UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

MÁSTER UNIVERSITARIO EN DIRECCIÓN DE PROYECTOS INFORMÁTICOS

Trabajo Fin de Máster

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE RECURSOS HUMANOS

XIAOYAN MA

2019/2020

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

MÁSTER UNIVERSITARIO EN
DIRECCIÓN DE PROYECTOS INFORMÁTICOS

Trabajo Fin de Máster

"DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE RECURSOS HUMANOS"

Autor: **XIAOYAN MA**

Director: **Mª JESÚS LAPEÑA**

Tribunal:

Presidente: .....

Vocal 1º: ..... Vocal 2º: .....

Calificación: .....

Fecha: ..... de ..... de .....

AGRADECIMIENTOS

Desde la selección del tema y la recopilación de datos hasta la finalización de la memoria, recibí ayuda de muchos profesores y compañeros de clase.

En primer lugar, agradezco a mi tutora, María Jesús Lapeña, por su apoyo fundamental, fuente inagotable de consejos. No solo presentó muchas opiniones valiosas sobre mi investigación, lo que me dio un objetivo y una dirección para escribir la memoria, sino también me ayudó a mejorar la redacción y revisar pacientemente y presentar opiniones valiosas, lo que hace que el documento sea más fácil de leer y más profesional. Dedicó mucho tiempo y esfuerzo a tutorizar mi trabajo.

Al profesor de seguridad informática, Pedro-Castro Valcárcel Lucas, quien abrió la puerta a la seguridad de la información; su profundo conocimiento profesional, su actitud científica seria, su riguroso espíritu académico y su incansable ética de la enseñanza me han impactado profundamente.

A la empresa COC M.T., cuyos gerentes y empleados me proporcionan la información y los documentos necesarios para apoyar el desarrollo de mi proyecto, especialmente el gerente de departamento del Centro de Tecnología de la Información.

A todos los profesores con los cuales tuve el honor de aprender, por su amabilidad, su compromiso por la labor que desempeñan, y por guiar cuidadosamente mi estudio e investigación.

A mi amigo de Venezuela, Adalberto, por su infinita paciencia, amabilidad y ayuda. Todas sus sugerencias y opiniones me ayudaron a encontrar información durante el proceso de redacción de la memoria, para poder completarla sin problemas.

A mi familia y amigos, como siempre, por sus confianza y apoyo, para mí la mayor motivación en mi vida.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto tiene como objetivo diseñar un sistema de gestión de seguridad de la información en una empresa de Recursos Humanos, COC M.T., para mejorar la seguridad de los activos informáticos de la empresa. Analizando el estado actual de la gestión de seguridad de la información de la compañía y los problemas a mejorar, se puede concluir que el sistema de gestión existente es inadecuado, la conciencia de seguridad es débil, el mecanismo de supervisión es incompleto, se ignoran los riesgos de seguridad, etc. Con base en el cumplimiento de cada medida de control determinada por el análisis de brechas GAP, y el análisis y evaluación de riesgos por el método MAGERIT, se proponen la política y los tratamientos para construir y mejorar el Sistema de Gestión de Seguridad de la Información de COC M.T., con el fin reducir los riesgos y vulnerabilidades que pueden afectar las operaciones comerciales para garantizar de manera efectiva la seguridad de la información. Este proyecto se basa en la norma ISO 27001: 2013 y la utiliza como una idea orientadora para ayudar a formular un sistema de gestión de seguridad de la información que sea adecuado para la empresa, de modo que la empresa pueda ser más segura, más rápida y proporcione referencias para que otras empresas crezcan en el futuro.

Palabras claves: SGSI, Activos informáticos, El análisis de brechas GAP, MAGERIT, Riesgos, Vulnerabilidades, Norma ISO 27001: 2013.

ABSTRACT

This project aims to design an information security management system in a Human Resources company, COC M.T., to improve the security of the company's Information Assets. Analyzing the current state of the company's information security management and the problems to be improved, it can be concluded that the existing management system is inadequate, security awareness is weak, the supervision mechanism is incomplete, the security risks, etc. Based on compliance with each control measure determined by the GAP analysis, and the risk analysis and assessment by the MAGERIT method, the policy and treatments are proposed to build and improve the Security Management System of the Information from COC M.T., in order to reduce the risks and vulnerabilities that can affect business operations to effectively guarantee information security. This project is based on ISO 27001: 2013 and uses it as a guiding idea to help formulate an information security management system that is appropriate for the company, so that the company can be more secure, faster and provide referrals for other companies to grow in the future.

Keywords: ISMS, Information Assets, GAP analysis, MAGERIT, Risks, Vulnerabilities, ISO 27001: 2013 Standard.

1. INTRODUCCIÓN

En la sociedad actual, la información masiva disponible sobre cada persona puede brindar a las compañías recursos ilimitados, oportunidades comerciales ilimitadas y riqueza infinita, pero las características del intercambio abierto y compartido han traído una enorme presión competitiva a la seguridad de la información.

A medida que la transformación digital de las empresas se desarrolla a nivel mundial, los riesgos emergentes en todos los niveles continúan aumentando. Los problemas de seguridad de la información se han vuelto cada vez más serios, y gradualmente se convierten en el factor principal que afecta las operaciones comerciales y limita el desarrollo comercial. Por lo tanto, las empresas deben prestar especial atención a la seguridad de la información.

La seguridad de la información debe contemplar tanto la seguridad física como la seguridad lógica. La seguridad física es el pilar de la seguridad lógica, que a su vez es complementaria de la seguridad física, razón por la cual, deben tomarse medidas razonables al realizar la protección de seguridad, teniendo en cuenta estos dos aspectos.

Para cualquier organización que utilice la tecnología de la información para promover el desarrollo, independientemente de su tamaño y naturaleza, la información puede ser robada o dañada, lo que puede causar pérdidas económicas, sanciones legales, daños a su imagen y reputación, y también puede amenazar la supervivencia de la empresa. Por esta razón, al garantizar la seguridad de la información empresarial, se deben considerar tanto la tecnología como la administración.

Se evidencia que la seguridad de la información de las empresas no es solo una cuestión técnica, sino que también requiere la ayuda de métodos de gestión para garantizarla. Esto indica, es necesario diseñar un Sistema de Gestión de la Seguridad de la Información para detectar y prevenir los riesgos en el contexto de la organización.

Las empresas de Recursos Humanos manejan grandes volúmenes de información que necesita ser protegida: tales como datos sobre empleados, clientes, salarios, beneficios y facturas etc.; estos datos se archivan archivando a través de dos formas: el almacenamiento digital en servidores y el almacenamiento físico en una sala de archivo.

Es evidente que, para la empresa de recursos humanos, la información es de vital importancia; una vez que se produce una fuga de información o corrupción de datos, afectará la imagen de la empresa e incluso estará sujeto a sanciones legales. Por lo tanto, para una empresa de recursos humanos quiere desarrollar mejor una estrategia de información, está obligada a establecer una gestión de seguridad de la información institucionalizada y estandarizada, lo que implica, que deben contar con los más altos niveles en el cumplimiento de los estándares de seguridad.

Este proyecto pretende revelar el estado de seguridad de la información de una empresa de recursos humano, analizar sus principales riesgos y amenazas en la seguridad de la información, diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, lo cual permitirá mejorar de manera continua y completa la gestión de seguridad de la información de la organización.

El presente trabajo se realizará en una empresa real de recursos humanos, pero por motivos de mantener su información confidencial, se utilizará el nombre de COC M.T.

1.1 PLANTEAMIENTO DEL PROBLEMA

La información de las empresas está expuesta diariamente a múltiples amenazas, con el correspondiente riesgo y repercusión en muchos aspectos.

COC M.T. se ha dado cuenta de que debe considerar la seguridad de la información, y establecer un mecanismo de prevención y un sistema que garantice el desarrollo a largo plazo de la empresa. Es urgente establecer un sistema de seguridad maduro en esta etapa.

En los últimos años, a pesar de que COC M.T. ha prestado gran atención a la gestión de la seguridad, y ha implementado una serie de mecanismos de seguridad, todavía está en alerta de riesgo por la falta de un sistema adecuado de gestión de seguridad de la información.

1.1.1 Presentación de la empresa - COC M.T.

COC M.T. es una empresa de servicios de Recursos Humanos, principalmente responsable de encargar la gestión de empleados y la atracción de talento para grandes empresas estatales, empresas privadas y unidades gubernamentales. Ha

establecido 10 sucursales en muchas provincias de China y colaborado con más de 2,000 clientes de subcontratación, incluyendo 22 compañías de Global 500, con un total de 100,000 empleados enviados.

COC M.T. cuenta con servicios avanzados de gestión de talentos y tecnología de información profesional para brindar a los clientes servicios de protección de talentos y contratación externa tecnológica. Su negocio incluye: agencia de personal, despacho de mano de obra, subcontratación, reclutamiento, capacitación de consultoría, servicio salarial, servicio comercial, beneficios flexibles, pago de gastos de personal jubilado, reembolso, etc.

La entidad dispone de un software específico de Recursos Humanos que realiza las funciones de gestión de empleados a través de su propio equipo de tecnología informática; dicho equipo es el principal responsable del diseño, desarrollo, integración de los sistemas de información, sistemas de aplicaciones de recursos humanos y mantenimiento de aplicaciones del sistema.

1.1.2 Definición del problema

Al analizar el estado actual de gestión de seguridad de la entidad, se pueden encontrar los siguientes problemas:

1) Inadecuado modelo de gestión de seguridad de la información

COC M.T. todavía utiliza el modelo de gestión fija anterior de "principalmente gestión de experiencia, complementado por gestión científica". Este modelo de gestión sencillo, pasivo y mecánico no puede adaptarse al entorno que cambia constantemente. Se ha detectado la falta de un programa integral de gestión de seguridad en la empresa.

2) La poca concienciación y formación en materia de seguridad

La entidad no presta atención a la seguridad de la información, y tampoco a las medidas preventivas de seguridad, por lo que los empleados no tienen ni la motivación ni la formación en seguridad informática, lo que lleva a operaciones irregulares y causa fuga de datos corporativos.

3) La responsabilidad se diluye

En COC M.T., se han establecido personas responsables legales y líderes de varios departamentos, pero falta el tema específico de la responsabilidad de gestión de seguridad de la información. Una vez que ocurre un incidente oculto de seguridad de la información, la división de responsabilidades entre varios departamentos y puestos es borrosa.

4) Falta de un Gobierno de Seguridad

COC M.T. utiliza una arquitectura cliente / servidor, que requiere red interna y acceso compartido a los recursos dentro de la empresa, pero se ignora el papel de una estructura organizativa razonable y una gestión institucionalizada y estandarizada en la seguridad de la información, lo que conduce a una gestión y responsabilidades poco claras e indirectamente aumenta los riesgos humanos. La información es manipulada por numerosos empleados sin las medidas de control necesarias.

5) La desconsideración por los riesgos de seguridad

COC M.T. no tiene figuras profesionales y autorizadas responsables de las evaluaciones de riesgos, por lo que tienden a sumergirse en situaciones peligrosas. De hecho, no presta suficiente atención a la importancia de la evaluación de riesgos de seguridad de la información de la compañía; tampoco cuenta con un conjunto de métodos científicos para evaluar y gestionar las amenazas y riesgos de los activos de información.

Teniendo en cuenta los aspectos mencionados anteriormente, es necesario realizar el diseño de un Sistema de Gestión de la Seguridad de la Información en la entidad, basado en la norma ISO/IEC 27001:2013, con el propósito de cumplir con los objetivos allí establecidos.

1.2 JUSTIFICAIÓN

A medida que el nivel de informatización de las empresas continúa aumentando, la seguridad de la información se ha convertido gradualmente en el foco de atención. Desde el país hasta la empresa, comprenden profundamente la necesidad de desarrollar la seguridad de la información. Con respecto a cómo utilizar la gestión de la seguridad y las medidas de seguridad para construir un buen sistema de seguridad de la información, todos los ámbitos están estudiando constantemente métodos prácticos.

Hoy en día, en términos de gestión de seguridad de la información, la norma ISO 27001 del Reino Unido se ha convertido en el estándar fundamental para la gestión de seguridad de la información a nivel mundial; en él se basa la construcción e implementación del Sistema de la Gestión de la Seguridad de la Información de muchas empresas y organizaciones de todo tipo.

El establecimiento de un sistema de gestión de la seguridad de la información aumenta la conciencia de los empleados sobre la seguridad de la información, mejora el nivel de gestión de la seguridad de la información empresarial y la capacidad de las organizaciones sociales para resistir eventos catastróficos; es un vínculo importante en la construcción de información empresarial y mejorará enormemente la confiabilidad y la seguridad de la gestión de la información, de modo que pueda servir mejor al desarrollo comercial de la empresa.

Es evidente que COC M.T. requiere el diseño de un sistema de gestión de seguridad de la información, partiendo de la situación real de la empresa, combinando las características de la industria, y formulando métodos e ideas para la construcción de un sistema de seguridad empresarial desde los niveles general estratégico, gerencial, operativo y técnico. El propósito es reducir los riesgos de seguridad de la información, prevenir accidentes relacionados y proteger la misión de seguridad de los activos de información de la empresa.

El diseño de un Sistema de Gestión de Seguridad de la Información establecerá un marco de sistema de información completo y una estrategia de sistema de seguridad que se ajustará al desarrollo de la entidad, basándose en los activos de información existentes y en el estado actual de COC M.T., con el objetivo de reducir los riesgos que representan las amenazas de seguridad de la información para la entidad. Se trata de mejorar el nivel de gestión de la seguridad de la información para favorecer el desarrollo seguro y saludable de la entidad, y darle más ventajas en la competencia del mercado.

1.3 OBJETIVOS

1.3.1 Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información en la empresa de Recursos Humanos, COC M.T., basado en la norma ISO/IEC 27001:2013.

1.3.2 Objetivos específicos

- Analizar la situación actual de la seguridad de la información de COC M.T.
- Identificar y clasificar los activos de información.
- Valorar y tratar los riesgos de seguridad sobre los activos de la empresa.
- Diseñar y desarrollar un Sistema de Gestión de Seguridad de la Información para la empresa COC M.T.

1.3.3 Alcance y limitaciones

El alcance del proyecto es diseñar un Sistema de Gestión de Seguridad de la Información para la empresa basándonos en la norma ISO/IEC 27001:2013 y utilizando la metodología de análisis de riesgo MAGERIT.

Este proyecto no implica la implementación, mantenimiento y revisión del sistema de gestión de seguridad de la información, solo el análisis y diseño.

1.4 ESTRUCTURA DEL TRABAJO

Este proyecto consta de cinco capítulos; a continuación, se describe el contenido de cada uno de ellos:

- **Capítulo 1 Introducción**

El propósito de este capítulo es plantear el problema y definir el alcance de este trabajo; se hace el planteamiento del problema, argumentamos su justificación e importancia y definimos los objetivos.

- **Capítulo 2 Marco de referencia**

Se presenta el marco teórico, marco conceptual y metodología utilizada para la realización del proyecto; todo ello compone el marco de referencia en el que basamos el desarrollo del TFM.

- **Capítulo 3 Diseño del Sistema de Gestión de Seguridad de la Información en COC M.T.**

Esta parte es el contenido clave, el núcleo central del TFM. Con referencia a los requerimientos de diseño del sistema de gestión de seguridad de la información

definidos en la norma ISO / IEC 27001: 2013, planteamos las siguientes fases del proyecto:

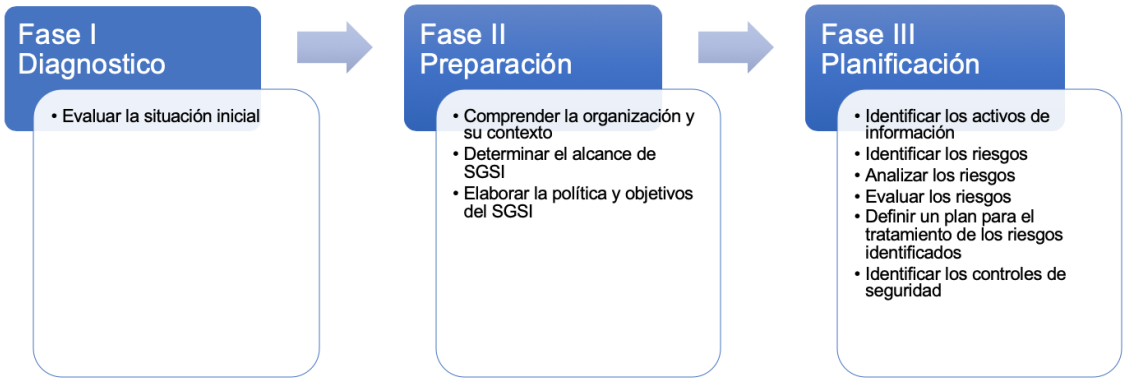

Figura 1. Las fases para el diseño del SGSI
Fuente: Elaboración propia

- **Capítulo 4 Conclusiones y recomendaciones**

Se concretan las conclusiones principales del trabajo, especialmente el trabajo creativo, y las recomendaciones para mejorar aquellos aspectos en los que se detectan deficiencias.

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

En este apartado, se describen conceptos referentes al presente trabajo para su mejor comprensión y desarrollo.

2.1.1 La información

Para las empresas, la información es un activo intangible con cierto valor comercial que debe protegerse, existe en varias formas, como electrónica, imágenes y palabras.

2.1.2 Seguridad de la Información

Para la gran mayoría de las empresas, la seguridad de la información sigue siendo una gran debilidad, y los problemas que de ello se derivan afectarán profundamente a toda la empresa. En el momento actual, la conciencia de la seguridad impulsada por el entorno externo o interno está ganando fuerza, el nivel de concienciación es mucho mayor y, por tanto, la demanda de construcción de seguridad también está aumentando. Desde que surgió esta necesidad de seguridad de la información, su crecimiento e interés es imparable.

Internacionalmente la investigación sobre la seguridad de la información tiene muchos antecedentes y siempre ha tenido un alto grado de atención. El concepto de seguridad de la información va más allá del concepto de seguridad informática, ya que esta última sólo se encarga de la seguridad en el medio informático, pero hay que tener en cuenta que la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos[1].

Podemos decir que la Seguridad de la Información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos[2].

De acuerdo con la Asociación Española para la Calidad, la Seguridad de la Información tiene como fin la protección de la información y de los sistemas que hacen

[1] Diaz, Matias (25 de julio de 2019). «Mapa de riesgos de una empresa». *TU ECONOMÍA FÁCIL*. Consultado el 25 de julio de 2019.
[2] https://es.wikipedia.org/wiki/Seguridad_de_la_información

posible el acceso, uso, divulgación, interrupción o destrucción no autorizada[3] de dicha información.

En resumen, la seguridad de la información se refiere a la protección de los activos de información (incluidos hardware, software, datos, personas, entorno físico e infraestructura básica) contra causas accidentales o maliciosas, daños, alteraciones y fugas. Su objetivo es asegurar la operación continua y confiable del sistema, servicios de información ininterrumpidos y, en última instancia, lograr la continuidad del negocio.

El significado real de la seguridad de la información es evitar que los activos de información sufran todo tipo de interferencias, reducir los posibles riesgos de seguridad y los peligros ocultos, y evitar daños.

En efecto, la seguridad de la información contempla las siguientes dimensiones:

- **Confidencialidad:** la información no se divulga a terceros no autorizados, y solo es utilizada por usuarios autorizados.
- **Disponibilidad:** los individuos, entidades o procesos autorizados pueden acceder a la información y utilizarla cuando lo requieran, es decir, cuando sea necesario, deberían poder acceder a la información que necesitan.
- **Integridad:** la información permanece sin modificaciones no autorizadas durante el almacenamiento o la transmisión.
- **Autenticación:** La información proviene de una fuente genuina, no de un tercero que intenta imitar.

2.1.3 Gestión de la Seguridad de la Información

La gestión de la seguridad de la información incluye una serie de actividades y procesos para guiar, estandarizar y gestionar la seguridad de la información. Específicamente, consiste en formular las medidas defensivas correspondientes para entornos de aplicaciones complejas como, por ejemplo, evitar la proliferación de virus, intrusión de hackers, malware e información fuera de control…, para proteger los activos de información del acceso no autorizado, uso abusivo, fugas, interrupción, modificación no autorizada y destrucción, manteniendo la confidencialidad, integridad y disponibilidad de la información.

[3] https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

2.1.4 Sistema de Gestión de la Seguridad de la Información

Las empresas pueden utilizar la plataforma de tecnología de seguridad de la información para una operación eficiente del mercado, en base a la gestión de la seguridad de la información. Un sistema de gestión adecuado puede hacer que la gestión de seguridad de la información de la empresa sea más eficaz.

El propósito del Sistema de Gestión de Seguridad de la Información es garantizar que la organización implemente la gestión de seguridad en el ciclo de vida del sistema de información en función del análisis y gestión de riesgos correspondiente. Se refiere a que la organización establece sus propias políticas, objetivos, procedimientos y métodos de gestión de seguridad dentro de un espacio específico para resolver los problemas de seguridad de la información en un sistema.

Un sistema de gestión adecuado puede hacer que la gestión de la seguridad de la información de la empresa sea más eficaz. Lo siguiente se centrará en la introducción de sistemas y modelos de gestión convencionales.

1) Sistema de gestión de seguridad de la información basado en ISO / IEC 17799

La norma internacional ISO / IEC17799 se deriva de la BS77999-1 formulada por el Comité Británico de Normas. La última versión es la edición de 2005. Contiene 11 elementos de control y 39 categorías de seguridad. Principalmente como referencia y orientación para desarrolladores de seguridad de la información. El sistema de gestión de seguridad establecido en base a ISO / IEC17799 se muestra en la Figura 2.

Figura 2. Estructura de los dominios de control
Fuente: http://mgd.redrta.org/directrices-seguridad-de-la-informacion/mgd/2015-01-22/145337.html

2) Sistema de gestión de seguridad de la información basado en ISO/IEC 27001:2013

El estándar internacional ISO / IEC 27001 se deriva de BS7799-2. Mediante el método de proceso PHVA, se ha establecido un conjunto integral de reglas de implementación compuesto por las mejores prácticas de seguridad de la información. Como se muestra en la Figura 3, el método de implementación es el siguiente:

Planificar (Plan): Mediante encuestas, a través de cuestionarios, entrevistas, etc., se comprende el contexto organizacional para establecer el alcance y objetivos del Sistema de Gestión de Seguridad de la Información.

Hacer (Do): Se ejecuta el plan especificado en la etapa anterior.

Verificar (Check): Se realiza principalmente durante y después de la ejecución del plan para verificar la ejecución los resultados esperados, monitorizando el desarrollo del proceso. Su objetivo es detectar y prevenir todos los incidentes de seguridad que se produzcan.

Actuar (Act): Consiste en implementar todas las mejoras identificadas y ejecutar las acciones de prevención necesarias establecidas en la norma ISO 27001.

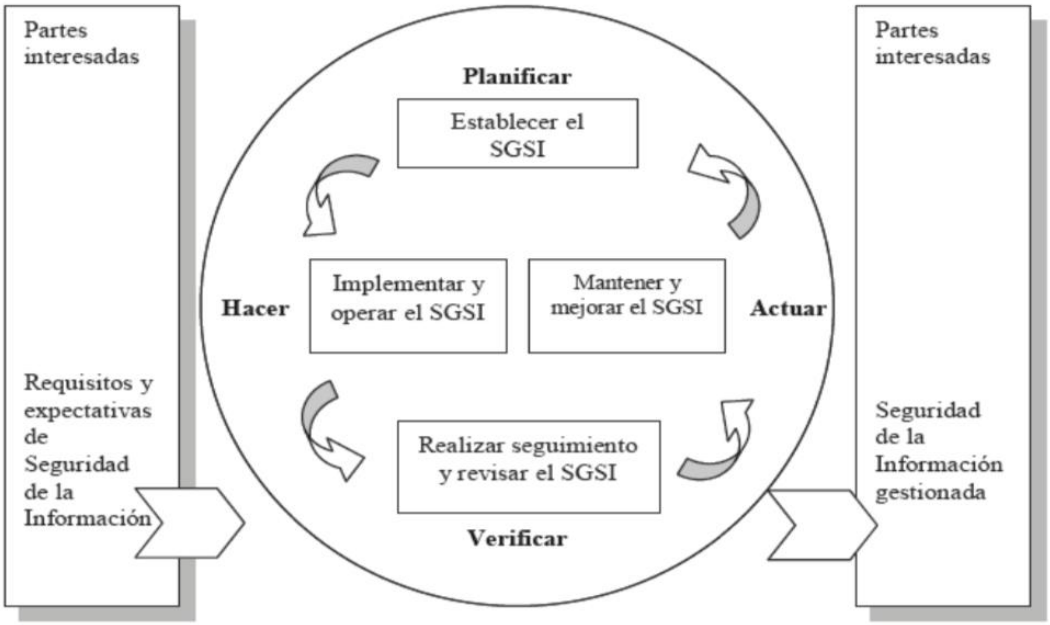

Figura 3. Modelo de PHVA aplicado a los procesos de SGSI
Fuente: https://ticcolombia.webnode.com.co/news/iso-9001/

Como un sistema de gestión estandarizado y sistemático, el Sistema de Gestión de Seguridad de la Información (SGSI) se ha convertido en el estándar internacional principal y en un método científico para resolver problemas de seguridad. La certificación SGSI se ha convertido en una forma de identificar el nivel de seguridad de la información corporativa.

El SGSI tiene aplicabilidad universal y es adecuado para empresas de diferentes tamaños y tipos. Como un sistema de ejecución que opera de acuerdo con el modelo PDCA, se refiere a ISO / IEC 27001. El sistema de gestión de seguridad de la información es un método de gestión de seguridad que toma prestada la gestión de riesgos mediante el establecimiento de objetivos y estrategias de gestión de seguridad.

2.1.5 Normas de seguridad de la información

En la actualidad, el estándar de seguridad de la información más autorizado del mundo es la serie de estándares ISO / IEC 27000.

Las normas ISO/IEC 27000 son una serie de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission)[4] para proporcionar un marco, lineamientos y mejoras a las prácticas de gestión de la seguridad de la información. Se definen los requerimientos para que varias organizaciones establecen, implementan y mejoren sistemas de gestión de seguridad de la información.

Esta serie (ISO/IEC 27000) contiene, entre otros, los siguientes estándares para el desarrollo, implementación y mantenimiento de las especificaciones del Sistema de Gestión de Seguridad de la Información:

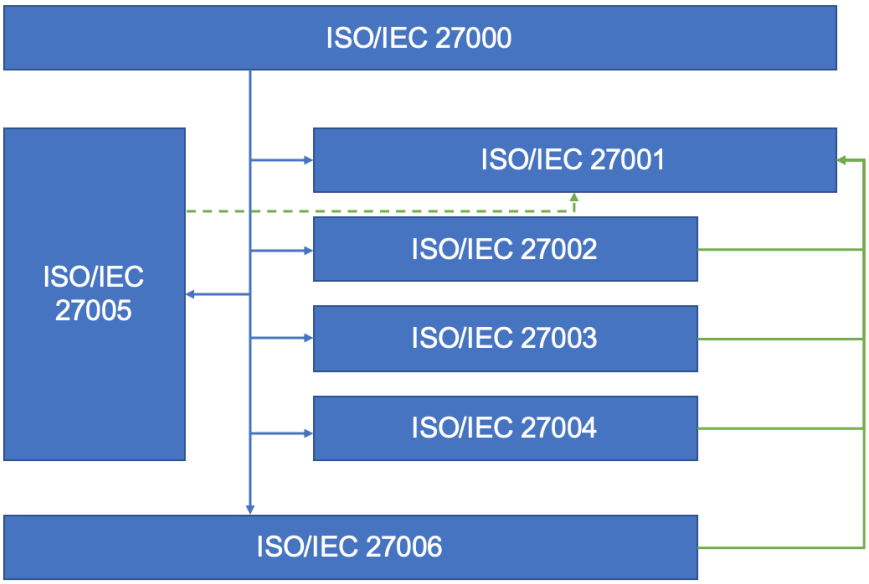

Figura 4. El marco de la familia ISO / IEC 27000
Fuente: Elaboración propia basada en
http://kuaibao.qq.com/s/20181022A1CYTU00?refer=spider

- **ISO/IEC 27000 Fundamentos y Vocabularios**

El estándar proporciona términos y definiciones comúnmente utilizados en diferentes estándares 27000, sentando las bases para toda la familia. La nueva versión lanzada en febrero de 2018 es adecuada para organizaciones de todo tipo y tamaño, desde compañías multinacionales hasta pymes.

[4] https://es.wikipedia.org/wiki/ISO/IEC_27000-series

- **ISO/IEC 27001 Requerimientos del Sistema de Gestión de Seguridad de la Información**

El origen es el estándar británico BS7799-2, que fue adoptado por ISO como ISO / IEC 27001 en noviembre de 2005. Especifica los requisitos para el desarrollo de un sistema de gestión de seguridad de la información y detalla el establecimiento, implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información que satisfaga las necesidades de la empresa.

Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptadas a las necesidades de la organización[5].

- **ISO/IEC 27002 Código de práctica de gestión de seguridad de la información**

La norma ISO/IEC 27002 describe una lista de los objetivos y medidas de control para proporcionar pautas y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización; está asociado con la última versión de ISO / IEC 27001 (la edición de 2013), del Artículo 5 al Artículo 18 (14 áreas, 113 elementos de control) proporcionando recomendaciones de implementación específicas y orientación para respaldar los requisitos especificados en ISO / IEC 27001: 2013.

- **ISO27003 Guía de implementación del sistema de gestión de seguridad de la información**

La norma ISO/IEC 27003 proporciona orientación sobre procedimientos para el diseño e implementación de ISO / IEC 27001; es un estándar de referencia importante y la versión de 2017 es su última edición.

- **ISO27004 Evaluación de la Seguridad de la Información**

El estándar ISO27004 proporciona pautas para medir los resultados del Sistema de Gestión de la Seguridad de la Información en ISO 27001; su objetivo es definir métricas y mejorar la efectividad del sistema de gestión de seguridad de la información, en otras palabras, cómo construir métricas, qué parámetros, cuándo y cómo medir, etc.

- **ISO27005 Gestión de riesgos de la Seguridad la Información.**

[5] NTC-ISO-IEC 27001:2013, Pág. 1

La gestión de seguridad de la información es esencialmente una gestión de riesgos, y el Sistema de Gestión de Seguridad de la Información es un componente importante de la gestión general de riesgos para toda la organización.

La norma ISO27005 describe los requisitos de la gestión de riesgos de seguridad de la información, que se pueden utilizar para la evaluación de riesgos, la identificación de requisitos de seguridad y respaldar el establecimiento y mantenimiento del sistema de gestión de seguridad de la información.

- **ISO/IEC 27006 Requisitos para los organismos que realizan la auditoría y certificación de sistemas de información de gestión de la seguridad**

Como complemento de los requisitos de ISO / IEC 27001, especifica requisitos y proporciona pautas para las organizaciones que implementan auditorías y certificaciones del Sistema de Gestión de Seguridad de la Información; es un estándar poco conocido, pero extremadamente importante, y la versión 2015 es la última.

2.2 MARCO CONCEPTUAL

En este apartado se hace una pequeña inducción a los términos relativos a la seguridad de la información, el análisis y gestión de riesgos que se sustenta esta tesis.

2.2.1 Términos de seguridad de la información

Incidente de seguridad de la información: Eventos que causan daño a los activos de información o tienen un impacto negativo en la sociedad debido a defectos naturales, artificiales o fallas de software y hardware**.**

Antivirus: Se utiliza para detectar y eliminar código malicioso (virus, troyanos, gusanos, etc.), proteger la computadora de otros programas peligrosos o malware[6].

Copia de seguridad: Se refiere a la copia de bases de datos o archivos físicos o virtuales en una ubicación secundaria para su conservación en caso de falla del equipo o desastre. Para un plan de recuperación ante desastres exitoso, es fundamental el proceso de copia de seguridad de datos.

[6] https://www.bankia.es/es/particulares/seguridad/ciberseguridad-glosario

Seguridad física: Proteger equipos, instalaciones y otros activos tangibles que almacenan o procesan información de accidentes ambientales como terremotos, inundaciones e incendios, y daños causados por errores humanos o varios delitos informáticos.

Seguridad lógica: Se refiere a garantizar que el acceso a la información sea confiable y auténtico, como control de acceso, la verificación de las contraseñas, el perfilado de usuarios.

Seguridad de aplicaciones: Es una manifestación de la calidad del software, que se refiere a la inserción de controles de seguridad en su ciclo de vida de desarrollo, puesta en producción y mantenimiento.

Ciberseguridad: Es una tecnología que protege computadoras y servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.

Criptografía: Técnica de proteger documentos y datos; funciona a través de convertir mensajes o textos en mensajes cifrados o contraseñas. El propósito es hacer imposible que cualquier persona que no entienda el sistema de cifrado pueda utilizarlo.

2.2.2 Términos del análisis de riesgos

Análisis de riesgos: El proceso de determinar la probabilidad y el impacto de cada factor de riesgo, cuyo objetivo final es determinar el nivel de riesgo.

Activo de información: El activo de información es un activo especial, cuya propiedad y control corresponde a la organización (para conseguir sus objetivos). Puede entenderse como información, inteligencia, datos o conocimiento, que son todos los objetos que las organizaciones pueden atacar.

Amenaza: Naturalmente, circunstancias desfavorables accidentales o intencionadas pueden conducir a incidentes de seguridad; tiene un impacto negativo en los activos, resultando en indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Riesgo: La combinación de la probabilidad y sus consecuencias provocadas por un determinado evento adverso.

Impacto: Se refiere a una consecuencia de la materialización de la amenaza.

Frecuencia: Una forma de medir la probabilidad de amenazas.

Vulnerabilidad: Una debilidad o fallo del sistema que amenaza la seguridad de la información, lo que puede ser utilizado por un atacante para destruir o dañar los activos de información de la organización.

Emergencia: Una situación causada por un evento peligroso de origen natural y antrópico, cuya ocurrencia o inminencia tiene el potencial para afectar el funcionamiento de una entidad, comunidad o sociedad.

Desastre: Tipos de eventos adversos son más graves que las emergencias; es un término general para cosas que pueden tener un impacto destructivo en los humanos y el medio ambiente del que dependen.

Identificación de riesgo: El proceso de identificación de la naturaleza de los riesgos por percepción, juicio o clasificación.

Evaluación de riesgos: Evaluar las amenazas, debilidades, impactos que enfrentan los activos de información, y los efectos combinados de los tres.

Análisis cualitativo: La valoración se realiza por el grado de importancia; permite centrarse en aspectos que son difíciles de cuantificar con precisión o de explicar con medidas cuantitativas.

Análisis cualitativo: La valoración se aplica de manera numérica; un estudio que recopila y analiza datos cuantitativos sobre variables.

2.2.3 Términos de la gestión de riesgos

Gestión del riesgo: Proceso de planificación y aplicación de medidas orientadas a minimizar o controlar riesgos y su impacto potencial. Incluye la prevención, mitigación, preparación, recuperación y reconstrucción.

Prevención: Conjunto de medidas y acciones encaminadas a evitar o reducir la ocurrencia de un fenómeno peligroso de desastres existentes y nuevos.

Mitigación: Actividades y métodos para reducir o minimizar el riesgo o los impactos de un posible evento.

Preparación: Conocimientos y capacidades desarrolladas por los gobiernos, las organizaciones de respuesta y recuperación, las comunidades y los individuos, para prever, responder a las amenazas y recuperarse de ellas de manera efectiva.

Reconstrucción: Corresponde a la restauración y mejora de los servicios públicos dañados por eventos adversos, evitando la recurrencia de condiciones de vulnerabilidad o la construcción de nuevos factores de riesgo.

Salvaguardas: Medidas preventivas tomadas para reducir o mitigar riesgos**.**

Plan de Tratamiento de Riesgos (PTR): Es un conjunto de proyectos interrelacionados que reúnen salvaguardas surgidas del análisis de riesgos.

Plan de contingencia: Es un plan para lidiar con pérdidas reales o potencialmente graves de un accidente peligroso, encaminados a conseguir una recuperación ordenada para respaldar los procesos comerciales vitales en el Plan de Continuidad de Negocio de la empresa.

Plan de Continuidad de Negocio: Es un conjunto de planes diseñados para reducir el impacto en la información de la empresa y los procesos comerciales debido a la acumulación de ciertos riesgos.

2.3 METODOLOGÍA

En este apartado, explicamos los métodos utilizados para diseñar el sistema de gestión de seguridad de la información para la empresa COC M.T., que se centra principalmente en el análisis teórico combinado con la investigación empírica. Con base en la norma ISO / IEC 27001: 2013, se utilizan el análisis de brechas GAP y el método MAGERIT para llevar a cabo los requisitos y actividades de desarrollar este Trabajo Fin de Máster.

A continuación, explicamos la metodología que vamos a utilizar para el desarrollo de este proyecto.

2.3.1 Metodología de investigación

En este Trabajo Fin de Máster, nos proponemos diseñar un Sistema de Gestión de Seguridad de la Información (basado en la norma ISO/IEC 27001:2013) para la empresa elegida. En primer lugar, hemos de analizar la situación inicial de la empresa;

hay que conocer hasta qué punto están implementados los controles recogidos en el Anexo de la norma ISO/IEC 27001:2013. Por ello, antes de comenzar el diseño del Sistema de Gestión de Seguridad de la información, hay que realizar un análisis inicial de cumplimiento de dichos requisitos y controles; para obtener el informe de auditoría de cumplimiento de la organización, se realizará un análisis de brechas de GAP.

Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito[7]. Gap se refiere al espacio entre "donde estamos" (el presente) y "donde queremos estar" (el objetivo a alcanzar)[8].

A través del análisis de brechas GAP, se puede medir cuantitativamente la brecha entre los propósitos de seguridad de la información y el estado de seguridad en términos de medidas de control de seguridad y capacidades de garantía de seguridad, lo cual permitirá mejorar el análisis y el diseño de la seguridad de la información.

2.3.2 Metodología para el análisis de riesgos

MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; ha sido elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, y enfocada a las Administraciones Públicas[9].

Esta metodología ofrece una guía técnica para realizar el análisis y gestión de riesgos. MAGERIT versión 3 se estructura en tres libros:

- **Método:** Se describe el marco de análisis y gestión de riesgos.
- **Catálogo de Elementos:** Ofrece unas pautas sobre activos, amenazas y salvaguardas y proporciona ayudas para acometer el análisis de riesgos, normalizando terminología y promoviendo criterios uniformes para homogeneizar resultados.
- **Guía de Técnicas:** Se detallan técnicas que se suelen utilizar para realizar proyectos de análisis y gestión de riesgos, como tablas, algoritmos, árboles de ataque, técnicas gráficas, etc.

[7] https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/
[8] https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/
[9] https://es.wikipedia.org/wiki/Magerit

MAGERIT persigue una aproximación metódica para el análisis y gestión de riesgos, basando en los siguientes pasos:

- Determinar los activos relacionados con la organización y medir el valor.
- Determinar las amenazas a estos activos.
- Valorar las vulnerabilidades.
- Estimar el riesgo.
- Definir las salvaguardas de seguridad.

La siguiente figura muestra el proceso de la metodología MAGERIT y los elementos del análisis de riesgos:

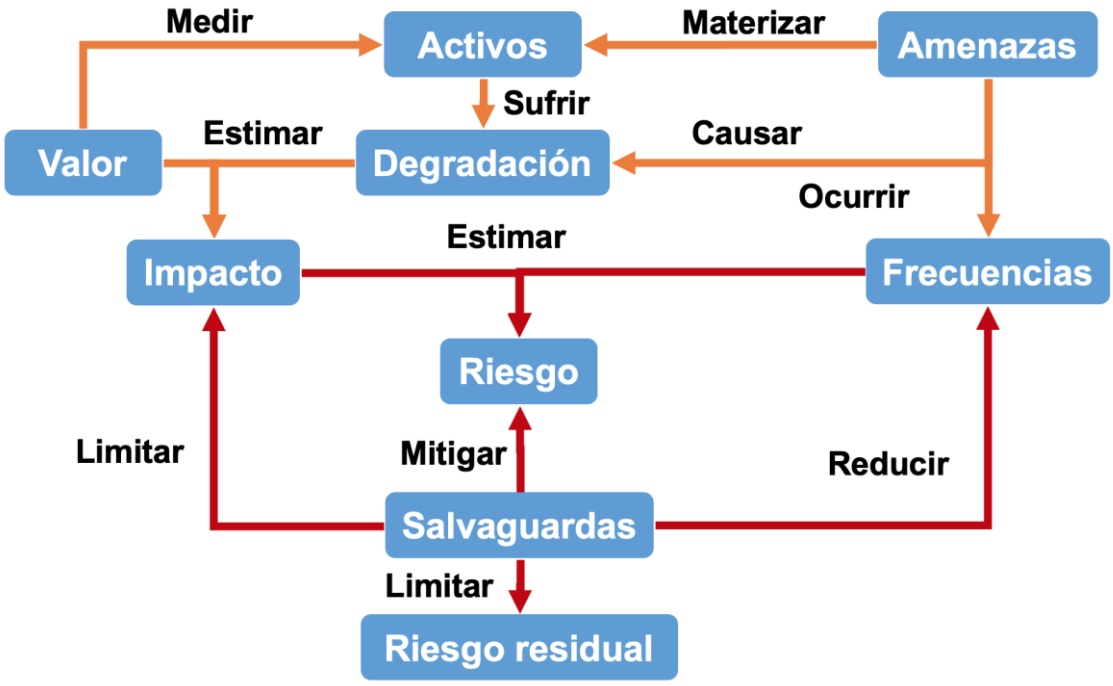

Figura 5. Nivel Cumplimiento Objetivos de Control

Fuente: Elaboración propia basada en

http://www.securitybydefault.com/2012/10/ccn-cert-magerit-v3-y-17-nuevas-guias.html

3. DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN COC M.T.

Este capítulo corresponde a las diferentes fases de desarrollo definidas para el diseño del Sistema de Gestión de Seguridad de la Información de COC M.T., las cuales una serie de actividades como el análisis de la situación actual de la empresa, encuestas, cuestionarios, y el análisis de riesgos para lograr los objetivos específicos establecidos para alcanzar el objetivo de este Trabajo Fin de Master.

3.1 FASE I: DIAGNÓSTICO

En la primera fase, se analizará la situación actual del Sistema de Gestión de Seguridad de la Información en la empresa COC M.T., y se realizará el análisis GAP de una lista de chequeo diseñada para verificar el grado de implementación de los controles del Anexo A de la norma ISO / IEC 27001:2013 (ver Anexo **A**).

Para realizar este diagnóstico, la técnica utilizada para obtener información es, como hemos dicho, una lista de chequeo diseñada en base a los controles definidos en el Anexo **A**, que fue respondida por el gerente del departamento del Centro de Tecnología de la Información.

Como se indica en el Anexo **B**, la lista de chequeo consta de los 114 controles contemplados en de la norma ISO 27001:2013, con opciones de respuestas "Completamente implementado" (C) , "Parcialmente implementado"(P), "No implementado"(N).

De acuerdo con la información recopilada en el Anexo **B**, calculamos la proporción de opciones y determinamos que el nivel de cumplimiento de completamente implementado es de 48%, lo que implica, que la empresa carece de muchas medidas de control o su nivel de cumplimiento es bajo.

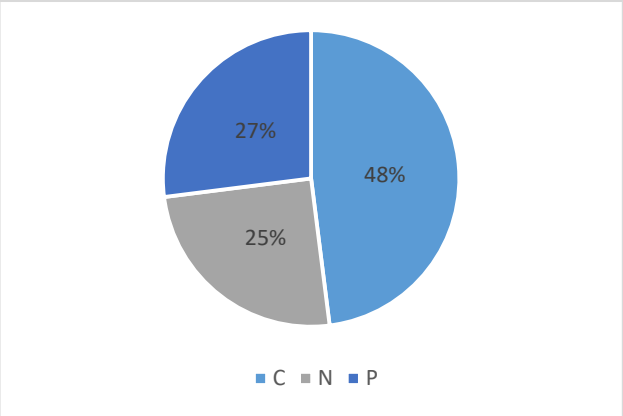

Figura 6. Nivel de controles de la empresa COC M.T.

Fuente: El Autor

A continuación, para calcular el cumplimiento de cada dominio, asignamos porcentajes a estas opciones:

Opción	Porcentaje
C	100%
P	50%
N	0%

Tabla 1 . Porcentaje de opciones

Como se muestra en el Anexo **C**, mostraremos los resultados de manera gráfica. En base a la evaluación de 114 controles, analizaremos el nivel de cumplimiento de cada control clasificado por dominio. Para facilitar el análisis de los resultados, el siguiente gráfico muestra el cumplimiento de todos los dominios:

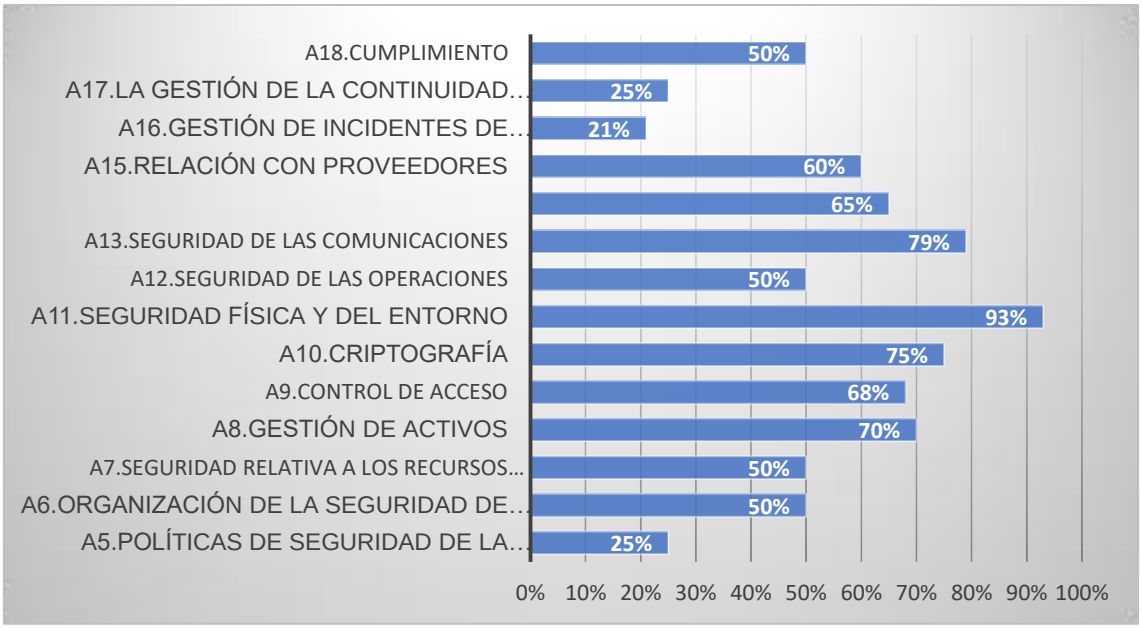

Figura 7. Nivel Cumplimiento Objetivos de Control

Fuente: Elaboración propia

3.1.1 Evaluación de la situación actual

A continuación, se analizará cada uno de los objetivos de control clasificados por el nivel de cumplimiento, de modo que tengamos una idea más específica sobre el trabajo requerido para cumplir con la norma ISO 27001 y el estado de cada control.

1) El nivel de cumplimiento 'Bajo'

En los siguientes dominios, el cumplimiento de los objetivos de control del Anexo A por parte de la empresa se encuentra en un nivel Bajo (Porcentaje: >=0% y <=39) debido a la falta de control o implementación inadecuada; representa un riesgo Alto para la empresa, lo que resulta una protección insuficiente de los activos de información e incluso puede afectar la continuidad del negocio.

Objetivos de control	Cumplimiento %
A5. Políticas de seguridad	**25%**
A16. Gestión de Incidentes de seguridad de la información	**21%**
A17. Continuidad de la seguridad de la información	**25%**

Tabla 2 . El nivel BAJO (Porcentaje: >=0% y <=39)

- **Dominio 5: Políticas de seguridad (Bajo: cumplimiento 25%)**

Actualmente, aunque la empresa ha definido políticas de seguridad, no han sido aprobadas ni revisadas por la Alta Dirección. Esto evidencia que los empleados y terceros que brindan servicios a la empresa no se dan cuenta de la importancia de cumplir con las regulaciones.

Es necesario establecer una estrategia de seguridad aprobada por la Alta Dirección, para especificar cómo se debe desarrollar el plan de seguridad y sus objetivos, asignar responsabilidades y describir cómo se debe implementar.

- **Dominio 16: Gestión de Incidentes de seguridad de la información (Bajo: cumplimiento 21%)**

La empresa no tiene una estrategia para los procesos de gestión de incidentes de seguridad de la información, ni tiene los históricos documentados. Se deben establecer los procedimientos o canales efectivos para permitir la notificación, gestión y evaluación de incidentes de seguridad de la información, y formular un plan de respuesta a emergencias para incidentes de seguridad de la información.

La estrategia debe hacer que todos los empleados sepan cómo enfrentar los incidentes de seguridad de la información, abordar las emergencias de manera oportuna y eficaz, minimizar el impacto de los incidentes de seguridad de la información en los sistemas de información, comunicaciones, etc., para que se puedan tomar medidas correctivas de inmediato.

- **Dominio 17: Continuidad de la seguridad de la información (Bajo: cumplimiento 25%)**

Se observa que la empresa no tiene definido ningún plan para garantizar la seguridad de la información en circunstancias adversas, lo que puede dañar la disponibilidad y continuidad del negocio de la empresa. La continuidad de la seguridad de la información es esencial, ya que permite establecer, registrar, implementar y mantener los procesos, procedimientos y controles necesarios para la seguridad de la información en diversas situaciones.

2) El nivel de cumplimiento ‘Medio’

En los siguientes dominios, el cumplimiento de los objetivos de control del Anexo A por parte de la empresa se encuentra en un nivel Medio (Porcentaje:>=40% y <=55%), debido a que algunos de los controles no se implementan, documentan o formalizan adecuadamente; lo que implica un riesgo Medio para la empresa; una vez que ocurre,

puede causar ciertos impactos económicos, sociales o de producción y operación, pero el grado de impactos no es grande.

Objetivos de control	Cumplimiento %
A6. Organización de la seguridad de la información	**50%**
A7. Seguridad de los recursos humanos	**50%**
A12. Seguridad en la Operativa	**50%**
A18: Cumplimiento	**50%**

Tabla 3 . El nivel MEDIO (Porcentaje:>=40% y <=55%)

- **Dominio 6: Organización de la seguridad de la información (Medio: cumplimiento 50%)**

A pesar de que la entidad define los roles y responsables de la seguridad de la información, y los asigna a todos los desarrolladores del departamento de la información; no existe un responsable a tiempo completo y estos no tienen la experiencia específica en seguridad de la información, lo que conduce a una división borrosa de responsabilidades dentro del departamento. Si existe un riesgo de seguridad de la información, no se puede ejercer el control adecuado para todos los activos informáticos y asegurar la seguridad sobre ellos.

- **Dominio 7: Seguridad de los recursos humanos (Medio: cumplimiento 50%)**

Con respecto al cumplimiento, el dominio 7 refleja que los empleados y terceros han sido informados sobre los roles y responsabilidades de la seguridad de la información a través de los términos del contrato, las políticas y procedimientos establecidos por la organización.

En cuanto al incumplimiento, la empresa no cuenta con una investigación de antecedentes respecto a la seguridad de la información antes de la contratación de personal, tampoco existe un mecanismo de gestión para tomar medidas contra los empleados que violen las normas de seguridad de la información. Es necesario desarrollar programas de capacitación destinados a aumentar la conciencia y el conocimiento de la seguridad de la información.

- **Dominio 12: Seguridad en la Operativa (Medio: cumplimiento 50%)**

Dado que el desarrollo, las pruebas y los entornos operativos no están separados, existe un alto riesgo de acceso no autorizado. En el proceso de registro y supervisión, no se generaron ni mantuvieron todos los registros necesarios, y no se establecieron medidas de protección y auditoría para ellos.

Estos resultados reafirman que el software de antivirus no es suficiente, la entidad debe implementar medidas de control para la detección, prevención y recuperación del software malicioso. Además, es necesario establecer auditorías periódicas de sistemas de información en cuanto a los procesos tales como implementar cambios, e instalación de software.

- **Dominio 18: Cumplimiento (Medio: cumplimiento 50%)**

Dentro de este objetivo de control, la entidad ha documentado la normatividad y leyes que deben seguirse de acuerdo con las operaciones comerciales. El departamento de Tecnología de Información es responsable de implementar procedimientos apropiados, con el propósito de garantizar que el uso de los derechos de propiedad intelectual relevantes y los productos de software cumplan con los requisitos de las leyes, reglamentos y contratos.

Con respecto a la protección de datos, esta carece de políticas de confidencialidad y de control sobre la manipulación de la información, lo que conlleva a riesgos de fuga de información y robo.

3) El nivel de cumplimiento 'Alto'

En los siguientes dominios, el cumplimiento de los objetivos de control del Anexo A por parte de la empresa se encuentra en un nivel Alto (Porcentaje:>=56% y <=100%), debido a la implementación de las medidas de control necesarias, pero aún existen algunas pequeñas omisiones en los detalles, lo que significa riesgo Bajo, generalmente limitado a la organización, y puede resolverse rápidamente a través de ciertos medios.

Objetivos de control	Cumplimiento %
A8. Gestión de activos	**70%**
A9. Control de acceso	**68%**
A10. Cifrado	**75%**
A11: Seguridad física y ambiental	**93%**

A13: Seguridad de las comunicaciones	**79%**
A14: Adquisición, desarrollo y mantenimiento de los sistemas	**65%**
A15: Relaciones con los proveedores	**65%**

Tabla 4. El nivel ALTO (Porcentaje: >=56 y <=100%)

- **Dominio 8: Gestión de activos (Alto: cumplimiento 70%)**

La entidad cuenta con un departamento de activos fijos encargado de realizar el inventario de todos los activos importantes, y que registra cada uno de los equipos e historial de mantenimientos. En la aplicación HRSC, existe un sistema de identificación y clasificación de activos, que se puede determinar de acuerdo con sus necesidades, prioridad y nivel de protección.

Las medidas de control para la manipulación de la información no son perfectas. Además del control de acceso del sistema de información, es necesario proponer estrategias para evitar la fuga de información. Por lo tanto, es importante garantizar la seguridad física y lógica de todos los activos de información y solo otorgar a los usuarios los permisos necesarios para acceder a la información.

- **Dominio 9: Control de acceso (Alto: cumplimiento 68%)**

En cuando al control de acceso, la entidad se encuentra en un nivel alto de cumplimiento debido a la implementación de políticas de control de acceso que gestionan los accesos a las redes y servicios. Por lo tanto, para mejorar el cumplimiento de este control, se recomiendan las siguientes medidas:

- Auditar los derechos de acceso de manera regular para asegurar estar en concordancia con los negocios y requisitos respecto a la seguridad de la información.
- Revisar el acceso y autenticación de usuario para verificar la validez de manera regular.
- Ajustar los derechos de acceso al momento de la designación, finalización del contrato o acuerdo cuando se modifiquen.
- Establecer un sistema interactivo de la gestión de contraseñas para garantizarlas en alta calidad.

- **Dominio 10: Cifrado (Alto: cumplimiento 75%)**

Se evidencia que la entidad ya ha aplicado una política de uso de los controles criptográficos para proteger la transmisión de información, pero no cuenta con un debido mecanismo de gestión de claves, lo cual representa un riesgo de que la clave se pierda o se filtre a personas no autorizadas.

- **Dominio 11: Seguridad física y ambiental (Alto: cumplimiento 93%)**

Se encuentra en un alto grado de cumplimiento debido a las instalaciones físicas de la empresa, mantiene una estructura moderna que garantiza en gran medida la seguridad de los activos de información desde la estructura física. Para dar total cumplimiento, la empresa debe establecer las medidas idóneas que protejan los equipos y el cableado contra las fallas u otros daños.

- **Dominio 13: Seguridad de las comunicaciones (Alto: cumplimiento 79%)**

Existe canales seguros para conectar usuarios externos o remotos, debido al uso de VPN que asegure los datos que transmiten a través del canal de comunicaciones. Para monitorear y controlar el tráfico de la red, la existencia de un software cortafuegos garantiza la ciberseguridad.

El único inconveniente es que no ha establecido y revisado periódicamente si los requisitos establecidos para los acuerdos de confidencialidad reflejan las necesidades de protección de la información de la organización.

- **Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas (Alto: cumplimiento 65%)**

El parte del incumplimiento de control se manifiesta principalmente en las siguientes situaciones:

- No incluye los requisitos de control de seguridad para los nuevos sistemas de información.
- No se controlan los cambios del sistema en el ciclo de vida del desarrollo mediante el uso de una plataforma formal de control de cambios; la mayoría de los cambios diarios se basan en la conciencia personal y la experiencia pasada de los empleados.
- No se incluyen pruebas de aceptación y estándares relacionados para los sistemas de información, lo que puede generar debilidades o vulnerabilidad que

pueden ser utilizado por atacantes para destruir o dañar los activos de información de la empresa.

En resumen, las restricciones de seguridad de la información para toda la vida del sistema deben fortalecerse. Especialmente en la seguridad de las aplicaciones, fortalecer la garantía de seguridad de los sistemas de aplicaciones durante todo el ciclo de vida. Al mismo tiempo, clasificar, analizar y resumir los problemas que se han descubierto para formar especificaciones de gestión de desarrollo para guiar la construcción de seguridad del sistema posterior.

Dominio 15: Relaciones con los proveedores (Alto: cumplimiento 65%)

Se evidencia que solo se monitorea, revisa y audita la presentación de servicios del proveedor regularmente, pero no existe una definición de las pautas de seguridad de la información del proveedor para evitar el acceso no autorizado a la información. No gestiona los cambios en las ofertas de servicios del proveedor; sobre la base de la reevaluación de riesgos, es necesario mantener y mejorar continuamente las estrategias, los procesos y las medidas de control de seguridad de la información existentes.

3.2 FASE II: PREPARACIÓN

Esta fase del trabajo consiste en desarrollar las siguientes actividades con el propósito de cumplir los requisitos de la norma ISO 27001:2013 recogidos en la cláusula 4[10]:

- Comprender contexto interno y externo de la organización para determinar la capacidad de lograr los objetivos del Sistema de Gestión de Seguridad de la Información.
- Definir el alcance del Sistema de Gestión de Seguridad de la Información para identificar qué se necesita proteger y qué restricciones.
- Elaborar la política del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta los objetivos de la organización.

3.2.1 Contexto de la organización

Es vital conocer y comprender las situaciones y factores externos e internos que la rodean, y que pueden tener un impacto positivo o negativo en el establecimiento del

[10] NTC-ISO-IEC 27001:2013, Pág. 1

Sistema de Gestión de Seguridad de la Información. Para determinar estas influencias, determinamos los siguientes pasos:

1) Conocimiento de la organización

COC M.T. es una subsidiaria del Grupo afiliada a una de las compañías de Global 500. Desde su creación, ha mejorado continuamente la calidad y el nivel de servicio y ha ganado la confianza y el completo apoyo de clientes y empleados.

COC M.T. es una empresa de Recursos Humanos, constituida con personería jurídica, certificaciones de despacho de recursos humanos y gestión de relaciones laborales. Combina medios tradicionales, medios en línea y tecnología de información avanzada, además de un equipo de consultores profesionales con experiencia para proporcionar una gama completa de servicios profesionales de recursos humanos que incluyen reclutamiento, capacitación y evaluación y subcontratación de personal.

Todo ello, junto con el sistema de información HRSC, permitirá proporcionar a sus clientes respuestas oportunas y verdaderas.

2) Misión

Siempre cumpliendo con el concepto de "tres victorias y sabiduría común" de clientes, empleados y la empresa, ofreciéndoles el mejor servicio.

3) Visión

Para el 2030 la perspectiva es convertirse en una de las empresas de servicios de recursos humanos profesionales más influyentes del mundo.

4) Estructura organizacional (Ver Anexo D)

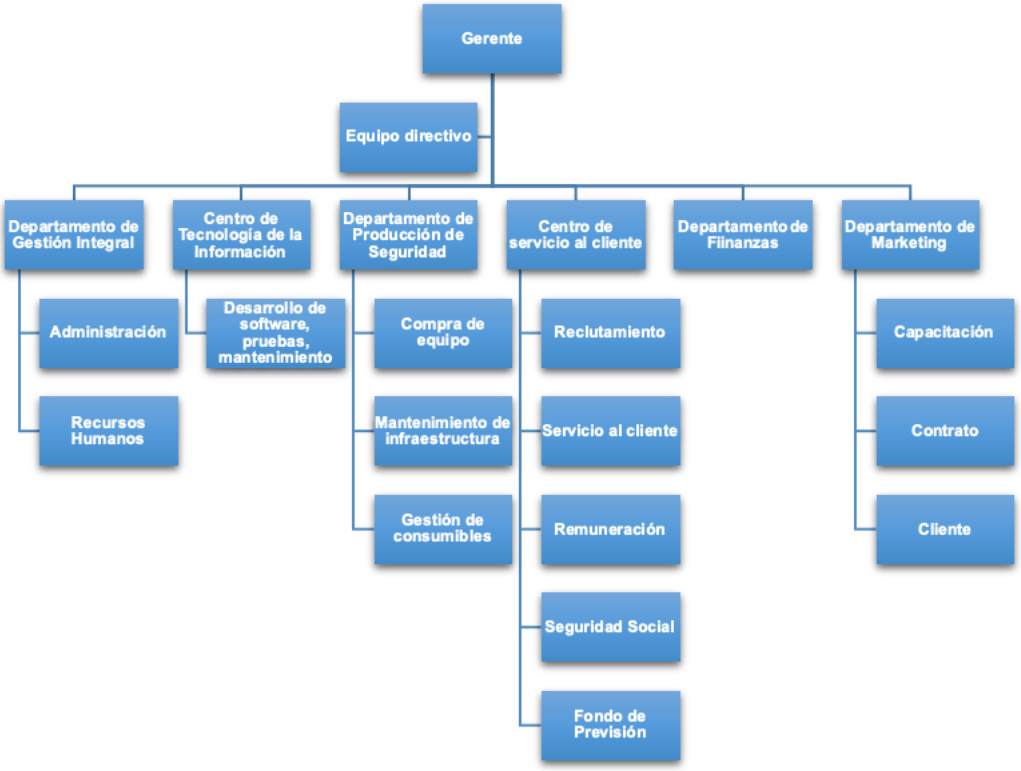

Figura 8. Organigrama de la empresa

Fuente: Elaboración propia basada en la empresa

En la empresa, hay dos áreas que realizan funciones de seguridad de la información: el Centro de Tecnología de la Información que desempeña las de seguridad lógica y seguridad de las aplicaciones, y el Departamento de Producción de Seguridad que desempeña las funciones de seguridad física. En el Anexo D, se presentan las otras áreas críticas de la empresa.

5) Mapa de proceso

Los procesos de una organización se dividen en 3 grandes grupos: procesos estratégicos, procesos operativos y procesos de soporte.

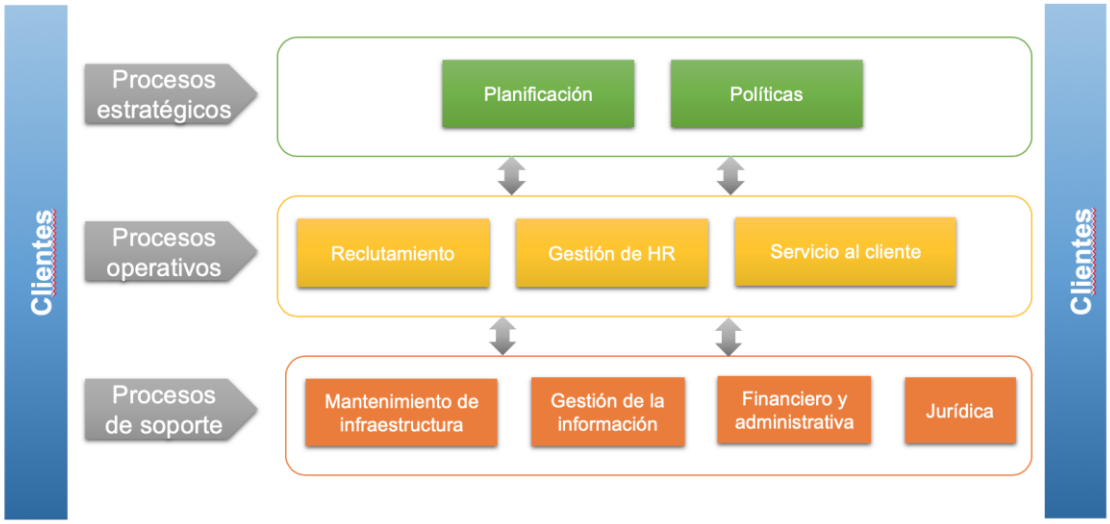

Figura 9. Macro procesos

Fuente: Elaboración propia basada en la entidad

La seguridad de información de la empresa COC M.T. está constituida principalmente por los siguientes procesos:

Mantenimiento de infraestructura. Su responsabilidad es garantizar la seguridad física que brinda el soporte al usuario en el proceso relacionado con los sistemas de información y equipos de comunicación. Administrar y soportar los recursos tecnológicos empresariales a través de los cuales se realiza el intercambio y el almacenamiento, cubriendo equipos informáticos, equipos de red, redes de datos y aplicaciones de oficina, con el objetivo de asegurar los activos de información y garantizar su mejora continua.

Gestión de la información. Su objetivo es desarrollar y mantener el funcionamiento normal de las aplicaciones y los sistemas de información utilizados en la empresa. Es responsable de garantizar la seguridad lógica y las aplicaciones diseñadas para evitar posibles ciberamenazas, y de tomar las medidas necesarias para prevenirlas o identificarlas.

6) Trámites

- **Políticas de seguridad de la información:** Actualmente la empresa simplemente cuenta con una política de seguridad del entorno de oficina, no aplica ni tiene una política establecida de seguridad de la información.

- **Medidas de emergencia:** Según los planes y políticas de la empresa, el mantenimiento y la actualización de cualquier equipo e infraestructura deben aplicarse a través del sistema HRSC para formar un registro de hechos. Para fallas en el servicio del equipo o en la red, se requiere la intervención del proveedor, solicitando y archivando copia del reporte. Para control de cambios de partes, daños, actualizaciones en los equipos de cómputo, son realizados en el sistema por el responsable.

3.2.2 El alcance del SGSI

El alcance trata de determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información de la empresa[11].

Como los requisitos para definir el alcance que dice la norma ISO 27001, el alcance del sistema de gestión de seguridad de la información de la empresa corresponde a lo siguiente:

El alcance del Sistema de Gestión de Seguridad de la Información cubre el proceso de Gestión de la Información y Mantenimiento de infraestructura de la entidad, que involucra el ciclo de vida de la información, desde su obtención hasta su disposición final.

El sistema de gestión de seguridad de la información solo es aplicable a la sede de la empresa (ubicada en Shenzhen), limitando la Tecnología de Comunicación de Información (TIC) entre las personas, los procesos y actividades desempeñadas por esta sede.

3.2.3 La política del SGSI

La norma ISO/IEC 27001:2013 en su numeral 5.2 Política, indica que la Alta Dirección de la entidad debe establecer una política de seguridad de la información adecuada al propósito de la organización, que incluya los objetivos de seguridad de la información, los requerimientos normativos vigentes relacionados con seguridad de la información y el compromiso de la mejora continua[12].

[11] Norma ISO/IEC 27001:2013, Pág. 2
[12] Norma ISO/IEC 27001:2013, Pág. 3

Atendiendo al estándar ISO 27001, es necesario tener en cuenta los procesos de negocio, servicios ofrecidos a los clientes y cualquier otra actividad relacionada con la operativa de la entidad para redactar una política.

Según los objetivos y el alcance de seguridad de la información de la empresa, la presente Política (ver Anexo E) especifica las responsabilidades y los principales de implementar la seguridad de la información.

El Equipo Directivo de la entidad debe conocer y aprobar la política de seguridad establecidas tanto como todo el personal de la empresa debe asumir la responsabilidad de la seguridad de la información, como parte de sus funciones de trabajo obligatorias dentro de la entidad.

3.3 FASE III: PLANIFICACIÓN

El presente trabajo se enfoca en el diseño, es decir, la planificación de un Sistema de Gestión de Seguridad de la Información es el núcleo de Trabajo Fin de Master.

En esta fase, basándonos en MAGERIT versión 3.0, consideramos las siguientes actividades para el análisis y la gestión de riesgos:

- Identificar los activos de información junto con sus amenazas y vulnerabilidades.
- Evaluar los riesgos de seguridad de la información.
- Definir un plan para el tratamiento de los riesgos identificados.
- Elaborar la declaración de aplicabilidad que detalle todos los controles aplicables y determine cuáles ya se han implementados y cuáles no son aplicables.

3.3.1 Identificación de los activos

Dado que la entidad tiene cientos o miles de activos (ver Anexo F), es difícil realizar un análisis de riesgos en todos ellos. Generalmente, se elige presentar y administrar activos relacionados con los procesos comerciales. Por lo tanto, se dibuja un mapa de activos que consta de tres niveles para agruparlos y asociarlos.

- Primer nivel - Proceso de negocio: Los procesos del negocio y los servicios de una organización.

- Segundo nivel - Proceso TI: Canales de información, internet o intranet, aplicaciones desarrolladas o adquiridas.
- Tercer nivel - Recurso TI: Resto de activos, tales como Hardware, Soportes de información, Instalaciones, Personas etc.

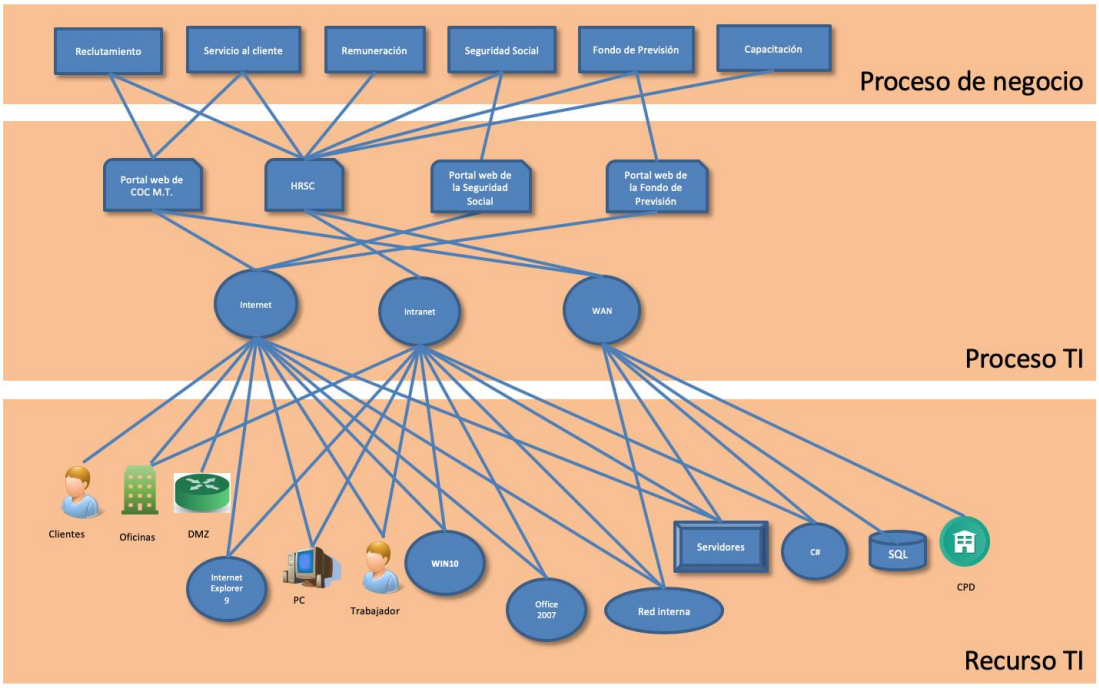

Figura 10. El mapa de activos

Fuente: Elaboración propia basada en la empresa

3.3.2 Valoración de los activos

El mapa de activos representa sus dependencias, y los problemas de seguridad de nivel inferior que afectarán los superiores. Por tanto, una vez que las dependencias entre los activos de la información se establecen de forma jerárquica, el valor del activo se puede calcular cuantitativa o cualitativamente.

En la metodología MAGERIT, se consideran las siguientes dimensiones de seguridad para realizar la evaluación correspondiente:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad
- Protección de Datos

En la tabla 6, los niveles "alto", "medio", "bajo" o "no aplicable" se asignan a cada dimensión.

Valor cualitativo	Valor cuantitativo	Criterio de Evaluación
No aplica	0	Daño insignificante para el negocio
Bajo	1-3	Daño bajo para el negocio
Medio	4-6	Daño medio para el negocio
Alto	7-10	Daño alto para el negocio

Tabla 5. La forma de valoración

A continuación, se analizará el valor del activo de cada nivel del mapa de activos bajo los criterios establecidos.

Niveles	Activos	Dimensiones						Vr Cuantitativa	Vr Cualititativo
		D	I	C	A	T	Pd		
Negocio	Reclutamiento	8	4	2	10	2	8	6	Medio
	Servicio al cliente	9	5	5	10	8	8	8	Alto
	Remuneración	7	5	6	10	10	8	8	Alto
	Seguridad Social	4	10	2	6	9	5	6	Medio
	Fondo de Previsión	4	10	2	6	9	5	6	Medio
	Capacitación	5	5	7	7	5	5	6	Medio
Proceso TI	Intranet	5	3	10	5	5	8	6	Medio
	WAN	5	3	10	5	5	8	6	Medio
	Internet	9	6	10	8	5	10	8	Alto
Recurso TI	CPD	5	5	5	3	7	10	6	Medio
	SQL	10	10	10	10	10	10	10	Alto
	Programas C#	10	8	8	9	9	10	9	Alto
	Servidores	7	8	10	8	9	10	9	Alto
	Red interna	10	7	6	9	3	8	7	Alto
	Office2010	6	3	0	0	0	0	2	Bajo
	WIN10	9	9	6	7	7	7	8	Alto
	IE9	6	0	9	7	8	10	7	Alto
	Trabajadores	3	3	5	8	8	8	6	Medio

	PCs	6	4	6	6	3	7	5	Medio
	DMZ	4	5	5	9	8	7	6	Medio
	Oficinas	2	6	4	0	3	7	4	Medio
	Clientes	3	3	5	8	8	5	5	Medio

Tabla 6. Valoración de activos

3.3.3 Identificación de las amenazas

Para proteger eficazmente los activos de la información, se deben encontrar las amenazas que pueden conducir a la seguridad de la información. Teniendo en cuenta la fuente, el agente y la motivación de la amenaza, como se muestra en el catálogo de amenazas, Anexo **G** del presente trabajo, que describe en detalle las amenazas que pueden enfrentar los activos de la información y el porcentaje de su impacto en cada dimensión de seguridad.

Según el catálogo de amenazas, combinado con los antecedentes de investigación de la empresa, se determinan las siguientes amenazas que pueden afectar los activos, y se analiza la vulnerabilidad.

Amenaza	Activos	Vulnerabilidad
[N] Desastres naturales	• Servidores • Pcs • Oficinas • CPD	• Ubicación física • Estructura del edificio • Inadecuada Administración de Seguridad Física
[E.2] Errores del administrador	• Reclutamiento • Servicio al cliente • Remuneración • Seguridad Social • Fondo de Previsión • Capacitación • WAN • Intranet • Internet	• Ausencia de capacitación en el uso del software • Gestión o asignación insuficiente de roles y permisos • Configuración incorrecta de las cuentas de usuario • Procedimientos de control de cambios faltantes o inadecuados
[E.3] Errores de monitorización (log)	• Reclutamiento • Servicio al cliente • Remuneración • Seguridad Social • Fondo de Previsión	• Inadecuado registro de actividades

	• Capacitación • Programas C#	
[E.7] Uso no previsto	• Trabajadores • Clientes	• Responsabilidades no están exactamente claros • Acciones descoordinadas • El acceso a los registros de acceso a los datos
[E.18] Destrucción de información	• SQL	• Inadecuado mecanismo de cifrado • La política no es aplicable • Gestión de seguridad insuficiente
[E.19] Divulgación de información	• SQL	• Inadecuado mecanismo de cifrado • Gestión de seguridad insuficiente • Gestión de claves inadecuada • La política no es aplicable • Pruebas de software insuficientes
[E.20] Vulnerabilidades de los programas (software)	• Programas C#	• Pruebas de software insuficientes • Defectos en el código
[E.21] Errores de mantenimiento / actualización de programas (software)	• Programas C#	• Procedimientos de control de cambios faltantes o inadecuados • Configuración y capacidad del entorno limitadas • Procedimientos de respaldo incompletos
[E.24] Caída del sistema por agotamiento de recursos	• Reclutamiento • Servicio al cliente • Remuneración • Seguridad Social • Fondo de Previsión • Capacitación • WAN • Red interna • Internet	• Falta de mantenimiento de equipos • Configuración y capacidad del entorno limitadas • Inadecuado inventario de activos físicos
[A.11] Acceso no autorizado	• Reclutamiento • Servicio al cliente • Remuneración • Seguridad Social • Fondo de Previsión • Capacitación	• Falta de configuración segura de la red • Gestión de claves inadecuada • Configuración incorrecta de las cuentas de usuario • La configuración del puerto de

	• WAN • Red interna • Internet • SQL • Servidores • DMZ • Programas C# • Pcs	red carece de seguridad
[A.14] Intercepción de información (escucha)	• Reclutamiento • Servicio al cliente • Remuneración • Seguridad Social • Fondo de Previsión • Capacitación • WAN • Red interna • Internet • SQL • Servidores • DMZ • Programas C# • Pcs	• La política no es aplicable • Gestión de seguridad insuficiente • Falta de configuración segura de la red • La configuración del puerto de red carece de seguridad
[A.30] Ingeniería social (picaresca)	• Trabajadores	• Falta de consentimiento

Tabla 7. Amenazas definidas

3.3.4 Valoración del riesgo

Una vez que se identifican las amenazas, es necesario determinar la probabilidad de su ocurrencia e impacto del mismo, y usar esto para determinar su valor.

Para determinar la probabilidad de que cada activo se vea amenazado, se utilizan los siguientes criterios de evaluación:

Rango	Nivel de probabilidad	Valor
Una vez cada año	Muy baja	0.1
Una vez cada seis (6) meses	Baja	0.3
Una vez cada tres (3) meses	Media	0.5
Una vez cada mes	Alta	0.7

Más de una vez al mes	Muy alta	0.9

Tabla 8. Valoración probabilidad

Para determinar el impacto de la amenaza en el activo, se utilizan los siguientes criterios de evaluación:

Impacto	Criterios	Valor
Muy bajo	Perdida menor a 30%	0.05
Bajo	Perdida mayor o igual a 30% y menor a 50%	0.10
Medio	Perdida mayor o igual a 50% y menor a 70%	0.20
Alto	Perdida mayor o igual a 70% y menor a 90%	0.40
Muy alto	Perdida mayor a 90%	0.80

Tabla 9. Valoración del impacto

Se considera que el riesgo es el producto de la probabilidad de impacto, que puede representarse mediante una matriz Probabilidad – Impacto, como se muestra en la siguiente tabla:

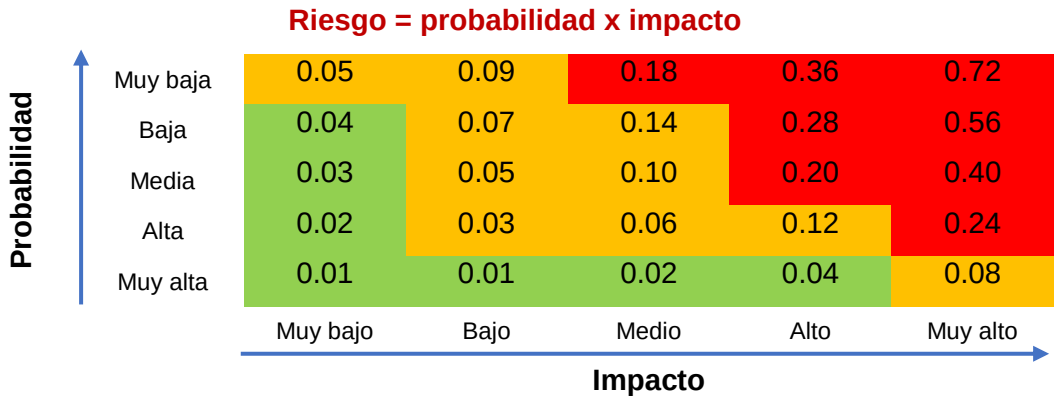

Tabla 10. La matriz Probabilidad

Los siguientes son los resultados de la evaluación de amenazas relacionadas con los activos comerciales:

Amenaza	Probabilidad	Impacto	Nivel de Riesgo
[N] Desastres naturales	Muy baja	Bajo	Bajo
[E.2] Errores del administrador	Alta	Bajo	Medio

[E.3] Errores de monitorización (log)	Muy alta	Alto	Alto
[E.7] Uso no previsto	Muy baja	Bajo	Medio
[E.18] Destrucción de información	Media	Alto	Alto
[E.19] Divulgación de información	Media	Medio	Medio
[E.20] Vulnerabilidades de los programas (software)	Media	Medio	Medio
[E.21] Errores de mantenimiento / actualización de programas (software)	Media	Bajo	Medio
[E.24] Caída del sistema por agotamiento de recursos	Muy baja	Alto	Alto
[A.11] Acceso no autorizado	Alta	Muy alto	Alto
[A.14] Intercepción de información (escucha)	Media	Medio	Medio
[A.30] Ingeniería social (picaresca)	Baja	Medio	Medio

Tabla 11. Evaluación de las amenazas

Finalmente, necesitamos analizar cuantitativamente el riesgo para determinar directamente si se deben tomar medidas de salvaguardia.

Todos los cálculos se basan en un libro de Excel. Al final, el valor de las amenazas se muestra en la siguiente figura:

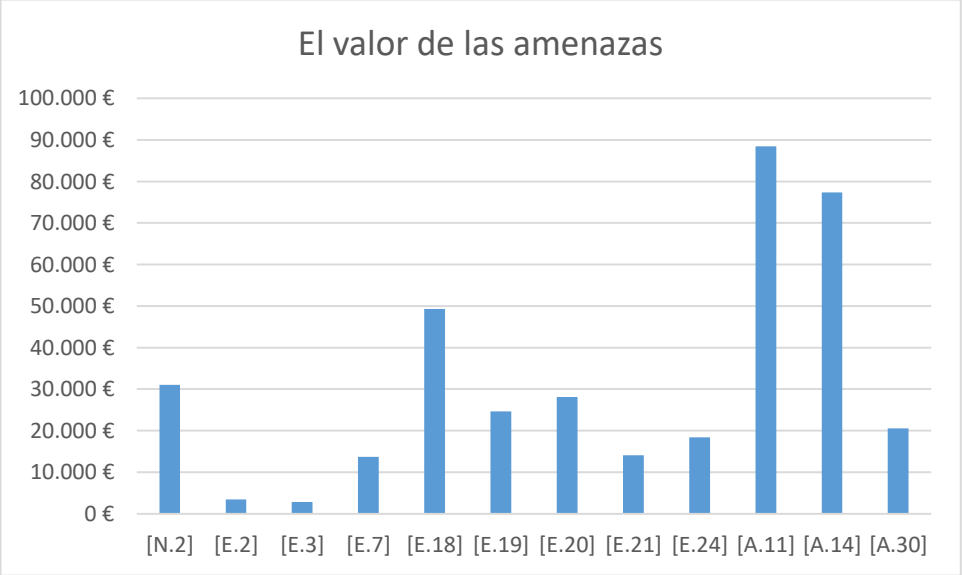

Figura 11. El valor de las amenazas

Fuente: Elaboración propia

3.3.5 Tratamiento de riesgos

Una vez identificados y evaluados los riesgos, el siguiente proceso es desarrollar un plan de tratamiento orientado a mitigar los riesgos identificados. El tratamiento del riesgo se basa en las siguientes cuatro opciones.

Opción	Acción de seguir
Evitar	Establecer medidas para evitarlo completamente, eliminando la causa que lo produce.
Transferir	Trasladar el riesgo a otras organizaciones, por ejemplo, a una aseguradora o al contratista.
Reducir	Establecer medidas para disminuir la probabilidad de que se produzca y para disminuir el impacto si se produce.
Aceptar	Si las consecuencias son pequeñas, se puede aceptar el riesgo, estableciendo un plan de contingencia para llevarlo a cabo cuando se produzca.

Tabla 12. Criterios para tratamiento de riesgos

De acuerdo con los criterios anteriores, se formulan las salvaguardas que sirven para evitar, disminuir o mitigar una amenaza determinada.

Amenaza	Opción	Salvaguarda
[N] Desastres naturales	Aceptar	Establecer las debidas pruebas de continuidad
		Formular planes de emergencia
[E.2] Errores del administrador	Reducir	Formación y concienciación
		Desarrollar el proceso de operación de auditoría
		Verificar el registro de eventos de seguridad regularmente.
[E.3] Errores de monitorización (log)	Evitar	Registrar toda la información posible relacionada con el acceso a servicios y configuraciones.
		SIEM (System Information and Event Monitoring)
[E.7] Uso no previsto	Reducir	Definir claramente el alcance, los roles y las responsabilidades del personal responsable de la seguridad de la información.
		Aumentar el acceso a los registros de acceso a los datos.
[E.18] Destrucción de	Evitar	Establecer políticas de transmisión de

información		información.
		Copias de seguridad en SQL
[E.19] Divulgación de información	Evitar	Cifrado de comunicaciones.
		Definir la política de protección de información
[E.20] Vulnerabilidades de los programas (software)	Reducir	Diseñar un procedimiento de los programas para incluir información confidencial en áreas con límites claros de confianza
		Realizar pruebas de penetración regularmente
[E.21] Errores de mantenimiento / actualización de programas (software)	Reducir	Separar los ambientes de Desarrollo y Pruebas
		Controlar y registrar cambios significativos sobre el proceso de actualización de programas.
[E.24] Caída del sistema por agotamiento de recursos	Reducir	Mantener y actualizar el equipo regularmente.
		Asignar recursos correctamente
[A.11] Acceso no autorizado	Reducir Evitar	Cifrado de comunicaciones.
		Vigilancia digital
		NAC (Network Access Control)
		Control de acceso
[A.14] Intercepción de información (escucha)	Evitar	Anti APT.
		Test de intrusión.
[A.30] Ingeniería social (picaresca)	Evitar	Formación y concienciación.
		Seguridad en los equipos informáticos.

Tabla 13. Salvaguarda de riesgos

En el Anexo **H**, basado en el principio de que el costo de una medida no puede ser mayor que los beneficios derivados de ella, las medidas de protección de seguridad que se aplicarán se seleccionan comparando los beneficios y los costos. Si su valor es "1", vale la pena adoptar esta medida porque sus beneficios son mayores que sus costos.

Estos proyectos se dividen en a corto, mediano o largo plazo, y se coordinan para que ciertos proyectos puedan ejecutar otros de acuerdo con el plan dependiente, por lo que obtenemos el Plan de Tratamiento de Riesgos (PTR) que se muestra a continuación:

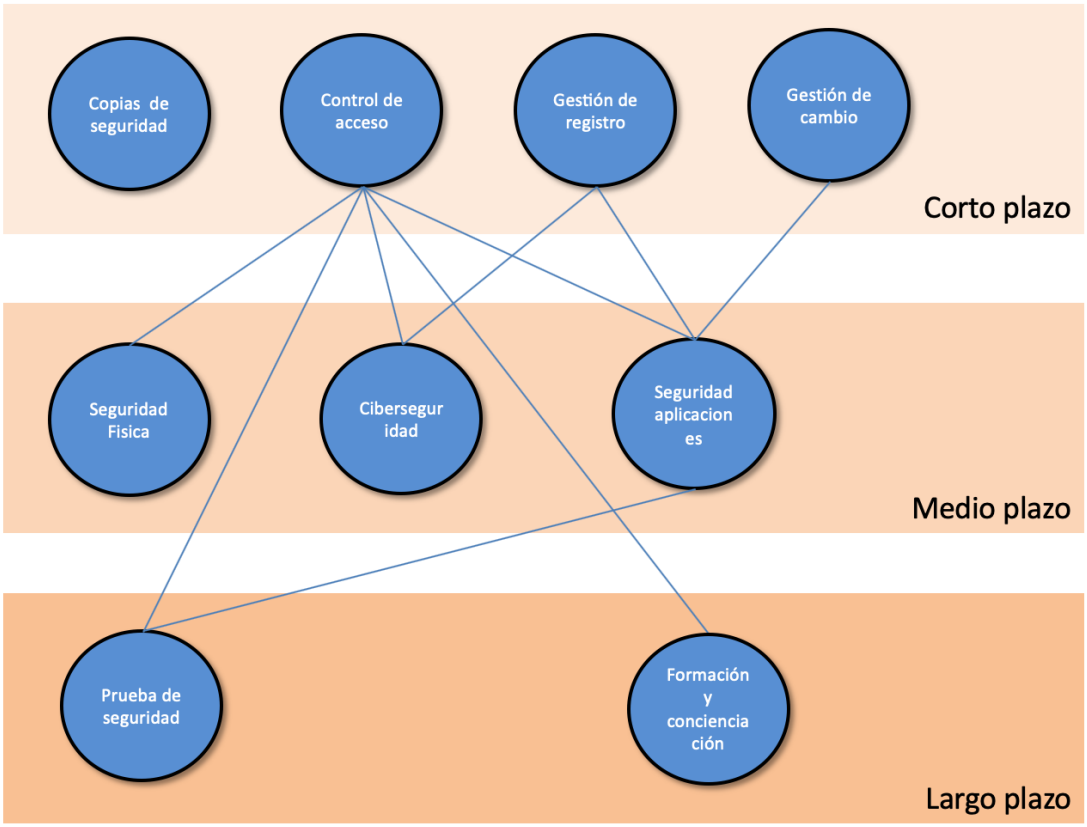

Figura 12. Plan de Tratamiento de Riesgos

Fuente: Elaboración propia

- **Copias de seguridad**

Las copias de seguridad se refieren a copiar los datos en el sistema de archivos o en el sistema de base de datos. En caso de desastre u operación errónea, los datos efectivos y el funcionamiento normal del sistema pueden restaurarse de manera conveniente y oportuna.

Objetivo: Garantizar la continuidad de negocio y la integridad de la información.

Ámbito: Los datos comerciales y en el entorno de desarrollo.

Responsable: Departamento de Producción de Seguridad, Centro de Tecnología de la Información

Tareas: Se muestra en la figura 9.

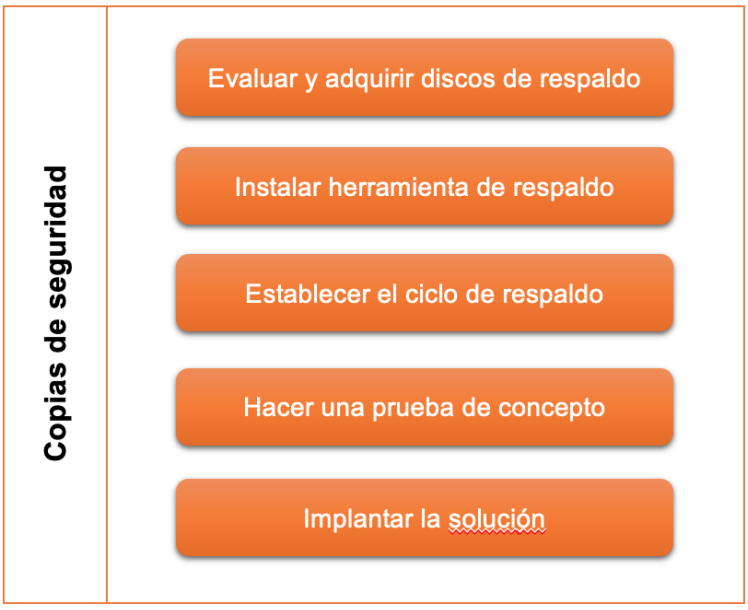

Figura 13. Copias de seguridad

Fuente: Elaboración propia

- **Control de acceso**

El control de acceso consiste en la verificación del acceso físico y lógico, especificando quién puede acceder y utilizar la información y los recursos de la empresa.

Objetivo: Proteger la información confidencial, como los datos del cliente, la información de identificación personal y la propiedad intelectual.

Ámbito: Las redes de comunicaciones, Programas C#, SQL, Servidores, PC, Oficinas etc.

Responsable: Departamento de Producción de Seguridad, Centro de Tecnología de la Información

Tareas: Se muestra en la figura 10.

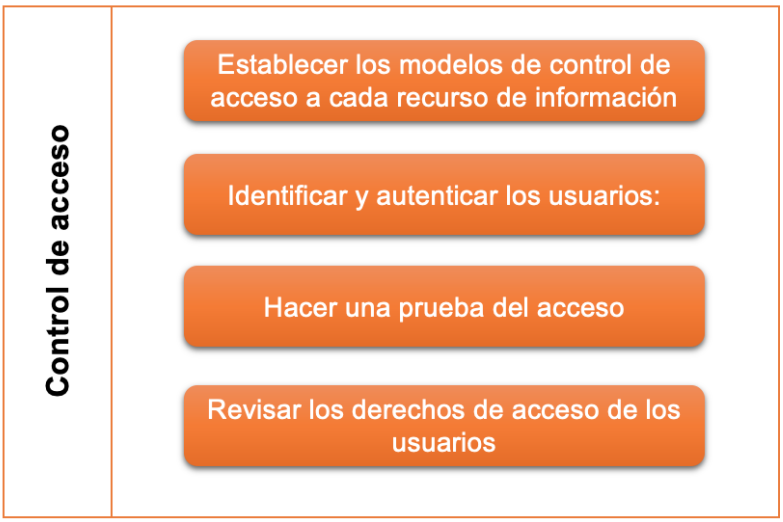

Figura 14. Control de acceso

Fuente: Elaboración propia

- **Seguridad física**

La seguridad física es un requisito previo para la seguridad de todo el sistema de información. Se refiere a proteger el equipo y las instalaciones informáticas, y proteger otros medios de accidentes ambientales como terremotos, inundaciones e incendios, errores de operación humana o daños causados por diversos delitos informáticos.

Objetivo: Proteger físicamente cualquier recurso del sistema.

Ámbito: Todos los equipos físicos.

Responsable: Departamento de Producción de Seguridad

Tareas: Se muestra en la figura 11.

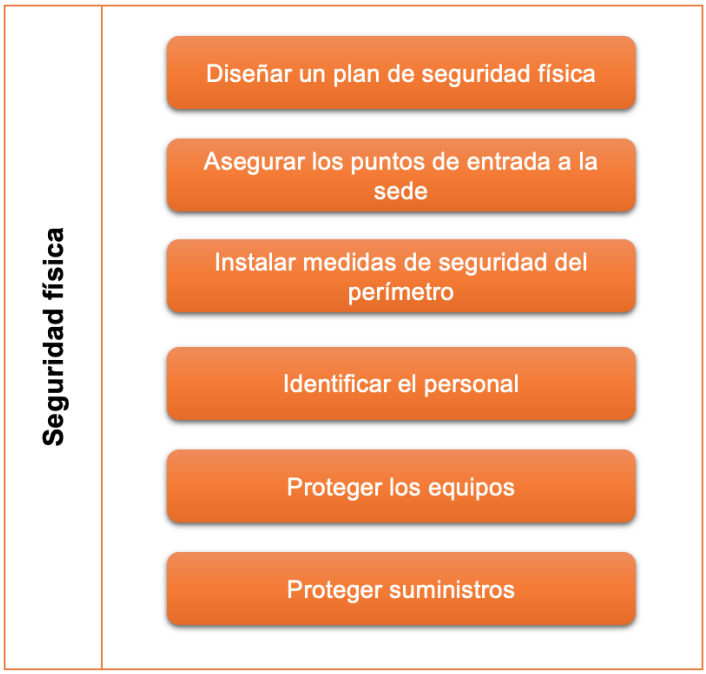

Figura 15. Seguridad física

Fuente: Elaboración propia

- **Gestión de registros**

La gestión de registros significa monitorear y administrar registros digitales o en papel, incluidas actividades como la creación, mantenimiento, recepción, uso y eliminación de registros. Permite que el análisis automático filtre los eventos más relevantes para sacar conclusiones, como errores específicos del sistema, problemas de rendimiento, errores inesperados e incluso detección de intrusos.

Objetivo: Facilitar las acciones tomadas contra los riesgos.

Ámbito: Todos los sistemas y equipos de información.

Responsable: Departamento de Producción de Seguridad, Centro de Tecnología de la Información

Tareas: Se muestra en la figura 12.

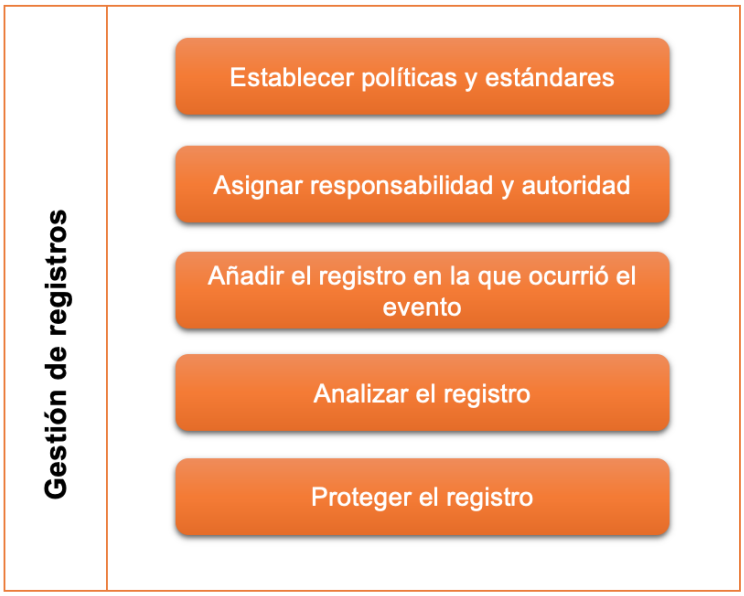

Figura 16. Gestión de registros

Fuente: Elaboración propia

- **Gestión de cambio**

Si se requieren cambios, deben ser controlados y gestionados. En particular, es necesario controlar los cambios en la organización, los procesos comerciales, las instalaciones de procesamiento de información y los sistemas que afectan la seguridad de la información de la organización.

Objetivo: Asegurar el logro de los objetivos de la organización.

Ámbito: Los cambios de los servicios y sistemas de procesamiento de información.

Responsable: Departamento de Producción de Seguridad, Centro de Tecnología de la Información

Tareas: Se muestra en la figura 13.

Figura 17. Gestión de cambio

Fuente: Elaboración propia

- **Prueba de seguridad**

Las pruebas de seguridad se centran en las amenazas de seguridad y en la consideración integral de amenazas de todos los aspectos y capas de software y hardware.

Objetivo: Confirmar la seguridad de los sistemas de información y bases de datos.

Ámbito: Todos los sistemas de hardware y software.

Responsable: Departamento de Producción de Seguridad, Centro de Tecnología de la Información

Tareas: Se muestra en la figura 14.

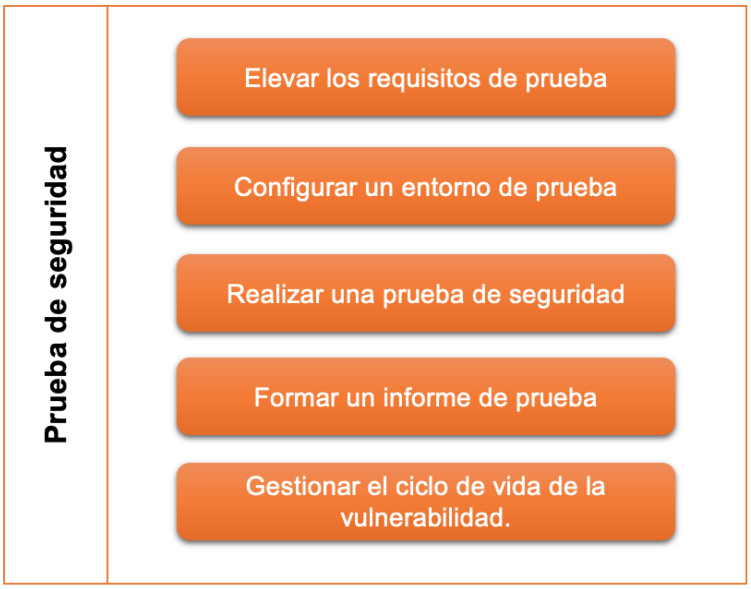

Figura 18. Prueba de seguridad

Fuente: Elaboración propia

- **Formación y concienciación**

La formación es un medio importante para mejorar la conciencia de seguridad del personal relevante de la compañía; en este caso, la capacitación se refiere específicamente a la seguridad de la información.

Objetivo: Aumentar la conciencia de los empleados sobre la importancia de la seguridad y mejorar el sentido de responsabilidad de ella.

Ámbito: Toda la organización.

Responsable: Departamento de Gestión integral

Tareas: Se muestra en la figura 15.

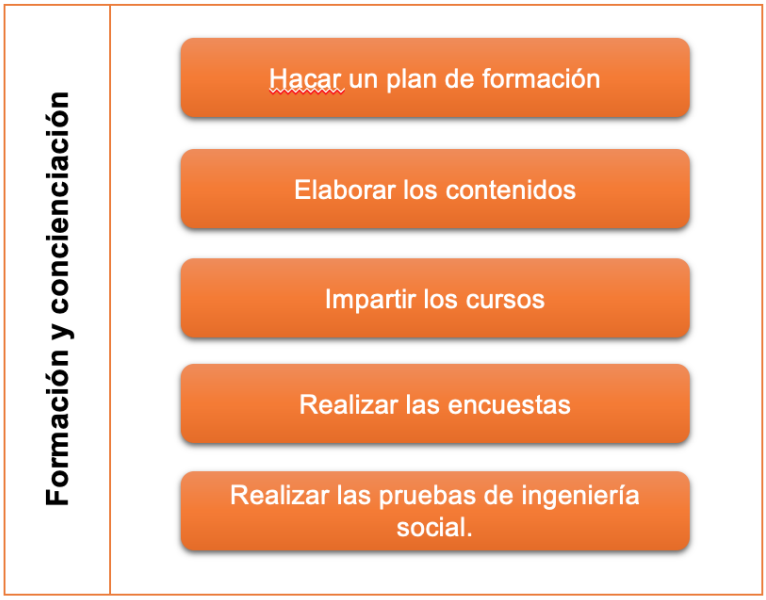

Figura 19. Formación y concienciación

Fuente: Elaboración propia

- **Seguridad de las aplicaciones**

La seguridad del software se refiere a la integridad, confidencialidad y disponibilidad de un sistema de información o su proceso de desarrollo. En otras palabras, se refiere al establecimiento de controles para garantizar la seguridad en el ciclo de vida de desarrollo, prueba y mantenimiento.

Objetivo: Garantizar la seguridad de las aplicaciones durante el desarrollo y uso.

Ámbito: Aplicaciones desarrolladas en la organización.

Responsable: Centro de Tecnología de la Información

Tareas: Se muestra en la figura 16.

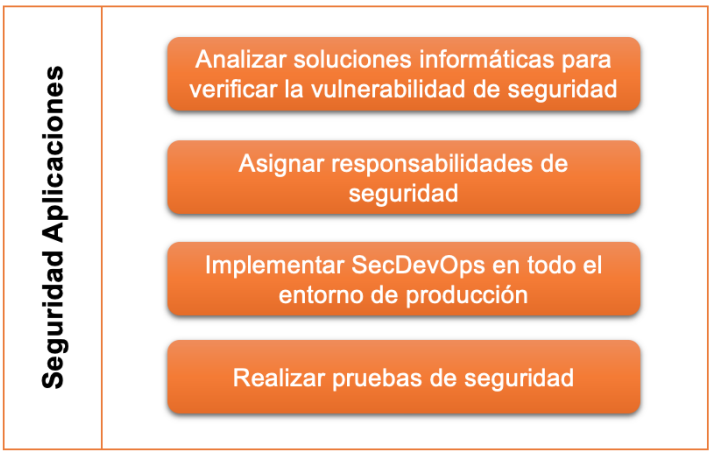

Figura 20. Seguridad aplicaciones

Fuente: Elaboración propia

- **Ciberseguridad**

La ciberseguridad se centra en tecnologías que protegen los activos informáticos de intrusos maliciosos.

Objetivo: Garantizar la seguridad de la transmisión de datos en el entorno de red.

Ámbito: Los equipos informáticos.

Responsable: Departamento de Producción de Seguridad

Tareas: Se muestra en la figura 17.

Figura 21. Ciberseguridad

Fuente: Elaboración propia

4. CONCLUSIONES

La gestión de la seguridad de la información es un proceso de desarrollo dinámico dado que la tecnología de la información cambia constantemente, así que la política de gestión de la seguridad de la información se ajustará dinámicamente en consecuencia.

En este Trabajo Fin de Máster, basándonos en la información recopilada sobre la empresa COC M.T., en primer lugar, realizamos una encuesta, a través de un cuestionario, sobre el personal involucrado en el proceso de gestión de seguridad de la información; a continuación, utilizando la metodología MAGERIT, realizamos el análisis de riesgos y analizamos los resultados; finalmente hacemos el diseño de un Sistema de Gestión de Seguridad de la Información acorde a las características de la empresa, detallando y justificando el proceso, tratamiento y sugerencias de construcción del mismo.

En el proceso de diseño del sistema de seguridad de la información, el presente trabajo prestó atención a la falta de gestión de la seguridad de la información de las empresas modernas de recursos humanos; analizó gradualmente los riesgos de los activos de información interna de la empresa a través del proceso de jerarquía analítica y subdividió los riesgos de seguridad, de modo que los resultados del análisis de riesgos estén más en línea con la situación real. Al final, se trata de hacer que todo el sistema de seguridad de la información sea más humano, científico y estandarizado.

Dado que el diseño del sistema es un proceso largo, no existe un modelo de sistema de gestión completamente maduro que se pueda aplicar. Este trabajo analizó preliminarmente el proceso de construcción del sistema a través del estudio de las características de la propia empresa, que se pueden resumir de la siguiente manera:

- Se realizó el análisis de brechas GAP para identificar la madurez de la empresa en relación con la gestión de seguridad de la información, aplicando un cuestionario estructurado con preguntas basadas en los objetivos de control de la ISO / IEC 27001:2013, con el objetivo de determinar qué requisitos y controles están incluidos en los estándares que hemos implementado en la organización y en qué medida están controlados.
- Los resultados muestran que el nivel de cumplimiento de completamente implementado con los requisitos del Anexo A de la norma ISO / IEC 27001: 2013 es de 48%. Dada la falta de mecanismos de supervisión y revisión por la Alta Dirección, la no existencia de evaluaciones de gestión de riesgos e incidentes y la

ausencia de plan de continuidad de negocio, el grado de cumplimiento de la norma sobre el sistema de gestión de seguridad de la información es bajo.

- A través de MAGERIT se identificaron los activos y riesgos de la información; los resultados determinaron las amenazas de la empresa, principalmente manifestadas en el sistema de información, control de acceso y ataques maliciosos desarrollados dentro de la organización.
- Con base en el contexto de la organización y los resultados del análisis de riesgos, se formuló el alcance, la política y el plan de tratamiento del sistema de gestión de seguridad de la información.

Como observación al caso de estudio, COC M.T. debe establecer un equipo dedicado a la gestión de seguridad de la información, independiente de la seguridad de producción, y definir claramente las responsabilidades de todos. Es importante resaltar que para que un sistema de gestión de seguridad de la información tenga éxito, debe ser aprobado y supervisado por la Alta Dirección de la empresa. Si no existe un compromiso de alto nivel para prestar atención a la seguridad de la información y a todos los activos informáticos, es inútil el diseño del sistema de gestión de seguridad de la información.

Este Trabajo Fin de Máster tendrá continuidad en el futuro; continuará rastreando el trabajo de diseño del sistema de gestión de seguridad de la información de COC M.T., teniendo como objetivo conseguir que el sistema de seguridad de la información de la empresa sea más científico, más completo, más instructivo y ajustado a la norma que tomamos como referencia.

BIBLIOGRAFIA

[1] ICONTEC, NTC-ISO-IEC 27001, 2013.

[2] Portal de ISO 27001 (2019), Guía paso a paso para implantar ISO 27001.

[3] Recuperado de: https://normaiso27001.es/

[4] Portal de ISO 27000 (2005), Serie 27K, Recuperado de https://www.iso27000.es/index.html

[5] Portal de Administración Electrónica (2012), MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[6] Roberto B., Pedro Castor C (2019-2020). Seguridad Informática Avanzada. Madrid: Universidad de Alcalá.

[7] Rolando C. (2015), *Planificación de un Sistema de Gestión de Seguridad de la Información para su aplicación en la Dirección Nacional de Operaciones de los Sistemas de Finanzas Públicas del Ministerio de Finanzas del Ecuador (*Tesis de posgrado*).* Recuperado de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Rolando_Coello_Neacato_2015.pdf

[8] Johana Carolina A. (2018), *Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal* (Tesis de posgrado)*.* Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/21259/1/27604094.pdf

[9] Carlos A. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso* (Tesis de posgrado). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/21259/1/27604094.pdf

ANEXOS

- **Anexo A. Controles de la Norma ISO 27001:2013**
- **Anexo B. Lista de Chequeo**
- **Anexo C. Los resultados de GAP análisis**
- **Anexo D. Estructura Organizacional**
- **Anexo E. Política del SGSI**
- **Anexo F. Inventario de Activos de COC M.T.**
- **Anexo G. Catálogo de Amenazas**
- **Anexo H. Relación entre amenazas y salvaguardas**

Anexo A. Controles de la Norma ISO 27001:2013

El Anexo A de ISO27001 es un estándar al que debemos referirnos al diseñar un sistema de gestión de seguridad de la información, es un modelo de lista de chequeo (Anexo B) para establecer el análisis de deficiencias GAP.

De acuerdo con estos problemas de diseño de control estándar y determinar su valor de madurez para explicar la situación actual del control interno de la gestión de seguridad de la información.

Tabla A.1 – Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Directrices de gestión de la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Control Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
A.6 Organización de la seguridad de la información		
A.6.1 Organization interna		
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades en seguridad de la información	Control Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de tareas	Control Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no auto- rizadas o no intencionadas o usos indebidos de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Control Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Control Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

A.6.1.5	Seguridad de la información en la gestión de proyectos	Control La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
A.6.2 Los dispositivos móviles y el teletrabajo		
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Control Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
A.6.2.2	Teletrabajo	Control Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
A.7 Seguridad relativa a los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.		
A.7.1.1	Investigación de antecedentes	Control La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Control Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A.7.2 Durante el employ		
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	Control La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Control Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

A.7.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
A.7.3 Finalización del empleo o cambio en el puesto de trabajo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.		
A.7.3.1	Responsabilidades ante la finalización o cambio	Control Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	Control La información y otros activos asociados a la información y a los recur- sos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	Control Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
A.8.1.4	Devolución de activos	Control Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
A.8.2.2	Etiquetado de la información	Control Debe desarrollarse e implantarse un conjunto adecuado de procedi- mientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

A.8.2.3	Manipulado de la información	Control Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3 Manipulación de los soportes		
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.		
A.8.3.1	Gestión de soportes extraíbles	Control Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	Control Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	Control Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información.		
A.9.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	Control Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A.9.2 Gestión de acceso de usuario		
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuario	Control Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	Control Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	Control La asignación y el uso de privilegios de acceso debe estar restringida y controlada.

A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Control La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	Control Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Retirada o reasignación de los derechos de acceso	Control Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información secreta de autenticación	Control Se debe requerir a los usuarios que sigan las prácticas de la organiza- ción en el uso de la información secreta de autenticación.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	Control Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	Control Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.4	Uso de utilidades con privilegios del sistema	Control Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política de uso de los controles criptográficos	Control

		Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

A.10.1.2	Gestión de claves	Control Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.		
A.11.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.
A.11.1.2	Controles físicos de entrada	Control Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, despachos y recursos	Control Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A.11.1.4	Protección contra las amenazas externas y ambientales	Control Se debe diseñar y aplicar una protección física contra desastres natu- rales, ataques provocados por el hombre o accidentes.
A.11.1.5	El trabajo en áreas seguras	Control Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
A.11.1.6	Áreas de carga y descarga	Control Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.
A.11.2 Seguridad de los equipos		
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de equipos	Control Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportu- nidades de que se produzcan accesos no autorizados.
A.11.2.2	Instalaciones de suministro	Control Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

A.11.2.3	Seguridad del cableado	Control El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A.11.2.4	Mantenimiento de los equipos	Control Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A.11.2.5	Retirada de materiales propiedad de la empresa	Control Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Control Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
A.11.2.7	Reutilización o eliminación segura de equipos	Control Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha elimi- nado de manera segura, antes de deshacerse de ellos.
A.11.2.8	Equipo de usuario desatendido	Control Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Control Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
A.12.1.1	Documentación de procedimientos operacionales	Control Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de capacidades	Control Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Control Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
A.12.2 Protección contra el software malicioso (malware)		
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.		
A.12.2.1	Controles contra el código malicioso	Control Se deben implementar los controles de detección, prevención y recupe- ración que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3 Copias de seguridad		
Objetivo: Evitar la pérdida de datos		
A.12.3.1	Copias de seguridad de la información	Control Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.4 Registros y supervisión		
Objetivo: Registrar eventos y generar evidencias.		
A.12.4.1	Registro de eventos	Control Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la infor- mación.
A.12.4.2	Protección de la información del registro	Control Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de administración y operación	Control Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
A.12.4.4	Sincronización del reloj	Control Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.
A.12.5 Control del software en explotación		
Objetivo: Asegurar la integridad del software en explotación.		
A.12.5.1	Instalación del software en explotación	Control Se deben implementar procedimientos para controlar la instalación del software en explotación.

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	Control Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre la auditoria de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.12.7.1	Controles de auditoría de sistemas de información	Control Los requisitos y las actividades de auditoría que impliquen comproba- ciones en los sistemas operativos deben ser cuidadosamente planifi- cados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.		
A.13.1.1	Controles de red	Control Las redes deben ser gestionadas y controladas para proteger la infor- mación en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	Control Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A.13.2 Intercambio de información		
Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de intercambio de información	Control Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

A.13.2.2	Acuerdos de intercambio de información	Control Deben establecerse acuerdos para el intercambio seguro de informa- ción del negocio y software entre la organización y terceros.
A.13.2.3	Mensajería electrónica	Control La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no revelación	Control Deben identificarse, documentarse y revisarse regularmente los requi- sitos de los acuerdos de confidencialidad o no revelación
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.14.1 Requisitos de seguridad en los sistemas de información		
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Control Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Control La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Control La información involucrada en las transacciones de servicios de aplica- ciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revela- ción, duplicación, o reproducción de mensaje no autorizadas.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte		
Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Control Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
A.14.2.2	Procedimiento de control de cambios en sistemas	Control La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.

A.14.2.4	Restricciones a los cambios en los paquetes de software	Control Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.

A.14.2.5	Principios de ingeniería de sistemas seguros	Control Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implemen- tación de sistemas de información.
A.14.2.6	Entorno de desarrollo seguro	Control Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Externalización del desarrollo de software	Control El desarrollo de software externalizado debe ser supervisado y controlado por la organización.
A.14.2.8	Pruebas funcionales de seguridad de sistemas	Control Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	Control Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos de prueba		
A.14.3.1	Protección de los datos de prueba	Control Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
A.15 Relación con proveedores		
A.15.1 Seguridad en las relaciones con proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Control Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organi- zación deben acordarse con el proveedor y quedar documentados.
A.15.1.2	Requisitos de seguridad en contratos con terceros	Control Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.

A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Control Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

A.15.2 Gestión de la provisión de servicios del proveedor		
Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores		
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Control Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Control Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A.16.1.3	Notificación de puntos débiles de la seguridad	Control Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Control Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad	Control

	de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	Control La organización debe definir y aplicar procedimientos para la identifi- cación recogida, adquisición y preservación de la información que puede servir de evidencia.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementar la continuidad de la seguridad de la información	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control La organización debe comprobar los controles establecidos e imple- mentados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias.		
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.		
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Control Los recursos de tratamiento de la información deben ser implemen- tados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mante- nerse actualizados para cada sistema de información de la organización.
A.18.1.2	Derechos de Propiedad Intelectual (DPI)	Control Deben implementarse procedimientos adecuados para

		garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
A.18.1.3	Protección de los registros de la organización	Control Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

A.18.1.4	Protección y privacidad de la información de carácter personal	Control Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.
A.18.1.5	Regulación de los controles criptográficos	Control Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la informa- ción, debe someterse a una revisión independiente a intervalos planifi- cados o siempre que se produzcan cambios significativos en la implan- tación de la seguridad.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correcta- mente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable
A.18.2.3	Comprobación del cumplimiento técnico	Control Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Anexo B. Lista de Chequeo

Esta es una lista de preguntas para llevar a cabo un análisis de brecha de GAP, utilizando niveles de madurez para evaluar el desarrollo de procesos de gestión de dirección de control interno.

Como primer paso tomaremos en cuenta los niveles de madurez:

Completamente implementado: Existe un control interno y continúo sobre la aplicación de controles y cumplimiento de requisitos

Parcialmente implementado: Existen los controles, pero no están documentados o no implementados.

No implementado: No Existen los controles.

Analizar el cumplimiento tanto con los requisitos de la norma ISO 27001 como de sus controles **Lista de Chequeo**			
"Completamente implementado" (C)， "Parcialmente implementado"(P), "No implementado"(N)	**C**	**P**	**N**
A.5 Políticas de seguridad			
1. ¿Existen políticas publicadas, aprobadas por la dirección, para apoyar la seguridad de la información?		✓	
2. ¿Las políticas de seguridad de la información son revisadas y actualizadas?			✓
A.6 Organización de la seguridad			
3. ¿Están definidas todas las responsabilidades de seguridad de la información?	✓		
4. ¿Los deberes y las responsabilidades son correctamente segregadas teniendo en cuenta las situaciones de conflicto de intereses?		✓	
5. ¿Existen definidos contactos con las autoridades competentes?		✓	
6. ¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?		✓	
7. ¿Los proyectos consideran aspectos relacionados con la seguridad de la información?		✓	
8. ¿Existen definidas reglas para el manejo seguro de los dispositivos móviles?			✓
9. ¿Existen reglas que definen cómo está protegida la información de la organización teniendo en cuenta el teletrabajo?		✓	

A.7 Seguridad relativa a los recursos humanos			
10. ¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?			✓
11. ¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de información?	✓		
12. ¿La dirección requiere activamente que todos los empleados y contratistas cumplan con las reglas de seguridad de la información?	✓		
13. ¿Los empleados y contratistas asisten a entrenamientos para realizar mejor sus tareas de seguridad, y existen programas de sensibilización?		✓	
14. ¿La organización tiene un proceso disciplinario?			✓
15. ¿Existen acuerdos que cubren las responsabilidades de seguridad de información que siguen siendo válidas después de la terminación del empleo?		✓	
A.8 Gestión de activos			
16. ¿Existe un inventario de activos?	✓		
17. ¿Todos los activos en el inventario de activos tienen un dueño designado?	✓		
18. ¿Existen definidas reglas para el manejo de activos y de información?	✓		
19. ¿Los activos de la organización son devueltos cuando los empleados y contratistas finalizan su contrato?	✓		
20. ¿Están definidos los criterios para clasificar la información?	✓		
21. ¿Existen procedimientos que definen cómo etiquetar y manejar información clasificada?	✓		
22. ¿Existen procedimientos que definen cómo manejar activos?	✓		
23. ¿Existen procedimientos que definen cómo manejar medios extraíbles en consonancia con las reglas de clasificación?			✓
24. ¿Existen procedimientos formales para la eliminación de medios?			✓
25. ¿Son protegidos los medios que contienen información sensible durante el transporte?			✓
A.9 Control de acceso			
26. ¿Existe una política de control de acceso que necesita ser apropiada para apoyar la seguridad de la información y los requerimientos del negocio?		✓	
27. ¿Los usuarios tienen acceso sólo a los recursos que se les permite?	✓		
28. ¿Los derechos de acceso son proporcionados mediante un proceso de registro formal?	✓		

29. ¿Existe un sistema de control de acceso formal para el inicio de sesión en sistemas de información?	✓		
30. ¿Los derechos de acceso privilegiado son manejados con especial cuidado?	✓		
31. ¿Las contraseñas, y otra información de autenticación secreta, es proporcionada de forma segura?			✓
32. ¿Los propietarios de activos comprueban periódicamente todos los derechos de acceso privilegiado?			✓
33. ¿Los derechos de acceso son actualizados cuando hay un cambio en la situación del usuario (por ejemplo: cambio organizacional o terminación)?		✓	
34. ¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?	✓		
35. ¿El acceso a la información en los sistemas es restringido según la política de control de acceso?	✓		
36. ¿Es requerido un sistema de login en los sistemas según la política de control de acceso?	✓		
37. ¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?			✓
38. ¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?		✓	
39. ¿El acceso al código fuente es restringido a personas autorizadas?	✓		
A.10 Criptografía			
40. ¿Existe una política para regular la encriptación y existen otros controles criptográficos?	✓		
41. ¿Están debidamente protegidas las claves criptográficas?		✓	
A.11 Seguridad física y del entorno			
42. ¿Existen zonas seguras que protegen la información sensible?	✓		
43. ¿Es protegida la entrada a las zonas seguras?	✓		
44. ¿Las zonas seguras están ubicadas en un lugar protegido?	✓		
45. ¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?	✓		
46. ¿Existen definidos procedimientos para las zonas seguras?	✓		
47. ¿Las zonas entrega y carga están protegidas?	✓		
48. ¿Los equipos son debidamente protegidos?	✓		
49. ¿Los equipos están protegidos contra las variaciones de energía?		✓	

50. ¿Están adecuadamente protegidos los cables de energía y telecomunicaciones?		✓	
51. ¿Existe mantenimiento de los equipos?	✓		
52. ¿La retirada de información y equipos fuera de la organización está controlada?	✓		
53. ¿Los activos de la organización son debidamente protegidos cuando no están en las instalaciones de la organización?	✓		
54. ¿Es correctamente eliminada la información de los equipos que se van a eliminar?	✓		
55. ¿Existen reglas para proteger los equipos cuando estos no estén siendo usados por los usuarios?	✓		
56. ¿Hay orientaciones a los usuarios sobre qué hacer cuando estos no están presentes en sus estaciones de trabajo?	✓		
A.12 Seguridad de las operaciones			
57. ¿Están documentados los procedimientos de TI?	✓		
58. ¿Los cambios que podrían afectar a la seguridad de la información son estrictamente controlados?	✓		
59. ¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?		✓	
60. ¿Se separan los entornos de desarrollo, pruebas y producción?			✓
61. ¿El software antivirus y otros programas para la protección de malware se instalan y utilizan correctamente?			✓
62. ¿Existe una política de backup definida y se lleva a cabo correctamente?	✓		
63. ¿Los eventos relevantes de lo sistemas son verificando periódicamente?		✓	
64. ¿Los registros están protegidos adecuadamente?			✓
65. ¿Están adecuadamente protegidos los logs de los administradores?		✓	
66. ¿Está la hora de todos los sistemas de TI sincronizada?	✓		
67. ¿La instalación de software es estrictamente controlada?		✓	
68. ¿La información de análisis de vulnerabilidades es correctamente gestionada?	✓		
69. ¿Existen reglas para definir restricciones de instalación de software a los usuarios?			✓
70. ¿Están las auditorías de sistemas de producción planeadas y se ejecutan correctamente?			✓
A.13 Seguridad de las comunicaciones			
71. ¿Las redes son gestionadas para proteger la información de sistemas y aplicaciones?	✓		

72. ¿Los requisitos de seguridad para servicios de red están incluidas en los acuerdos?	✓		
73. ¿Existen redes segregadas considerando los riesgos y la clasificación de los activos?	✓		
74. ¿Las transferencias de información están debidamente protegidas?		✓	
75. ¿Los acuerdos con terceras partes consideran la seguridad durante la transferencia de información?	✓		
76. ¿Los mensajes que se intercambian sobre las redes están protegidos correctamente?	✓		
77. ¿La organización posee una lista sobre todas las cláusulas de confidencialidad que deben ser incluidos en los acuerdos con tercero, revisadas y documentadas?			✓
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información			
78. ¿Se definen requisitos de seguridad para nuevos sistemas de información, o para cualquier cambio sobre ellos?			✓
79. ¿La información de aplicaciones transferida a través de redes públicas es adecuadamente protegida?	✓		
80. ¿Las transacciones de información a través de redes públicas son adecuadamente protegidas?	✓		
81. ¿Existen definidas reglas para el desarrollo seguro de software y de los sistemas?	✓		
82. ¿Se controlan los cambios en los sistemas nuevos o existentes?			✓
83. ¿Las aplicaciones criticas son debidamente probadas después de los cambios realizados en los sistemas operativos?		✓	
84. ¿Se realizan sólo los cambios necesarios a los sistemas de información?	✓		
85. ¿Los principios de ingeniería de sistemas seguros son aplicados al proceso de desarrollo de sistemas de la organización?			✓
86. ¿Es seguro el entorno de desarrollo?	✓		
87. ¿Es monitorizado el desarrollo externalizado de sistemas?	✓		
88. ¿Los requisitos de implementación de seguridad son probada durante el desarrollo del sistema?	✓		
89. ¿Existe definido un criterio para aceptar los sistemas?			✓
90. ¿Los datos de prueba son cuidadosamente seleccionados y protegidos?	✓		
A.15 Relación con proveedores			
91. ¿Existe una política para el tratamiento de los riesgos relacionados con proveedores y socios?		✓	

92. ¿Los requisitos de seguridad son incluidos en los acuerdos con los proveedores y socios?		✓	
93. ¿Los acuerdos con los proveedores incluyen requisitos de seguridad?	✓		
94. ¿Son supervisados regularmente los proveedores?	✓		
95. ¿Los cambios relacionados con los acuerdos y contratos con proveedores y socios tienen en cuenta los riesgos existentes?			✓
A.16 Gestión de incidentes de seguridad de la información			
96. ¿Los incidentes son gestionados adecuadamente?		✓	
97. ¿Los eventos de seguridad son reportados adecuadamente?		✓	
98. ¿Los empleados y contratistas informan sobre las debilidades de seguridad?			✓
99. ¿Los eventos de seguridad son evaluados y clasificados correctamente?			✓
100. ¿Están documentados los procedimientos para dar respuesta a los incidentes?		✓	
101. ¿Se analizan los incidentes de seguridad correctamente?			✓
102. ¿Existen procedimientos que definen cómo recopilar evidencias?			✓
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			
103. ¿Existen definidos requisitos para la continuidad de la seguridad de la información?			✓
104. ¿Existen procedimientos que aseguren la continuidad de la seguridad de la información durante una crisis o un desastre?		✓	
105. ¿Se realizan tests y pruebas de continuidad?			✓
106. ¿La infraestructura IT está redundada, incluyendo su planeamiento y operación?		✓	
A.18 Cumplimiento			
107. ¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?	✓		
108. ¿Existen procedimientos para proteger los derechos de propiedad intelectual?	✓		
109. ¿Los registros están protegidos adecuadamente?		✓	
110. ¿La información personal está protegida adecuadamente?			✓
111. ¿Se utilizan controles criptográficos correctamente?		✓	
112. ¿La seguridad de la información es revisada regularmente por un auditor independiente?			✓

113. ¿Los gerentes revisan regularmente si las políticas de seguridad y procedimientos son llevadas a cabo adecuadamente en sus áreas de responsabilidad?		✓	
114. ¿Los sistemas de información son revisados regularmente para comprobar su cumplimiento con los estándares y las políticas de seguridad de la información?		✓	

Anexo C. Los resultados de GAP análisis

Este análisis consta de 114 ítems de acuerdo a la lista de chequeo Anexo **B**, con opciones de respuestas "Completamente implementado" (C)， "Parcialmente implementado"(P), "No implementado"(N), que fue respondida por funcionarios de las áreas informáticas.

A continuación, se determina los niveles de cumplimiento de los controles que se clasifica en Alto, Medio y Bajo. Con base en la siguiente tabla de medición:

Tabla 1. Valoración de controles

Porcentaje	Valoración
>=56 y <=100%	Alto
>=40% y <=55%	Medio
>=0% y <=39	Bajo

De acuerdo con la siguiente grafica, el nivel de cumplimiento de esta entidad con respecto al control del Anexo A de la norma ISO/IEC 27001:2013 es 47%:

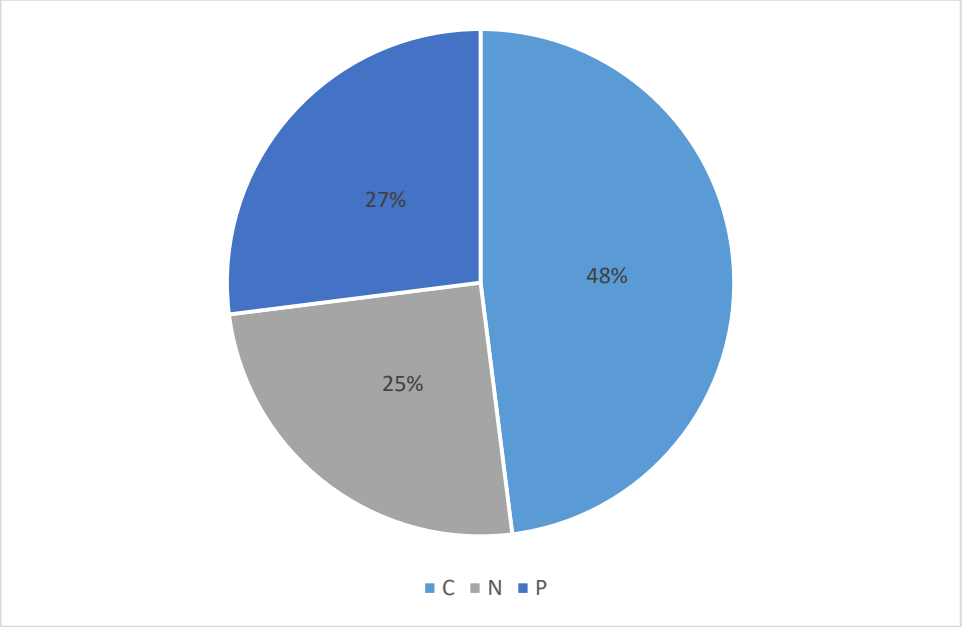

Figura 1. Nivel de cumplimiento controles Anexo A ISO 27001:2013

Fuente: El Autor

El siguiente es el resultado del nivel de cumplimiento de cada uno de los controles clasificados por dominio.

- **Dominio 5: Políticas de seguridad (Bajo: cumplimiento 25%)**

Figura 2. Resultado de la lista de chequeo del Dominio 5

Fuente: El Autor

- **Dominio 6: Organización de la seguridad de la información (Medio: cumplimiento 50%)**

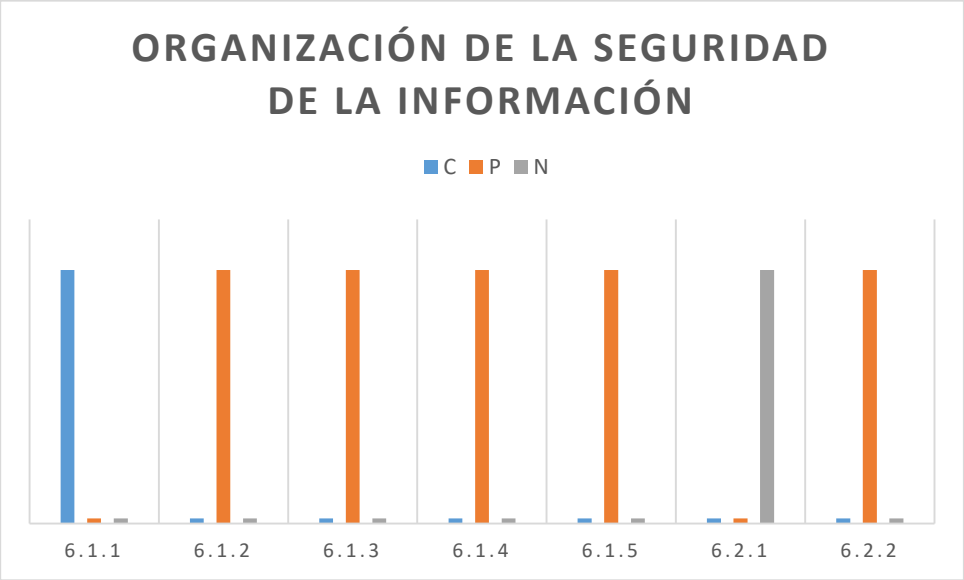

Figura 3. Resultado de la lista de chequeo del Dominio 6

Fuente: El Autor

- **Dominio 7: Seguridad de los recursos humanos (Medio: cumplimiento 50%)**

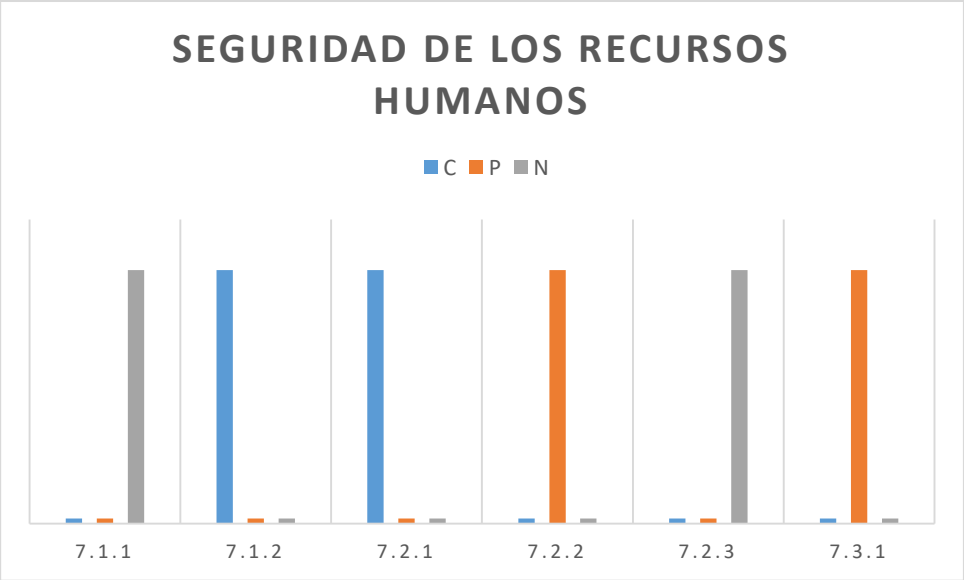

Figura 4. Resultado de la lista de chequeo del Dominio 7

Fuente: El Autor

- **Dominio 8: Gestión de activos (Alto: cumplimiento 70%)**

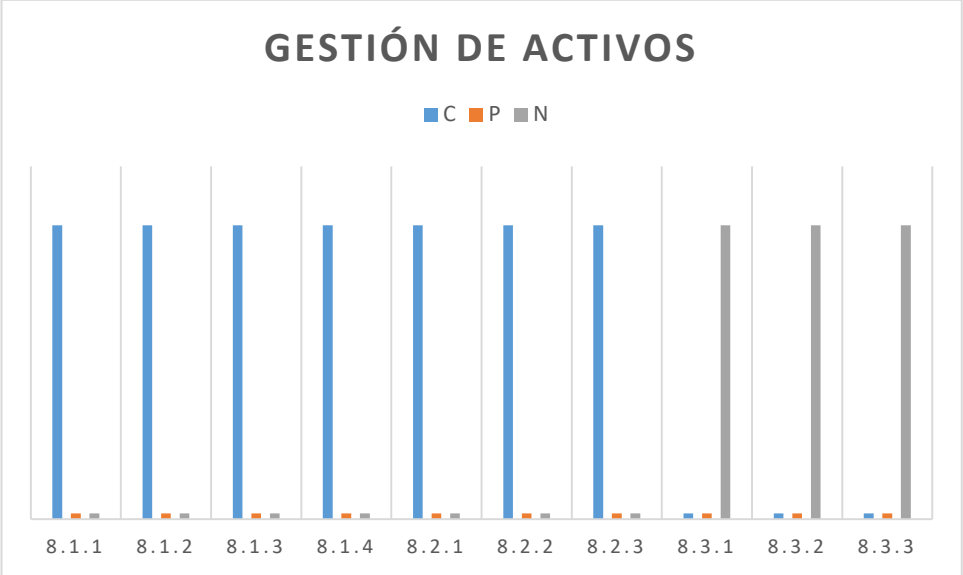

Figura 5. Resultado de la lista de chequeo del Dominio 8

Fuente: El Autor

- **Dominio 9: Control de acceso (Alto: cumplimiento 68%)**

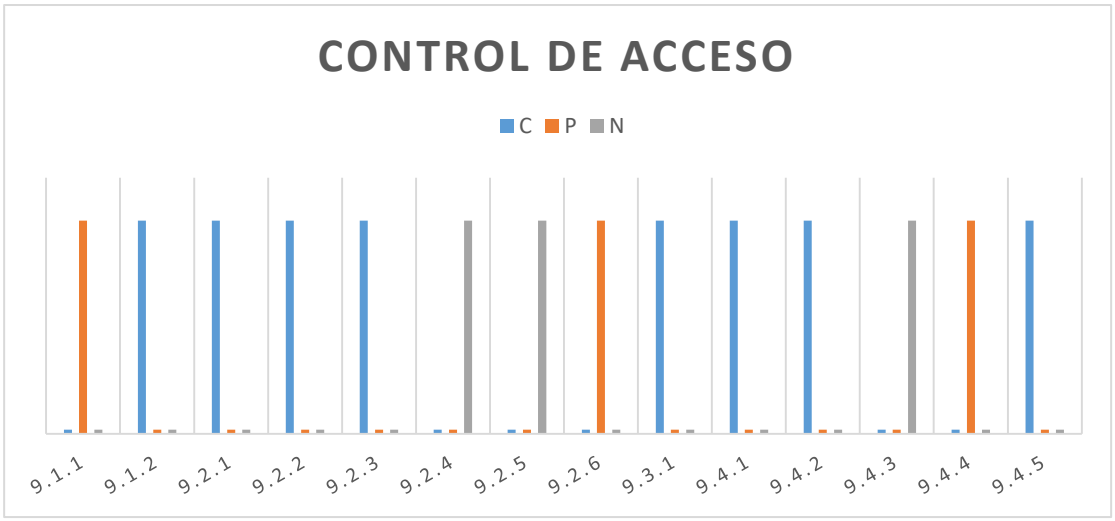

Figura 6. Resultado de la lista de chequeo del Dominio 9

Fuente: El Autor

- **Dominio 10: Cifrado (Alto: cumplimiento 75%)**

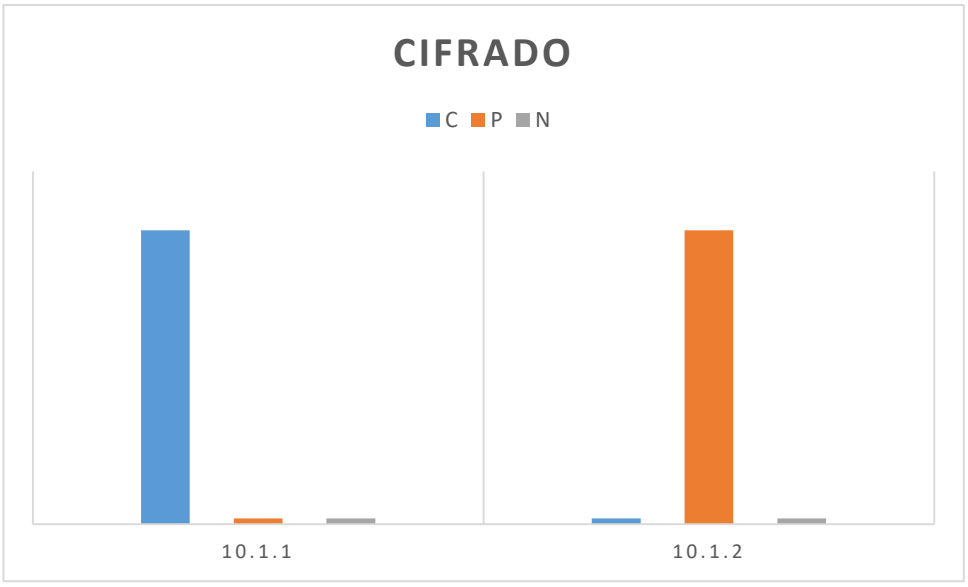

Figura 7. Resultado de la lista de chequeo del Dominio 10

Fuente: El Autor

- **Dominio 11: Seguridad física y ambiental (Alto: cumplimiento 93%)**

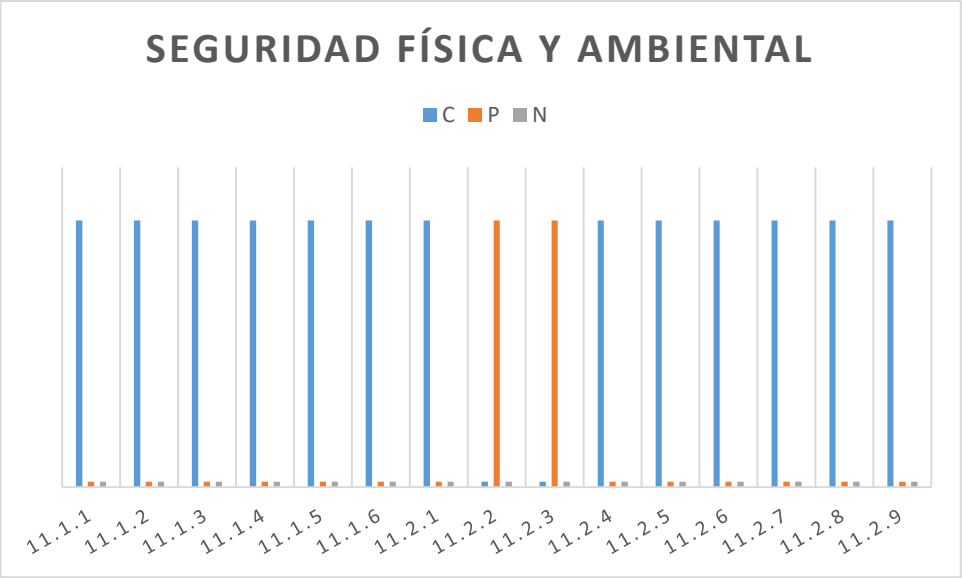

Figura 8. Resultado de la lista de chequeo del Dominio 11

- **Dominio 12: Seguridad en la Operativa (Medio: cumplimiento 50%)**

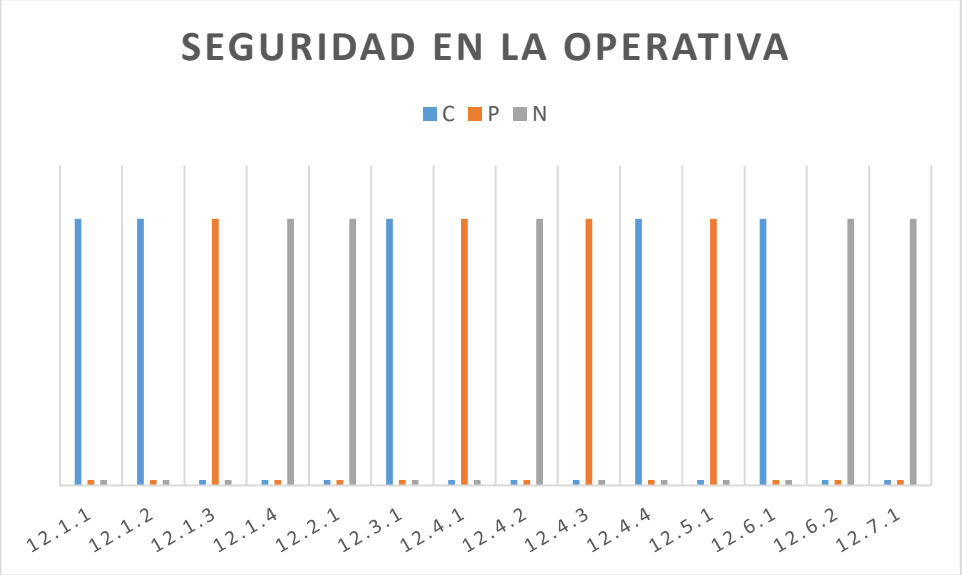

Figura 9. Resultado de la lista de chequeo del Dominio 12

Fuente: El Autor

- **Dominio 13: Seguridad de las comunicaciones (Alto: cumplimiento 79%)**

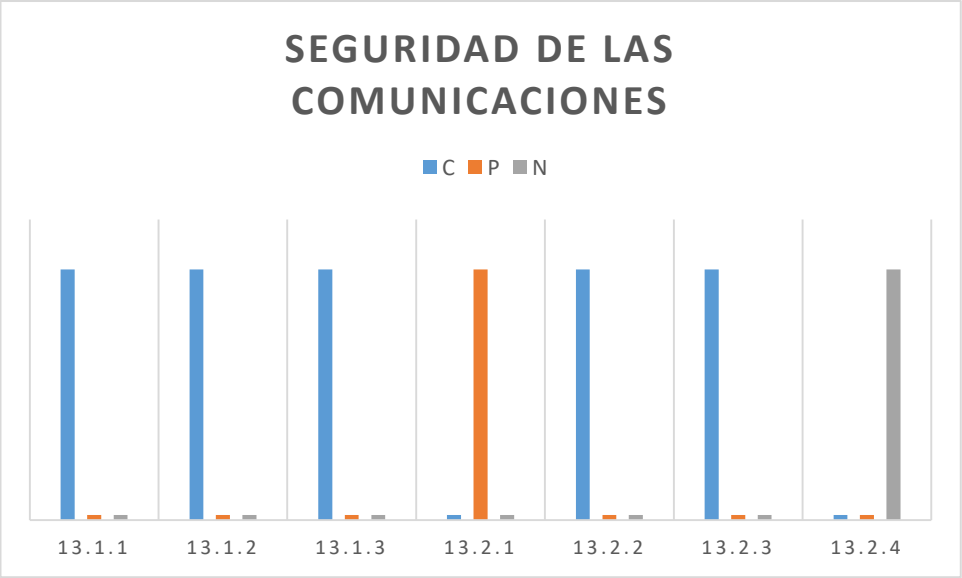

Figura 10. Resultado de la lista de chequeo del Dominio 13

Fuente: El Autor

- **Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información (Alto: cumplimiento 65%)**

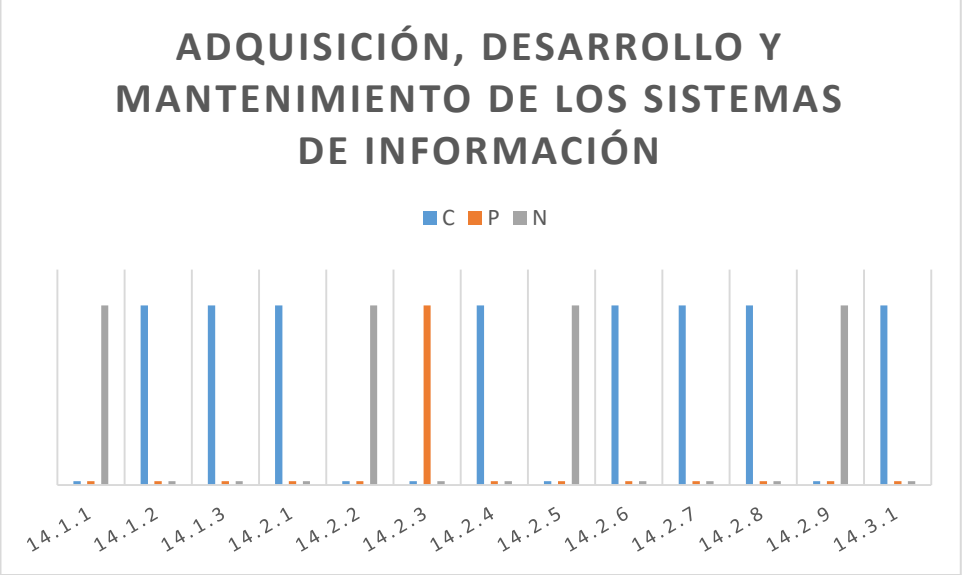

Figura 11. Resultado de la lista de chequeo del Dominio 14

Fuente: El Autor

- **Dominio 15: Relaciones con los proveedores (Alto: cumplimiento 65%)**

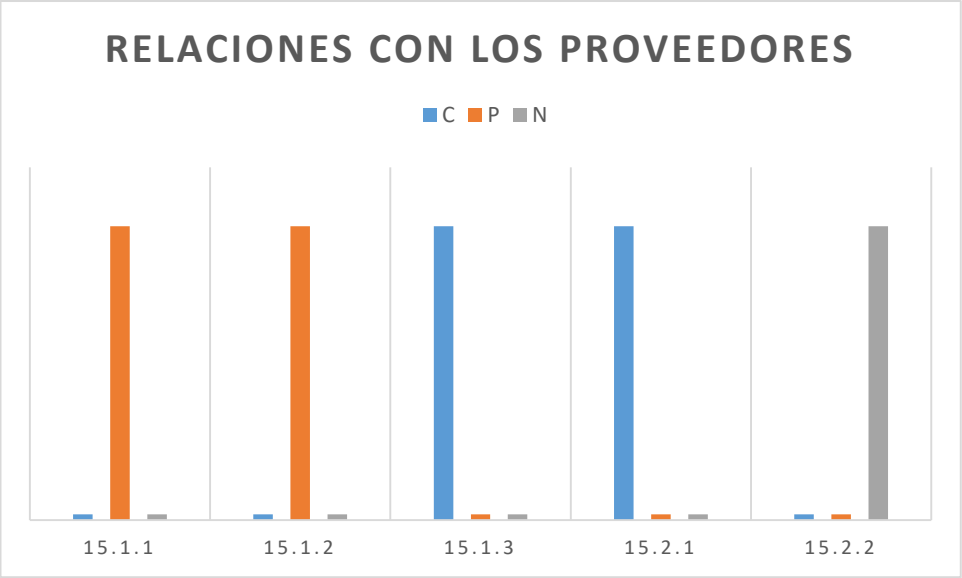

Figura 12. Resultado de la lista de chequeo del Dominio 15

Fuente: El Autor

- **Dominio 16: Gestión de Incidentes de seguridad de la información (Bajo: cumplimiento 21%)**

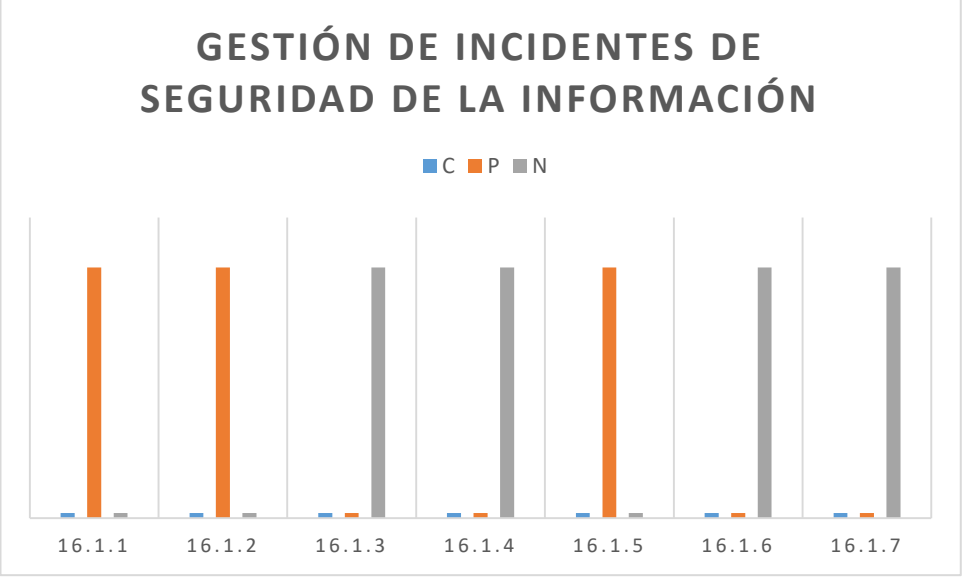

Figura 13. Resultado de la lista de chequeo del Dominio 16

Fuente: El Autor

- **Dominio 17: Continuidad de la seguridad de la información (Bajo: cumplimiento 25%)**

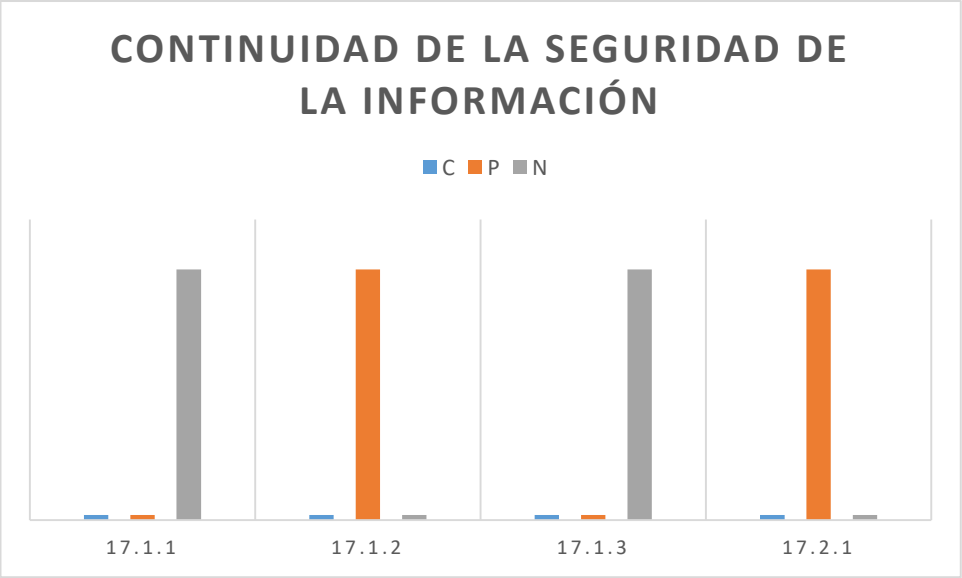

Figura 14. Resultado de la lista de chequeo del Dominio 17

Fuente: El Autor

- **Dominio 18: Cumplimiento (Medio: cumplimiento 50%)**

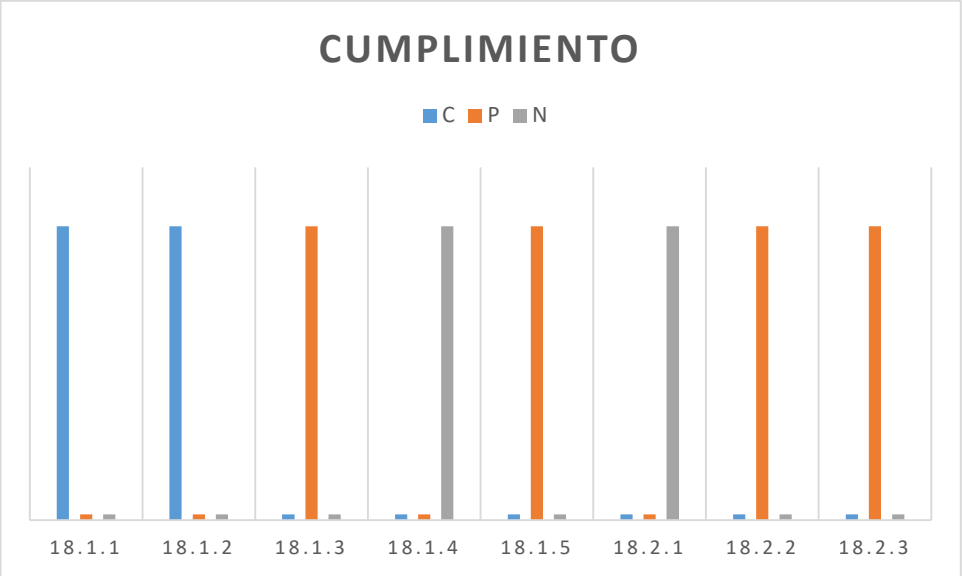

Figura 15. Resultado de la lista de chequeo del Dominio 18

Fuente: El Autor

Anexo D. Estructura Organizacional

El Anexo D es una explicación complementaria de la estructura organizacional y una explicación de cada área, lo que conduce a una mejor comprensión del perfil de la organización.

La empresa COC M.T. está constituida por las siguientes áreas:

- **Gerente general.** Los gerentes de más alto rango y personas responsables en toda la organización, coordinando los asuntos de varios departamentos comerciales.
- **Equipo directivo.** Integrada por el gerente y subgerente. Los cuales son los responsables de tomar las decisiones importantes dentro de la empresa.
- **Departamento de Gestión Integral.** Principalmente responsable de varios trabajos administrativos y de recursos humanos de la entidad, también hay funciones como la planificación de organización, implementación estándar, I + D de la entidad y contacto con otros departamentos.
- **Centro de Tecnología de la Información.** Encarga de desarrollar las aplicaciones del sistema HRSC, administrar las bases de datos y sistemas de respaldo para soportar los sistemas de información requeridos para la operación del negocio. El Centro de Tecnología de la Información cuenta con las medias y mecanismos de seguridad físicas y lógicas con el objetivo de prevenir accesos no autorizado a esta instalación y por ende a los equipos ubicados dentro de la misma.
- **Departamento de Producción de Seguridad.** Su responsabilidad principal es garantizar la disponibilidad, continuidad, confiabilidad y seguridad de la infraestructura tecnológica y de telecomunicaciones que soportan los sistemas de información y recursos tecnológicos necesarios para la operación del negocio. Así mismo, tiene función de gestionar todos los materiales de la en la entidad y mantener medidas y controles orientados a evitar, prevenir o mitigar las amenazas que atentar contra la disponibilidad, integridad y confidencialidad de la información de la entidad.
- **Centro de servicio al cliente.** Este es el departamento central de la empresa. Área responsable de hacer cumplir las operaciones negocias, es decir, las funciones de Recursos Humanos tales como el reclutamiento, la selección de personal, la gestión administrativa del personal, retribución, formación, etc. Para el desarrollo de estas actividades, las terminales de los funcionarios de esta área tienen conexión a los siguientes sistemas o portales de información:

- **HRSC.** Un software utilizado por la entidad para gestionar funciones de Recursos Humanos, es desarrollado y mantenido por el Centro de Tecnología de la Información, incluyendo gestión de datos de empleados, como nómina, reclutamiento, beneficios, capacitación, gestión de talentos, compromiso de los empleados y asistencia de los empleados, etc.
- **Portal web de COC M.T.** La plataforma de reclutamiento de la compañía, responsable de la publicidad de la compañía y la publicación de información de reclutamiento.
- **Portal web de la Seguridad Social.** Un sitio web del gobierno para pedir la Tarjeta Sanitaria y actualizar el estado de pago y las tarifas de los empleados.
- **Portal web de la Fondo de Previsión.** Un sitio web del gobierno para pedir la Tarjeta de Fondo de Previsión y actualizar el estado de pago y las tarifas de los empleados.

Esta área cuenta con las medidas de seguridad físicas y lógicas orientadas a evitar el acceso por parte de personas no autorizadas, con el propósito de evitar la modificación, manipulación, divulgación no autorizada, pérdida y robo de la información, y el uso inadecuado de los sistemas para fraudes.

- **Departamento de Finanzas.** Encargada de las operaciones financieras y de tesorería, y de la administración de ingresos y pagos de la entidad.
- **Departamento de Marketing.** Entre sus funciones principales esta, establecer y mejorar los sistemas operativos de recolección de información, procesamiento, comunicación y confidencialidad.

La sede principal de COC M.T. cuentan con 96 trabajadores, como la siguiente tabla presenta:

Área	Responsable	Cantidad
Gerente general	Representante corporativo	1
Equipo directivo	El gerente general y subgerente	12
Departamento de Gestión integral	Gerente	1
	Recursos Humanos	3
	Administración	3
Centro de Tecnología de la Información	Gerente	1
	Desarrollo de software, pruebas, mantenimiento	5
Departamento de Producción de Seguridad	Gerente	1
	Compra de equipo	3
	Mantenimiento de infraestructura	2
	Gestión de consumibles	3
Centro de servicio al cliente	Gerente	2
	Reclutamiento	6

	Servicio al cliente	10
	Remuneración	3
	Seguridad Social	2
	Fondo de Previsión	2
Departamento de Finanzas	Gerente	2
	Cobro y pago en efectivo	2
	Liquidación bancaria	2
	Mantenimiento de archivos	1
	Facturación	3
	Salario de trabajadores internos	1
	Salario del empleado	9
Departamento de Marketing	Gerente	2
	Capacitación	7
	Contrato/ Abogado	2
	Gestión de Cliente	5
Total		**96**

Anexo E. Política del SGSI

1. **Resumen de la política:** La información procesada por los recursos tecnológicos y humanos que forman parte de la empresa debe ser siempre protegida.
2. **Introducción:**

- La información como un recurso, su universalidad, intercambio, valor agregado, disponibilidad y versatilidad es la vital importancia para los seres humanos.
- La esencia de la seguridad de la información es proteger los recursos de información en el sistema o la red de información de varios tipos de amenazas, interferencia y destrucción, es decir, para garantizar la seguridad de la información.
- COC M.T. como una empresa de Recursos Humanos que lleva años dando servicios a clientes, es vital garantizar la seguridad de la información para las actividades de negocio y los servicios
- Las Tecnologías de la Información y Comunicaciones (TIC) desempeñen un rol estratégico dentro de los procesos claves de la empresa.

3. **Alcance**

- El alcance del SGSI cubre el proceso de Gestión de la Información y Mantenimiento de infraestructura de la entidad, que involucra el ciclo de vida de la información, desde su obtención hasta su disposición final.
- La aplicabilidad del SGSI es solo para la sede de la entidad que, ubicada en la ciudad de Shenzhen, limitando La Tecnología de Comunicación de Información (TIC) entre las personas, los procesos y actividades desempeñadas por esta sede.

4. **Objetivos**

- Cumplir los objetivos de negocio a través de la aplicación de una Metodología de Análisis y Gestión de Riesgos para identificar, evaluar y tratar los riesgos.
- Cumplir con los requerimientos legales y reglamentarios aplicables a la entidad y al Sistema de Gestión de Seguridad de la Información.
- Mantener la Disponibilidad, Integridad y Confidencialidad de la información y de los registros, proporcionando confianza en las partes interesadas.
- Implementar el sistema de gestión de seguridad de la información.
- Desarrollar y planes de formación a los colaboradores para fortalecer la cultura de seguridad de la información.

- Garantizar la continuidad del negocio y la seguridad de la información.

5. Principales

- Esta entidad implanta un Sistema de Gestión de Seguridad de la Información (SGSI), en basa a la norma internacional ISO/UNE 27001
- La política del SGSI describe información detallada para la evaluación de riesgos y su tratamiento.
- Revisará y actualizará la política al menos anualmente.
- Los informes periódicos proporcionarán información con información de la situación de la seguridad.
- La violación de las leyes y normas legales no serán toleradas.
- Esta política aplicará a toda la entidad, sus colaboradores, proveedores, terceros, permanecerá disponibles en la intranet de la organización y se actualizará regularmente.

6. Responsabilidades

- El Equipo Directivo de la entidad debe conocer y aprobar la política de seguridad establecidas.
- Cada gerente del departamento es responsable de garantizar que los subordinares protejan la información de acuerdo con las reglas establecidas por la organización.
- El gerente de gestión de información de seguridad formulará, implementará y monitorizará la política de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.
- El responsable de seguridad brinda asesoramiento al equipo de administración, proporciona apoyo profesional a la organización y garantiza la provisión de informes de estado de seguridad de la información.
- Todos los trabajadores deben asumir la responsabilidad de la seguridad de la información, como parte de sus funciones de trabajo obligatorias dentro de la entidad, se comunicarán al responsable de seguridad y serán investigados.
- Las visitas y personal externo que accedan a las instalaciones cumplirán los requisitos indiciados en la documentación del SGSI.

Anexo F. Inventario de Activos de COC M.T.

El Anexo F se relaciona el inventario de los activos de información que se pudieron identificar en el proceso de tecnología:

Tipo de Activo	Nombre	Descripción del Activo		
		Cantidad	Ubicación	Propietario / custodio
Organizacioón	Proveedor de Comunicaciones	1	N/A	N/A
	Proveedor de impresoras	1	N/A	N/A
Datos / Información	Base de Datos	3	Sala de máquinas	Centro de Tecnología de la Información
	Documentos (contratos de servicio y personal)	>1000	Archivo físico, HRSC	Archivista
	Egresos y Recibos de pago	>1000	Archivo físico	Archivista
	Facturas	>1000	Archivista, HRSC	Archivista
	Backups de base de datos	2	Sala de máquinas	Centro de Tecnología de la Información
Servicios	Servicio al Cliente	N/A	N/A	Centro de servicio al cliente
	Reclutamiento	N/A	Portal web de COC M.T. HRSC	Centro de servicio al cliente
	Seguridad Social	N/A	Portal web de la Seguridad Social HRSC	Centro de servicio al cliente
	Fondo de Previsión	N/A	Portal web de la Fondo de Previsión	Centro de servicio al cliente

			HRSC	
	Capacitación	N/A	Depende de la ubicación del cliente	Centro de servicio al cliente
	Remuneración	N/A	HRSC	Centro de servicio al cliente
	Almacenamiento Compartido	N/A	Computadora pública	Coordinadora de IT
	Impresión y escaneo en red	N/A	Computadora pública	Coordinadora de IT
	Mantenimiento de Equipo	N/A	Todas las áreas de la empresa	Coordinadora de IT
	Sistema de Información	3	N/A	Centro de Tecnología de la Información
Software	SQL	1	Servidores	Centro de Tecnología de la Información
	Ofimática	10	Equipos de usuarios finales y servidores	Coordinadora de IT
	Sistemas Operativos	1	Equipos de usuarios finales y servidores	Coordinadora de IT
	HRSC	1	Equipos de usuarios finales y servidores	Centro de Tecnología de la Información
Hardware	Servidores	2	Sala de máquinas	Centro de Tecnología de la Información
	Impresoras Multifuncionales	3	Todas las áreas de la empresa	Coordinadora de IT
	PC	96	Todas las áreas de la empresa	Coordinadora de IT
	Equipos de red	20	Todas las áreas de la empresa	Coordinadora de IT
	Disco duro móvil	9	Cuarto de equipos	Coordinadora de IT

	Disco U	15	Cuarto de equipos	Coordinadora de IT
	Portátil	30	Cuarto de equipos	Coordinadora de IT
Comunicaciones	WIFI	1	Rack secundario	Coordinadora de IT
	LAN	1	Rack secundario	Coordinadora de IT
	WAN	1	Rack secundario	Coordinadora de IT
Instalaciones	Sala de máquinas	1	N/A	Centro de Tecnología de la Información
	Zona de accesos, seguridad, oficinas y equipos	4	N/A	Coordinadora de IT
	Archivo físico	1	N/A	Archivo físico
	Cuarto de equipos	1	N/A	Coordinadora de IT
Personal	Administrador del Sistema	5	N/A	N/A
	Gerente	1	N/A	N/A
	Usuarios finales	>1000	N/A	N/A

Anexo G. Catálogo de Amenazas

En esta solapa aparece el listado o catálogo de amenazas, junto con su porcentaje de afectación a cada dimensión de seguridad.

	Threats	**D**	**I**	**C**	**A**	**T**	**Pd**	**Ajustado al 100%**
[N] Desastres naturales	[N.1] Fuego.	**60%**	**20%**		**20%**			Si
	[N.2] Daños por agua	**60%**	**20%**		**20%**			Si
	[N.*] Otros desastres naturales	**60%**	**20%**		**20%**			Si
[I] De origen industrial	[I.1] Fuego	**60%**	**20%**		**20%**			Si
	[I.2] Daños por agua	**60%**	**20%**		**20%**			Si
	[I.*] Desastres industriales	**60%**	**20%**		**20%**			Si
	[I.3] Contaminación mecánica	**60%**	**20%**		**20%**			Si
	[I.4] Contaminación electromagnética	**60%**	**20%**		**20%**			Si
	[I.5] Avería de origen físico o lógico	**60%**	**20%**		**20%**			Si
	[I.6] Corte del suministro eléctrico	**60%**	**20%**		**20%**			Si
	[I.7] Condiciones inadecuadas de temperatura o humedad	**60%**	**20%**		**20%**			Si
	[I.8] Fallo de servicios de comunicaciones	**100 %**						Si
	[I.9] Interrupción de otros servicios y suministros esenciales.	**100 %**						Si
	[I.10] Degradación de los soportes de almacenamiento de la información		**50%**		**50%**			Si
	[I.11] Emanaciones electromagnéticas.			**100 %**				Si
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	**10%**	**30%**	**30%**	**30%**			Si
	[E.2] Errores del administrador.	**10%**	**30%**	**30%**	**30%**			Si
	[E.3] Errores o manipulación de registros de actividad (log)					**100 %**		Si
	[E.4] Errores o manipulación de la configuración		**50%**		**50%**			Si
	[A.5] Suplantación de la identidad del usuario		**40%**	**20%**	**40%**			Si
	[A.6] Abuso de privilegios de acceso		**40%**	**20%**	**40%**			Si
	[E.7] Uso no previsto		**40%**	**20%**	**40%**			Si
	[E.8] Difusión de software dañino.	**10%**	**30%**	**30%**	**30%**			Si
	[E.9] Errores de re-encaminamiento.			**100 %**				Si
	[E.10] Errores o alteración de secuencia		**50%**		**50%**			Si
	[E.18] Destrucción de información		**80%**		**20%**			Si
	[E.19] Fugas o revelación de información.			**100 %**				Si

	[E.20] Vulnerabilidades de los programas (software).		**30%**	**60%**	**10%**			Si
	[E.21] Errores de mantenimiento / actualización de programas (software)		**60%**	**20%**	**20%**			Si
	[A.22] Manipulación de programas.		**40%**	**20%**	**40%**			Si
	[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)		**40%**	**20%**	**40%**			Si
	[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	**100 %**						Si
	[E.25] Robo o Pérdida de equipos	**20%**		**80%**				Si
(Pd) Amenazas relacionadas con el cumplimiento	[Pd.1] Ataque a los derechos de los afectados (ARCO, información, consentimiento, portabilidad)						**100 %**	Si
	[Pd.2] Carencia de legitimación en el tratamiento de la información						**100 %**	Si
	[Pd.3] Falta de transparencia en el tratamiento de la información						**100 %**	Si
	[Pd.4] Transferencias internacionales de datos sin estar justificadas o sin las medidas de seguridad adecuadas						**100 %**	Si
	[Pd.5] Incumplimiento del Principio de Calidad de los datos						**100 %**	Si
	[Pd.6] Falta de control de los tratamientos derivados de un inadecuado registro y notificación						**100 %**	Si
	[Pd.7] Incumplimiento de las medidas de seguridad			**60%**			**40%**	Si
	[Pd.8] Divulgación que origina incumplimiento en el deber de secreto			**60%**			**40%**	Si
	[Pd.9] Errores de los usuarios o en el tratamiento de la información por falta de sensibilización y conocimiento experto de la normativa						**100 %**	Si
	[Pd.10] Errores, pérdidas de información, incumplimiento medidas de seguridad por un control, gestión o elección deficiente del Encargado del Tratamiento						**100 %**	Si
[A] Ataques intencionados	[A.11] Acceso no autorizado.		**40%**	**60%**				Si
	[A.12] Análisis de tráfico			**100 %**				Si
	[A.13] Repudio				**100 %**			Si
	[A.14] Interceptación de información (escucha).			**100 %**				Si
	[A.26] Ataque destructivo	**20%**	**60%**		**20%**			Si
	[A.27] Ocupación enemiga	**10%**	**30%**	**50%**	**10%**			Si
	[E.28] Indisponibilidad del personal	**100 %**						Si
	[A.29] Extorsión		**20%**	**60%**	**20%**			Si
	[A.30] Ingeniería social (picaresca)			**100 %**				Si

Anexo H. Relación entre amenazas y salvaguardas

En esa hoja se deben seleccionar las salvaguardas de seguridad a aplicar en función de las amenazas y los activos.

En ella, el analista de riesgos debe introducir:

La salvaguarda de seguridad. Esta selección depende del conocimiento general de las medidas de seguridad del analista de riegos.

El coste de implantación. Los costes dependen de la naturaleza de la salvaguarda y del tamaño y características de la organización. Como directrices muy generales en cuanto al coste puede decirse que:

- Organizaciones con decenas de trabajadores implican costes de miles de euros.
- Organizaciones con cientos de trabajadores implican costes de decenas de miles de euros.
- Organizaciones con miles de trabajadores implican costes de cientos de miles de euros.

En la hoja se deben introducir los costes de implantación y se calcula automáticamente los anuales (de mantenimiento) a partir de un coeficiente genérico.

La efectividad de las salvaguardas en cada una de las dimensiones de seguridad. Un valor del 100% significa que la salvaguarda elimina completamente la amenaza en cuestión.

En este caso se aplica el principio de proporcionalidad, que establece que el coste de una medida no puede ser mayor que el beneficio obtenido en ella. En nuestro caso se comparan:

- El coste es el mantenimiento anual de una medida
- El beneficio de reducción de riesgo. El producto del coste de implantación (que incluye la compra del producto, su adaptación y su mantenimiento) y la efectividad máxima en alguna de las dimensiones Dictad.

En una misma celda se deben introducir las salvaguardas que sirven para reducir una amenaza determinada. Aunque puedan no tener unas con otras se debe hacer así. En el paso de la Definición de proyectos de seguridad se deben agrupar y coordinar las amenazas que deban implementarse.

El libro Excel selecciona automáticamente, de las introducidas previamente por el analista, las salvaguardas que deben incluirse en el plan director de seguridad, a través de la columna “A incluir en el PTR”. Indica que, si tiene valor “1”, la medida vale la pena tomarla porque su beneficio es mayor que su coste. Solo las salvaguardas con ese valor vale la pena incluirlos en el PTR.

Universidad de Alcalay

PDS. Relación entre amenazas y salvaguardas

Versión 5.5

COC M.T.

Factor coste anual de mantenimiento 30%

PDS salvaguardas											Amenazas								Reduced risk							
Salvaguarda	Proyecto	Coste de implementación	Coste Anual de Mantenimiento	Efectividad							No.	Riesgo residual	D	I	C	A	T	Cu	Cantidad	Para insertar en PDS (1 - si)	D	I	C	A	Cu	Cost
				Max	D	I	C	A	T	Cu																
Impermeabilización del CPD	Seguridad física	900,000 €	270,000 €	60%	60%	40%	0%	40%	0%	20%	[N.2]	11,351 €	60%	20%	0%	20%	0%	0%	6,811 €	0	6,811 €	4,541 €	0 €	4,541 €	2,270 €	0 €
Cifrado de comunicaciones	Prueba de seguridad	10,000 €	3,000 €	60%	20%	40%	60%	40%	0%	20%	[E.1]	24,633 €	0%	0%	100%	0%	0%	0%	14,780 €	1	4,927 €	9,853 €	14,780 €	9,853 €	4,927 €	3,000 €
Formación y concienciación	Formación y concienciación	4,000 €	1,200 €	40%	10%	40%	0%	30%	0%	30%	[E.2]	3,425 €	10%	30%	30%	30%	0%	0%	1,370 €	1	342 €	1,370 €	0 €	1,027 €	1,027 €	1,200 €
Registrar toda la información	Gestión de los registros	10,000 €	3,000 €	80%	20%	20%	0%	40%	80%	20%	[E.3]	14,060 €	0%	0%	0%	0%	0%	0%	11,248 €	1	2,812 €	2,812 €	0 €	5,624 €	2,812 €	3,000 €

Aumentar el acceso a los registros de acceso a los datos.	Control de acceso	20,000 €	6,000 €	40%	20%	0%	0%	0%	40%	20%	[E.7]	685 €	0%	40%	20%	40%	0%	0%	274 €	0	137 €	0 €	0 €	0 €	137 €	0 €
Copias de seguridad en SQL	Copias de seguridad	20,000 €	6,000 €	80%	40%	80%	0%	80%	40%	30%	[E.18]	49,266 €	0%	80%	0%	20%	0%	0%	39,413 €	1	19,706 €	39,413 €	0 €	39,413 €	14,780 €	6,000 €
Cifrado de comunicaciones	Ciberseguridad	10,000 €	3,000 €	80%	40%	20%	60%	20%	0%	80%	[E.19]	24,633 €	100%	0%	0%	0%	0%	0%	19,706 €	1	9,853 €	4,927 €	14,780 €	4,927 €	19,706 €	3,000 €
Diseñar un procedimiento de los programas para incluir información confidencial en áreas con límites claros de confianza	Seguridad aplicaciones	30,000 €	9,000 €	60%	60%	20%	20%	40%	0%	60%	[E.20]	28,120 €	0%	30%	60%	10%	0%	0%	16,872 €	1	16,872 €	5,624 €	5,624 €	11,248 €	16,872 €	9,000 €
Controlar y registrar cambios significativos sobre el proceso de actualización de programas.	Gestión de cambios	9,000 €	2,700 €	60%	60%	20%	0%	20%	0%	60%	[E.21]	14,060 €	0%	60%	20%	20%	0%	0%	8,436 €	1	8,436 €	2,812 €	0 €	2,812 €	8,436 €	2,700 €
Mantener y actualizar el equipo regularmente	Seguridad física	24,000 €	7,200 €	80%	80%	20%	0%	20%	0%	40%	[E.24]	18,379 €	0%	40%	60%	0%	0%	0%	14,703 €	1	14,703 €	3,676 €	0 €	3,676 €	7,352 €	7,200 €
Determinación de procedimientos de acceso y revisión	Control de acceso	30,000 €	9,000 €	80%	30%	40%	80%	80%	60%	60%	[A.11].	88,465 €	0%	40%	60%	0%	0%	0%	70,772 €	1	26,539 €	35,386 €	70,772 €	70,772 €	53,079 €	9,000 €
Vigilancia digital	Ciberseguridad	60,000 €	18,000 €	80%	20%	20%	80%	0%	0%	40%	[A.14]	77,385 €	0%	0%	100%	0%	0%	0%	61,908 €	1	15,477 €	15,477 €	61,908 €	0 €	30,954 €	18,000 €
Formación y concienciación	Formación y concienciación	4,000 €	1,200 €	80%	0%	40%	80%	40%	0%	80%	[A.30]	20,550 €	0%	0%	100%	0%	0%	0%	16,440 €	1	0 €	8,220 €	16,440 €	8,220 €	16,440 €	1,200 €