Este modelo se guarda en un archivo de texto, tal como se ejemplificó en las figuras 5.7 y 5.8.

Una vez construido el modelo, la herramienta resuelve automáticamente el modelo. Para ello, la aplicación hace uso de los motores gratuitos de resolución de problemas de optimización NEOS-Server (ver figura 5.9), que están disponibles en la red. La herramienta sube el archivo al portal web y recibe el archivo de respuesta entregado por el portal. Estas respuestas son desplegadas por la herramienta, y constituyen la propuesta de selección de controles.

Con esto se completa el proceso de selección, desde el levantamiento de información o diagnóstico, hasta la resolución del modelo de optimización generado según el tipo de problema que se desea resolver y la configuración de los parámetros de optimización introducida por el usuario.

Figura 7.7: Ventana para subir modelo GAMS

7.3 Limitaciones de la herramienta

La herramienta desarrollada es un primer prototipo que, aunque funcional y completo para un subconjunto de los casos descritos en esta propuesta, adolece de diversas carencias:

- No cubre toda la casuística posible de problemas de optimización.
- Por el momento la herramienta no despliega informes o interpretaciones respecto del conjunto de controles seleccionados, sino que se limita a entregar el archivo proporcionado por NEOS-Server para una lectura manual.

De esto se desprenden como oportunidades de mejora y/o trabajo futuro en lo que respecta al desarrollo de la herramienta:

- Continuar con la inclusión de los casos de optimización descritos en la propuestas, con sus respectivas variantes.
- Mejorar la forma en que se despliegan los resultados y desarrollar nuevas vistas para la visualización e interpretación de informes con los resultados del proceso de optimización.
- Validar el uso de la herramienta mediante un estudio empírico que muestre su impacto en el trabajo del asesor.

Sin embargo, más allá del trabajo futuro, la herramienta supone un primer paso en la mejora de las principales deficiencias que posee el enfoque metodológico, que, como vimos en la sección 6.4 tienen que ver principalmente con la dificultad de la modelación y resolución del problema de optimización. Esta herramienta permite automatizar esta

parte del enfoque metodológico, de tal manera que resulta “transparente” para el usuario.

Parte III

Conclusiones

8. Contribuciones, Conclusiones y Trabajos Futuros

En este capítulo se detallan las principales contribuciones, conclusiones, líneas de trabajo y publicaciones generadas como consecuencia del trabajo en esta tesis doctoral.

En la sección 8.1 se comentan las principales contribuciones realizadas en el ámbito de la gestión de la seguridad de la información en las organizaciones.

En la sección 8.2, se describen las principales conclusiones de cada uno de los hitos principales de la tesis.

En la sección 8.3 se plantean las principales líneas de trabajo futuro abiertas por esta tesis doctoral.

Por último, en la sección 8.4 se enumeran las principales publicaciones generadas a partir de este trabajo de tesis, así como las publicaciones adicionales del doctorando en las líneas de investigación relacionadas de (a) docencia y (b) Ingeniería del Software.

8.1 Principales contribuciones de la investigación

Como resultado directo de este proyecto de investigación, se pueden enumerar las siguientes contribuciones al área en estudio:

1. **Enfoque metodológico para la selección de controles**.

   El principal aporte de este proyecto de investigación es la propuesta de un enfoque metodológico para la selección óptima de controles de seguridad, lo que permite sistematizar un proceso que al día de hoy no está estructurado, sino que depende de cada experto en seguridad. Este trabajo define las diversas etapas del proceso, categoriza las posibles situaciones que se pueden enfrentar, define las técnicas a aplicar en cada categoría y los productos que se deben obtener en cada etapa del proceso.

   El enfoque desarrollado es aplicable en una gran cantidad de contextos, ya que se basa en situaciones que se pueden presentar en diversos tipos de organizaciones, ya sean grandes o pequeñas, públicas o privadas. La hipótesis, que todavía no ha sido contrastada, es que esta propuesta puede ser utilizada tanto por expertos en seguridad como por personas que no tengan grandes conocimientos en seguridad o en optimización.

   Las ventajas que presenta este enfoque se refieren principalmente a la sistematización del proceso, la posibilidad de resolver problemas complejos de selección aunque no se tengan grandes conocimientos del área y la disminución de los tiempos de resolución del problema.

2. **Revisión de la literatura**.

   Como parte de este proyecto, se realizó un mapeo sistemático mediante el que se logró identificar el estado actual de la literatura en lo que respecta a la aplicación de métodos para la selección de controles de seguridad. Siguiendo este protocolo, se obtuvo una visión de las técnicas y métodos utilizados por la comunidad científica para la selección de controles de seguridad. Este mapeo mostró cómo la mayoría de los artículos encontrados dan cuenta de la aplicación de técnicas para facilitar actividades concretas, más que la propuesta de métodos que cubran todas las fases de una auditoría. Por otra parte, se determinó que las propuestas permiten la selección de controles, pero no definen una programación de la implementación de los controles seleccionados. En resumen, esta revisión bibliográfica ha permitido recopilar los artículos en el ámbito de la selección de controles de seguridad y visualizar el grado de madurez en la investigación del área.

3. **Modelo conceptual integrado**.

   Otra de las actividades importantes desarrolladas como parte de este proyecto de investigación fue la definición de un modelo conceptual que sustentara la modelación de los problemas de selección. A partir de la revisión bibliográfica de los modelos ya propuestos en la literatura, se evidenció que no existe un único modelo aceptado por la comunidad, sino que existen diversas propuestas que difieren respecto de la proposición de algunos conceptos. Dado que el modelo de selección de controles que se propone en este trabajo debe basarse en un marco conceptual bien definido, se definió de manera sistemática un modelo conceptual que integra las diversas visiones encontradas en la litera-

tura. Con esta definición común de las variables involucradas en el problema se busca, por un lado, tener una base de variables que se pueden utilizar en el modelo de optimización, y por otro lado, permitir la navegación a través del modelo conceptual para identificar diversos escenarios para el modelo de optimización.

4. **Identificación de escenarios y técnicas de solución**.

   Uno de los resultados más relevantes para el diseño del enfoque metodológico propuesto tiene relación con la identificación y clasificación de los problemas o escenarios que, por un lado, caracterizan a cada organización, y por otro lado, definen la situación hacia la cual desea avanzar. En este sentido, esta propuesta identifica un conjunto de 7 escenarios posibles en los que puede categorizarse el problema que la organización desea resolver para avanzar en el logro del estándar de seguridad. A partir de esta clasificación, esta tesis propone las técnicas de optimización que cubren la solución a cada situación planteada. La definición de la relación entre el problema y la técnica de solución aplicable se configura como el núcleo o la base de la propuesta para la selección de controles de seguridad utilizando técnicas de la IO, y permite simplificar de manera notable la labor del auditor.

5. **Evaluación de la metodología**.

   Este trabajo también presenta una evaluación de la propuesta, a través de la aplicación de UMAM. Este estudio empírico proporciona información relevante respecto de la adopción de la propuesta metodológica por un conjunto de asesores noveles en análisis de la seguridad de la información. En este sentido, se evidenció una tendencia hacia la adopción de la propuesta

por parte de los sujetos de estudio, constatándose que el modelo propuesto se percibe como una herramienta útil para realizar recomendaciones de inversión en seguridad. Sin embargo, también se evidenció que el diseño del modelo de optimización resulta complejo de estructurar para alguien que no tiene mayores conocimientos en dicha área.

6. **Herramienta informática para la selección de controles**.

   Otro aporte importante de esta tesis es el diseño e implementación de un prototipo de herramienta informática que soporta la propuesta de selección de controles propuesto. Esta herramienta apoya al usuario desde las etapas iniciales del proceso y soporta todas sus fases, desde desde el levantamiento de la información hasta la resolución del modelo de optimización.

   A través de esta herramienta se espera superar la dificultad de uso que plantea el enfoque metodológico a la hora del diseño del modelo de optimización que representa la problemática de la organización. Este problema fue puesto en evidencia durante la evaluación de la propuesta.

8.2 Conclusiones del trabajo

La SI ha cobrado una gran relevancia dentro del quehacer de las organizaciones. Durante este último tiempo se han reportado casos de graves vulneraciones que diversas organizaciones han sufrido en sus sistemas, lo que ha significado pérdidas de cientos de millones de dólares a la economía mundial.

Poco a poco, ha crecido a nivel mundial la conciencia del peligro latente que representa no considerar aspectos mínimos de SI dentro de sus procesos. La minimización del riesgo de ataques a través de la eliminación de las vulnerabilidades se ha tornado, en muchos casos, un objetivo prioritario de las organizaciones.

Esta necesidad es transversal al tipo de organización, ya sea una empresa privada o una organización gubernamental, una gran empresa o una pyme, ya que cualquiera se encuentra expuesta a ataques maliciosos que buscan sacar provecho de alguna vulnerabilidad. La multiplicidad de tipos de ataques que existen obliga a las organizaciones a tomar un conjunto de acciones que elimine cualquier tipo de vulnerabilidad que presente o minimice el impacto del ataque.

Esto implica que las organizaciones estén constantemente alerta, generando una defensa proactiva de sus activos de información. Una forma de protegerse es mediante la implementación de un conjunto de buenas prácticas en el quehacer de la organización, de tal manera que se minimicen las vulnerabilidades. En este sentido, los estándares de SI proponen ese conjunto de buenas prácticas de seguridad a través de la implementación de un SGSI. Las acciones propuestas por un estándar son transversales a la organización, afectando a la estructura organizacional de la misma, sus políticas, infraestructura tecnológica, Recursos Humanos y procesos, entre otras áreas.

Este amplio espectro de aplicación y las limitaciones de recursos complican la decisión respecto de la forma en que se debe implementar el SGSI. Si bien es cierto que el estándar es claro respecto de lo que se debe implementar a largo plazo, pueden existir diferencias respecto a qué es lo que se debe implementar en qué momento, ya que las organizaciones poseen características diferentes y distintas capacidades y recursos. Por tanto, la decisión respecto del avance en el logro del

estándar no es trivial, ya que debe considerar diversos aspectos de la organización, como es el riesgo, los costos, los tiempos de implementación, las priorizaciones y las políticas, entre otros.

Actualmente, las recomendaciones de avance son realizadas por expertos del área que presentan una gran experiencia en la implementación de un SGSI. Sin embargo, esta forma de actuar es subjetiva y no asegura una recomendación óptima, ya que no obedece a un proceso estandarizado, con pasos bien definidos y técnicas de apoyo probadas. Por tanto, aunque este tipo de recomendaciones pueden cumplir con los requerimientos y las características de las organizaciones, no optimizan la utilización de los recursos.

En este contexto, se torna relevante contar un apoyo para la toma de decisiones respecto del avance en el logro de un estándar. La multiplicidad de factores que involucra este proceso complica la resolución de la problemática. Elementos como el riesgo, el costo o el tiempo, entre otros, transforman este problema en un problema multiobjetivos sujeto a restricciones de recursos.

En este contexto, un enfoque metodológico como el propuesto en este trabajo, que defina un proceso sistemático y repetible, apoyado por técnicas matemáticas de modelación y resolución de problemas multiobjetivos, y soportado por herramientas informáticas, puede suponer un gran apoyo a la toma de decisiones, disminuyendo el tiempo de la decisión y aumentando la precisión de la recomendación desde la perspectiva de la optimización de los recursos

8.2.1 Conclusiones respecto de la propuesta

La investigación de la literatura evidenció que la selección de controles de seguridad mediante técnicas de optimización es un problema relevante para la comunidad, que ha generado diversos estudios al respecto. Sin embargo, los trabajos propuestos son limitados en su alcance, ya que resuelven el problema de la selección de controles pero no plantean la programación de la implementación de dichos controles. Además, de entre las propuestas encontradas, son pocas las que plantean la utilización de métodos cuantitativos. Por último, no se encontraron evidencias de herramientas informáticas que apoyen las propuestas.

Esta revisión permitió detectar oportunidades de investigación y de aporte en forma de enfoque metodológico que sistematice un proceso para la recomendación de la selección de controles de seguridad, utilizando métodos cuantitativos que incluyan la programación de los mismos y que, además, esté sustentado por una herramienta.

Así, la propuesta de este trabajo no solo categoriza los distintos tipos de escenarios que las organizaciones pueden considerar, desde las situaciones más simples de selección hasta la programación de éstos, sino que también asocia los escenarios con las diversas técnicas de optimización que pueden aplicarse en cada caso, simplificando así la labor del analista.

La propuesta divide el proceso en tres etapas: (i) Diagnóstico, (ii) Recomendación y (iii) Comunicación.

La etapa de diagnóstico permite levantar la información del estado actual de la organización, identificando las necesidades de la organización frente al logro de un estándar.

La etapa de recomendación es el núcleo de la propuesta, en la cual se identifica el problema, se modela y se resuelve. Es en esta etapa dónde se encuentran los mayores aportes de la propuesta. En primer lugar, este enfoque caracteriza un conjunto de escenarios en los cuales se identifican las variables que describen la situación de la organización y el objetivo que ésta espera lograr. La definición conceptual de la problemática nos ha permitido definir estas variables y la relación que existe entre ellas. Esta definición permite el modelado, en base a técnicas cuantitativas de optimización, del escenario que la organización desea alcanzar. La aplicación de estas técnicas nos permite objetivizar el proceso de selección, ya que disminuye la complejidad del problema, facilitando el actuar del asesor de seguridad, entregando recomendaciones sobre las cuales no se requiere realizar mayores análisis. Por último, la resolución del modelo se basa en técnicas de optimización y cuenta con el apoyo de herramientas informáticas especializadas, lo que implica que el usuario del enfoque no requiere de mayores conocimientos a este respecto.

La etapa de comunicación se refiere a la presentación de los resultados de la recomendación. Para esta etapa se recomienda seguir las indicaciones propuestas en el estándar ISO19011:2018 [53].

En resumen, la propuesta presentada en esta tesis define un proceso sistemático y cuantitativo que puede ser aplicado tanto por un novato como por un experto en seguridad. Además permite acortar el tiempo de la recomendación a segundos, frente a otros tipos de soluciones, tal como se muestra en [34]. Por último, se desarrolla el prototipo de una herramienta informática que automatiza gran parte del proceso propuesto. Esta herramienta facilita la aplicación del enfoque, lo que permite que prácticamente cualquier persona pueda involucrarse en el proceso.

Para ilustrar las capacidades de esta propuesta, se ha aplicado el modelo utilizando un conjunto real de controles provenientes de diversos estándares y/o guías de seguridad de la información. De lo observado, la literatura revisada ha mostrado soluciones hasta problemas del Tipo 3, de acuerdo a nuestra categorización. Con el fin de avanzar en esta línea, en esta tesis se ha presentado, bajo configuraciones reales de controles, una solución clasificada en el Tipo 4, lo que es un aporte en sí mismo. El caso de estudio desarrollado muestra que se pueden lograr reducciones en el tiempo y costo de los estudios sobre seguridad de la información, además de mostrar la precisión que se puede lograr en las recomendaciones de seguridad.

En términos generales, se ha demostrado que situaciones de gestión de la seguridad pueden ser enfocadas y solucionadas desde la perspectiva de la IO, a través de la aplicación de soluciones modernas de optimización. En consecuencia, es posible plantear que la gestión de la seguridad de la información no solo tiene una buena oportunidad para mejorar su enfoque incorporando la perspectiva de la IO, sino que la IO también tiene, en la gestión de la seguridad de la información, un dominio interesante para estudiar.

8.2.2 Conclusiones respecto de la evaluación

Para la evaluación de la propuesta se ha desarrollado y validado un modelo de adopción de métodos (UMAM) y su correspondiente cuestionario (UMAM-Q).

La evaluación de la propuesta ha permitido evidenciar, en un contexto académico, el impacto de ésta en un asesor de seguridad. A través de un estudio de adopción de métodos se logró determinar que existe una inclinación positiva por parte de los sujetos del estudio hacia la

utilización de este enfoque metodológico frente a la solución tradicional, basada en la interpretación de los estándares.

En general, los resultados de la experiencia por cada dimensión estudiada tienden hacia los extremos positivos de la escala. El análisis de los estadísticos descriptivos de cada dimensión evidencian que los sujetos estudio perciben el enfoque como un proceso útil y compatible con su forma de trabajar. Además, evidencian su predisposición a adoptar la propuesta en un futuro si tienen ocasión.

Por otro lado, el estudio también ha puesto en relieve las debilidades que presenta la propuesta. La principal debilidad, de acuerdo con lo expresado por los sujetos que participaron en el estudio, radica en la complejidad de modelación del escenario que representa la situación que la organización desea resolver. Este modelo debe realizarse en un lenguaje de optimización que, por lo general, no está en el dominio de conocimientos de un asesor de seguridad.

Fueron estas declaraciones las que sirvieron para decidir incluir como parte sustancial del proyecto de investigación una herramienta informática que permitiera automatizar, en la mayor medida posible, el modelamiento del escenario. Con la herramienta desarrollada, el asesor en seguridad solo necesita ingresar los parámetros y las características del tipo de problema que desea representar y resolver. Además, una vez obtenido el modelo, es la misma herramienta la que interactúa con un servicio web de resolución de problemas de optimización, proveyendo el modelo obtenido y recibiendo la respuesta del servicio. De esta manera, gran parte del proceso de modelación y resolución del problema de optimización es transparente para el asesor, lo que facilita su trabajo y lo libera para que pueda enfocarse en el análisis de la recomendación realizada.

Los resultados obtenidos en el análisis del modelo de regresión lineal, el análisis de los estadísticos descriptivos y el análisis cualitativo son consistentes, y apuntan en la misma dirección en cuanto a aspectos importantes para los sujetos y oportunidades de mejora. Sin embargo, es necesario reconocer algunas limitaciones del estudio realizado. Las más importantes son sin duda el tamaño del grupo y las características del mismo, lo que hace que haya que interpretar con mucho cuidado las conclusiones obtenidas.

Dicho esto, se debe consignar que la evaluación realizada era de tipo formativo y no sumativo, y que por tanto no tiene por objetivo estudiar un producto finalizado, sino que busca, al ser la primera aplicación del modelo, determinar un conjunto de percepciones que proporcione una serie de oportunidades de mejora, tanto sobre la propuesta como de su aplicación, para, tras una segunda iteración de mejora, realizar una posterior evaluación mucho más completa con asesores de seguridad con mayor experiencia.

8.2.3 Conclusiones respecto de la herramienta informática

La herramienta informática complementa el enfoque metodológico propuesto y se genera a partir de los análisis realizados sobre las respuestas de los sujetos del estudio de adopción de métodos. De este análisis se desprendió la necesidad de apoyar al usuario de la propuesta tanto en la modelación como en la resolución del modelo, dado el poco conocimiento de los sujetos en el campo de las técnicas de modelamiento y resolución de problemas de optimización. La aplicación desarrollada va un paso más allá y cubre todas las etapas de la propuesta metodológica, lo que dota de un apoyo aún mayor al asesor de seguridad

en la aplicación de la propuesta.

La herramienta facilita el diagnóstico de la situación actual de la organización, al apoyar el levantamiento de la información de la misma, a través de un cuestionario generado a partir de los estándares de seguridad ISO27001:2018, DS83 y GUI. Esto permite trazar una línea base de conformidad respecto del estándar, sobre la cual la organización puede configurar escenarios de avance y definir las necesidades de inversión en seguridad. La herramienta, además, genera el modelamiento de dichos escenarios, a través de los parámetros que el usuario le ingresa, tales como el tipo de problema a resolver, el riesgo, el costo o el beneficio, entre otros. A partir de estos parámetros, la herramienta modela el problema en el lenguaje de optimización GAMS y lo sube al servicio web de resolución de problemas de este tipo, NEOS-Server. Estas tareas permiten recibir la resolución del modelo de optimización para el posterior análisis del asesor de seguridad.

Esta automatización permite al experto abstraerse de la complejidad de la modelación y resolución del problema, y enfocar su esfuerzo en el análisis de la respuesta, donde se explicita la recomendación del conjunto de controles óptimo. Esto facilita la tarea del asesor y la aplicación del enfoque metodológico. De esta manera, se espera dar cuenta de las observaciones realizadas a la facilidad de Uso de la propuesta, disminuyendo la complejidad del proceso.

Aunque el impacto de la herramienta sobre la aplicación de la propuesta por parte del asesor aún no se ha evaluado experimentalmente, es posible estimar que la utilización de esta mejore el índice de facilidad de uso del modelo UMAM. Como consecuencia, se espera que la automatización de estos procesos del enfoque metodológico propuesto incremente la intención de adopción de los asesores de seguridad.

8.3 Trabajo futuro

Si bien es cierto que la propuesta presentada en este trabajo se ha definido en su totalidad, principalmente en su marco conceptual, no es menos cierto que, desde la práctica, se debe continuar trabajando para completar un proceso que sea 100 % aplicable. Por tanto, el trabajo futuro de la propuesta se centra en principalmente en este punto.

Se plantean como principales trabajos futuros los siguientes puntos:

- Tal como se ha planteado la propuesta, ésta abarca un conjunto de situaciones que describen los posibles escenarios sobre los cuales una organización podría querer avanzar. Sin embargo, se reconoce que este conjunto no es definitivo, sino que puede completarse a través de la identificación de nuevos escenarios particulares que las organizaciones quisieran ir incorporando al modelo.

  Por tanto, un camino a seguir es identificar, en conjunto con expertos de seguridad y/u organizaciones, enfoques adicionales a los ya propuestos, que permitan tanto identificar nuevos modos de completar y mejorar los presentados en este trabajo como identificar casos adicionales a los tipos ya reconocidos.

  Este trabajo se puede realizar a través de técnicas de recopilación de información como entrevistas o focus groups con expertos de seguridad, de tal manera que sea posible revisar los escenarios propuestos e identificar escenarios que no hayan sido contemplados. Con esta información, se puede realizar una nueva consulta a la literatura, para identificar aquellas técnicas o modelos de optimización que permitirían solucionar los nuevos escenarios

planteados.

- Otro camino de investigación tiene relación con la conceptualización del ámbito de la seguridad de la información, en el sentido de identificar las variables que interactúan en este ámbito y la relaciones que existen entre ellas.

  En este trabajo presentamos un marco conceptual que integra un conjunto de visiones del problema. Sin embargo, se cree que es posible expandirlo para considerar nuevas variables o relaciones que no fueron identificadas en esta propuesta.

  Para esta identificación se pueden utilizar las mismas técnicas que para el punto anterior, como son entrevistas o focus groups con expertos de seguridad.

- La tercera línea de investigación que ha abierto esta tesis se centra en el avance en el desarrollo de la herramienta que da soporte a la propuesta, de forma que sea mucho más robusta que en la actualidad. Se espera que, una vez se hayan incluido todos los tipos de problema y los servicios de optimización, esta herramienta sea capaz de guiar las decisiones de SI de los asesores de seguridad en las organizaciones.

  El desarrollo futuro de esta herramienta se considera desde la perspectiva de sistemas inteligentes, de tal manera que el recomendador, que es lo que se ha presentado hasta el momento, se transforme en un asistente del experto en seguridad, capaz de apoyarlo en la toma de decisiones y de guiar la creación y

resolución de escenarios que no se hayan contemplado desde un inicio. En otras palabras, se espera que el sistema pueda asistir al usuario en la creación de sus propios modelos que representan la realidad de la organización, aunque esos casos no estén considerados en la base de la aplicación.

8.4 Principales publicaciones

Como parte de la etapa de comunicación propuesta como parte del paradigma Design Science, se puede mencionar un conjunto de 9 publicaciones, que tributan a la temática de este trabajo. Estas publicaciones dan cuenta de los avances y resultados de las distintas fases del presente trabajo de investigación. Estos artículos son: una publicación en una revista internacional (JCR Q2), una revista internacional no JCR (indexación SCOPUS), 5 congresos internacionales (3 con indexación SCOPUS y WoS CPCI, y uno de ellos considerado el mejor artículo de la conferencia) y 2 congresos nacionales (1 con indexación SCOPUS-IEEE).

A continuación se presentan las contribuciones mencionadas, junto con el resumen de cada una de ellas y su principal aportación en relación a esta tesis.

8.4.1 Artículo revista internacional JCR

Diéguez, M., Bustos, J., & Cares, C. (2020). Mapping the variations for implementing information security controls to their operational research solutions. Information Systems and e-Business Management,

18(2), 157–186.

Electronic version ISSN 1617-9854
DOI: 10.1007/s10257-020-00470-8
Journal Impact Factor 2020: 5.073

Abstract. Information Security Management is currently guided by process-based standards. Achieving one or some of these standards means deploying their corresponding set of security controls under different constraints on resources, budgets, information assets to protect, and risks to avoid or mitigate, among other factors. This constitutes a complex combinatorial problem in the decision-making process. To select, schedule and deploy these security controls, qualitative approaches have mainly been proposed. Quantitative approaches to information security management are just emerging, and they have been applied only to simplified theoretical cases. The purpose of this paper is to support the notion that the problems of implementing information security controls, in the sense of being put into effect, can be formulated as a family of existing and already solved optimization problems. The main result is a mapping from a set of seven information security management types of problems to their corresponding operational research formulations. A solved case from a governmental institution illustrates the use of the proposed map.

Principales contribuciones. Este artículo condensa la mayor parte de las contribuciones de este proyecto de investigación. En primer lugar se presenta el problema de la selección de ISC y se propone la formulación como un problema de optimización en base a las técnicas y modelos de la IO. El artículo presenta una revisión bibliográfica, basada en un protocolo de mapeo sistemático, donde se clasifican los distintos trabajos encontrados. Se concluye que existen oportunidades de investigación, ya que existen pocos trabajos que se desarrollen en el

ámbito de esta propuesta. Además, se presenta el modelo conceptual que se ha desarrollado en proyecto y que se utiliza como base para la modelación del problema de optimización. También detalla la categorización de los escenarios o tipos de problemas de optimización que se pudieran presentar en las organizaciones, describiendo cada categoría y proponiendo técnicas de modelación y resolución del problema para cada caso. Para ilustrar la propuesta se presenta un caso de estudio con características distintas a las de los casos propuestos en la bibliografía consultada, y se modela y resuelve el problema de optimización en base a las técnicas propuestas en la categorización. Por último, se analizan los resultados obtenidos y se destacan las bondades de la propuesta.

8.4.2 Artículo revista internacional No JCR

Diéguez, M., & Cares, C. (2019). Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (32), 113–128.

Electronic version ISSN 1646-9895
DOI: 10.17013/risti.32.113-128

Resumen. Proporcionar procesos y herramientas sistemáticos para tomar una decisión sobre inversiones en seguridad en un escenario con restricciones presupuestarias, es de suma importancia para asegurar que dichas decisiones se tomen adecuadamente. Presentamos un enfoque de programación de conjunto de respuestas (ASP) para resolver este problema. Nuestra propuesta se compara con el desarrollo del problema utilizando programación lineal (PL). Ilustramos la fase de modelado y el rendimiento computacional de ambas soluciones. El

modelo ASP presenta tiempos de resolución del tipo exponencial a medida que aumenta el número de controles sobre los que debe decidirse. Por otro lado, el modelo basado en PL no presenta variaciones importantes en sus tiempos de resolución de problemas. Sin embargo, el problema es más fácil de modelar en ASP. Luego, esta propuesta tiene ventajas para modelar y resolver problemas específicos en los que se requiere una respuesta rápida con una baja cantidad de controles.

Principales contribuciones. Este artículo presenta la comparación del desempeño de dos métodos cuantitativos de resolución de un problema de optimización. El primer método, denominado Answer Set Solution, es una solución que se basa en la programación lógica y la satisfacción de restricciones para hacer frente principalmente a problemas difíciles de decisión. El segundo método es una técnica clásica de IO, denominada Programación Lineal. De esta comparación se evidenció la mejor eficiencia de la Programación Lineal sobre Answer Set Solutions, reflejada en el tiempo de resolución del problema y en las capacidades de cómputo requeridas. Esta comparación es útil para la investigación, ya que respalda la decisión de utilizar métodos y técnica de la IO sobre otros métodos.

8.4.3 Artículos congresos internacionales

Artículo 1

Diéguez, M., Sepúlveda, S., & Cares, C. (2012). On Optimizing the Path to Information Security Compliance. In Procedings of Eighth International Conference on the Quality of Information and Communications Technology. pp 182-185. Lisboa, Portugal.

DOI: 10.1109/quatic.2012.44

Abstract. Information Security Management has been contemporarily confronted by standards covering business aspects related to Information Technology. Different standards map the problem of information security to a set of controls that represent safeguards for different security vulnerabilities. Several procedure-oriented maturity models have been proposed for managing the progress on information security; however, few approaches use quantitative techniques for analyzing the progress on information security. In this paper we propose that the problem of becoming security compliance can be analyzed as a problem of multi-paths where checking different controls means choosing different ways of reaching a security compliance. We identify a set of concepts from security ontologies in order to identify a set of variables influencing these paths. The main contribution is formulating the problem of reaching some standard compliance in the shape of optimization problems, thus existing optimization techniques can be applicable.

Principales contribuciones. Este artículo presenta por primera vez, y de manera general, el problema de la selección de ISC y la propuesta de enfrentar esta situación utilizando métodos de la IO. Aquí se justifica la problemática y se realiza una búsqueda bibliográfica de propuesta de solución presentes en la comunidad. Además, presenta una primera versión del marco conceptual requerido para modelar el problema y presenta un ejemplo de aplicación de solución a un caso particular.

Artículo 2

Diéguez, M., Sepúlveda, S., & Cachero, C. (2012). UMAM-Q: An instrument to assess the intention to use software development methodologies. In Procedings of 7th Iberian Conference on Information Systems and Technologies (CISTI 2012), 2012, pp. 1-6. Madrid, España.

Abstract. The Software Engineering discipline has devoted much effort to the definition of new methods and paradigms that, even if empirically proven to provide certain gains in terms of process productivity and product quality, are difficult to transfer to industry. We claim that this fact is largely due to methodologists not taking into account the - largely subjective - set of variables that influence innovation adoption, together with its tailoring and operationalization to the particulars of software methodologies: we lack reliable and valid measurement instruments that allow for the early detection of methodologies weaknesses with respect to their ability to catch among practitioners. This paper reports on the development of one such instrument designed to measure the various perceptions that an individual may have with respect to adopting a software development methodology innovation. Our questionnaire is aimed at allowing methodologists not only to compare their methodologies with respect to others - in terms of variables such as ease of use, usefulness or compatibility - but also to avoid well-known mistakes such as forcing - as opposed to convincing - method adoption in organizations.

Principales contribuciones. Este artículo es importante para esta tesis porque es aquí donde se presenta el modelo UMAM y la validación del cuestionario UMAM-Q, que han sido utilizados en este proyecto de investigación para realizar la evaluación de la propuesta del enfoque metodológico. En este artículo se justifica la necesidad de crear el modelo UMAM, se presenta el diseño del modelo y el instru-

mento de evaluación (Cuestionario UMAM-Q). Por último, se realiza una validación del cuestionario, a través de un quasi-experimento y una evaluación estadística. De esta evaluación, se concluyó la pertinencia de utilizar tanto el modelo como el cuestionario para predecir el nivel de adopción de métodos en Ingeniería del Software.

Artículo 3

Diéguez, M., & Cares, C. (2017). Modelos de anticipación (antimodelos) para una ciberdefensa proactiva. In Procedings of IX Congreso Internacional de Computación y Telecomunicaciones, COMTEL 2017. Lima, Perú.

Resumen. Los principios y vocabulario de la defensa se han llevado a la ciberdefensa y hoy se entiende por ciberdefensa proactiva a la capacidad de los sistemas de software para adelantarse a los posibles tipos de ataques y amenazas y tomar los resguardos y las precauciones correspondientes. Sin embargo, poco se ha difundido de los modelos que permiten el diseño de los sistemas de software que implementen una ciberdefensa proactiva. Con este objetivo se introdujo, a inicios de este siglo, el concepto de antimodelo como aquel tipo de modelo que considera amenazas a su funcionamiento. En este artículo presentamos una recopilación de tres tipos de antimodelos y mostramos cómo existe un espacio de investigación aún abierto en aspectos de modelado no cubiertos por la ciberdefensa, para estos modelos revisamos un conjunto de vulnerabilidades y delineamos las principales características que debieran considerarse en sus antimodelos correspondientes.

Principales contribuciones. Este artículo presenta una enfoque alternativo al modelo presentado en este trabajo para la protección de los activos de información de una organización. Esta propuesta radica

en la modelación de los requisitos de seguridad, previo a la implementación de los sistemas. Este enfoque es diferente al de esta investigación, que plantea la incorporación de buenas prácticas en la utilización del sistema de gestión ya implementado. El artículo presenta un enfoque proactivo de defensa a través de los denominados antimodelos, que son modelos que buscan anticipar el comportamiento de los atacantes del sistema, para así definir cuál debe ser el comportamiento del mismo frente a dichos ataques. Del artículo se desprende que los dos enfoques no son puntos de vistas antagonistas, sino que pueden ser complementarios. Además, este artículo permitió evidenciar la necesidad de continuar con este enfoque basado en la aplicación de buenas prácticas para operar correctamente el sistema de gestión.

Artículo 4

Dieguez, M., Cares, C., & Cachero, C. (2017). Methodology for the information security controls selection. In Procedings of 12th Iberian Conference on Information Systems and Technologies (CISTI).

DOI:10.23919/cisti.2017.7975811

Abstract. Managing Information Security controls is not an easy process, since it must be adjusted to the characteristics of each organization. Currently, much of the process relies on the experience of experts, that is, in qualitative methods. However, we believe it is possible to incorporate quantitative methods that support the security adviser in its recommendations. We plan to study the techniques and methodologies of Operations Research, used in solving optimization problems. We hope that with the incorporation of these techniques, we will obtain advantages of precision, cost and time, in the security advisor's recommendation, to what is achieved today with the tradi-

tional forms.

Principales contribuciones. Este artículo fue presentado en el simposio doctoral del 12th Iberian Conference on Information Systems and Technologies, y detalla el proyecto de tesis presentado en este documento. En él se presenta el problema a resolver, los objetivos del proyecto de tesis, el método de investigación a utilizar para desarrollar el proyecto y las principales características del enfoque metodológico propuesto como solución.

Artículo 5

Cares, C., & Diéguez, M. (2017). An Answer Set Solution for Information Security Management. In proceedings of the Eighth International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking (pp. 11-15). Athens, Greece.

Electronic version ISSN 2308-4170
ISBN: 978-1-61208-535-7
Best Paper Award de la conferencia

Abstract. Information Security Management is focused on processes and it is currently guided by control-based standards such as ISO27002. Controls may be: management objectives, available resources or desired behaviours that contribute to information security. Under this process perspective, to reach some security level means to accomplish a specific set of controls. There are qualitative approaches and maturity models that help managers to select what controls to implement next, whilst quantitative approaches have just recently emerged under simplified formulations. The purpose of this paper is to show an answer set solution to the problem of selecting what con-

trols to implement next, based on a given budget, security profit, and temporal dependencies between controls. The solution is illustrated by using Clingo.

Principales contribuciones. Este artículo presenta una técnica alternativa para la modelación y resolución del problema de la selección de ISC. Si bien este artículo mantiene la idea de plantear la problemática como un problema de optimización, se recurre a la programación declarativa para formular el modelo de decisión. En el artículo se presenta el problema y la formulación general. Además, se desarrolla un caso de ejemplo para mostrar el funcionamiento de la técnica. Este artículo obtuvo el Best Paper Award de la conferencia.

8.4.4 Artículos congresos nacionales

Artículo 1

Diéguez, M. (2013). Optimización de la ruta de cumplimiento de un estándar de Seguridad de la Información. In proceedings of the V International Workshop on Advanced Software Engineering - IWASE, Jornadas Chilenas de la Computación. Temuco, Chile.

Resumen. La Gestión de Seguridad de la Información dentro de una organización es confrontada con los estándares que la regulan, pero pocos enfoques utilizan técnicas cuantitativas para el análisis de la planificación del logro de los controles de la norma. De acuerdo a esto, proponemos que el problema de lograr el cumplimiento de un estándar, puede ser analizado como un problema de múltiples rutas de progreso para llegar a una conformidad con el estándar. En otras palabras, se puede modelar la ruta de acciones a ejecutar para lograr la conformidad, como un problema de optimización, por lo tanto se puede

aplicar alguna técnica cuantitativa para encontrar esta ruta óptima, en particular, técnicas provenientes de la disciplina de la Investigación de Operaciones. En este trabajo se muestra los avances en la investigación de este problema, la cual busca aplicar técnicas cuantitativas en la selección de los controles de seguridad a implementar y en la planificación de la ruta de implementación.

Principales contribuciones. Este artículo presenta la descripción del problema de la selección de ISC y la justificación de la utilización de modelos de optimización de IO como solución a la problemática. Además, se presenta una primera propuesta de clasificación de escenarios o tipos de problemas, la descripción de cada categoría y una propuesta de técnica de IO aplicable en cada caso.

Artículo 2

Valenzuela-Toledo, P., Cares, C., & Diéguez, M. (2019). Search Based Risk Reduction Supporting the Intelligent Components Selection Process. In proceedings of the 2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). Valparaíso, Chile.

Abstract. In Component-Based Software Engineering, the problem of selecting software components involve several risk factors. Traditionally, these have been identified and mitigated using software project management techniques. However, the new demand for intelligent components has added complexity to the process. Despite the success and technological advances, its development in an environment ready for production faces many challenges. There are numbers of technical issues that limit their adoption and selection, due to the introduction of new risk factors, different from traditional ones. Thus,

our goal is to formulate a technique to minimize the risk in the intelligent component selection process. To achieve this goal, first, we review the literature to figure out how software project management takes care of the risk and to identify and classify the risks factor associated with intelligent software components. Second, we formulate the component selection problem as a search based optimization problem. And Third, we illustrate our proposal by presenting an example in the context of an air pollution forecasting component. As a result, we were able to: (1) identify a lack of useful tools to manage the risk factor effectively in a software project; (2) we classify intelligent component associated risk; and (3) we introduce a risk management technique that supports the component selection process by maximizing requirement accomplishment, that is, minimizing the risk of the provision of the functionalities that satisfy the requirements. Overall, our work is an initial step in using search-based optimization in risk management to the component selection process.

Principales contribuciones. Este artículo presenta la aplicación de las técnicas propuestas al problema de selección de ISC, pero sobre un problema de decisión distinto a la SI. En particular, el artículo presenta la problemática de la selección de componentes de software que minimiza el riesgo asociado al proyecto de desarrollo de software. En el trabajo se describe la problemática y se formula el problema de búsqueda como un problema de optimización, se modela y se resuelve la situación utilizando técnicas de IO.

8.5 Otros Artículos

En esta sección se presenta un conjunto de 13 publicaciones adicionales, desarrollados en líneas de investigación distintas a la presentada en

este trabajo, ya sea como autor principal o colaborador con otros investigadores. Estos artículos pertenecen a los ámbitos de la Formación en Ingeniería Informática (8 artículos, divididos en 1 revista internacional no JCR, 3 congresos internacionales y 4 congresos nacionales) y la Ingeniería de Software (5 publicaciones, divididos en 1 revista internacional JCR, 2 congresos internacionales y 2 congresos nacionales). Además, cabe destacar que uno de los artículos presentados a conferencias internacionales recibió el Best Pape Award de la conferencia.

8.5.1 Artículos en la línea de Formación en Ingeniería Informática

Revista Internacional no JCR

Vidal, E., Gacitúa, R., & Diéguez, M. (2020). Desarrollando de habilidades blandas en etapas tempranas en la formación de Ingenieros de Software. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (28), 423–436.

Congresos Internacionales

Vidal, E., Gacitúa, R., Diéguez, M., & Cachero, C., (2019). Correspondence analysis between programming teaching approaches. In proceedings of the XIV Jornadas Iberoamericanas de Ingenieria de Software e Ingenieria del Conocimiento. pp. 177-188.

Diéguez, M., Gacitúa, R., & Vidal, E. (2018). Evaluating the impact of training software engineers using the R&G methodology. In proceedings of the JIISIC 2018-Jornadas Iberoamericanas de Ingeniería de

Software e Ingeniería del Conocimiento, pp. 185-196.

Cachero, C., Diéguez, M., Pérez, C., & Meliá, S. (2012). Influence of software engineering courses on intention to adopt software methods. In EDULEARN12 Proceedings. pp. 5844-5852. IATED.

Congresos Nacionales

Sepúlveda, S., & Diéguez, M. (2020). EM-(RA)2: a tool support proposal for Learning Outcomes and the Teaching-Learning Process. 2020 39th International Conference of the Chilean Computer Science Society (SCCC).
doi:10.1109/sccc51225.2020.9281186

Gacitúa, R., Diéguez, M., Díaz, J., & Sepúlveda, S. (2019). A flexible and systematic teaching framework to develop cognitive skills through programming courses. 2019 38th International Conference of the Chilean Computer Science Society (SCCC).
doi:10.1109/sccc49216.2019.8966409

Sepúlveda, S., & Diéguez, M. (2019). Learning Outcomes and the Teaching-Learning Process: A proposal. 2019 38th International Conference of the Chilean Computer Science Society (SCCC).
doi:10.1109/sccc49216.2019.8966404

Gacitúa, R., Diéguez, M., & Vidal, E. (2017). Forming software architects in early stages: From craft to engineering. 2017 36th International Conference of the Chilean Computer Science Society (SCCC).
doi:10.1109/sccc.2017.8405130

8.5.2 Artículos en la línea de Ingeniería de Software

Revista Internacional JCR

En proceso de publicación.
Hochstetter, J., Díaz, J., Diéguez, M., Espinosa, R., Arango-López, J., & Cares, C. (2021). Assessing Transparency in eGovernment Electronic Processes. in IEEE Access.
doi: 10.1109/ACCESS.2021.3059866.

Congresos Internacionales

Hochstetter, J., Díaz, C., Diéguez, M., & Díaz, J. (2021). Proposal for a Classifier for Public Tenders for Software Based on Standard IEEE830. Cloud Computing, Big Data & Emerging Topics, 73–88.
doi:10.1007/978-3-030-84825-5_6

Toala, G., Diéguez, M., Cachero, C., & Meliá, S. (2018). Evaluating the Impact of Developers' Personality on the Intention to Adopt Model-Driven Web Engineering Approaches: An Observational Study.International Conference on Web Engineering, 3–16.
doi:10.1007/978-3-319-91662-0_1
Best Paper Award de la conferencia.

Congresos Nacionales

Diéguez, M., & Cares, C. (2011). Composabilidad de Arquitecturas: Hacia un Modelo de Calidad. In proceedings of the V International Workshop on Advanced Software Engineering - IWASE, Jornadas Chilenas de la Computación. Curicó, Chile.

Diéguez, M., Sepúlveda, S., & Hochstetter, J. (2009). Propuestas de Integración de Sistemas de Gestión Pública. CEUR Workshop Proceedings, Workshop Internacional 3er Encuentro de Informática y Gestión. Temuco, Chile.

Bibliografía

[1] R. Agarwal and J. Prasad. A field study of the adoption of software process innovations by information systems professionals. *IEEE Transactions on Engineering Management*, 47(3):295–308, 2000.

[2] Sahar Al-Dhahri, Manar Al-Sarti, and A Abdul. Information security management system. *International Journal of Computer Applications*, 158(7):29–33, 2017.

[3] Nadher Al-Safwani, Suhaidi Hassan, and Norliza Katuk. A multiple attribute decision making for improving information security control assessment. *International Journal of Computer Applications*, 89(3):19–24, 2014.

[4] Christopher J. Alberts and Audrey J. Dorofee. OCTAVE method implementation guide version 2.0. volume 1: Introduction. Technical report, jun 2001.

[5] Ali Allahverdi. The third comprehensive survey on scheduling problems with setup times/costs. *European Journal of Operational Research*, 246(2):345–378, oct 2015.

[6] Luís Almeida and Ana Respício. Decision support for selecting information security controls. *Journal of Decision Systems*, 27(sup1):173–180, may 2018.

[7] Adel Alshamrani and Abdullah Bahattab. A comparison between three sdlc models waterfall model, spiral model, and in-

cremental/iterative model. *International Journal of Computer Science Issues (IJCSI)*, 12(1):106, 2015.

[8] Daniel Bachlechner, Ronald Maier, Frank Innerhofer-Oberperfler, and Lukas Demetz. Understanding the management of information security controls in practice. In *9th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th -7th December, 2011*, 2011.

[9] Wade Baker and Linda Wallace. Is information security under control?: Investigating quality in information security management. *IEEE Security and Privacy Magazine*, 5(1):36–44, jan 2007.

[10] David Basin, Jürgen Doser, and Torsten Lodderstedt. Model driven security for process-oriented systems. In *Proceedings of the eighth ACM symposium on Access control models and technologies - SACMAT 03*. ACM Press, 2003.

[11] David Basin, Jürgen Doser, and Torsten Lodderstedt. Model driven security. *ACM Transactions on Software Engineering and Methodology*, 15(1):39–91, jan 2006.

[12] Y. Benslimane, Z. Yang, and B. Bahli. Information security between standards, certifications and technologies: An empirical study. In *2016 International Conference on Information Science and Security (ICISS)*. IEEE, dec 2016.

[13] Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti. Using cp-nets as a guide for countermeasure selection. In *Proceedings of the 2007 ACM Symposium on Applied Computing*, SAC '07, pages 300–304, New York, NY, USA, 2007. ACM.

[14] Carlos Blanco, Joaquín Lasheras, Eduardo Fernández-Medina, Rafael Valencia-García, and Ambrosio Toval. Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards & Interfaces*, 33(4):372–388, jun 2011.

[15] Rok Bojanc and Borka Jerman-Blažič. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413–422, 2008.

[16] R. Bonazzi, L. Hussami, and Y. Pigneur. Compliance management is becoming a major issue in IS design. In *Information Systems: People, Organizations, Institutions, and Technologies*, pages 391–398. Physica-Verlag HD, 2009.

[17] Jakub Breier. Security evaluation model based on the score of security mechanisms. *Information Sciences and Technologies*, 6(1):19–27, 2014.

[18] Jakub Breier and Ladislav Hudec. New approach in information system security evaluation. In *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, pages 1–6. IEEE, oct 2012.

[19] Jakub Breier and Ladislav Hudec. On identifying proper security mechanisms. In *Lecture Notes in Computer Science*, pages 285–294. Springer Berlin Heidelberg, 2013.

[20] Jakub Breier and Ladislav Hudec. On selecting critical security controls. In *2013 International Conference on Availability, Reliability and Security*, pages 582–588. IEEE, sep 2013.

[21] David Budgen, Mark Turner, Pearl Brereton, and Barbara A Kitchenham. Using mapping studies in software engineering. In *Ppig*, volume 8, pages 195–204, 2008.

[22] Edmund K Burke, Edmund K Burke, Graham Kendall, and Graham Kendall. *Search methodologies: introductory tutorials in optimization and decision support techniques*. Springer, 2014.

[23] Tom Butler and Damien McGovern. A conceptual model and IS framework for the design and adoption of environmental compliance management systems. *Information Systems Frontiers*, 14(2):221–235, jul 2009.

[24] José A. Caballero and Ignacio E. Grossmann. Una revisión del estado del arte en optimización. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, 4(1):5–23, jan 2007.

[25] Jordi Cabot and Martin Gogolla. Object constraint language (OCL): a definitive guide. In *Formal methods for model-driven engineering*, pages 58–90. Springer, 2012.

[26] Jiaqiong Chen and Ronald G. Askin. Project selection, scheduling and resource allocation with time dependent returns. *European Journal of Operational Research*, 193(1):23–34, feb 2009.

[27] Lin Chen, Li Li, Yong Hu, and Ke Lian. Information security solution decision-making based on entropy weight and gray situation decision. In *2009 Fifth International Conference on Information Assurance and Security*. IEEE, 2009.

[28] T.C.E. Cheng, C.T. Ng, J.J. Yuan, and Z.H. Liu. Single machine scheduling to minimize total weighted tardiness. *European Journal of Operational Research*, 165(2):423–443, sep 2005.

[29] Kim Kwang Choo, Sameera Mubarak, Deepa Mani, et al. Selection of information security controls based on ahp and gra. Pacific Asia Conference on Information Systems, 2014.

[30] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1):37–46, apr 1960.

[31] Xu Cuihua and Lin Jiajun. An information system security evaluation model based on AHP and GRAP. In *2009 International Conference on Web Information Systems and Mining*, pages 493–496. IEEE, nov 2009.

[32] Adiel Teixeira de Almeida and Marina D.O. Duarte. A multicriteria decision model for selecting project portfolio with consideration being given to a new concept for synergies. *Pesquisa Operacional*, 31(2):301–318, aug 2011.

[33] Secretariat General de la Defense Nationale. Ebios: Expression of needs and identification of security objectives, 2005.

[34] Mauricio Diéguez, , and Carlos Cares and. Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (32):113–128, jun 2019.

[35] Mauricio Diéguez, Jaime Bustos, and Carlos Cares. Mapping the variations for implementing information security controls to their operational research solutions. *Information Systems and e-Business Management*, 18(2):157–186, apr 2020.

[36] Rainer Diesch, Matthias Pfaff, and Helmut Krcmar. A comprehensive model of information security factors for decision-makers. *Computers Security*, 92:101747, 2020.

[37] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 04(02):92–100, 2013.

[38] Mauricio Diéguez, Samuel Sepúlveda, and Cristina Cachero. Umam-q: An instrument to assess the intention to use software development methodologies. In *7th Iberian Conference on Information Systems and Technologies (CISTI 2012)*, pages 1–6, 2012.

[39] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering*, pages 289–306. Springer Berlin Heidelberg, 2010.

[40] Steve Easterbrook, Janice Singer, Margaret-Anne Storey, and Daniela Damian. Selecting empirical methods for software engineering research. In *Guide to Advanced Empirical Software Engineering*, pages 285–311. Springer London, 2008.

[41] Emrah B. Edis, Ceyda Oguz, and Irem Ozkarahan. Parallel machine scheduling with additional resources: Notation, classification, models and solution methods. *European Journal of Operational Research*, 230(3):449–463, nov 2013.

[42] Jens Egeblad and David Pisinger. Heuristic approaches for the two- and three-dimensional knapsack packing problem. *Computers & Operations Research*, 36(4):1026–1049, apr 2009.

[43] Abdel Ejnioui, Angel R Otero, G Tejay, CE Otero, and AA Qureshi. A multi-attribute evaluation of information security controls in organizations using grey systems theory. In *Proceedings of the International Conference on Security and Management (SAM)*, pages 1–7. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[44] S Yu Eric. Social modeling and i. In *Conceptual Modeling: Foundations and Applications*, pages 99–121. Springer, 2009.

[45] Daniel Espinoza, Marcos Goycoolea, and Eduardo Moreno. The precedence constrained knapsack problem: Separating maximally violated inequalities. *Discrete Applied Mathematics*, 194:65–80, oct 2015.

[46] James P. Farwell and Rafal Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, jan 2011.

[47] Stefan Fenz and Andreas Ekelhart. Formalizing information security knowledge. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS 09*. ACM Press, 2009.

[48] Stefan Fenz and Andreas Ekelhart. Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy Magazine*, 9(2):58–65, mar 2011.

[49] Kostas Florios, George Mavrotas, and Danae Diakoulaki. Solving multiobjective, multiconstraint knapsack problems using mathematical programming and evolutionary algorithms. *European Journal of Operational Research*, 203(1):14–21, may 2010.

[50] International Organization for Standardization. Iso/iec guide 73:2009 - risk management – vocabulary. `https://www.iso.org/standard/44651.html`, 2009. 2018-10-20.

[51] International Organization for Standardization. Iso/iec 27001:2013 - information security management. `http://www.iso.org/iso/home/standards/management-standards/iso27001.htm`, 2013. 2018-10-20.

[52] International Organization for Standardization. Iso/iec 27002:2013 - information technology – security techniques – code of practice for information security controls. http://www.iso.org/iso/catalogue_detail?csnumber=54533, 2013. 2017-12-20.

[53] International Organization for Standardization. Iso/iec 19011:2018 - guidelines for auditing managementsystems. https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es, 2018. 2021-01-15.

[54] L. Alberto Franco and Raimo P. Hämäläinen. Behavioural operational research: Returning to the roots of the OR profession. *European Journal of Operational Research*, 249(3):791–795, mar 2016.

[55] gams Development Corporation. General algebraic modeling system. http://www.gams.com/, 2017.

[56] Cuixia Gao, Zhitang Li, and Haigang Song. Security evaluation method based on host resource availability. In *2009 Third International Conference on Multimedia and Ubiquitous Engineering*, pages 499–504. IEEE, jun 2009.

[57] Paul R Garvey. *Analytical methods for risk management: A systems engineering perspective*. Chapman and Hall/CRC, 2008.

[58] S. I. Gass and Thomas L. Saaty. Parametric objective function (part 2)—generalization. *Journal of the Operations Research Society of America*, 3(4):395–401, nov 1955.

[59] Neil Geismar. *Single Machine Scheduling*. American Cancer Society, 2011.

[60] Taha Ghasemi and Mohammadreza Razzazi. Development of core to solve the multidimensional multiple-choice knapsack problem. *Computers & Industrial Engineering*, 60(2):349–360, mar 2011.

[61] Shahram Gilaninia, Seyyed Javad Mousavian, Orang Taheri, Hamid Nikzad, Hoda Mousavi, and Fatemeh Zadbagher Seighalani. Information security management on performance of information systems management. *Journal of Basic and Applied Scientific Research, J. Basic. Appl. Sci. Res*, 2(3):2582–2588, 2012.

[62] de Chile Gobierno. Decreto 83: Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos. `http://www.leychile.cl/Navegar?idNorma=234598`, 2017.

[63] de Chile Gobierno. Programa de mejoramiento de la gestión sistema de seguridad de la información: Versión 2011. `http://www.dipres.gob.cl/594/w3-propertyvalue-16887.html`, 2017.

[64] Giancarlo Guizzardi, Heinrich Herre, and Gerd Wagner. Towards ontological foundations for UML conceptual models. In *On the Move to Meaningful Internet Systems 2002: CoopIS, DOA, and ODBASE*, pages 1100–1117. Springer Berlin Heidelberg, 2002.

[65] Sönke Hartmann and Dirk Briskorn. A survey of variants and extensions of the resource-constrained project scheduling problem. *European Journal of Operational Research*, 207(1):1–14, nov 2010.

[66] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, apr 2009.

[67] Willy Herroelen and Roel Leus. Project scheduling under uncertainty: Survey and research potentials. *European Journal of Operational Research*, 165(2):289–306, sep 2005.

[68] Alan Hevner and Samir Chatterjee. Design science research in information systems. In *Integrated Series in Information Systems*, pages 9–22. Springer US, 2010.

[69] Han Hoogeveen. Multicriteria scheduling. *European Journal of Operational Research*, 167(3):592–623, dec 2005.

[70] PJ Huber and EM Ronchetti. Robust statistics, ser. *Wiley Series in Probability and Mathematical Statistics. New York, NY, USA, Wiley-IEEE*, 52:54, 1981.

[71] Edward Humphreys. Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4):247–255, nov 2008.

[72] Edward Humphreys. Information security management system standards. *Datenschutz und Datensicherheit - DuD*, 35(1):7–11, jan 2011.

[73] ISACA. Control objectives for information and related technologies (cobit). `http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx`, 2017. 2018-12-20.

[74] Stacy L. Janak, Xiaoxia Lin, and Christodoulos A. Floudas. A new robust optimization approach for scheduling under uncertainty. *Computers & Chemical Engineering*, 31(3):171–195, jan 2007.

[75] Ritsuko Kawasaki and Takeshi Hiromatsu. Proposal of a model supporting decision-making on information security risk treat-

ment. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 8(4):583–589, 2014.

[76] Yau Hon Keung. Information security controls. *Advances in Robotics & Automation*, 03(02), 2013.

[77] Hamid Khajouei, Mehdi Kazemi, and Seyed Hamed Moosavirad. Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and e-Business Management*, 15(1):1–19, feb 2016.

[78] Naurin Farooq Khan and Naveed Ikram. Security requirements engineering: A systematic mapping (2010-2015). In *2016 International Conference on Software Security and Assurance (ICSSA)*. IEEE, aug 2016.

[79] E. Kiesling, C. Strausss, and C. Stummer. A multi-objective decision support framework for simulation-based security control selection. In *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, aug 2012.

[80] Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christine Strauß, and Christian Stummer. Simulation-based optimization of it security controls: Initial experiences with meta-heuristic solution procedures. In *Proceedings of the workshop of the EURO working group on metaheuristics*, pages 18–20, 2013.

[81] Elmar Kiesling, Christine Strauss, Andreas Ekelhart, Bernhard Grill, and Christian Stummer. Simulation-based optimization of information security controls: An adversary-centric approach. In *2013 Winter Simulations Conference (WSC)*, pages 2054–2065. IEEE, dec 2013.

[82] Kevin W Knight et al. As/nzs iso 31000: 2009-the new standard for managing risk. *Keeping good companies*, 62(2):68, 2010.

[83] Rainer Kolisch and Konrad Meyer. Selection and scheduling of pharmaceutical research projects. In *Perspectives in Modern Project Scheduling*, pages 321–344. Springer US.

[84] Ella Kolkowska and Gurpreet Dhillon. Organizational power and information security rule compliance. *Computers & Security*, 33:3–11, mar 2013.

[85] Stavros G. Kolliopoulos and George Steiner. Partially ordered knapsack and applications to scheduling. *Discrete Applied Mathematics*, 155(8):889–897, apr 2007.

[86] Christos Koulamas. The single-machine total tardiness scheduling problem: Review and extensions. *European Journal of Operational Research*, 202(1):1–7, apr 2010.

[87] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy Magazine*, 9(3):49–51, may 2011.

[88] F Liu and W Lee. Constructing Enterprise Information Network Security Risk Management Mechanism by Ontology. *Tamkang Journal of Science and Engineering*, 13(1):79–87, 2010.

[89] Yuri Gama Lopes and Adiel Teixeira de Almeida. Assessment of synergies for selecting a project portfolio in the petroleum industry based on a multi-attribute utility function. *Journal of Petroleum Science and Engineering*, 126:131–140, feb 2015.

[90] Jun-Jie Lv and Yuan-Zhuo Wang. A ranking method for information security risk management based on AHP and PROMETHEE. In *2010 International Conference on Management and Service Science*, pages 1–4. IEEE, aug 2010.

[91] Jun-Jie Lv, Yong-Sheng Zhou, and Yuan-Zhuo Wang. A multicriteria evaluation method of information security controls. In

2011 Fourth International Joint Conference on Computational Sciences and Optimization, pages 190–194. IEEE, apr 2011.

[92] Qingxiong Ma, Allen C. Johnston, and J. Michael Pearson. Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, 16(3):251–270, jul 2008.

[93] NJ Manson. Is operations research really research? *ORiON*, 22(2), dec 2006.

[94] Malek Masmoudi and Alain Haït. Project scheduling under uncertainty using fuzzy modelling and solving techniques. *Engineering Applications of Artificial Intelligence*, 26(1):135–149, jan 2013.

[95] Yuri Mauergauz. Multi-criteria models and decision-making. In *Advanced Planning and Scheduling in Manufacturing and Supply Chains*, pages 127–162. Springer International Publishing, 2016.

[96] John McCumber. Information systems security: A comprehensive model. In *Proceedings of the 14th National Computer Security Conference*. National Institute of Standards and Technology, 1991.

[97] Daniel Mellado, Carlos Blanco, Luis E Sánchez, and Eduardo Fernández-Medina. A systematic review of security requirements engineering. *Computer Standards & Interfaces*, 32(4):153–165, 2010.

[98] Meng Meng and Enping Liu. The application research of information security risk assessment model based on AHP method. *Journal of Advances in Information Technology*, pages 201–206, 2015.

[99] Parastoo Mohagheghi. An approach for empirical evaluation of model-driven engineering in multiple dimensions. In *EEMDD Workshop at ECMFA 2010*, 2010.

[100] Mirko Montanari, Ellick Chan, Kevin Larson, Wucherl Yoo, and Roy H. Campbell. Distributed security policy conformance. *Computers & Security*, 33:28–40, mar 2013.

[101] Thomas Morton and David W Pentico. *Heuristic scheduling systems: with applications to production systems and project management*, volume 3. John Wiley & Sons, 1993.

[102] Haralambos Mouratidis. Secure information systems engineering: a manifesto. *International Journal of Electronic Security and Digital Forensics*, 1(1):27–41, 2007.

[103] Kiyoshi Nagata, Michio Amagasa, Yutaka Kigawa, and Dongmei Cui. Method to select effective risk mitigation controls using fuzzy outranking. In *2009 Ninth International Conference on Intelligent Systems Design and Applications*, pages 479–484. IEEE, 2009.

[104] Wisconsin Institutes for Discovery NEOS. Neos server for optimization web portal. `http://www.neos-server.org/neos/`, 2017. 2017-12-20.

[105] J.F. Van Niekerk and R. Von Solms. Information security culture: A management perspective. *Computers & Security*, 29(4):476–486, jun 2010.

[106] Helen Nissenbaum. Where computer security meets national security. *Ethics and Information Technology*, 7(2):61–73, jun 2005.

[107] National Institute of Standards NIST and Technology. Cybersecurity. `https://www.nist.gov/topics/cybersecurity`, 2017. 2017-12-20.

[108] Association of European Operational Research Societies. Web page euro. `http://www.euro-online.org/web/pages/1/home`, 2019.

[109] Andres Ojamaa, Enn Tyugu, and Jyri Kivimaa. Pareto-optimal situaton analysis for selection of security measures. In *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pages 1–7. IEEE, nov 2008.

[110] Angel R. Otero, Abdel Ejnioui, Carlos E. Otero, and Gurvirender Tejay. Evaluation of information security controls in organizations by grey relational analysis. *International Journal of Dependable and Trustworthy Information Systems*, 2(3):36–54, jul 2011.

[111] Angel R. Otero, Carlos E. Otero, and Abrar Qureshi. A multicriteria evaluation of information security controls using boolean features. *International Journal of Network Security & Its Applications*, 2(4):1–11, oct 2010.

[112] Angel R. Otero, Gurvirender Tejay, Luis Daniel Otero, and Alex J. Ruiz-Torres. A fuzzy logic-based information security control assessment for organizations. In *2012 IEEE Conference on Open Systems*, pages 1–6. IEEE, oct 2012.

[113] Simon E. Parkin, Aad van Moorsel, and Robert Coles. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2nd international conference on Security of information and networks - SIN 09*. ACM Press, 2009.

[114] Teresa Pereira and Henrique Santos. Challenges in information security protection. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*, pages 160–166, 2014.

[115] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64:1–18, aug 2015.

[116] Venkataraman Ramesh, Robert L Glass, and Iris Vessey. Research in computer science: an empirical study. *Journal of systems and software*, 70(1-2):165–176, 2004.

[117] Singiresu S Rao. *Engineering optimization: theory and practice*. John Wiley & Sons, 2009.

[118] Loren Paul Rees, Jason K. Deane, Terry R. Rakes, and Wade H. Baker. Decision support for cybersecurity risk planning. *Decision Support Systems*, 51(3):493–505, jun 2011.

[119] CheckPoint Research. 2018 security report. `https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf`, 2018.

[120] Malik F Saleh. Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, 5(3):316–337, 2011.

[121] Mehran Samavati, Daryl Essam, Micah Nehring, and Ruhul Sarker. A methodology for the large-scale multi-period precedence-constrained knapsack problem: an application in the mining industry. *International Journal of Production Economics*, 193:12–20, nov 2017.

[122] N. Samphaiboon and Y. Yamada. Heuristic and exact algorithms for the precedence-constrained knapsack problem. *Journal of Optimization Theory and Applications*, 105(3):659–676, jun 2000.

[123] L Sánchez, D Villafranca, E Fernandez-Medina, and M Piattini. MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. *In proceedings of V Congreso Iberoamericano de Seguridad Informática*, 2009.

[124] Lidia Sanchez and Beatriz Blanco. Three decades of continuous improvement. *Total Quality Management & Business Excellence*, 25(9-10):986–1001, jan 2014.

[125] R. Sarala, G. Zayaraz, and V. Vijayalakshmi. Optimal selection of security countermeasures for effective information security. In *Proceedings of the International Conference on Soft Computing Systems*, pages 345–353. Springer India, dec 2015.

[126] Tadeusz Sawik. Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55(1):156–164, apr 2013.

[127] Maryam Shahpasand, Mehdi Shajari, Seyed Alireza Hashemi Golpaygani, and Hoda Ghavamipoor. A comprehensive security control selection model for inter-dependent organizational assets structure. *Information and Computer Security*, 23(2):218–242, jun 2015.

[128] A. Shameli-Sendi. Fuzzy multi-criteria decision-making for information security risk assessment. *The Open Cybernetics & Systemics Journal*, 6(1):26–37, jun 2012.

[129] Mikko Siponen and Robert Willison. Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270, jun 2009.

[130] S Staab and R Studer. Handbook on Ontologies. *Springer Science & Business Media.*, 2009.

[131] Heru Susanto and Mohammad Nabil Almunawar. Managing compliance with an information security management standard. In *Encyclopedia of Information Science and Technology, Third Edition*, pages 1452–1463. IGI Global, 2015.

[132] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. Information security challenge and breaches: novelty approach on measuring iso 27001 readiness level. *International Journal of Engineering and Technology. IJET Publications UK*, 2(1):67–75, 2012.

[133] Symantec Corporation. 2018 Internet security threat report. `https://www.symantec.com/security-center/threat-report`, 2018.

[134] Seren Ozmehmet Tasan and Mitsuo Gen. An integrated selection and scheduling for disjunctive network problems. *Computers & Industrial Engineering*, 65(1):65–76, may 2013.

[135] The New York Times. What intelligence agencies concluded about the russian attack on the u.s. election. `https://www.nytimes.com/2017/01/06/us/politics/russian-hack-report.html`, 2017. artículo de Scott Shane, 6 de enero de 2017.

[136] The New York Times. What we know and don't know about the international cyberattack. `https:`

//www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html, 2017. artículo de Russel Goldman, 12 de mayo de 2017.

[137] Dan Constantin Tofan. Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, 3(3):128–135, 2011.

[138] Silvano Colombo Tosatto, Guido Governatori, and Pierre Kelsen. Business process regulatory compliance is hard. *IEEE Transactions on Services Computing*, 8(6):958–970, 2015.

[139] Alejandro Amigo Tossi. Consideraciones sobre la ciberamenaza a la seguridad nacional. *Revista Política y Estrategia*, (123):83, sep 2017.

[140] Ambrosio Toval, Joaquín Nicolás, Begoña Moros, and Fernando García. Requirements reuse for improving information systems security: A practitioner's approach. *Requirements Engineering*, 6(4):205–219, jan 2002.

[141] Valentina Viduto, Carsten Maple, Wei Huang, and David López-Peréz. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, 53(3):599–610, jun 2012.

[142] S.H. (Basie) von Solms. Information security governance – compliance management vs operational management. *Computers & Security*, 24(6):443–447, sep 2005.

[143] Fredrik Vraalsen and Tobias Mahler. Assessing enterprise risk level: The coras approach. In *Advances in enterprise information technology security*, pages 311–333. Igi Global, 2007.

[144] Ling Wang, Sheng yao Wang, and Ye Xu. An effective hybrid EDA-based algorithm for solving multidimensional knapsack problem. *Expert Systems with Applications*, 39(5):5593–5599, apr 2012.

[145] Jan Weglarz, Joanna Józefowska, Marek Mika, and Grzegorz Waligóra. Project scheduling with finite or infinite number of activity processing modes – a survey. *European Journal of Operational Research*, 208(3):177–205, feb 2011.

[146] Michael Whitman and Herbert Mattord. *Management of information security*. Nelson Education, 2013.

[147] Roel Wieringa. Design science as nested problem solving. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST 09*. ACM Press, 2009.

[148] Andrzej P. Wierzbicki. The use of reference objectives in multiobjective optimization. In *Lecture Notes in Economics and Mathematical Systems*, pages 468–486. Springer Berlin Heidelberg, 1980.

[149] Wayne L Winston and Jeffrey B Goldberg. *Operations research: applications and algorithms*, volume 3. Thomson/Brooks/Cole Belmontˆ eCalif Calif, 2004.

[150] Gerhard Wäscher, Heike Haußner, and Holger Schumann. An improved typology of cutting and packing problems. *European Journal of Operational Research*, 183(3):1109–1130, dec 2007.

[151] Cheng Yameng, Shen Yulong, Ma Jianfeng, Cui Xining, and Li Yahui. AHP-GRAP based security evaluation method for

MILS system within CC framework. In *2011 Seventh International Conference on Computational Intelligence and Security*, pages 635–639. IEEE, dec 2011.

[152] Yu-Ping Yang, How-Ming Shieh, Jun-Der Leu, and Gwo-Hshiung Tzeng. A vikor-based multiple criteria decision method for improving information security risk. *International Journal of Information Technology & Decision Making*, 08(02):267–287, jun 2009.

[153] Yu-Ping Ou Yang, How-Ming Shieh, and Gwo-Hshiung Tzeng. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, 232:482–500, may 2013.

[154] Iryna Yevseyeva, Vitor Basto-Fernandes, Michael Emmerich, and Aad van Moorsel. Selecting optimal subset of security controls. *Procedia Computer Science*, 64:1035–1042, 2015.

[155] Byungjun You and Takeo Yamada. A pegging approach to the precedence-constrained knapsack problem. *European Journal of Operational Research*, 183(2):618–632, dec 2007.

[156] He Zhang, Kaushal Chari, and Manish Agrawal. Decision support for the optimal allocation of security controls. *Decision Support Systems*, 115:92–104, nov 2018.

Parte IV

Anexos

A. Cuestionario de diagnóstico

Dominios

Política de Seguridad

1.1 Política de Seguridad de la Información

PREGUNTAS ASOCIDAS AL CONTROL
¿Hay una política de seguridad documentada?
¿El documento se publica y comunica a todos los empleados?
¿El documento de publica y comunica a todas las entidades externas relevantes?
¿Se relaciona la política de seguridad con los objetvos institucionales?
¿Se relaciona la política de seguridad con leyes y regulaciones relevantes?
¿Existe una emisión y mantenimiento (actualización) de un documento de la política de seguridad de la información?
¿Los cambios introducidos dicen relación a la pertinencia, eficiencia y efectividad de las medidas de seguridad?
¿La actualización ocurre a lo menos cada 3 años?
¿Está previsto que la actualización debe ocurrir anticipadamente si hay cambiios que lo justifiquen?
¿Queda explícito en la política de seguridad la frecuencia de revisión del documento?
¿Existe una defínción de documento electrónico y su seguridad como parte de la política de seguridad?

Organización de la Seguridad de la Información

2.1 Organización Interna

PREGUNTAS ASOCIDAS AL CONTROL
¿Los planes operacionales incluyen directivas o establecimiento de objetivos en términos de seguridad de la información?
¿La dirección denota un compromiso real con la seguridad de la información en términos de dedicación temporal, recursos, participación?
¿Hay comités para la seguridad de información?
¿Hay roles relacionados a seguridad de la información?
¿Hay asignación formal de profesionales a cumplir los roles en seguridad de la información?
¿Quiénes cumples roles de seguridad son los miembros del comité de seguridad?
¿Hay un responsable de la seguridad de la información?
¿El responsable de seguridad de la información está asignado por resolución?
¿La asignación del responsable de seguridad incluye la mantención de la política de seguridad, su control y correcta implementación?
¿La asignación del responsable de seguridad incluye la coordinación de respuestas a incidencias computacionales?
¿La asignación del responsable de seguridad incluye actalizarse en tendencias en seguridad?
¿La asignación del responsable de seguridad incluye mantenerse en contacto con otros encargados de seguridad y especialistas en la materia?
¿El encargado de seguridad actúa como asesor del Jefe de Servicio?
¿Se ha evaluado la necesidad de contar con una consultoría interna sobre seguridad de la información al interior de la organización?
Siendo positiva la evaluación anterior, ¿se cuenta con dicha consultoría disponible al interior de la organización?
¿Se promueve que los integrantes del comité de seguridad pertenezcan a distintas disciplinas de conocimiento?
¿Los intergrantes del comité de seguridad poseen cargos relevantes al interior de la organización?
¿Los integrantes del comité de seguridad representan todas las áreas de la organización?

¿Los miembros del comité de seguridad son efectivamente un grupo interdisciplinario?
¿Existe un procedimiento definido para la autorización (puesta en marcha) de los nuevos medios de procesamiento de información (incluye hardware, software y servicios de procesamiento externo?
¿El procedimiento anterior incluye la gestión de los acuerdos de confidencialidad?
¿La revisón de la organización de la seguridad -incuye objetivos, política, procesos, procedimientos - se realiza de manera independiente ?

2.2 Entidades Externas

PREGUNTAS ASOCIDAS AL CONTROL

¿Se identifican los riesgos asociados a la información en términos de confidencialidad?
¿Se identifican los riesgos asociados a los sistemas de procesamiento de la información?
¿Existe un procedimiento para otorgar acceso a entidades externas a la información de la organización?

¿El procedimiento para otorgar acceso a entidades externas es seguido y la documentación está disponible?

Gestión de Activos

3.1 Responsabilidad por los Activos

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un instructivo para clasificar la información de la organización (esquema de clasificación de la seguridad de la información)?
¿La clasificación de la información incluye el valor para la organización (necesidad), requerimientos legales, confidencialidad (grado de protección) y grado crítico (prioridad) para la organización?
¿Los documentos electrónicos están identificados, clasificados y etiquetados de acuerdo a necesidad, grado de protección y prioridad para la organización?
¿Los sistemas de procesamiento de la información están identificados, clasificados y etiquetados de acuerdo a necesidad, grado de protección y prioridad para la organización?
¿Existe la definición de uno o varios procedimientos cuyo objetivo sea aplicar el esquema de clasificación de la seguridad de la información a los documentos de la organización?
¿Existe evidencia que el procedimiento anterior se ha seguido para los documentos electrónicos de la organización?
¿Cada sistema de información existente tiene formalmente asignado un responsable?

¿Los sistemas de información en cuanto productos de software y datos están debidamente inventariados?
¿El responsable del sistema de información ha sido quien lo ha clasificado y etiquetado?
¿El responsable de seguridad conoce y aplica el sistema de etiquetado de acuerdo al decreto 26 de 2001 de la Secretaría General de La Presidencia?
¿Existe un instructivo que identifique implícita o explícitamente a los responsables de los documentos electrónicos?
¿Existe un instructivo que identifique implícita o explícitamente a los responsables de los sistemas de información?
¿El encargado de seguridad se encarga de generar, distribuir y actualizar este instructivo?
¿El instructivo incluye el detalle de qué hacer para las acciones de copiado, almacenamiento, envío por medios electrónicos y destrucción?
¿Todos los documentos reservados o secretos están correspondientemente etiquetados, incluyendo las salidas por pantallas, impresiones de sistemas de información, y adjuntos de correo electrónico?

Seguridad de los Recursos Humanos

4.1 Antes del Empleo

PREGUNTAS ASOCIDAS AL CONTROL

¿Se han definido los roles y responsabilidades en seguridad de los empleados de acuerdo a las políticas de seguridad?

¿Se han definido los roles y responsabilidades en seguridad de contratistas y terceros de acuerdo a las políticas de seguridad?

¿Están identificados los riesgos de seguridad de la información asociados a los roles del personal en la organización, asociados a la función y clasificación de la documentación correspondiente?

¿Existe un listado de los riesgos de seguridad de la información asociados a áreas de actividad de la organización?

¿Se verifican los antecedentes de todos los candidatos a un empleo de acuerdo a la legislación y regulaciónes internas al hacer una selección de personal en proporción a los riesgos de seguridad identificados para su rol?

¿Se recogen antecedentes de todos los candidatos a un empleo en concordancia a un comportamiento ético en términos de seguridad de la información acorde a los riesgos identificados para su rol?

¿Se recogen antecedentes de todos los postulantes a un contrato externo de acuerdo a leyes y regulaciones según los riesgos asociados identificados a las áreas de actividad de la organización que tendrá acceso?

¿Se recogen antecedentes éticos de todos los postulantes a un contrato externo según los riesgos asociados identificados a las áreas de actividad de la organización que tendrá acceso?

¿Los términos de los contratos de empleo incluyen los aspectos de seguridad de la información, es decir, obligaciones del empleado y de la organización a este respecto?

- ¿Los aspectos de seguridad de la información son claramente informados a los candidatos antes de la contratación?

¿Los términos de los contratos de terceros incluyen los aspectos de seguridad de la información, es decir, obligaciones del empleado y de la organización a este respecto?

4.2 Durante el Empleo

PREGUNTAS ASOCIDAS AL CONTROL

¿Existen procedimientos definidos para verificar que los empleados están cumpliendo con las recomendaciones de seguridad de la información asociados a su rol?

¿Existen procedimientos definidos para verificar que los contratistas están cumpliendo con las recomendaciones de seguridad de la información asociados a su contrato?

¿Los empleados tienen una adecuada inducción a los temas de seguridad de la información asociados a su rol?

¿Está definido un procedimiento de auditoría permanente para detectar cumplimiento de las reglamentaciones de seguridad?

¿Existe un proceso formal que defina la forma en que se entregan los identificadores (usuarios/claves) de los Sistemas Informáticos?

- ¿El procedimiento formal para entegar identificadores exige que sea el jefe del solicitante el que se responsabiliza de la petición?
- ¿Este procedimiento formal incluye: la obligación de mantener confidencial los identificadores?

¿Este procedimiento formal incluye: la obligación de no registrar los identificadores en papel?
¿Este procedimiento formal incluye: la prohibición de no almacenar identificadores en computadores de manera no protegida?
¿Este procedimiento formal incluye: el deber de no compartir los identificadores de usuarios individuales?
¿Este procedimiento formal incluye: el mandato de no incluir los identificadores como parte de una sesión de inicio de un proceso automático?
¿Este procedimiento formal incluye: la indicación de cambiar los identificadores cuando hay indicios de un compromiso del identificador del sistema (hackeo)?
¿Este procedimiento formal incluye: la recomendación de elegir identificadores (claves) seguros -no uso de fechas clásicas, nombres de la familia, longitud mínima, etc?

¿Este procedimiento formal incluye: la indicación de cambiar los identificadores a intervalos regulares?

¿Este procedimiento formal incluye: la indicación de cambiar los identificadores a intervalos regulares?
¿Este procedimiento formal incluye: normas para evitar el reciclaje de identificadores ya usados?
¿Este procedimiento formal incluye: una forma segura de entregar el identificador por primera vez (no terceras partes, no uso de email)?
¿Este procedimiento formal incluye: la indicación de cambiar el primer identificador (temporal) al iniciar la primera sesión?
¿Este procedimiento formal incluye: la indicación que los usuarios deben dajar constancia de su recepción?
¿Este procedimiento formal incluye el caso de usuarios con múltiples identificadores y la exigencia que debe usar identificadores distintos en cada caso?
¿Todos los sistemas informáticos están programados de tal manera que los usuarios se ven compelidos -obligados- a cumplir las normas anteriores?

¿Se incentiva a los usuarios a configurar sus sistemas (operativos) para cerrar las sesiones activas al final de la labor?
¿Se incentiva a los usuarios a configurar sus sistemas (operativos) para cerrar las sesiones de los computadores principales cuando la sesión finaliza?
¿Se incentiva a los usuarios a configurar sus sistemas (operativos) para que en los momentos que no se use queden bloqueados -por ejemplo claves en el refrescador de pantalla-?
¿Se incentiva y facilita el uso de certificados de firma electrónica
Cuando se detectan carencias o falencias en la gestión de la seguridad por parte de los empleados, ¿se realiza una capacitación al respecto?
Cuando se detectan carencias o falencias en la gestión de la seguridad por parte de los **contratistas** ¿se realiza una capacitación al respecto?
¿Están definido el procedimiento disicplinario para violaciones de la reglamentación de la seguridad de la información para el caso de los empleados?
¿Están definido el procedimiento a seguir para violaciones de la reglamentación de la seguridad de la información para el caso de los contratistas?
¿El procedimiento disciplinario a violaciones de la seguridad de la información se ha aplicado a los empleados cuando ha correspondido?
¿El procedimiento a violaciones de la seguridad de la información se ha aplicado a los contratistas cuando ha correspondido?

4.3 Terminación o cambio de empleo

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento que defina de manera general o particular por roles las acciones a considerar respecto de seguridad de la información en los cambios de roles al interior de la organización (licencias, renuncias, permisos, termino de contrato)?
¿Existe un procedimiento que defina las acciones a considerar respecto de seguridad de la información en el término del trabajo de un contratista?
¿Existe un catálogo de sofware autorizado para instalar en la organización?

¿El procedimiento para los empleados considera la prohibición de instalación de software no autorizado?
¿Existe un instructivo específico en términos de seguridad de la información para el uso de correo electrónico?
¿Existe un instructivo en términos de seguridad de la información para el acceso compartido a recursos electrónicos por parte de la organización?
¿Existe un instructivo específico en términos de seguridad de la información para el uso seguro de servicios de mensajería y comunicación remota ?
¿El procedimiento para los empleados considera la devolución de activos o destrucción de copias de documentos electrónicos cuando corresponde?
¿El procedimiento para los contratistas considera la devolución de activos o destrucción de copias de documentos electrónicos cuando corresponde?
¿El procedimiento para los empleados considera la devolución de activos o destrucción de copias de documentos electrónicos cuando corresponde?
¿El procedimiento para los contratistas considera la devolución de activos o destrucción de copias de documentos electrónicos cuando corresponde?
¿El procedimiento para los empleados incluye cambios de reglas de acceso a la información según corresponda?
¿El procedimiento para los contratistas asegura que los permisos de acceso caducan?
¿El procedimiento para los empleados se ha aplicado cuando ha correspondido?
¿El procedimiento para los contratistas se ha aplicado cuando ha correspondido?
¿Existe un catálogo de los Sistemas Informáticos de la organización?
¿Los procedimientos de seguridad incluyen la transimisión de datos, almacenamiento y procesamiento de la información de los Sistemas Informáticos de la organización?
¿Se reitera y queda claro que tanto los procedimientos como los instructivos es una iniciativa de la Jefatura del Servicio?
¿Existe un procedimiento para reportar los incidentes de seguridad?
¿El procedimiento para reportar los incidentes de seguridad se ha usado cuando ha correspondido?

Seguridad Física y Ambiental

5.1 Áreas Seguras

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe una política de seguridad física en la empresa y está actualizada?

¿Esta política de seguridad física incluye el consumo de bebidas, comida, tabaco en las carcanías de instalaciones informáticas?

¿Esta política de seguridad física incluye condiciones ambientales y climatológicas que podrían alterar el buen funcionamiento de sistemas informáticos? (campos magnéticos, estufas, …)

¿Esta política de seguridad física promociona una práctica de escritorio limpio?

¿La política de seguridad incluye el caso de computadores portátiles y su protección fuera de la organización?

¿La política de seguridad incluye la adecuada protección de los cableados de red de datos?

¿La política de seguridad incluye una normativa para el caso de traslado de infraestructura informática fuera de la organización?

¿La política de seguridad es debidamente difundida entre los usuarios?

¿Existe y se difunden los planes de contingencia/emergencia?

¿Existe un registro de todos los incidentes de seguridad y están clasificados según su gravedad?

¿Se dan conferencias de seguridad física a todos los empleados al incorporarse al trabajo y de forma periódica?

En los contratos de comunicaciones, ¿están claramente reflejados los parámetros que definen la calidad de servicio, como ancho de banda, CIR, tiempo de respuesta de averías, etc.?

¿Se ha hecho un análisis de los riesgos de seguridad física?

¿Todos los documentos caracterizados como reservados o secretos están protegidos con barreras físicas?

¿Todos los documentos caracterizados como reservados o secretos están protegidos además de físicamente con los procedimientos de acceso que resguarden su intervención por personas no autorizadas?

¿Los resguardos fisicos y de procedimiento de acceso están acorde a los riesgos de seguridad física identificados?

¿Tiene todo el personal disponible un listado con los números de teléfono más importantes en caso de emergencia?

¿Se realizan simulacros / ejercicios en caso de emergencia?

¿Tiene la empresa contratados seguros generales?

¿Tiene la empresa contratados seguros específicos de las tecnologías de la información?

¿tiene la empresa un seguro específico de responsabilidad civil?

¿Existen un contrato / seguro que garantice la continuidad del negocio en caso de emergencia?

¿Existen planos de las rutas de emergencia?

¿Están bien señalizadas las rutas y salidas de emergencia?

¿La ubicación del Centro de Procesamiento de Datos (CPD) está estudiada y documentada de tal manera de minimizar efectos negativos de percances y descuidos?

¿Se ha evaluado el riesgo del edificio y zonas aledañas?

¿Existe un estudio de las condiciones estructurales del edificio (tipo y espesor de paredes, vigas, suelos y techos?

¿Hay una separación física del Centro de Procesamiento de Datos por medio de Barreras o Paredes?

¿Existen planos de todas las conducciones y están actualizados (climatización, agua, eléctrica, comunicaciones…)?

¿Tiene el edificio escaleras de emergencia?

¿Las salas de ordenadores están alejadas y aisladas de los ruidos y vibraciones?

¿el tiempo de respuesta de los servicios de emergencia (bomberos, ambulancia, policía, etc.) es inferior a 15 minutos?

¿Existe un sistema de climatización adecuado?

¿Existe un sistema de climatización de emergencia?

¿Hay un sistema de vigilancia de la instalación, de climatización y de medida de las características ambientales (humedad, temperatura, partículas en suspensión…)?

¿Se realiza un mantenimiento adecuado del sistema de climatización (inspecciones, cambio de filtros, limpieza de conductos…)?

¿Se ha realizado un estudio de riesgo de intrusión en el edificio?

¿Se ha realizado un análisis de riesgos de acceso al CPD?

¿El CPD está completamente aislado del resto del edificio y sus accesos controlados?

¿Existe un circuito cerrado de TV que controle el acceso al CPD y las puertas de emergencia?

¿Existe un registro escrito o impreso de todos los accesos a todas las salas de equipos informáticos?
¿Existe un sistema de control de acceso biométrico?
¿Todas las personas con acceso autorizado tienen una tarjeta de identificación y están controlados?
¿toda la persona, ajeno o no a la empresa, exhibe de forma clara la tarjeta de identificación?
¿Se utiliza un sistema de control de acceso automático para el acceso al CPD?
¿El acceso al CPD está auditado, tanto para la entrada como para la salida?
¿Existen procedimientos específicos de control de acceso para el personal ajeno a la empresa?
¿Existe una vigilancia exterior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?
¿Existe una vigilancia interior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?
¿Todas las salidas de emergencia están equipadas con un dispositivo de control, unido a un puesto permanente de vigilancia que alerte su apertura?
¿Las oficinas se cierran con llave y se verifica su cierre al terminar la jornada laboral?
¿Se aplica en la empresa una política de mesas vacías?
¿Se ha verificado la resistencia de los muros del edificio ante un intento de intrusión?
¿Se ha verificado la resistencia de las puertas (calidad de los marcos, resistencia de la puerta, calidad de los cerrojos y cerraduras, etc.)?
¿Se ha verificado la resistencia de las ventanas?
¿Las ventanas de las plantas bajas disponen de rejas o barrotes y se ha verificado su resistencia?
¿Se necesita un permiso expreso para acceder al CPD?
¿Se notifican al CPD con suficiente antelación las visitas previstas?
¿Hay un control y archivo diarios de las grabaciones del sistema de vigilancia?
¿Existe un servicio de vigilantes de seguridad?
¿Existe un procedimiento de rondas y de verificación de la seguridad física?
¿Existe un procedimiento de recepción de materiales, que garanticen su inspección antes de su traslado al interior del edificio?
¿Existe un control de entrada y salida de material?
¿Existe un sistema de detección de metales?
¿Existe un procedimiento específico de control de acceso del personal de limpieza?

5.2 Seguridad del Equipo

PREGUNTAS ASOCIDAS AL CONTROL

¿Se ha realizado un estudio de los riesgos de incendio que cubra tanto la prevención cómo la protección?
¿Los tabiques y revestimientos de muros, techos y suelos están fabricados con materiales ignífugos?
¿Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?
¿Los conductos de aire acondicionado/ventilación están equipados con válvulas automáticas contra incendios?
¿Se activa automáticamente el sistema de corte de energía eléctrica tras la detección de un incendio?
¿Hay barreras como puertas anti fuego y barra / cortinas anti humo en los lugares susceptibles de ser utilizadas?
¿Las puertas cortafuegos se cierran automáticamente al saltar la alarma?
¿Existe un instalación fija de contra incendios en el CPD?
¿Existe un suministro adecuado de agua para los sistemas de extinción de incendios?
¿La instalación de detección automática de incendios está compuesta por al menos dos tipos de detectores (por ejemplo: detectores de humo iónico y óptico)?
¿Existe un indicador luminoso y sonoro fuera del CPD cuando el sistema contra incendios se dispara?

¿Estas instalaciones son revisadas periódicamente conforme a la reglamentación y tienen un mantenimiento adecuado?
¿El número de distribución de dispositivos de alarma contra incendios es el adecuado?
¿Las instalaciones de extinción automática están realizadas según la normativa vigente y estar certificadas como tales?
¿Las instalaciones de extinción automática se verifican periódicamente de acuerdo a la normativa y su mantenimiento se realiza regularmente?
Cuando las instalaciones de extinción automática se quedan fuera de servicio, ¿se señaliza automáticamente en un puesto permanente de vigilancia ocupado por dos personas como mínimo?
¿Existe una instalación de extintores portátiles en el conjunto de los locales informáticos y el equipamiento del entorno?
¿la instalación de extintores portátiles cumple la normativa vigente?
¿Existen indicaciones claramente visibles acerca de las condiciones de uso de los extintores?
¿Los extintores portátiles se verifican periódicamente de acuerdo con la normativa y su mantenimiento se realiza adecuadamente?
¿Se utilizan solo papeleras metálicas en el edificio y papeleras ignifugas con sus correspondientes tapas en las salas de ordenadores?
¿La cantidad de papel almacenada en las salas de impresión es inferior a las necesidades de un día de producción?
Los productos diversos de mantenimiento, fácilmente inflamables, ¿se almacenan fuera del CPD?
¿Los documentos o soportes informáticos de interés para la empresa se guardan en armarios ignífugos?
¿Está prohibido fumar en el CPD y se respeta la prohibición?
¿Se efectúa una limpieza periódica de los espacios ocultos (bajo el falso suelo, escaleras, etc.)?
¿Se evita la acumulación de material innecesario en el CPD?
¿Se utilizan contenedores de basura resistentes al fuego?
¿Existe un procedimiento de contingencia para caso de inundaciones?
Los problemas relacionados con el agua (lluvia, goteras, agua presión de dispositivos contra incendios, inundaciones…), ¿han sido tratados adecuadamente (filtración, drenaje, sifones, sumideros…)?
¿Existe un plan de contingencia para el caso de inundaciones o filtraciones de agua?
¿Se ha hecho un estudio acerca de la posibilidad de inundaciones en la zona?
¿El techo de la sala donde se encuentran los equipos informáticos es impermeable?
¿Existe un sistema automático de detección de fugas de agua (en los locales superiores al CPD)?
¿Existen planos actualizados con la situación de todas las tuberías (agua potable, desagües, aire acondicionado?
¿Existe un sistema de llaves de paso, así como planos claros, actualizados y fácilmente disponibles de las canalizaciones?
¿Existe un sistema de drenaje adecuado en falso suelo y en salas adyacentes al CPD?
¿Hay instaladas bombas de achique por si fueran necesarias?
¿Se realiza una revisión periódica del estado de las tuberías, llaves de paso y canalizaciones?
¿Existen detectores de humedad/agua en el falso suelo?
¿Están los sistemas de detección conectados con un puesto permanente de vigilancia con al menos 2 personas?
¿Se revisan periódicamente los detectores?
¿Todo el sistema de cableado está protegido contra inundaciones / humedad?
¿Hay instaladas bombas de achique como mecanismo de emergencia en caso de inundación?

PREGUNTAS ASOCIDAS AL CONTROL

¿La instalaciones eléctricas respetan la norma NCh 4/2003 de seguridad de instalaciones eléctricas ?

¿Existe un sistema de vigilancia de la calidad y continuidad del suministro eléctrico?
¿Existe un sistema de alimentación ininterrumpida (SAI)?

¿El tipo de SAI y el mantenimiento de este es adecuado (inspecciones, pruebas, revisiones de baterías…)?
¿La autonomía proporcionada por el SAI es suficiente para bajar los servicios de manera segura?
¿Existe un sistema autónomo de generación de energía eléctrica?
La capacidad de generación de estos grupos electrógenos, ¿es suficiente para garantizar la seguridad de los edificios y el funcionamiento de los equipos informáticos?
¿Se realizan pruebas periódicas de las instalaciones de los grupos electrógenos?
¿Los paneles de control de energía eléctrica están cerrados con llave?
¿se realizan inspecciones periódicas de todas las instalaciones de suministro eléctrico?
¿Existen elementos de protección contra sobretensión?
¿Existe un dispositivo de corte manual de energía para emergencia (machete corte)?
¿se verifica su funcionamiento?
¿Se encuentran los interruptores de emergencia ubicados cerca de las salidas de emergencia?
¿Está restringido el acceso a los tableros de alimentación?
¿Están claramente indicados los locales o puntos de riesgo de descarga eléctrica?
¿Está el personal instruido y existen carteles claramente visibles sobre las acciones a tomar en caso de descarga eléctrica?
¿Tiene los equipos informáticos placas para que el personal se descargue de la electricidad estática?

Gestión de las Comunicaciones y Operaciones

6.1

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un catastro de los procedimientos de operación?
¿Estos procedimientos están debidamente detallados en cuanto a sus etapas?
¿Estos procediminientos se difunden adecuadamente a los usuarios que los necesiten?
¿Estos procedimientos tienen un mecanismo definido de mantención (actualización)?
¿El procedimiento de actualización considera la incorporación de expertos en la materia?
¿Existe un procedimiento que define la forma de desarrollar los cambios en la infraestructura de Tecnologías de Información?
¿Este procedimiento incluye un registro del origen de las peticiones?
¿Este procedimiento incluye trazabilidad de las etapas de acuerdo al procedimiento definido?

¿En el caso de códificación, se dispone de un sistema de gestión de versiones de productos de software?
¿Este procedimiento incluye cambios directos de datos sobre bases de datos corporativas?

¿Este procedimiento incluye la getión de cambios a nivel de hardware e infraestructura de comunicaciones?
¿Los procedimientos de operación tienen responsables separados y asignados por la jefatura del servicio?
¿Cada sistema de información tiene un encargado de operación el que es debidamente comunicado a los usuarios?
Independiente del responsable, ¿el registro de trazabilidad de los cambios incluye la identificación de la persona que ejecuta los pasos administrativos correspondientes?
¿Existe un procedimiento interno que especifique cómo separar las etapas de desarrollo, prueba y explotación de los sistemas informáticos?
¿La explotación ocurre en equipos diferentes de los de testing y desarrollo?

6.2 Gestión de la entrega de servicios de terceros

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento para aceptar y explotar (usar) los servicios informáticos provistos por terceros?

¿Este procedimiento incluye una secuencia de pasos para aceptar un nuevo servicio provisto por terceros?
¿Este procedimiento incluye monitoreo de la satisfacción de usuarios?
¿Este procedimiento incluye monitoreo de rendimiento del sistema informático?
¿Este procedimiento incluye monitoreo de la integridad de la información?
¿Este procedimiento incluye monitoreo de la seguridad de la información?

¿Los servicios informáticos de terceros son auditados regularmente?

¿Existe un procedimiento para registrar los cambios en los servicios de terceros?
¿Este procedimiento permite registrar el motivo que origina el cambio?
¿Este procedimiento permite la trazabilidad de las acciones que permiten obtener finalmente el cambio deseado?
¿La trazabilidad incluye el registro de la persona que realizó un cambio específico?

¿Este procedimiento incluye la revisión y corrección del mismo -del mismo sistema de gestión de cambio-?
¿Esta actualización considera los cambios en las políticas de seguridad?
¿Esta actualización considera la re-evaluación de riesgos?
¿Esta actualización considera el grado crítico de la información en los sistemas subcontratados?

6.3 Planeación y aceptación de Sistemas

PREGUNTAS ASOCIDAS AL CONTROL

¿Los productos de software autorizados cuentan con las licencias respectivas debidamente registradas?

¿Se registra periódicamente el consumo de recursos de los diversos sistemas computacionales -CPU, disco, etc..?

¿El uso de los recursos de los sistemas se proyecta en el tiempo y se prevé necesidades de recursos adicionales?

¿La previsiónso de uso de recursos incluye la puesta en marcha de nuevos sistemas informáticos?

¿El consumo de los recursos de los nuevos sistemas informáticos es probado durante su desarrollo y antes de su aceptación?

¿La aceptación de sistemas incluye la verificación de requerimientos no funcionales como por ejemplo robustez, eficiencia, seguridad entre otros?

6.4 Protección contra software malicioso y código móvil

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento establecido para protegerse contra software malicioso?
¿Este procedimiento incluye las acciones para detectar código malicioso?

¿Este procedimiento incluye las acciones para prevenir la infección de virus informáticos u otras formas de código malicioso (malwares en general) siendo consciente de las diferentes vías (email,downloading)?
¿Este procedimiento incluye la recuperación ante eventos de intrusión de código de malicioso tanto en computadores personales como los del CPD?
¿Este procedimiento incluye una difusión de buenas prácticas de protección y prevensión ante los usuarios de la organización?

¿Existe un procedimiento establecido para velar por la seguridad de códigos móviles -funciones javascript, html, ajax, applets etc… -?
¿Este procedimiento incluye las condiciones para autorizar un determinado código móvil?
¿Existe un registro de todos los códigos móviles autorizados y el responsable de dicha autorización?

¿Este procedimiento incluye un mecanismo para evitar que se ejecute código móvil no apropiado?

6.5 Política de respaldos

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento que defina la política de respaldo de almacenamiento de la información?
¿Este procedimiento incluye una norma de registro y custodia de los respaldos?
¿Se considera una política de respaldos que considere por lo menos un respaldo anual para el caso de computadores personales?
¿Se considera una política de respaldos que considere por lo menos un respaldo mensual para el caso de computadores del CPD?
¿Es necesaria una autorización para permitir la salida de respaldos de su lugar de almacenamiento?
¿se registran y respetan los tiempos de vida medios de los soportes de respaldo y las condiciones de almacenamiento sugeridas por los fabricantes?
¿Existen mecanismos para verificar la integridad de los datos almacenados en los respaldos?
¿Los datos de los respaldos se mantienen por una cantidad fija de ciclos mínimos de respaldo?
¿Existen al menos 2 copias de software de aplicación y de base de datos almacenadas en lugares distintos a su utilización (al menos una de las copias) ?
¿La infraestructura es suficiente y está dispoinble de tal manera que se permita, aún después de una falla general, poner en funcionamiento los sistemas?
¿Existe un procedimiento para recuperarse de fallas generales - procedimiento de reestablecimiiento -?
¿Este procedimiento incluye la necesidad de practicar restauraciones y comprobar su correcto funcionamiento?
¿Se han realizado prácticas de restauración en los últimos dos años?
¿Este procedimiento se almacena de manera remota junto con las copias de los respaldos de Sistemas Informáticos?
¿El almacenamiento remoto de los respaldos es lo suficientemente lejano que permita aislarse de un desastre en el sitio principal?
¿El almacenamiento remoto de respaldos sigue los mismos procedimientos de seguridad que el CPD?

6.6 Gestión de Seguridad de Redes

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento definido para la seguridad de redes?
¿Este procedimiento promueve la existentencia de sistemas de comunicación alternativos en caso de avería o fallo?
¿Este procedimiento promueve la existencia de 2 proveedores de comunicaciones, o en su defecto de un único proveedor con dos puntos de acceso distintos y que recorran distintos caminos?
En los contratos de comunicaciones, ¿están claramente reflejados los parámetros que definen la calidad de servicio, como ancho de banda, CIR, tiempo de respuestas de averías, etc.?
¿Existe algún plano de la instalación del cableado y sistemas de comunicaciones en el edificio?
¿Se realizan pruebas periódicas para garantizar la calidad de las líneas y sistemas de comunicación?
En cableado de comunicaciones, ¿es fácilmente accesible para las labores de mantenimiento?
El personal de mantenimiento, ¿es custodiado mientras realiza sus labores?
Los paneles de control de las comunicaciones, ¿son revisados periódicamente?
El cableado, ¿está protegido frente a accesos no autorizados, sabotaje, interceptación, etc.?
Los equipos de comunicaciones, ¿se encuentran en un lugar de acceso restringido?
¿El cableado de comunicaciones está separado de la instalación eléctrica?

¿Existe alguna protección física para los principales cables de conexión con el proveedor de comunicaciones?

¿Se he realizado un estudio sobre la problemática TEMPEST - seguridad de emisiones detectables -?

¿El procedimiento de seguridad en redes incluye ye una revisión y mejoramiento del mismo en plazos determinados?

6.7 Gestión de Medios

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento que regule la seguridad en torno a la divulgación, modificación, eliminación y destrucción de medios de almacenamiento?

¿El procedimiento de seguridad de medios incluye una revisión y mejoramiento del mismo en plazos determinados?

¿Este procedimiento incluye el borrado seguro de los respaldos antes de ser reutilizados?

¿Este procedimiento incluye la destrucción de respaldos magnéticos como parte previa de darlos de baja ?

¿Este procedimiento incluye una política que prohiba la libre circulación de medios de almacenamiento - pendrives, discos, dvds?

¿Este procedimiento incluye una promoción de uso de sistemas de cifrado?

¿Este procedimiento incluye las políticas de traslado de medios removibles (transportables) -por ejemplo a lugar seguro de almacenamiento de respaldos-?

¿Este procedimiento incluye una forma de verificar la integridad de la información de documentación de los sistemas?

6.8 Intercambio de Información

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe un procedimiento formal para establecer acuerdos que regulen el intercambio de información y software con entidades externas?

¿Los acuerdos actuales de intercambio de información están registrados y regidos por algún convenio o acuerdo formal?

¿Existe un procedimiento para proteger los intercambios de información a través de todos los tipos de transferencia de información?

¿Este procedimiento incluye las políticas de traslado de medios removibles (transportables) -por ejemplo a lugar seguro de almacenamiento de respaldos-?

¿Este procedimiento incluye la forma de regular información vía correo electrónico - sobre todo re envío - y otros medios de mensajería electrónica?

¿Este procedimiento incluye la forma de resguardar la originalidad (no alteración) de la información en páginas web?

¿Este procedimiento incluye advertencias sobre la vulnerabilidad de la información enviada en correos electrónicos?

¿Este procedimiento incluye advertencias sobre el peligro asociado a los archivos adjuntos sean o no ejecutables?

¿Este procedimiento inlcluye advertencias sobre la inconveniencia de enviar claves de acceso mediante correos electrónicos?

¿Este procedimiento incluye una recomendación que los usuarios tengan un correo electrónico diferente para su uso personal?

¿Este procedimiento prohibe el uso de correos electrónicos grupales?

¿Este procedimiento incluye un listado de situaciones en las cuales NO usar correo electrónico?

¿Este procedimiento incluye una forma de inducir al tema de firma electrónica?

¿Este procedimiento incluye una prevensión respecto de comprobar el origen, despacho, entrega y aceptación mediante firma electrónica?

¿Este procedimiento incluye una precisión de las responsabilidades en caso de comprometer a la institución mediante correos electrónicos - difamación, hostigamiento, acoso, compras no autorizadas - ?

6.10 Monitoreo

PREGUNTAS ASOCIDAS AL CONTROL
¿Se registran sistemáticamente las excepciones de los Sistemas Informáticos?
¿Se registran sistemáticamente las irrupciones a las medidas de seguridad?
¿Existen actividades de auditoría sistemáticas y son debidamente registradas?
¿Los resultados de las auditorías son mantenidos por periodos de tiempo suficiente permitiendo su análisis posterior?
¿Se han establecido los procedimientos para monitorear permanentemente los Sistemas de Información?
¿Las operaciones (comandos) tanto de los adminitradores de sistema como de los operadores forman parte de la información de monitoreo?
¿Los registros del procedimiento de monitoreo se revisan periódicamente como parte de un procedimiento ?
¿Los resultados de las auditorías se protegen bajo reglas de control de acceso adecuadas?
¿Los resultados del monitoreo de los sistemas (logs) se protegen bajo reglas de acceso adecuadas?
¿Los registros de las auditorías y de monitoreo forman parte de la información que se respalda?
¿Existe un procedimiento (sistema) para registrar, trazar y resolver las fallas de los sistemas informáticos?
¿Los relojes de los diferentes sistemas operativos que sostienen sistemas están coordinados en base a una fuente única?

Control de Acceso

7.1 Requerimiento comercial para el control de acceso

PREGUNTAS ASOCIDAS AL CONTROL
¿Existe una política documentada de control de acceso a los sistemas informáticos?
¿Esta política incluye el ciclo de vida completo, desde la asignación hasta la caducación?
¿Esta política trata de manera separada agregando restricciones especiales cuando se trata de usuarios con claves de accesos con privilegios que permitirían acciones de riesgo para los sistemas?
¿Esta política tiene un proceso de revisión períodico tendiente a su actualización?

7.2 Gestión del acceso del usuario

PREGUNTAS ASOCIDAS AL CONTROL
¿Existe un proceso formal que defina la forma en que se entregan los identificadores (usuarios/claves) de los Sistemas Informáticos?
¿Existe una recomendación formal de seguir buenas prácticas en el uso de las claves e identificadores?

7.3 Responsabilidad del Usuario

PREGUNTAS ASOCIDAS AL CONTROL

¿Los términos de los contratos de empleo incluyen los aspectos de seguridad de la información, es decir, obligaciones del empleado y de la organización a este respecto?

¿Este procedimiento formal incluye: la obligación de mantener confidencial los identificadores?

¿Este procedimiento formal incluye: la obligación de no registrar los identificadores en papel?

¿Este procedimiento formal incluye: la prohibición de no almacenar identificadores en computadores de manera no protegida?

¿Este procedimiento formal incluye: el deber de no compartir los identificadores de usuarios individuales?

¿Este procedimiento formal incluye: el mandato de no incluir los identificadores como parte de una sesión de inicio de un proceso automático?

¿Este procedimiento formal incluye: la indicación de cambiar los identificadores cuando hay indicios de un compromiso del identificador del sistema (hackeo)?

¿Este procedimiento formal incluye: la recomendación de elegir identificadores (claves) seguros -no uso de fechas clásicas, nombres de la familia, longitud mínima, etc?

¿Este procedimiento formal incluye: la indicación de cambiar los identificadores a intervalos regulares?

¿Este procedimiento formal incluye: la indicación de cambiar los identificadores a intervalos regulares?

¿Este procedimiento formal incluye: normas para evitar el reciclaje de identificadores ya usados?

¿Este procedimiento considera el registro de los usuarios y sus privilegios en sistemas informáticos específicos?

¿Existe un procedimiento de auditoría permanente que verifique que los accesos a los sistemas corresponden a los privilegios otorgados?

¿Existe una política para equipo desatendido

¿Se incentiva a los usuarios a configurar sus sistemas (operativos) para cerrar las sesiones de los computadores principales cuando la sesión finaliza?

¿Se incentiva a los usuarios a configurar sus sistemas (operativos) para que en los momentos que no se use queden bloqueados -por ejemplo claves en el refrescador de pantalla-?

¿Existe un práctica de escritorio limpio que inclye medios removibles y pantalla limpia para equipos de procesamiento de datos?

¿Esta política de seguridad física promociona una práctica de escritorio limpio?

7.4 Control de acceso a redes

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe una política documentada de control de acceso a los sistemas informáticos?

¿Esta política de control de acceso considera el acceso a las redes?

¿Se considera métodos de autenticación para usuarios remotos?

¿Se considera la identificación del equipo cómo parte del acceso remoto?

¿El acceso a puertos de diagnóstico y configuración (físicos y lógicos) están bajo control y monitoreo?

¿Existe una política de segregación de redes de acuerdo a riesgos identificados y rendimiento?

¿Esta política se ejecuta con los registros correspondientes?

¿Se restringe el acceso a los usuarios a las redes compartidas de acuerdo a esta política de seguridad?

¿Esta política de seguridad incluye el monitoreo de routers y equipos de comunicación?

¿Este monitoreo se ejecuta con los registros correspondientes?

¿Existe un sistema de monitoreo que detecte intentos fallidos de acceso?

7.5 Control de acceso a Sistemas Operativos

PREGUNTAS ASOCIDAS AL CONTROL

¿Se utiliza algún método de acceso a S.O. con autentificación segura?

¿Este procedimiento está formalizado en procedimientos o política?

Para el acceso a los Sistemas Operativos, ¿Cada usuario tiene un identificador único y exclusivo?
¿Este hecho está formalizado en procedimientos o política?

¿Se utiliza un sistema de gestión de claves que asegura claves de buena calidad en los Sistemas Operativos?
¿Existe un procedimiento norma que regule la instalación de utilidades en el Sistema Operativo (Personales o del CPD) de manera de evitar la acción de software de protección o de monitoreo?
¿Se limita el acceso remoto de tal manera que ante tiempos máximos de inactividad se produce una desconexión del Sistema Operativo?
¿Lo anterior está formalizado en la política de seguridad u otra norma?

7.6 Control de acceso a la aplicación o información

PREGUNTAS ASOCIDAS AL CONTROL

¿Los sistemas con información sensible corren de manera dedicada (aislada)?
¿Todos los sistemas de información de nivel de aplicación tienen control de acceso?
¿Existe un sistema de alarmas sobre intentos o irrupciones a la seguridad?

7.7 Computación Móvil y Teletrabajo

PREGUNTAS ASOCIDAS AL CONTROL

¿Existe una política o norma que regule el teletrabajo?
¿Existe una política o norma que regule el desarrollo, prueba y uso de los sistemas informáticos que pueden ser accedidos por medio de dispositivos móviles?
¿Existe una restricción de uso de computadores de propiedad de las personas?

Adquisición y Desarrollo de Sistemas Informáticos

8.1 Requerimiento de la Seguridad de los Sistemas

PREGUNTAS ASOCIDAS AL CONTROL

¿Se incluye la seguridad en las especificaciones de Sistemas nuevos?

¿Los requerimientos de seguridad son acordados, justificados y documentados en las especificaciones de los sistemas a desarrollar?

8.2 Procesamiento correcto de las aplicaciones

PREGUNTAS ASOCIDAS AL CONTROL

¿Se realizan pruebas estructuradas a los sistemas?
¿Es parte del procedimiento asegurar que los datos de prueba son correctos y apropiados?
¿Se prueban los sistemas activando procedimientos de verificación que tiendan a detectar corrupciones o itnervenciones de terceros en los datos?
¿Para el caso de los sistemas se incluyen los requerimientos para asegurar la integridad de los mensajes cuando los hay?
¿Existe un procedimiento para asegurar que los datos de prueba son correctos y apropiados?
¿Es parte del procedimiento asegurar que los datos de salida corresponden a los datos de entrada procesados?

8.3 Controles Criptográficos

PREGUNTAS ASOCIDAS AL CONTROL

¿El procedimiento para especificar sistemas incluye requerimientos de criptografía para manejo de información sensible cuando corresponde?

¿Se especifica en los requerimientos control de acceso para los nuevos sistemas?
¿Este procesamiento esta formalizado?

8.4 Serguridad de los archivos de los sistemas

PREGUNTAS ASOCIDAS AL CONTROL

¿Se controla la instalación de software?
¿Los sets de pruebas de sistemas permanecen protegidos?
¿Los código fuentes de los programas estpan debidamente protegidos?
¿Existen procedimientos formalizados de control de cambios de los sistemas desarrollados ad hoc?
¿Las condiciones para activar cambios en los sistemas están restringidos y existe un procedimiento que aprueba sólo cambios específicos?
Los productos cuyos desarrollos son externalizados ¿son debidamente supervisados y monitorizados durante el desarrollo?
Existe un procedimiento que permita detectar las vulnerabilidades de los sistemas informáticos desarrollados para la organización
- ¿Se evaluan estas vulnerabilidades e identifican los riesgos para la organización de las respectivas exposiciones de información?
- ¿Se toman las medidas adecuadas para superar estas vulnerabilidades?

Gestión de incidentes en la seguridad de la Información

PREGUNTAS ASOCIDAS AL CONTROL

¿Se registran las incidencias de seguridad de la información?
¿Las incidencias de seguridad de la información se reporten a la gerencia de manera rápida (jefatura de servicio)?
¿Los procedimientos formales requieren a los usuarios que reporten las fallas a la seguridad de la información?

¿Están definido un procedimiento formal sobre el cual la autoridad se guíe para responder rápidamente a los incidentes de seguridad?
- ¿Este procedimiento es debidamente difundido a todos los funcionarios y se conocen sus pasos y consecuencias?

¿Existen los mecanismos para permitir cuantificar y monitorear los tiempos, volúmenes y costos de los incidentes en la seguridad de la información?
¿El procedimiento para dirimir las incidencias de seguridad de la información considera las evidencias correspondientemente a cada caso?
¿Este procedimiento considera revisarse y mejorarse de manera continua?

Gestión de Continuidad del Negocio

PREGUNTAS ASOCIDAS AL CONTROL

¿La continuidad operativa o continuidad del negocio es un concepto difundido al interior de la organización?
¿La continuidad operativa, o continuidad del negocio es una preocupación del jefe de servicio?
¿La continuidad operativa forma parte de una política de seguridad de la organzación?
¿Se han identificado los procesos críticos (y mínimos) los cuales, de estar operando, se puede afirmar que la organización está desarrollando su función?
¿Se han estudiado las fallas de seguridad, pérdida del servicio y disponibilidad del servicio en cuanto a su impacto en los procesos críticos?
¿Existe un política de proteger estos procesos críticos en cuanto a respaldar la documentación que indique cómo deben llevarse a cabo (descripción del proceso)?
¿Existe la política de mantener estos procesos críticos operando tomando las precauciones necesarias para que esto ocurra así (reemplazos, restauración de estado de los procesos) ?
¿La política de respaldos incluye de manera diferenciada el respaldo de información de los procesos críticos de la organización?
¿Existe una política que índique que deben realizarse pruebas de restauración de los procesos críticos?
¿Existe evidencia de prácticas en la restauración de los procesos críticos?

Cumplimiento

11.1 Cumplimientos legales

PREGUNTAS ASOCIDAS AL CONTROL

¿Se tienen identificados los reglamentos, normas y leyes que regulan la operación de la organzación y sistemas de información?
Estos reglamentos, estatutos, normas y leyes, ¿se mantienen disponibles y actualizados?
¿Se han implantado los procedimientos administrativos que aseguren el cumplimiento de los requerimientos legislativos - derechos de copia, patentes de software, propiedad intelectual en general?
¿Se categorizan los datos en la organización de acuerdo a su requerimiento en términos legales, estatutarios, normativo y contraactuales?
¿Existe una política de protección de datos acuerdo a estas categorías?
¿Existe una política de preservación y destrucción de datos de acuerdo a estas categorías?
¿Esta política de preservación y destrucción se ha traducido en procedimientos que se aplican regularmente?
Durante período de preservación, ¿existen los controles adecuados para proteger los datos de pérdidas, destrucción o falsificación?
Para la destrucción, ¿existen los controles adecuados que permitan asegurar la pertinencia de dicha destrucción?

11.1 Prevención de mal uso de información

PREGUNTAS ASOCIDAS AL CONTROL

¿Se difunde a los usuarios sobre las limitaciones de su rango de acción en los accesos a sistemas?
¿Se difunde a los usuarios sobre la existencia de sistemas de monitorización sobre sus acciones en los sistemas de información?
¿Los monitoreos incluyen inspección de contenidos, prevención y detección de intrusiones al sistema?
¿Las técnicas de protección y criptografía están de acuerdo a la ley?

¿Existe una revisión periódica que verifique el cumplimiento de los procedimientos y normas internas de seguridad?
¿Existe una verificación periódica que los sistemas cumplen con los requerimientos internos de seguridad, especialmente (pero no limitado a) pruebas de penetración y evaluación de vulnerabilidades?
¿Las políticas de recolección de datos y procedimintos de auditoría se han diseñado para que tengan un impacto mínimo en el normal uso de los sistemas y procedimientos?
¿El acceso a información y herramientas de auditoría está limitado de acuerdo a privilegios y seguridad establecidos?
¿Las actividades relacionadas a "Cumplimiento" son asesoradas por personas calificadas en derecho ya sean externos o internos?

B. Cuestionario UMAM-Q

Intention to Adopt Software Methodologies: the UMAM-Q Instrument

Estudio de Adopción del Enfoque Metodológico para la Selección de Controles de Seguridad Informática

Estimado Estudiante

Muchas gracias por contestar este cuestionario y ayudarnos así a evaluar la intención de adopción del enfoque metodológico para la selecciones de controles de seguridad informática.

La respuesta a esta encuesta debe ser considerada en el contexto del desarrollo del proyecto de auditoría realizado en la asignatura de Auditoría Informática. Te solicitamos que contestes en base a tu experiencia en la utilización del enfoque metodológico que plantea la selección de controles de seguridad como un problema de optimización y utiliza técnicas de optimización para su resolución.

Tus respuestas serán totalmente anónimas y no se solicitan datos sensibles. Al contestar a estas preguntas, estás dando tu permiso para que los datos proporcionados se puedan utilizar para evaluar el método de selección de controles y poder mostrar o publicar los resultados de dicha evaluación.

Gracias!

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación del enfoque metodológico para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Usar esta metodología mejora mi efectividad	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me permite realizar las tareas más rápidamente	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología mejora la calidad del trabajo realizado	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me facilita realizar mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me da más control sobre mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología mejora mi rendimiento en el trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me permite terminar mis tareas más rápidamente	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología para realizar mi trabajo es intuitivo	❍	❍	❍	❍	❍	❍	❍

Usar esta metodología me hace más cómoda la realización de mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me ayuda a producir mejores aplicaciones	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me ayuda a producir aplicaciones más mantenibles	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me permite prevenir errores durante la realización de mi trabajo	❍	❍	❍	❍	❍	❍	❍
En conjunto, encuentro que usar esta metodología es ventajoso para mi trabajo	❍	❍	❍	❍	❍	❍	❍
En conjunto, creo que utilizar esta metodología es útil para mi trabajo	❍	❍	❍	❍	❍	❍	❍

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación del enfoque metodológico para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Usar esta metodología es a menudo frustrante	❍	❍	❍	❍	❍	❍	❍
Creo que esta metodología es muy pesada de utilizar	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me supone mucho esfuerzo mental	❍	❍	❍	❍	❍	❍	❍
Creo que aprender a usar esta metodología es fácil	❍	❍	❍	❍	❍	❍	❍
En conjunto, encuentro que esta metodología es fácil de utilizar	❍	❍	❍	❍	❍	❍	❍
Creo que esta metodología es clara y comprensible	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me quita mucho tiempo de mis tareas habituales	❍	❍	❍	❍	❍	❍	❍
Creo que usar esta metodología es sencillo	❍	❍	❍	❍	❍	❍	❍
Creo que olvidaré cómo aplicar esta metodología muy pronto	❍	❍	❍	❍	❍	❍	❍

Usar esta metodología requiere mucha formación previa	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me hace sentir que no tengo el control de mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usando esta metodología siento que puedo realizar mi trabajo exactamente como pretendo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me ayuda a entender mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología me ayuda a realizar mi trabajo en el modo que deseo	❍	❍	❍	❍	❍	❍	❍

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación del enfoque metodológico para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Usar esta metodología es compatible con todos los aspectos de mi trabajo	❍	❍	❍	❍	❍	❍	❍
Creo que usar esta metodología encaja bien con el modo en que trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología encaja con mi estilo de trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología es completamente compatible con mi situación actual	❍	❍	❍	❍	❍	❍	❍
Esta metodología es compatible con el modo en que desarrollo software	❍	❍	❍	❍	❍	❍	❍
Esta metodología es compatible con el modo en que organizo mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología se adapta bien a la realidad de mi trabajo	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología satisface mis necesidades a la hora de realizar mi	❍	❍	❍	❍	❍	❍	❍

trabajo							
Usar esta metodología me parece un modo lógico de trabajar	❍	❍	❍	❍	❍	❍	❍
Puedo adaptar el uso de esta metodología para que encaje con mis necesidades y preferencias	❍	❍	❍	❍	❍	❍	❍
Siento que usar esta metodología me da libertad para trabajar como más me gusta	❍	❍	❍	❍	❍	❍	❍
Siento que esta metodología me permite personalizar el modo en que trabajo	❍	❍	❍	❍	❍	❍	❍
Esta metodología me hace sentir que no tengo restricciones durante mi trabajo	❍	❍	❍	❍	❍	❍	❍
Siento que esta metodología se adapta bien a mi forma de trabajar	❍	❍	❍	❍	❍	❍	❍

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación del enfoque metodológico para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Las personas que influencian mi comportamiento piensan que debería utilizar esta metodología	❍	❍	❍	❍	❍	❍	❍
Las personas que son importantes para mí piensan que debería usar esta metodología	❍	❍	❍	❍	❍	❍	❍
Mis compañeros piensan que debería utilizar esta metodología	❍	❍	❍	❍	❍	❍	❍
Me siento obligado a utilizar esta metodología	❍	❍	❍	❍	❍	❍	❍
Mi entorno de trabajo me anima a que use esta metodología	❍	❍	❍	❍	❍	❍	❍
Las personas que habitualmente sigo en la red recomiendan usar esta metodología	❍	❍	❍	❍	❍	❍	❍
Los medios sociales que leo habitualmente (wikis, blogs, etc.) recomiendan usar esta metodología	❍	❍	❍	❍	❍	❍	❍
Creo que las	❍	❍	❍	❍	❍	❍	❍

personas que realizan tareas similares a las mías están usando esta metodología							
Creo que mi reputación en el trabajo mejoraría si la gente supiera que estoy utilizando esta metodología	❍	❍	❍	❍	❍	❍	❍
Creo que la gente me tomaría de referente si utilizase esta metodología	❍	❍	❍	❍	❍	❍	❍
Usar esta metodología mejoraría mi estatus social en el trabajo	❍	❍	❍	❍	❍	❍	❍
Las personas con las que asisto a reuniones, congresos, etc. recomiendan usar esta metodología	❍	❍	❍	❍	❍	❍	❍
En conjunto, siento que mi estatus social mejoraría si utilizase esta metodología	❍	❍	❍	❍	❍	❍	❍
En conjunto, siento que mi entorno piensa que debo utilizar esta metodología	❍	❍	❍	❍	❍	❍	❍

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación del enfoque metodológico para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Mis superiores esperan que utilice esta metodología	❍	❍	❍	❍	❍	❍	❍
Mi jefe/supervisor no requieren que utilice esta metodología	❍	❍	❍	❍	❍	❍	❍
El uso de esta metodología es un requisito para mi trabajo	❍	❍	❍	❍	❍	❍	❍
Aunque podría ayudar, usar esta metodología no es obligatorio en mi trabajo	❍	❍	❍	❍	❍	❍	❍
El que yo use esta metodología depende de mí, es voluntario	❍	❍	❍	❍	❍	❍	❍
Mi organización me impone esta metodología en mi trabajo	❍	❍	❍	❍	❍	❍	❍
Depende de mí decidir si utilizo esta metodología o no	❍	❍	❍	❍	❍	❍	❍
El usar o no esta metodología depende en gran medida de mis preferencias	❍	❍	❍	❍	❍	❍	❍
En conjunto, encuentro que usar esta metodología es voluntario en mi trabajo	❍	❍	❍	❍	❍	❍	❍

Por favor, evalúa tu grado de acuerdo con las siguientes afirmaciones según tu experiencia en la aplicación de la metodología para la definición del plan de mejora dentro de un proceso de Auditoría Informática, revisado en este curso (1: totalmente en desacuerdo a 7: totalmente de acuerdo)

	1 (Totalmente en desacuerdo)	2	3	4	5	6	7 (Totalmente de acuerdo)
Creo que usaré esta metodología para mi trabajo siempre que sea posible	❍	❍	❍	❍	❍	❍	❍
Si me dan la opción, creo que preferiría utilizar esta metodología en cualquier proyecto futuro	❍	❍	❍	❍	❍	❍	❍
Pretendo incrementar mi uso de esta metodología en el trabajo en un futuro	❍	❍	❍	❍	❍	❍	❍
Pretendo utilizara esta metodología en el futuro para mi trabajo	❍	❍	❍	❍	❍	❍	❍
Pretendo proponer el uso de esta metodología a mi equipo de trabajo en el futuro	❍	❍	❍	❍	❍	❍	❍
Apoyaré el uso de esta metodología en mi trabajo siempre que se presente la ocasión	❍	❍	❍	❍	❍	❍	❍
Si puedo tomar la decisión, utilizaré esta metodología en mi trabajo futuro	❍	❍	❍	❍	❍	❍	❍

Por favor, nombra las tres principales razones por las que usarías este enfoque metodológico en un futuro.

Por favor, nombra las tres principales razones por las que NO usarías este enfoque metodológico en el futuro.

C. Casos de estudio

C.1 Caso de estudio 1

Realice una recomendación de controles, a partir del diagnóstico proporcionado. Debe indicar el conjunto de controles que satisfaga la siguiente pregunta: ¿Cuál es el mejor conjunto de controles que maximiza el beneficio, dado un determinado presupuesto?

Para resolver el problema debe estimar los costos y los beneficios de los controles no implementados. Considere el costo en función de ahorros y horas hombres involucradas. Los beneficios estímelos como 1, 2 o 3, en función del impacto en la mitigación del riesgo (1=Bajo; 2=Medio; 3=Alto).

Construya el modelo que represente esta situación en lenguaje GAMS y resuelva utilizando el sitio https://neos-server.org

Considere 3 casos, de acuerdo al presupuesto:

Caso 1: Presupuesto del 25 % del costo total de implementación.

Caso 2: Presupuesto del 50 % del costo total de implementación.

Caso 3: Presupuesto del 80 % del costo total de implementación.

C.2 Caso de estudio 2

Suponga que está evaluando la conformidad de una organización respecto de los siguientes dominios de la norma ISO27002:2013. Dentro de las actividades que debe realizar como parte de la auditoría, debe

entrevistar al gerente de la organización.

Al ser consultado el gerente respecto de si el manejaba equipamiento de la organización, el responde que tiene un PC en su oficina, un teléfono celular y un notebook. Al preguntarle por la gestión de estos equipos, el responde que cada vez que fallan, se contacta con la oficina de informática, sin embargo prefiere molestar lo menos posible, ya que entiende lo colapsada que está la unidad, por lo que siempre le pide a su hijo que intente arreglarlo primero antes de llevarlo a la oficina.

Durante la entrevista, el gerente contestó su celular un par de veces, al ser consultado si ese era el celular que le proporcionó la empresa, este respondió que no, ya que encuentra que se encuentra desactualizado, por lo que prefiere utilizar su celular personal. Además, no recuerda dónde se encuentra ya que le fue otorgado hace más de 3 años.

En base a esta situación, determine:

1. Identifique los controles y los dominios que se están vulnerando con la situación descrita.

2. Genere una recomendación de implementación de controles basado en los costos estimados de implementación de cada control y de un nivel de presupuesto del 40 % del costo total estimado.

C.3 Caso de estudio 3

Usted está auditando el departamento de Mantenimiento en una organización que proporciona y mantiene el espacio de oficinas e instalaciones de una gran organización, incluidos los controles de seguridad física. Hay una seria denuncia del director de operaciones: EL personal llegó a trabajar esta mañana y se encontraron que nadie podía acceder

al edificio usando sus tarjetas de identificación. El área de servicios de apoyo al cliente se retrasó y un ingeniero forzó la entrada y desactivó manualmente los controles de acceso de la puerta, además, usted encontrará que el evento coincide con la sustitución durante la noche del sistema de circuito cerrado de televisión (CCTV), este sistema está conectado a la WAN y monitoreado desde la sala de control central. Los controles de acceso de tarjeta magnética también son monitoreados centralizadamente a través de la conexión WAN.

Los ingenieros de servicio TI en el sitio están teniendo dificultades para determinar la causa raíz, pero especulan que la configuración red por defecto del sistema de circuito cerrado de televisión está en conflicto con los del sistema de control de acceso de la puerta. Usted revisa el documento de control de cambios X134, fechado 3 meses antes y nota que los servicios de seguridad corporativa se muestran antes y nota que los servicios de seguridad corporativos se muestran como 'N/A' en la lista de colaboradores. Usted confirma con el encargado de las instalaciones que esta revisión es la versión final del documento de control de cambios y que servicio de TI y de seguridad corporativa no revisó el cambio planificado. Usted le pregunta al encargado de las instalaciones por qué no tenían que ver con el cambio y él contesta que en realidad no era necesario ya que el cambio de sistema de circuito cerrado de televisión no era técnicamente complicado. "El antiguo sistema se desconecta de la red y el nuevo sistema sólo es enchufado, al igual que la conexión de un PC nuevo". Él va más allá al señalar que los controles de acceso de la puerta 'Fracasaron, pero fue seguro' por que impidieron el acceso no autorizado al edificio".

La actividad consiste en informar los hallazgos identificados en la situación descrita respecto de los controles proporcionados por la Norma ISO 27002. Los hallazgos se reportarán en el archivo dispuesto, respetando el formato de éste.

A continuación, deberán ordenar las no conformidades respecto de la importancia subjetiva que se le asigne a cada hallazgo. Es decir, de acuerdo a algún criterio, elegido por el grupo, se deberá ordenar de mayor a menor importancia el hallazgo.

Construya el modelo, análisis en lenguaje GAMS, que represente la situación resultante de su y resuelva utilizando el sitio https://neos-server.org

A partir de los hallazgos indique las fortalezas y debilidades de la organización y describa el plan de mejora que le proporciona el modelo obtenido.

El trabajo es grupal, con un máximo de 3 integrantes.

C.4 Caso de estudio 4

Analice y evalué la siguiente situación. Construya un informe de hallazgos, de acuerdo al formato que se encuentra en el campus. Considere los controles de la norma ISO 27002, como los criterios de evaluación.

Suponga la siguiente situación: Usted como auditor, en un proceso de auditoría interna a una determinada organización, ha realizado entrevistas y evaluaciones de campo. De este proceso usted se encuentra con las siguientes situaciones:

1.- Al entrevistarse con el área informática de la empresa, al ser consultados por los activos de información que pertenecen a la organización, éstos responden que todo el equipamiento adquirido se

encuentra asignado a una persona y/o unidad dentro de la empresa. Es la misma unidad la encargada de configurar e instalar el software y/o las aplicaciones necesarias, antes de ser destinadas a los usuarios. Al ser consultados por los mecanismos para dar de baja algún tipo de equipamiento, responden que se este se inicia a partir del requerimiento del usuario del equipo y el proceso se ciñen a un instructivo que indica que al ser recibido el equipo, se formatea el disco duro y se estudia si el equipo puede ser reinsertado en la organización. Respecto de las políticas para la utilización de los equipos personales, el jefe de la unidad responde que la unidad ha definido un protocolo que indica que éstos deben ser notificados en la unidad para ser configurados para su utilización en la red de la empresa.

2.- Durante una visita a la oficina de finanzas, usted busca a la contadora de la organización, pero ésta no se encuentra en su oficina, ya que estaba en una reunión con el jefe de la unidad, al mirar su oficina usted observa que ésta tiene algunos cuadros personales y fotos familiares sobre los muebles que tienen los archivadores y documentación contable de la organización, además, observa algunas plantas que están sobre el equipo de su escritorio. Al observar la pantalla del equipo, usted se percata que en el escritorio del equipo, aparece un mensaje de activación de Windows y de actualización de antivirus. Además, se percata un conjunto elevado de iconos y accesos directos en el mismo escritorio. Además, observa que en la barra de tareas, se encuentra abierto Word, Excel y el correo del usuario.

A partir de los hallazgos modele y resuelva el problema de optimización, diseñando al menos dos escenarios de presupuesto.

C.5 Asignación de tratamientos

La asignación de qué casos de estudio debían ser resueltos con cada nivel del tratamiento (con/sin ayuda de la propuesta) puede verse en la tabla C.1.

Tabla C.1: Asignación de tratamientos a sujetos.

	Caso 1	Caso 2	Caso 3	Caso 4
Sujeto 1	SP	SP	CP	CP
Sujeto 2	CP	SP	SP	CP
Sujeto 3	SP	CP	CP	SP
Sujeto 4	CP	CP	SP	SP
Sujeto 5	SP	SP	CP	CP
Sujeto 6	CP	SP	SP	CP
Sujeto 7	SP	CP	CP	SP
Sujeto 8	CP	CP	SP	SP
Sujeto 9	SP	SP	CP	CP
Sujeto 10	CP	SP	SP	CP
Sujeto 11	SP	CP	CP	SP
Sujeto 12	CP	CP	SP	SP

Reunido el Tribunal que suscribe en el día de la fecha acordó otorgar, por a la Tesis Doctoral de Don Mauricio Rubén Diéguez Rebolledo la calificación de

Alicante, de de

El Presidente, El Secretario,

UNIVERSIDAD DE ALICANTE. CEDIP

La presente Tesis de D. Mauricio Rubén Diéguez Rebolledo ha sido registrada con el nº del registro de entrada correspondiente.

Alicante, de de

El encargado del registro,