ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO DE UN PLAN DIRECTOR DE SEGURIDAD PARA UNA EMPRESA PRIVADA QUE BRINDA SERVICIOS DE AUDITORÍA PARA REDUCIR RIESGOS EXPUESTOS EN UN ENTORNO SEGURO”

TRABAJO DE TITULACIÓN

Previa a la obtención del Título de:

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

ING. DOUGLAS STEEVEN MARÍN VELÁSQUEZ

ING. CÉSAR XAVIER MEDINA SOLÓRZANO

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Quiero agradecer a Dios por este trabajo y por la oportunidad que me da por haberlo finalizado sin duda pienso que nada es posible si no fuera por su voluntad. Agradecer a mis Padres por su apoyo y su compañía en todo este proceso. También quiero agradecer a la organización donde laboro actualmente por su apoyo, a mi jefe y amigo por su ejemplo e influencia en alcanzar logros académicos, gracias a todos mis compañeros de la maestría que fueron parte en este camino donde nos brindamos apoyo mutuamente.

Ing. Douglas Steeven Marín Velásquez

AGRADECIMIENTO

Agradezco a Dios y a mi familia por apoyarme en este largo camino. Agradezco también a la empresa donde laboro, ya que fueron ellos los que me motivaron a crecer profesionalmente. Este trabajo tampoco hubiera sido posible gracias a todo el camino recorrido junto a los compañeros de maestría.

Ing. César Xavier Medina Solórzano

DEDICATORIA

Dedico este trabajo a mi hijo, a mis padres y hermanos. Gracias por siempre estar presentes y por la paciencia que han tenido en todo este camino.

Ing. César Xavier Medina Solórzano

DEDICATORIA

Dedico este trabajo a Dios, a mi Padre y a mí, por todo el esfuerzo y tiempo invertido en este título alcanzado.

Titulo dado por el fruto del esfuerzo, porque todo aquel que tiene sus metas claras alcanzara sus objetivos.

Ing. Douglas Steeven Marín Velásquez

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Freire C.

DIRECTOR MSIG

RAUL VICENTE GONZALEZ CARRION
Firmado digitalmente por RAUL VICENTE GONZALEZ CARRION
Fecha: 2024.06.27 13:32:12 -05'00'

Mgs. Raúl González C

DIRECTOR DEL PROYECTO DE GRADUACIÓN

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

MSc. Juan Carlos García

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”.

.

DOUGLAS STEEVEN MARIN VELASQUEZ
Firmado digitalmente por DOUGLAS STEEVEN MARIN VELASQUEZ
Fecha: 2024.06.25 09:58:43 -05'00'

Douglas Steeven Marin Velásquez

CESAR XAVIER MEDINA SOLORZANO
Firmado digitalmente por CESAR XAVIER MEDINA SOLORZANO
Fecha: 2024.06.25 09:50:19 -05'00'

César Xavier Medina Solórzano

RESUMEN

El objetivo principal del presente trabajo de titulación es la creación de un Plan Director de Seguridad (en adelante “PDS”) en el departamento de TI de la empresa de servicio de auditoría.

Dentro de este documento se describen conceptos importantes sobre la Seguridad de la Información como en sus normas internacionales ISO/IEC 27001 y 27002. También se detalla la guía ISO 27005, guía elegida para el análisis, gestión y tratamiento de riesgo en los activos de la empresa junto a la norma ISO 27002 para la implementación de controles. Para llevar a cabo un PDS se dio a conocer la estrategia de la organización y sus alcances, realizando un levantamiento de la información y tratamiento de los activos con el fin de conocer los riesgos dentro de la empresa.

Posteriormente se dio a conocer un Plan Director de Seguridad para mitigar todos los riesgos inherentes en un mediano plazo por medio de implementación de políticas y controles derivadas de la ISO/IEC 27001 y 27002.

INDICE GENERAL

ABREVIATURAS

PDS	Plan Director de Seguridad
SI	Seguridad de la Información
SOA	Declaración de Aplicabilidad
GAP	Análisis de Brechas
INCIBE	Instituto Nacional de Ciberseguridad
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de los Administradores
ISO	International Organization for Standardization
SGSI	Sistema de Gestión de Seguridad de la Información

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la era digital actual, la creciente interconexión y dependencia de sistemas informáticos han resaltado la vulnerabilidad de la información sensible. En este contexto, la seguridad informática se consolida como un elemento esencial para salvaguardar la confidencialidad, integridad y disponibilidad de los datos. Los lineamientos de seguridad informática no solo son imperativos para proteger activos críticos de las organizaciones, sino también para preservar la confianza en entornos digitales.

Ante el creciente número de amenazas cibernéticas, que van desde ataques sofisticados hasta vulnerabilidades comunes, es esencial implementar de manera efectiva directrices de seguridad. Resulta crucial examinar cómo estas medidas influyen en la mitigación de riesgos y en el fortalecimiento de la infraestructura digital en un contexto de creciente interconexión a nivel. La seguridad informática requiere una atención meticulosa, ya que implica analizar cada activo en busca de posibles vulnerabilidades. En lo que respecta al análisis de riesgos, es necesario seguir normas, estándares y pautas que garanticen un nivel más alto de seguridad [1].

Nuestro análisis se centrará en la necesidad de que una empresa importante dedicada a la auditoría tenga lineamientos de seguridad muy bien establecidos, para lo cual iremos explorando políticas y metodologías con la finalidad de llenar las expectativas de la empresa.

La implementación exitosa de políticas de seguridad en una empresa, en nuestro caso en una empresa dedicada a la auditoría, requiere un enfoque integral, priorizando la evaluación de los riesgos identificando las vulnerabilidades que podrían tener las organizaciones. Luego se establecen las políticas adaptadas a las necesidades. Es importante la inversión en tecnologías de seguridad actualizadas y la monitorización constante para garantizar una respuesta proactiva a posibles amenazas.

Es fundamental recordar que la seguridad total es inalcanzable; no existe un sistema que pueda asegurar completamente la disponibilidad, integridad y confidencialidad de los activos de una empresa. Los riesgos siempre estarán presentes, independientemente de las medidas tomadas, las cuales deben derivar de un proceso metódico, registrado y conocido por la empresa [2]

CAPITULO I.

GENERALIDADES

1.1. Antecedentes

La empresa Servicios de auditoria es una organización privada que inicia sus actividades el 01 de septiembre del 2014, para brindar el apoyo administrativo que requería en aquel entonces un Grupo Corporativo de compra y venta de oro, con el fin de llevarlo al correspondiente desarrollo formal, en vista de que dicho grupo inició como un mediano emprendimiento y fue creciendo paulatinamente, por ende, surgió la necesidad de que todas sus operaciones vayan tomando un rumbo más estructurado.

Con el pasar del tiempo, el alcance de esta empresa de servicios de auditoria también tomó un rumbo de franco desarrollo y los profesionales que la componen, sumaron a su experiencia, conocimientos actualizados por medio de formación en cuanto a tendencias actuales en sus profesiones, aplicándolas al Grupo corporativo de compra y venta de oro, y extendiendo sus alcances a otras empresas que requieran sus servicios profesionales en los ámbitos legal, financiero, de tecnologías de la información, de recursos humanos, de auditoría, entre otros.

1.2. Descripción del Problema

En la actualidad, la empresa auditora maneja un amplio volumen de datos confidenciales de sus clientes, incluyendo datos financieros, legales y de negocios.

Sin embargo, no cuentan con planes integrales de seguridad de la información, exponiéndose a diversos riesgos de ciberseguridad.

Esta situación se hace evidente en los crecientes casos reportados de fugas de datos, ransomware y otros incidentes de seguridad que han afectado a firmas auditoras en los últimos años.

Esta situación tiene graves consecuencias, como la pérdida de credibilidad y fiabilidad de los clientes hacia la firma, multas por incumplimiento de regulaciones, interrupción de operaciones, y daños financieros por posibles litigios. Según analistas del sector, los costos estimados por incidentes de seguridad en empresas de auditoría alcanzan los $2.5 millones de dólares anuales.

Es importante resolver este problema y que la empresa implemente planes integrales de seguridad de la información, dado el carácter sensible de los datos que manejan y su responsabilidad ante clientes y reguladores. Contar con un plan director de seguridad mitigaría los riesgos y sentaría las bases para una ciber-resiliencia efectiva en el largo plazo. Los que proponen una solución para este problema tienen acceso a la información de la empresa para la implementación de un Plan Director de Seguridad y el interés de la alta gerencia para apoyar este tipo de iniciativas de mejora en los controles de seguridad informática.

1.3. Solución Propuesta

Una forma de mitigar este problema es a través de la creación de un Plan Director de Seguridad, ya que nos ayuda a gestionar de manera integral los riesgos de

ciberseguridad y cumplir con estándares de responsabilidad ante clientes y autoridades.

En primer lugar, es necesario adquirir comprensión y examinar la situación actual de la empresa. Este proceso resulta desafiante, ya que implica tener en cuenta diversos aspectos y demanda la participación de todas las áreas dentro de la organización[1]. El objetivo es mejorar la seguridad llevando a cabo un análisis de riesgos para determinar un plan de acción[3]. Para realizar un correcto estudio y análisis de viabilidad es necesario conocer claramente cuáles son los objetivos específicos del proyecto.

En términos generales, al realizar un análisis de viabilidad, necesitamos tener en cuenta los siguientes elementos: impacto en el riesgo, estimación de los tiempos y plazos de ejecución, recursos humanos, estructura de costos, relaciones con otras iniciativas y criterios de seguimiento [3].

Es crucial que las empresas den prioridad a la implementación de políticas adecuadas en seguridad de la información, y no limiten su preocupación únicamente al ámbito comercial. El Plan Director de Seguridad establecerá internamente el curso a seguir para lograr un nivel óptimo de seguridad de la información [4].

En nuestra investigación, hemos encontrado a varios profesionales implementando el Plan Director de Seguridad en empresas y universidades en varios países, como se puede observar en las citas referenciales, y llegan a la conclusión de la importancia de llevar a cabo el seguimiento del diseño de lineamientos del Plan Director de Seguridad.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar un plan director de seguridad integral para el departamento de TI a través de un proceso de análisis de riesgos, definición de política de Seguridad de la Información, controles y procedimientos de seguridad, con el fin de proveer una hoja de ruta y prioridades claras que permitan gestionar efectivamente los riesgos de ciberseguridad de la organización.

1.4.2. Objetivos Específicos

- Conocer la situación actual de la organización, elaborando la estructura organizacional, definiendo la política de roles y responsabilidades dentro del SGSI ISO 27001. También es importante realizar un levantamiento del inventario de activos de información, identificándolos y definiendo a sus responsables. Elaborar la política general de Seguridad de la Información para la organización.
- Elaborar una matriz de riesgo que sirva para analizar y gestionar los activos de la organización, basándose en la guía de la ISO/IEC 27005 para identificar posibles amenazas, evaluando los riesgos asociados y realizando un tratamiento de estos para fortalecer la seguridad de los activos por medio de controles, garantizando la integridad, confidencialidad y disponibilidad de la información.
- Definir el Plan Director de Seguridad con varias opciones de presupuesto para selección de alguno de ellos por parte de la directiva, esto permitirá mitigar o

gestionar la criticidad de los riesgos, con el fin de priorizar los proyectos más importantes para salvaguardar la seguridad de los activos de la información.

1.5. Metodología

Este estudio tiene un alcance no experimental tipo descriptivo de enfoque transversal, ya que su fin es caracterizar de forma detallada la situación actual de seguridad informática en la empresa de auditoría, para luego diseñar un plan director que gestione los riesgos identificados. El trabajo se enfocará en describir exhaustivamente los activos informáticos críticos, mapeando sus vulnerabilidades y el nivel de cumplimiento con políticas y estándares aplicables. Este diagnóstico preciso permitirá determinar las necesidades puntuales de seguridad. Así mismo, el plan director en sí será una descripción pormenorizada de la estrategia requerida, estableciendo procesos, roles y acciones específicas para gestionar riesgos. En vez de explicar o demostrar relaciones entre variables, el propósito es especificar características, procedimientos y parámetros del fenómeno en estudio. Se busca medir y describir de forma independiente la realidad actual y la estrategia futura dado que el objetivo no es analizar correlaciones ni poner a prueba hipótesis, más bien se centrará en detallar cualitativamente las propiedades y particularidades del caso bajo análisis. En conclusión, el proyecto de titulación de los autores se enfoca en describir exhaustivamente el estado de seguridad informática y diseñar una solución acorde, lo que refleja un alcance eminentemente descriptivo.

De un total de 118 empleados de la empresa auditora, utilizaremos 9 informantes, de los cuales 3 pertenecen al departamento de TI y 6 a los directivos de la empresa auditora. La información para analizar son los activos de la empresa junto a los

procesos y políticas existentes acorde la seguridad de la información digital o física, toda esta información será entregada por los informantes antes mencionados.

Para realizar este estudio se realizará las siguientes fases:

1. Conocer la situación actual.
2. Conocer la estrategia de la organización.
3. Definir proyectos e iniciativa.
4. Clasificación y priorización.
5. Aprobación por la dirección.
6. Puesta en marcha.

Para el levantamiento de información realizaremos entrevistas a 3 personas del departamento de TI y 6 directivos de la empresa auditora.

La entrevista constará de varias preguntas claves para entender las necesidades específicas con respecto a la seguridad y riesgos que tienen la información digital y física para poder mitigarla en un futuro con proyectos.

Una vez que tengamos los resultados de las entrevistas, se analizarán las amenazas y riesgos de los activos recopilados por la sección de informantes mediante la guía de análisis de riesgo basada en la norma ISO/IEC 27005.

Con esto conoceremos las fortalezas y debilidades, para poder proponer un Plan director de Seguridad que sea efectivo.

CAPITULO II.

MARCO TEÓRICO

En el presente trabajo nos orientamos en listar los lineamientos fundamentales para la elaboración de un Plan Director de Seguridad, el cuál sirva como camino para la elaboración de políticas y proyectos en el ámbito de la seguridad informática.

2.1. Gobierno de Seguridad de la Información

La Gobernanza de la Seguridad de la Información constituye una parte integral del gobierno corporativo de la organización, proporcionando dirección estratégica, asegurando el logro de objetivos, gestionando riesgos de manera efectiva, utilizando los recursos de manera responsable y evaluando el resultado positivo o negativo del programa de seguridad de la información. Este enfoque abarca liderazgo, estructura organizativa y procesos destinados a salvaguardar la información. La Gobernanza de la Seguridad de la Información destaca la importancia de los roles y responsabilidades de la alta dirección, buscando la alineación entre la seguridad de la información y los objetivos comerciales. En consecuencia, se requiere el cumplimiento de leyes, regulaciones y políticas de seguridad de la información [5].

Comúnmente, la seguridad de la información se fundamenta en la política de seguridad, la cual se crea mediante la formulación de un Plan Director de Seguridad (PDS). La dirección de la empresa es responsable de identificar todas las acciones relacionadas con la seguridad. El equipo de seguridad informática será el encargado de ejecutar las medidas técnicas necesarias para cumplir con la política de seguridad

y llevar a cabo el análisis de riesgos en el que dicha política debería fundamentarse [6].

2.1.1 Gestión de la Seguridad de la Información

La Gestión de la Seguridad de la Información hace referencia a un conjunto de prácticas y procesos, los cuales fueron diseñados para salvaguardar la confidencialidad, integridad y disponibilidad de la información. El objetivo principal es asegurar que la información sensible y critica de una empresa se maneje de manera segura, con el fin de protegerla contra amenazas internas y externas. La Gestión de Seguridad de la Información es esencial en un entorno empresarial en constante evolución, donde la información es el principal activo y el más crítico. Mantener políticas sólidas de Gestión de Seguridad de la Información garantiza que las organizaciones puedan minimizar el riesgo de brechas de seguridad, y protege la información sensible de manera efectiva. Para conseguirlo se emplea el Sistema de Gestión de Seguridad de la Información.

2.1.2 Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) se compone de políticas, procesos, directrices y recursos diseñados para estructurar y abordar los elementos que conforman la seguridad en una empresa. Su finalidad es asegurar la protección de la información. Un SGSI habilita a una organización para establecer los procesos necesarios en el diseño, implementación, supervisión y mantenimiento, con

el propósito de gestionar de manera efectiva el acceso a la información y garantizar la confidencialidad, integridad y disponibilidad de los activos de información [7].

Un SGSI está definido por un proceso de cuatro etapas:

- **Planificar:** Definir la política, metas, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información (SGSI) relacionados con la gestión de riesgos, con el propósito de elevar la seguridad de la información y lograr resultados alineados con las políticas y metas generales de la empresa.
- **Implementar:** Implementar y gestionar la política, controles, procesos y procedimientos del SGSI.
- **Medir:** Evaluar el desempeño del proceso en comparación con la política, los objetivos y la experiencia práctica del Sistema de Gestión de Seguridad de la Información (SGSI). Comunicar los resultados.
- **Mejorar:** Implementar medidas correctivas y preventivas, fundamentadas en los resultados de auditorías internas del Sistema de Gestión de Seguridad de la Información (SGSI) y en la revisión de la gestión, así como en otra información pertinente, con el objetivo de alcanzar una mejora continua del SGSI [8].

2.1.2.1 ISO 27001

La norma ISO 27001 establece un conjunto de criterios a nivel mundial que detalla los requisitos para establecer, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema se establece con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. La norma

proporciona una estructura para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar de manera eficaz sus riesgos de seguridad de la información. Su aplicación abarca diversos tipos de organizaciones, tales como pequeñas y medianas empresas, grandes corporativos, entidades gubernamentales y organizaciones sin fines de lucro, siendo relevante para cualquier sector. El proceso de implementación de la norma ISO 27001 se divide en cuatro fases:

- **Planificación:** Se identifica los requisitos de seguridad de la información y se establece un plan para implementar el SGSI.
- **Implementación:** Creación de políticas, procedimientos y controles para proteger la información.
- **Evaluación:** La empresa evalúa la eficacia de su SGSI e identifica áreas de mejora.
- **Mejora continua:** Identificación y aplicación de mejoras a los procesos y controles del SGSI [9].

La estructura de la norma ISO 27001 está diseñada para ser coherente con otras normas de sistemas de gestión, como la ISO 9001, y mantiene una neutralidad tecnológica y de proveedores, lo que implica que es completamente independiente de la plataforma de tecnologías de la información (IT). Como resultado, es necesario proporcionar educación a todos los miembros de la organización sobre el significado y la extensión de la norma [10].

2.1.2.2 ISO 27002

La norma ISO 27002 ofrece una solución directa para desarrollar políticas y controles con el fin de mitigar los riesgos que enfrentan los activos de la organización. Al implementar esta norma, logramos una disminución de riesgos mediante la creación y el seguimiento de controles efectivos.

Esto conduce a la disminución de las amenazas a un nivel que la organización puede asumir. De esta manera, en caso de producirse un incidente, se minimizan los daños y se garantiza la continuidad del negocio. Cada control establecido por la norma ISO 27002 cuenta con una guía de implementación que facilita su comprensión. La norma proporciona una adaptación sencilla para las empresas y sirve como una guía para mejorar la seguridad de la información [11].

El propósito fundamental de la norma ISO 27003 es proporcionar pautas y principios generales para comenzar, llevar a cabo, mantener y mejorar la administración de la seguridad de la información en una organización. Las ventajas proporcionadas por la ISO 27002 son representativas para las empresas, sobre todo porque son reconocidas internacionalmente:

- Mejor concienciación sobre la seguridad de la información
- Mayor control de activos e información sensible.
- Ofrece un enfoque para la implementación de políticas de control
- Oportunidad de identificar y corregir puntos débiles
- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos.
- Conformidad con la legislación y otras reglamentaciones [12].

2.2 Plan Director de Seguridad

El Plan Director de Seguridad (PDS) representa una faceta esencial de la seguridad de la información, consistente en evaluar la situación inicial de una empresa con el fin de desarrollar un conjunto de iniciativas dirigidas a mitigar los riesgos a niveles aceptables. Este plan incluye la identificación de prioridades, la asignación de responsabilidades, la disponibilidad de recursos para la ejecución de proyectos de seguridad y las prácticas recomendadas que deben seguir todos los individuos directamente vinculados con la empresa. Los proyectos integrados en un PDS varían según diversos factores, tales como el tamaño de la organización, su grado de avance tecnológico, el sector en el que opera, las regulaciones legales que rigen sus actividades, la naturaleza de la información y el alcance del propio PDS, entre otros. Para elaborar y poner en marcha un PDS se necesitan 6 fases:

- Conocer la situación actual.
- Conocer la estrategia de la organización.
- Definir proyectos e iniciativas.
- Clasificación y priorización.
- Aprobación por la Dirección.
- Implantación del PDS [1].

2.2.1 Objetivos generales del PDS

Un Plan de Desarrollo de Seguridad (PDS) tiene como meta principal establecer pautas para la seguridad de la información que deben implementarse en la empresa de acuerdo con los objetivos comerciales. Estas pautas buscan mantener un nivel de riesgo apropiado para las necesidades presentes y futuras de la organización. Para lograr este propósito, es esencial abordar los siguientes aspectos: consolidar la información de proyectos existentes, involucrar a la dirección en la gestión de la seguridad de la información, realizar un análisis de seguridad que abarque la estrategia, la organización, los procesos y la tecnología, priorizar la seguridad de la información, establecer directrices para asegurar la seguridad en diversas ubicaciones geográficas, evaluar la situación de la organización en relación con las buenas prácticas internacionales, revisar el cumplimiento en la protección de datos personales, evaluar el nivel de protección de la organización frente a nuevas amenazas y riesgos, proporcionar un plan de proyectos de seguridad priorizado en términos de costo, esfuerzo y beneficio, y finalmente, garantizar la implementación y control del plan de acción definido[3].

2.2.2 Fases del PDS

Como se observa en la Figura 2.1, para el correcto diseño e implementación de un PDS se siguen seis fases:

- **Conocer la situación actual de la organización:** Es esencial realizar diversos análisis que abarquen aspectos técnicos, organizativos, regulatorios y normativos durante la fase más crucial y compleja de la creación del PDS. Esta complejidad surge de la participación de diversas personas y de la

necesidad de garantizar que la información de la empresa, fundamental para comprender y evaluar su situación actual, sea confiable, completa y actualizada. En esta etapa, contar con el respaldo de la Dirección resulta fundamental.

- **Conocer la estrategia de la organización:** Es necesario tener en cuenta los proyectos actuales y venideros, proyecciones de expansión, modificaciones en la estructura organizativa debido a reestructuraciones, entre otros aspectos.
- **Definición de proyectos e iniciativas:** Establecer la estrategia a seguir y seleccionar los proyectos más idóneos para manejar los riesgos que superan nuestro nivel de riesgo aceptable.
- **Clasificar y priorizar los proyectos a realizar:** Se sugiere reunir las iniciativas o fragmentar las propuestas con el fin de uniformizar el conjunto de proyectos previamente establecidos. Al clasificar estas iniciativas, es posible utilizar como criterios tanto su origen como el tipo de acción.
- **Aprobar el PDS:** En esta fase, ya tendremos una versión preliminar del PDS. Este plan debe revisarlo y aprobarlo la Dirección.
- **Puesta en marcha:** Después de obtener la aprobación de la Dirección, el PDS establece la ruta a seguir para lograr el nivel de seguridad requerido por nuestra organización. Al iniciar el proyecto, es crucial realizar una presentación integral a las personas involucradas, involucrándolas y proporcionándoles información sobre los trabajos y los resultados que se buscan [13].

FIGURA 2.1: FASES DE UN PLAN DIRECTOR DE SEGURIDAD

Fuente: INCIBE

2.3. Gestión y análisis de riesgo

Los ciberataques a los sistemas informáticos han experimentado un incremento debido a los avances en servicios, modelos de comunicación, y el auge de las Tecnologías de la Información y Comunicación (TIC), así como al uso continuo de internet. Este aumento de ataques ha llevado a las empresas a buscar estrategias que les permitan llevar a cabo análisis preventivos, de control y reducción de riesgos relacionados con la vulnerabilidad de la información. Las organizaciones enfrentan diariamente amenazas tanto internas como externas que pueden dar lugar al robo de

identidad e información, acceso no autorizado a bases de datos, compromiso de información sensible de clientes, pérdida de credibilidad y daños financieros que podrían afectar la sostenibilidad de la empresa. Por lo tanto, es fundamental contar con el conocimiento y la aplicación de metodologías para realizar análisis de riesgos y proteger los principios de seguridad de la información [14].

El propósito del análisis de riesgo es examinar, valorar, cuantificar y prevenir posibles fallos en los sistemas técnicos que puedan originar y desencadenar eventos no deseados con impacto en personas, información, propiedades y el entorno. Para el análisis de riesgo rigen las siguientes normativas:

- **ISO 27001:** Comprende un grupo de reglas o normas en relación con la estabilidad informática.
- **ISO/IEC 27002:** Es un estándar para la estabilidad de la información que utiliza una guía de buenas prácticas en la cual se integran los diversos tipos de control recomendados.
- **ISO/IEC 27003:** Estándar internacional que constituye una guía para la fijación de un SGSI.
- **ISO/IEC 27004:** Esta norma indica como se estructura el sistema de medición, valores limite, a qué hora y como medirlo. Ayuda a las organizaciones al establecimiento de fines involucrados con el rendimiento y los criterios de triunfo.
- **MAGERIT V3:** Proporciona un enfoque estructurado para evaluar, tratar y gestionar los riesgos de seguridad, abordando aspectos como la confidencialidad, integridad y disponibilidad de la información. Se centra en el sector público, pero también puede aplicarse en entidades privadas.

- **ISO/IEC 27005:** Es un instrumento que nos posibilita detectar las amenazas a las que se exponen todos los activos. Se considera la frecuencia en la que se materializan cada una de las amenazas y valora el efecto que implica que se materialice en la organización [15].

Para el trabajo presentado por los autores, utilizaremos una guía de análisis de gestión de riesgo basada en la norma ISO/IEC 27005 y para la clasificación de sus activos utilizaremos lo recomendado por MAGERIT V3.

2.3.1 Norma ISO/IEC 27005

La norma ISO/IEC 27005 proporciona orientación sobre la gestión de riesgos en seguridad de la información dentro de una organización, complementando los requisitos generales del Sistema de Gestión de Seguridad de la Información (SGSI) delineados en las normas ISO 27001 y 27002. Para comprender completamente la ISO 27005, es fundamental tener conocimiento de los conceptos, modelos, procesos y términos detallados en estas normativas. Diseñada para facilitar la aplicación efectiva de la seguridad de la información con un enfoque en la gestión de riesgos, esta norma es relevante para una variedad de organizaciones, incluyendo empresas comerciales, entidades gubernamentales y organizaciones sin fines de lucro. La ISO 27005 no prescribe una metodología específica, ya que esto depende de factores como el alcance del SGSI, el tamaño o el sector industrial de la organización. La primera versión fue publicada el 4 de junio de 2008, y la versión más reciente se publicó en 2018. La gestión del riesgo puede aplicarse a toda la organización, a una parte de ella, a una sección separada, a cualquier sistema de información existente o planificado, o aspectos particulares de control [16].

Dado que es una guía, la norma carece de la estructura de alto nivel, aunque incluye secciones relacionadas con el proceso de gestión de riesgos en la seguridad de la información. Comienza con una introducción general al proceso de gestión de riesgos, haciendo una clara alusión a la estructura establecida por la norma ISO 31000:2018. La gestión de riesgos no es un evento único, sino un proceso continuo que requiere revisión y actualización regular. Por tanto, resulta crucial que la organización disponga de una metodología documentada y registros que posibiliten su ejecución de manera frecuente, generando resultados coherentes y rastreables[17].

La gestión de riesgos puede seguir un enfoque iterativo en las fases de evaluación y tratamiento de riesgos. Inicialmente, se establece el contexto, después se realiza la evaluación de riesgos y, posteriormente, en la fase de tratamiento de riesgos, es esencial proporcionar información adecuada que facilite la determinación de las acciones necesarias para mitigar los riesgos[16]. Como observamos en la Figura 2.2, la estructura de la norma ISO/IEC 27005 está definida por:

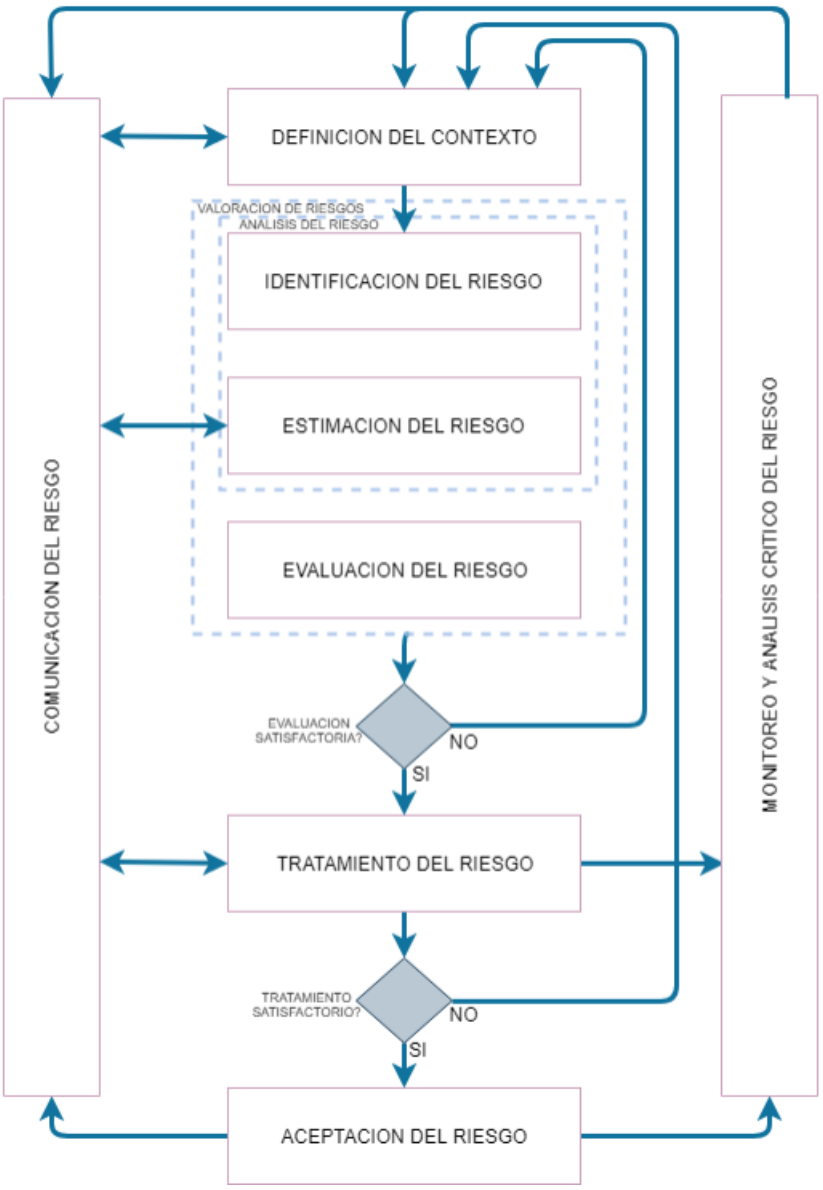


FIGURA 2.2: PROCESO DE GESTION DE RIESGO

Fuente: Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005

La ISO/IEC 27005 fue creada específicamente para abordar los riesgos informáticos. Está alineada con la ISO 31000 y, como muchas otras normas ISO, sigue el ciclo de Planificar, Hacer, Verificar y Actuar (PHVA) para su implementación y mejora continua como se observa en la Figura 2.3, aplicado a la Gestion de Riesgo de la Seguridad de la información [16].

FIGURA 2.3: ETAPAS DE LA METODOLOGÍA CON BASE AL CICLO PHVA

Fuente: Metodología para la incorporación y evaluación de los atributos del TEC

CAPITULO III.

CONOCER LA SITUACION ACTUAL DE LA ORGANIZACIÓN

3.1 Contexto de la organización

La empresa Servicios de auditoria es una organización privada que inicia sus actividades el 01 de septiembre del 2014, para brindarle el apoyo administrativo que requería en aquel entonces un Grupo corporativo de compra y venta de oro, con el fin de llevarlo al correspondiente desarrollo formal, en vista de que dicho grupo inició como un mediano emprendimiento y fue creciendo paulatinamente, por ende, surgió la necesidad de que todas sus operaciones vayan tomando un rumbo más estructurado.

Con el pasar del tiempo, el alcance de esta empresa de servicios de auditoria también tomó un rumbo de franco desarrollo y los profesionales que la componen, sumaron a su experiencia, conocimientos actualizados por medio de formación en cuanto a tendencias actuales en sus profesiones, aplicándolas al Grupo corporativo de compra y venta de oro, y extendiendo sus alcances a otras empresas que requieran sus servicios profesionales en los ámbitos legal, financiero, de Tecnologías de la información, de Recursos Humanos, de Auditoría, entre otros.

3.1.1 Estructura Organizacional

La estructura organizacional de la empresa auditora es un componente fundamental para el funcionamiento eficiente y eficaz de la organización. Con ella garantizamos la claridad en las responsabilidades, coordinación y colaboración, eficiencia operativa,

una correcta toma de decisiones, la oportunidad del desarrollo de carrera dentro de la empresa y la cultura organizacional.

A continuación, se presenta la estructura organizacional de la empresa auditora en la Figura 3.1:

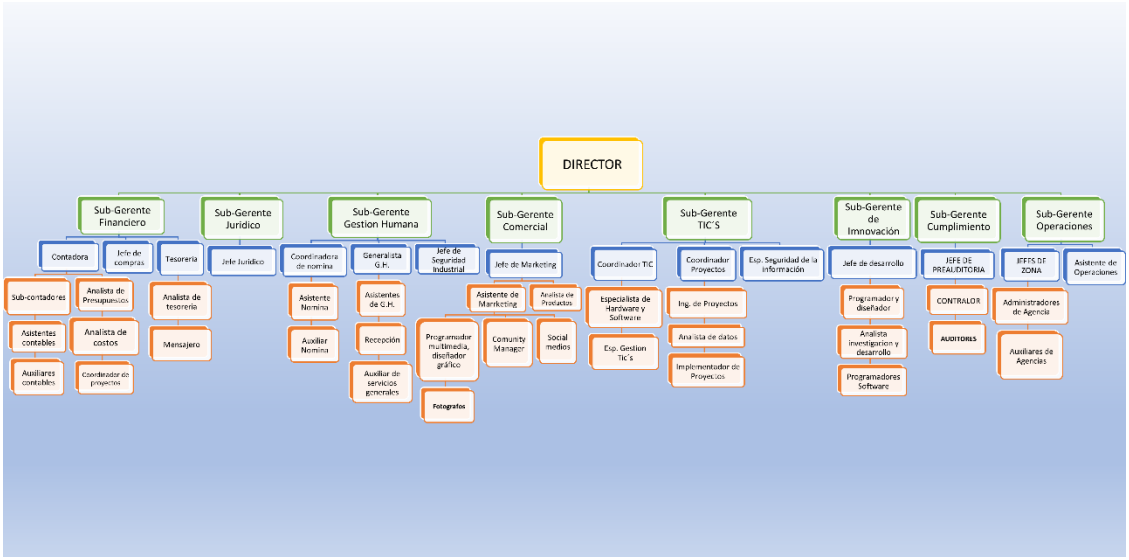


FIGURA 3.1: ORGANIGRAMA DE LA EMPRESA AUDITORA

Fuente: Douglas Marín

3.1.1.1 Sede y servicios ofrecidos

La empresa auditora ofrece sus servicios al grupo corporativo de compra y venta de joyas en diferentes áreas administrativas por más de 8 años aportando al desarrollo corporativo y transformación digital, a continuación, observaremos como está organizados los diferentes departamentos con los servicios que ofrecen:

Edificio	Departamento	Servicios
Piso 1	Gestión Humana	• Recepción

	Comercial	• Marketing • Fotografía • Diseño Multimedia • Estrategias Comerciales • Community manager
Piso 1	Tecnología de Información	• Gestión TIC • Soporte Hardware • Soporte Software • Desarrollo de Software • Implementación de Proyecto • Análisis de Datos • Seguridad de la Información
	Data Center	• Servidores
	Cumplimiento y Control Interno	• Auditoría Interna • Auditoría Externa • Compliance
Piso 2	Gestión Humana	• Nomina • Reclutamiento • Bienestar Social •Desarrollo Organizacional • Seguridad Industrial
	Gerencia General	• Dirección General
	Innovación y Desarrollo	• Desarrollo de Software
	Jurídico	• Legal

		• LPODP
	Operaciones	• Gestión Logística y Operaciones
Piso 3	Financiero	• Gestión en Finanzas
	Contabilidad	• Gestión Contable
	Tesorería	• Pagos a proveedores • Pagos a colaboradores
	Compras	• Gestión de Compras
Piso 4	Comedor	• N/A
Piso 5	Auditorio	• Sala de capacitación

Tabla 1: Disposición de los departamentos en la empresa auditora

Fuente: Douglas Marín

3.1.2 Antecedentes

Para conocer a la empresa auditora a fondo, es necesario abordar los aspectos técnicos a detalle. Para esto se realiza un levantamiento de información técnica que engloba la infraestructura, los equipos informáticos, los puestos de trabajo y los servicios contratados con terceros en materia de tecnología.

3.1.2.1 Infraestructura

La Infraestructura tecnológica es un componente critico en el diseño y la operación eficientes de sistemas de comunicación. La elección adecuada de la topología puede tener un impacto significativo en la seguridad de la red. La empresa auditora cuenta

con equipamiento tecnológico para el que presta servicio en todas sus plataformas. La infraestructura está conformada según se observa en la Figura 3.2:

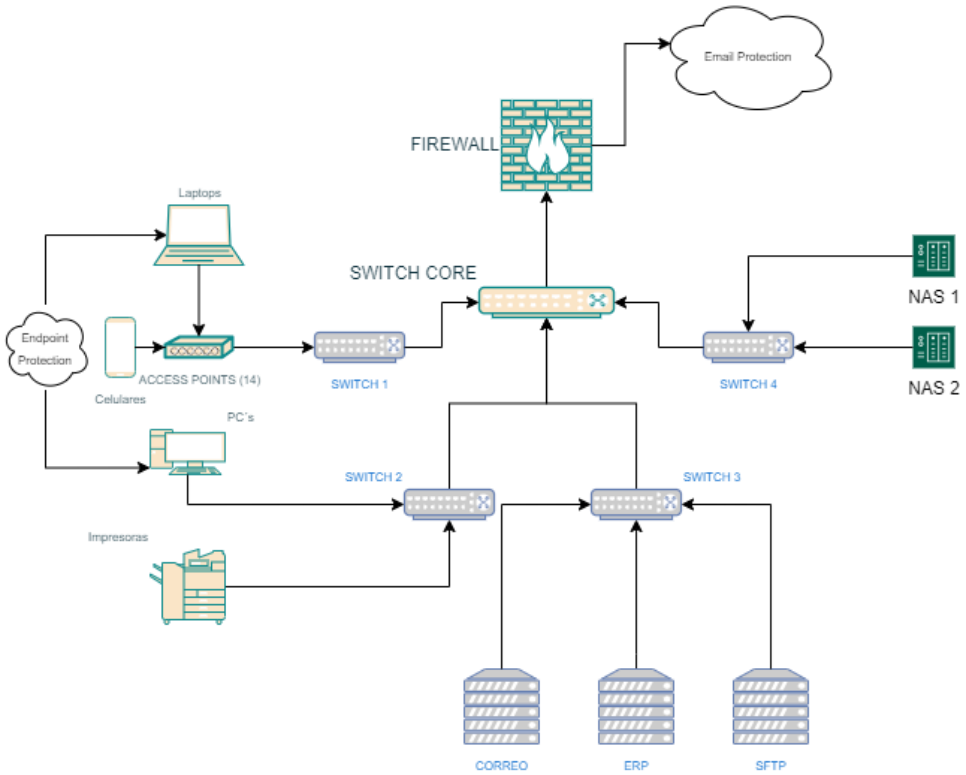


FIGURA 3.2: TOPOLOGÍA DE LA EMPRESA AUDITORA

Fuente: Douglas Marín

3.1.2.2 Equipos Informáticos

Los equipos informáticos existentes en la empresa auditora componen un pilar fundamental para el funcionamiento de todos los servicios que esta ofrece. Estos pueden ser desde puestos de trabajo para usuario final, hasta Firewalls para proteger a la empresa contra ataques cibernéticos. A continuación, se detalla que equipos informáticos existen dentro de la empresa auditora:

- Servidores
- Routers
- Switches
- NAS
- Equipos PC
- Laptops
- Impresoras
- Monitores
- Teclados
- Mouses
- Access Point
- Tablets
- Teléfonos móvil
- Proyectores
- Scanners
- Modem
- Firewalls
- Cámaras
- UPS

3.1.2.3 Puestos de trabajo

Un puesto de trabajo abarca las diversas responsabilidades que un trabajador debe cumplir como parte integral del sistema laboral. De igual manera, implica los derechos

asociados con dicho acuerdo, siendo el más importante el derecho a recibir una remuneración, generalmente mensual, como compensación por las labores realizadas. La empresa auditora cuenta con los siguientes puestos de trabajo por departamentos:

Edificio	Departamento	Puestos de trabajo
Piso 1	Recepción	1
	Comercial	10
	Tecnología de Información	13
	Data Center	N/A
	Cumplimiento y Control Interno	5
Piso 2	Gestión Humana	6
	Implementación	2
	Gerencia General	1
	Innovación y Desarrollo	4
	Jurídico	5
	Operaciones	2
Piso 3	Financiero	7
	Contabilidad	18
	Tesorería	3
	Compras	1
Piso 4	Comedor	N/A
Piso 5	Auditorio	1

Tabla 2: Disposición de los puestos de trabajo en la empresa auditora

Fuente: Douglas Marín

3.1.2.4 Servicios subcontratados

Un servicio subcontratado se realiza en base a un contrato con un tercero, el cual es un compromiso legal entre dos partes, donde una se compromete a brindar un servicio específico a cambio de una compensación económica. A diferencia de un contrato laboral, este tipo de acuerdo se utiliza cuando los profesionales trabajan de manera autónoma. Este tipo de contrato abarca diversas áreas, como proyectos de ingeniería, asesorías profesionales y servicios publicitarios. A continuación, detallamos los servicios subcontratados por la empresa auditora:

- Servicio de Enlace Internet 1:1 400 Mbps
- Servicio EndPoint Kaspersky
- Servicio Antiphishing & AntiSpam Sophos
- Servicio Licencia Microsoft Office 365

3.1.3 Valoración inicial

Realizar la valoración inicial en cuanto a la seguridad de la información en la empresa auditora es un paso crucial para identificar y etiquetar posibles riesgos y establecer medidas de protección. Una valoración inicial solida brindará una base para la mejora continua y la implementación de medidas de seguridad que sean efectivas. Para nuestro caso, realizaremos en conjunto con la empresa auditora la valoración de la

situación actual de la empresa, tomando en cuenta la norma ISO/IEC 27001:2022 en su Anexo A.

3.1.3.1 Definir el modelo de madurez

Se utilizarán los siguientes niveles mostrados en la Figura 3.3 para medir la madurez de los controles de la norma ISO/IEC 27001:

FIGURA 3.3: MEDICIÓN DE MADUREZ PARA CONTROLES DE NORMA ISO/IEC 27001

Fuente: Douglas Marín y César Medina

3.1.3.2 Declaración Aplicabilidad (SOA)

Se elaboró un documento con los controles que aplican a la empresa para verificar su grado de madurez. A continuación, mostramos el detalle de la Declaración de Aplicabilidad:

ANEXO A - Estado y aplicabilidad de los controles de seguridad de la información

Claúsula	Título del control	Calificación	Descripción del control
5	Controles Organizacionales		
5,1	Políticas de seguridad de la información	NI	*La política de seguridad de la información y un conjunto de políticas temáticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.*
5,2	Roles y responsabilidades de seguridad de la información	IN	*Todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.*
5,3	Segregación de deberes	IN	*Las funciones y áreas de responsabilidad en conflicto deben segregarse. Realizar una segregación de las funciones y áreas de responsabilidad en conflicto para reducir oportunidades de modificación no autorizada o no intencional, o mal uso de los activos de la organización.*
5,4	responsabilidades de la dirección	NI	*La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información, las políticas temáticas y sus procedimientos específicos establecidos en la organización.*
5,5	Contacto con autoridades	IN	*Deben establecerse y mantenerse los contactos adecuados con las autoridades pertinentes.*
5,6	Contacto con grupos de interés especial	NA	*Deben establecerse y mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.*

FIGURA 3.4: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 5, CONTROL 5,1 AL 5,6

Fuente: Douglas Marín y César Medina

5,7	Inteligencia de Amenazas	GE	*La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas.*
5,8	Seguridad de la información en la gestión de proyectos.	NI	La seguridad de la información debería integrarse en la gestión de proyectos.
5,9	Inventario de información y otros activos asociados	GE	*Debería elaborarse y mantenerse un inventario de la información y otros activos asociados, incluyendo la identificación de sus propietarios.*
5,10	Uso aceptable de la información y otros activos asociados	GE	*Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de información y otros activos asociados.*
5,11	Devolución de activos	GE	*Todos los empleados y otras terceras partes, según procedan, deben devolver todos los activos de la organización en su poder tras el cambio o la terminación de su trabajo, contrato o acuerdo.*
5,12	Clasificación de la información	NI	*La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.*
5,13	Etiquetado de información	GE	*Debería desarrollarse e implementarse un conjunto adecuado de procedimientos para el etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.*
5,14	Transferencia de información	NI	*Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de medios de transferencia dentro de la organización y entre la organización y otras partes.*
5,15	Control de acceso	IN	*Se deben establecer e implementar reglas de control de acceso físico y lógico a la información y otros activos asociados, basadas en los requisitos de negocio y de seguridad de la información.*

FIGURA 3.5: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 5, CONTROL 5,7 AL 5,15

Fuente: Douglas Marín y César Medina

5,16	Gestión de identidad	GE	*Permitir la identificación única de los individuos y sistemas que acceden a la información de la organización y otros activos asociados y permitir la adecuada asignación de los derechos de acceso.*
5,17	Información de autenticación	GE	*La asignación y gestión de la información de autenticación debe controlarse mediante un proceso formal de gestión, incluyendo el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación.*
5,18	Derechos de acceso	GE	*Los derechos de acceso a la información y otros activos asociados deben aprovisionarse, revisarse, modificarse y eliminarse de conformidad con la política específica de la organización y las reglas sobre control de acceso*
5,19	Seguridad de la información en las relaciones con los proveedores	NI	*Se deberían identificar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores.*
5,20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	NI	*Deben establecerse y acordarse con cada proveedor los requisitos pertinentes de seguridad de la información en función del tipo de relación con el proveedor.*
5,21	Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)	IN	*Se deben definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de Tecnologías de la Información y de las Comunicaciones (TIC).*
5,22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	NI	*La organización debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información y prestación de servicios de los proveedores.*
5,23	Seguridad de la información para el uso de servicios en la nube	NI	*Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.*
5,24	Planificación y preparación de la gestión de incidentes de seguridad de la información	IN	*La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, roles y responsabilidades de gestión de los incidentes de seguridad de la información.*

FIGURA 3.6: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 5, CONTROL 5,15 AL 5,24

Fuente: Douglas Marín y César Medina

5,25	Evaluación y decisión sobre eventos de seguridad de la información	GE	*La organización debe evaluar los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información..*
5,26	Respuesta a incidentes de seguridad de la información	IN	*Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.*
5,27	Aprender de los incidentes de seguridad de la información	GE	*El conocimiento adquirido a partir de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.*
5,28	Recolección de evidencia	IN	*La organización debe establecer e implementar procedimientos para la identificación, recogida, adquisición y preservación de evidencias relacionadas con eventos de seguridad de la información.*
5,29	Seguridad de la información durante la interrupción	NI	*La organización debe planificar cómo mantener la seguridad de la información a un nivel adecuado durante la interrupción.*
5,3	Preparación de las TIC para la continuidad del negocio	NI	*La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC*
5,31	Requisitos legales, estatutarios, reglamentarios y contractuales	NA	*Los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenerse actualizados.*
5,32	Derechos de propiedad intelectual	IN	*La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual (DPI).*
5,33	Protección de registros	GE	*Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.*

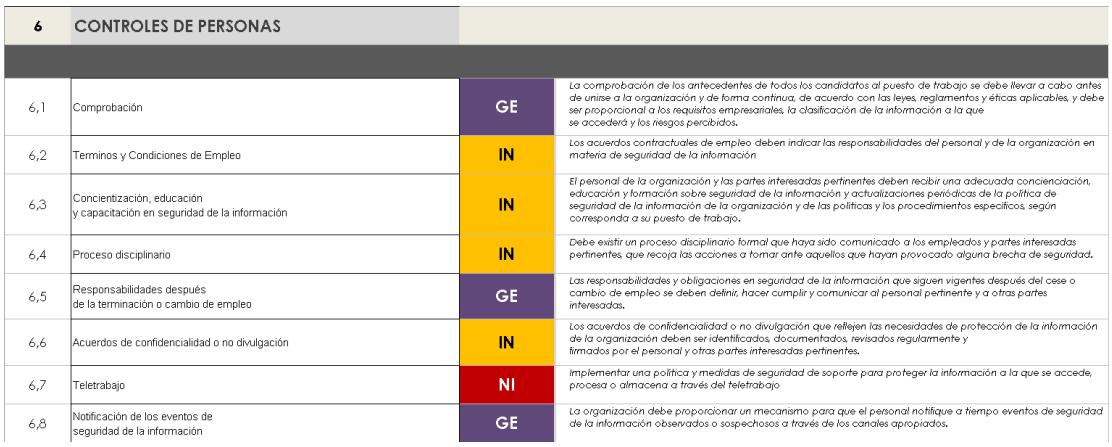
FIGURA 3.7: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 5, CONTROL 5,25 AL 5,33

Fuente: Douglas Marín y César Medina

5,34	Privacidad y Proteccion de la Informacion de Identificacion personal (DCP)	NI	*La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.*
5,35	Revisión independiente de la seguridad de la información.	NI	*El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidos los procesos, la tecnología y las personas, debe revisarse de forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.*
5,36	Cumplimiento de políticas, normas y estándares de seguridad de la información	NI	*Debe comprobarse periódicamente el cumplimiento con la política de seguridad de la información, las políticas temáticas específicas, las reglas y las normas de la organización.*
5,37	Procedimientos operativos documentados	ES	*Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.*

FIGURA 3.8: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 5, CONTROL 5,34 AL 5,37

Fuente: Douglas Marín y César Medina



6	CONTROLES DE PERSONAS		
6,1	Comprobación	GE	*La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo antes de unirse a la organización y de forma continua, de acuerdo con las leyes, reglamentos y éticas aplicables, y debe ser proporcional a los requisitos empresariales, la clasificación de la información a la que se accederá y los riesgos percibidos.*
6,2	Terminos y Condiciones de Empleo	IN	*Los acuerdos contractuales de empleo deben indicar las responsabilidades del personal y de la organización en materia de seguridad de la información*
6,3	Concientización, educación y capacitación en seguridad de la información	IN	*El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concienciación, educación y formación sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.*
6,4	Proceso disciplinario	IN	*Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.*
6,5	Responsabilidades después de la terminación o cambio de empleo	GE	*Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cese o cambio de empleo se deben definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.*
6,6	Acuerdos de confidencialidad o no divulgación	IN	*Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.*
6,7	Teletrabajo	NI	*Implementar una política y medidas de seguridad de soporte para proteger la información a la que se accede, procesa o almacena a través del teletrabajo*
6,8	Notificación de los eventos de seguridad de la información	GE	*La organización debe proporcionar un mecanismo para que el personal notifique a tiempo eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.*

FIGURA 3.9: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 6, CONTROL 6,1 AL 6,8

Fuente: Douglas Marín y César Medina

7	CONTROLES FISICOS		
7,1	Perimetros fisicos de seguridad	ES	*Se deben definir y utilizar perimetros de seguridad para proteger áreas que contengan información y otros activos asociados.*
7,2	Entrada Fisica	GE	*Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.*
7,3	Asegurar oficinas, salas e instalaciones	GE	*Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.*
7,4	Monitoreo de Seguridad Fisica	GE	*Las instalaciones deben ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.*
7,5	Protección contra amenazas físicas y ambientales	GE	*Se debe diseñar e implementa una protección a las infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.*
7,6	Trabajar en áreas seguras	GE	*Diseñar e implementar procedimientos para el trabajo en áreas seguras*
7,7	Escritorio despejado y pantalla despejada	NI	*Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información. (Realizar politicas)*
7,8	Emplazamiento y protección de equipos	GE	*Los equipos deben situarse de forma protegida y segura*
7,9	Seguridad de los activos fuera de las instalaciones	IN	*Los activos fuera de las instalaciones deben estar protegidos.*

FIGURA 3.10: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 7, CONTROL 7,1 AL 7,9

Fuente: Douglas Marín y César Medina

7,10	Medios de Almacenamiento	ES	*Los soportes de almacenamiento deben gestionarse durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.*
7,11	Utilidades de Apoyo	GE	*Las instalaciones de procesamiento de información deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.*
7,12	Seguridad del Cableado	GE	*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*
7,13	Mantenimiento de Equipo	ES	*Los equipos deben recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.*
7,14	Eliminación segura o reutilización de equipos	GE	*Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia, han sido eliminados o sobrescritos de manera segura, antes de deshacerse de ellos o reutilizarlos*

FIGURA 3.11: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 7, CONTROL 7,10 AL 7,14

Fuente: Douglas Marín y César Medina

8	CONTROLES TECNOLOGICOS		
8,1	Dispositivos de punto final de usuario	GE	*La información almacenada, procesada o accesible a través de dispositivos finales de usuario debe protegerse.*
8,2	Derechos de acceso privilegiado	GE	*La asignación y el uso de derechos de acceso con privilegios deben restringirse y controlarse.*
8,3	Restricción de acceso a la información	GE	*Se debe restringir el acceso a la información y otros activos relacionados, de acuerdo con las políticas específicas de control de acceso definidas.*
8,4	Acceso al código fuente	GE	*Se debe gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.*
8,5	Autenticación segura	GE	*Las tecnologías y procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.*
8,6	Gestión de capacidad	PR	*Se debe supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.*
8,7	Protección contra malware	GE	*Se debe implementar una protección contra el código malicioso, respaldada por una concienciación adecuada al usuario.*
8,8	Gestión de vulnerabilidades tecnicas	IN	*Se debe obtener información 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.*
8,9	Gestión de la configuración	IN	*Se debe ser establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.*

FIGURA 3.12: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 8, CONTROL 8,1 AL 8,9

Fuente: Douglas Marín y César Medina

8,10	Eliminación de información	IN	*La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.*
8,11	Enmascaramiento de datos	NI	*El enmascaramiento de datos debe utilizarse de acuerdo con la política específica del tema de la organización sobre el control de acceso, con otras políticas temáticas relacionadas, así como con los requisitos de negocio, teniendo en cuenta los requisitos legales aplicables.*
8,12	Prevención de fuga de datos	NI	*Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.*
8,13	Copia de seguridad de la información	ES	*Las copias de seguridad de la información, del software y de los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad específica acordada.*
8,14	Redundancia de las instalaciones de procesamiento de información	NA	*Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad*
8,15	Registro de eventos	GE	*Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.*
8,16	Actividades de Seguimiento	IN	*Las redes, los sistemas y las aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.*
8,17	Sincronizacion de Reloj	IN	*Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.*
8,18	Uso de programas de utilidad privilegiada	GE	*Se debe restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.*
8,19	Instalación de software en sistemas operativos	GE	*Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas en producción.*
8,20	Seguridad en redes	ES	*Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones*

FIGURA 3.13: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 8, CONTROL 8,10 AL 8,20

Fuente: Douglas Marín y César Medina

8,21	Seguridad de los Servicios de Red	ES	*Se deben identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.*
8,22	Segregacion de redes	GE	*Los grupos de servicios de información, de usuarios y de sistemas de información deben ser segregados en las redes de la organización.*
8,23	Filtrado web	IN	*El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.*
8,24	Uso de Criptografía	NA	*Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida para la gestión de claves criptográficas.*
8,25	ciclo de vida de desarrollo seguro	NI	*Se deben establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas.*
8,26	Requisitos de Seguridad de la Aplicación	NI	*Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.*
8,27	Principios de arquitectura e ingeniería de sistemas seguros	NA	*Los principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.*
8,28	Codificacion Segura	NI	*Principios de codificación segura deben aplicarse al desarrollo de software.*
8,29	Pruebas de seguridad en desarrollo y aceptacion	IN	*Deben definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.*
8,30	Desarrollo subcontratado	NA	*La organización debe controlado, monitorizar y revisar las actividades relativas al desarrollo externalizado de sistemas.*

FIGURA 3.14: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 8, CONTROL 8,21 AL 8,30

Fuente: Douglas Marín y César Medina

8,31	Separación de los entornos de desarrollo, prueba y producción	GE	*Deben separarse y protegerse los entornos de desarrollo, prueba y producción.*
8,32	Gestion del Cambio	GE	*Los cambios en las instalaciones de tratamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.*
8,33	Informacion de Prueba	NA	*Seleccionar, proteger y controlar los datos de prueba utilizando técnicas de Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.*
8,34	Protección de los sistemas de información durante las pruebas de auditoría	NI	*Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.*

FIGURA 3.15: DECLARACIÓN DE APLICABILIDAD CLÁUSULA 8, CONTROL 8,31 AL 8,34

Fuente: Douglas Marín y César Medina

3.1.3.3 Resumen del estado inicial de la empresa

El estado inicial de una empresa implica conocer los controles existentes en los activos y procesos garantizando el funcionamiento eficiente y seguro. Los controles organizacionales se fundamentan en las políticas y procedimientos de la estructura organizativa mientras que los controles de personas se basan en el proceso de

selección, formación y concientización a usuarios. Los controles físicos aseguran el acceso a las instalaciones y la seguridad física, y los controles tecnológicos evalúan la seguridad de la red, la gestión de identidad y acceso, y por último el respaldo y recuperación de datos. En las ilustraciones 19, 20 y 21, se presentan el resumen de los controles enfocados en la empresa auditora para conocer su estado inicial:

Controles	Optimizado	Predecible	Establecido	Gestionado	Inicial	No impementada	No aplica	Calificación
5 - Controles Organizacionales	0	0	1	11	9	14	2	Básico
6 - Controles de Personas	0	0	0	3	4	1	0	Básico
7 - Controles Fisicos	0	0	3	9	1	1	0	Básico
8 - Controles Tecnologicos	0	1	3	12	7	6	5	Básico
Total	0	1	7	35	21	22	7	93

FIGURA 3.16: ESTADO INICIAL DE LA EMPRESA, BASADO EN CONTROLES APLICADOS

Fuente: Douglas Marín y César Medina

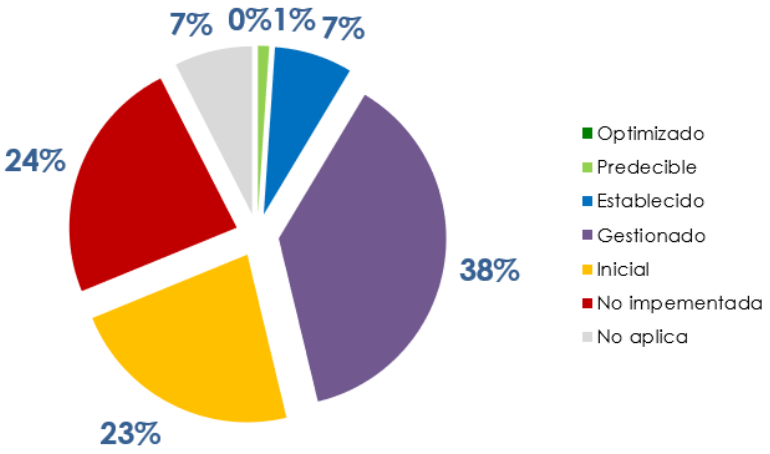


FIGURA 3.17: PORCENTAJE DE CONTROLES EN EL ESTADO INICIAL DE LA EMPRESA

Fuente: Douglas Marín y César Medina

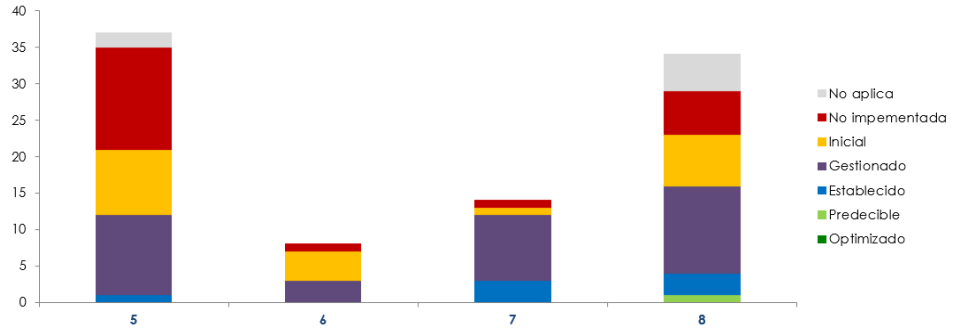


FIGURA 3.18: GESTIÓN DE CONTROLES ACORDE A LAS CLÁUSULAS DE LA NORMA ISO 27001

Fuente: Douglas Marín y César Medina

3.1.4 Análisis GAP

Se realizaron reuniones con el personal de los diferentes departamentos o áreas involucradas con el desarrollo del plan para evaluar la implantación de los controles de seguridad de acuerdo con los niveles indicados. La mayor parte de los controles corresponderán al área de TI, sin embargo, fue necesaria la participación de otros departamentos como el de Gestión Humana, Jurídico, Finanzas, Comercial etc. En la empresa auditora a través de su dirección traslado a cada área y sus responsables la importancia del desarrollo del plan, así como el apoyo que se espera de ellos en cada fase. De acuerdo con el análisis de los resultados se estableció en conjunto con la empresa auditora los objetivos a cumplir en materia de ciberseguridad de la empresa, lo que permitirá determinar los aspectos a mejorar y en los que se deberá enfocar los esfuerzos. A continuación, se presenta los indicadores de referencial respecto a los

resultados de la evaluación de los aspectos normativos y regulatorios en una organización tomando como referencia los controles de la norma ISO/IEC 27002:2022 y que sirva como herramienta de control y seguimiento de los avances:

· La línea naranja representa el grado de cumplimiento actual.

· La línea roja representa el grado de cumplimiento básico.

· La línea celeste un posible objetivo de cumplimiento a medio / largo plazo

· La línea verde representa el nivel de cumplimiento óptimo.

Los números que se muestran en la Figura 3.19 hacen referencia al nivel de implantación de los controles según su estado.

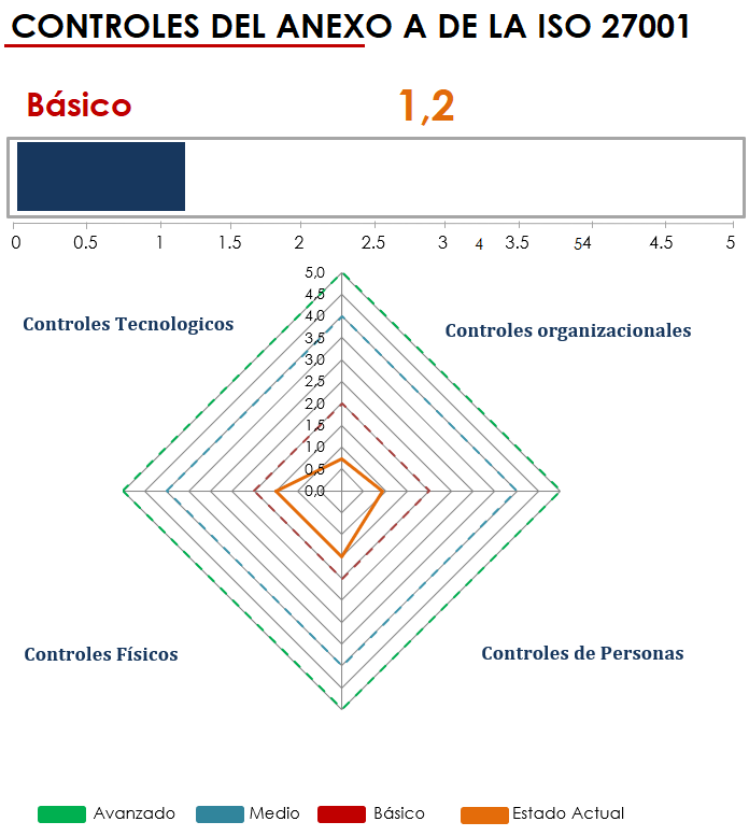


FIGURA 3.19: NIVEL DE IMPLEMENTACIÓN DE LOS CONTROLES DE LA NORMA ISO 27001

Fuente: Douglas Marín y César Medina

3.2 Levantamiento de información

El levantamiento de información es un proceso crucial que tiene como propósito establecer los objetivos y metas, para determinar qué tipo de información se necesita recopilar.

También es necesario para evaluar los procesos críticos de la empresa y que puedan tratarse para mitigar los riesgos existentes. La información que se recopilará estará dentro del alcance definido en el siguiente punto donde se definirá el alcance.

3.2.1 Acotar y establecer el alcance

El alcance del proyecto se centrará exclusivamente en la parte de elaboración del Plan director de Seguridad (PDS), dejando la implantación de las iniciativas de seguridad resultantes para proyectos posteriores a este.

Los departamentos con mayor análisis dentro del alcance PDS serán:

- Departamento TI (activos, responsables, procesos críticos, sistemas)
- Departamento de Innovación (Plataformas digitales)
- Departamento Comercial (Plataformas digitales)
- Departamento Jurídico (Términos de confidencialidad y procesos normativos)
- Departamento Gestión Humana (Términos organizativos)

- Departamento Cumplimiento y control Interno (Políticas y procesos acorde a la SI)

En el alcance del PDS se evaluarán los activos considerados críticos acordes a su proceso en la empresa. Se necesita la colaboración de la alta dirección y de los encargados de los procesos, dentro y fuera del alcance mediante entrevistas programadas si se solicita información importante.

3.2.2 Definición de política de SI

La definición de una Política de Seguridad de la Información (SI) es fundamental para garantizar el correcto funcionamiento y protección de una organización en el entorno digital. Esta política establece los principios, directrices y procedimientos que guían la gestión segura de la información dentro de la empresa. A continuación, se muestra la política de Seguridad de la Información (SI) que será aplicada en la empresa auditora:

FIGURA 3.20: POLÍTICA DE SI (PARTE 1)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 2 de 8

CONTROL DE VERSIONES

Versión	Cambios de la versión	Fecha
0.0	Emisión del documento	15/01/2024

FIGURA 3.21: POLÍTICA DE SI (PARTE 2)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 3 de 8

I. CONTEXTO

La empresa Servicios de auditoria es una organización privada que inicia sus actividades el 01 de septiembre del 2014, para brindarle el apoyo administrativo que requería en aquel entonces un Grupo corporativo de compra y venta de oro, con el fin de llevarlo al correspondiente desarrollo formal, en vista de que dicho grupo inició como un mediano emprendimiento y fue creciendo paulatinamente, por ende, surgió la necesidad de que todas sus operaciones vayan tomando un rumbo más estructurado.

Con el pasar del tiempo, el alcance de esta empresa de servicios de auditoria también tomó un rumbo de franco desarrollo y los profesionales que la componen, sumaron a su experiencia, conocimientos actualizados por medio de formación en cuanto a tendencias actuales en sus profesiones, aplicándolas al Grupo corporativo de compra y venta de oro, y extendiendo sus alcances a otras empresas que requieran sus servicios profesionales en los ámbitos legal, financiero, de Tecnologías de la información, de Recursos Humanos, de Auditoría, entre otros.

Al ser una empresa que ofrece una variedad extensa de servicios financieros, posee una gran cantidad de información sensible y confidencial tanto de sus colaboradores como de sus clientes corporativos; dentro de esta información se puede encontrar los datos personales (ficha de cliente) que permite a los clientes establecer relaciones con el grupo organizacional, información referida a transacciones que producen las joyerías al cliente final y captaciones la cual debe ser mantenida en secreto, entre otras.

Un mal uso de los activos de información y una pérdida en las características de seguridad de la información puede materializar consecuencias tales como:

FIGURA 3.22: POLÍTICA DE SI (PARTE 3)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 4 de 8

- Pérdida de los activos de información (datos, equipos, documentación, secretos).
- Pérdida de imagen como como Grupo comercial.
- Interrupción total o parcial de los procesos claves para el funcionamiento del negocio.
- Consecuencias legales derivadas del no cumplimiento de la ley de información sensible.

Por esto, la Alta Dirección de la empresa de servicios Auditora ha decidido implementar un Plan director de Seguridad que permita reflejar los riesgos para que por medio de proyectos que son resultados del PDS, proteger los activos críticos de información. Como parte de este PDS se debe establecer una Política de Seguridad de la Información con lineamientos para regular el manejo y protección de la información en la organización.

II. OBJETIVO GENERAL

Establecer los lineamientos institucionales de la empresa de servicios de auditoría referentes a la responsabilidad, resguardo y gestión de riesgos de la información, así como definir la implementación de un marco de referencia del Sistema de Gestión de Seguridad de la Información (SGSI).
El SGSI busca proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información de la organización, considerando elementos de procesamiento, soporte, almacenamiento, transporte y transmisión, en formatos físicos, electrónicos, virtuales u otros.

III. OBJETIVOS ESPECÍFICOS

(i) Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que cumpla con los requisitos de la norma ISO 27001.
(ii) Identificar, evaluar y mitigar los riesgos de seguridad de la información a los que está expuesta la información de la empresa.
(iii) Establecer y mantener las medidas de seguridad necesarias para proteger la información confidencial de la empresa
(iv) Sensibilizar y concientizar al personal de la empresa sobre la importancia de la seguridad de la información y la responsabilidad de su tratamiento.
(v) Resguardar la confidencialidad, integridad y disponibilidad de la información organizacional, de los clientes y personal.
(vi) Mantener la integridad de los activos de información.
(vii) Garantizar la disponibilidad continua de los servicios.
(viii) Cumplir con las normas ISO 27001, ISO 27002 e ISO 27003.

FIGURA 3.23: POLÍTICA DE SI (PARTE 4)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 5 de 8

IV. ALCANCE

(i) Personas

La Política General de Seguridad de Información se aplica a todo el personal de la empresa de servicios de auditoría, en cualquier modalidad de contratación, clientes y a todos los proveedores tecnológicos, al igual que todos aquellos que tengan relación con el procesamiento, almacenamiento y/o tratamiento de la información y sus activos de información relacionados en cualquiera de las formas.

(ii) Activos

La Política General de Seguridad de la Información se aplica a todos los activos de información, independiente de su forma (digital, físico, escrito, transmitido de forma oral, o cualquier otro medio de almacenaje y distribución) que contengan información confidencial de los clientes y/o de la empresa.

(iii) Estructuras Organizacionales

La Política General de la Seguridad de la Información se aplica a todas las unidades organizacionales de la empresa (incluyendo departamentos, unidades, subdivisiones, etc.).

FIGURA 3.24: POLÍTICA DE SI (PARTE 5)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 6 de 8

V. POLÍTICA DE SEGURIDAD

- La Política de Seguridad de la Información de la empresa auditora ha sido elaborada en concordancia con la legislación vigente y en base a los requisitos y/o directrices de las normas ISO 27001, ISO 27002 e ISO27003.
- La seguridad de la información es una responsabilidad de todos los empleados de la empresa de auditoría. Todos los empleados tienen la responsabilidad de proteger la información confidencial de la empresa, utilizando los medios y procedimientos establecidos en esta política.
- La Alta Dirección deberá liderar, dirigir y colaborar en la implementación del SGSI y la adopción de la Política de Seguridad. Además, se compromete a realizar las acciones necesarias para garantizar la seguridad de la información, la continuidad de los servicios y los procesos del negocio.
- Los dueños de los activos como los dueños de los riesgos serán responsables de identificar, controlar, prevenir y mitigar todos los riesgos de seguridad de la información que puedan materializarse dentro de sus activos y/o procesos.
- Los proveedores tendrán la responsabilidad de garantizar el cumplimiento de esta política y de los procesos y procedimientos necesarios para preservar la confidencialidad, integridad y disponibilidad de la información de acuerdo con los requerimientos que la empresa posea.
- Auditoría interna deberá entregar soporte a todas las áreas para asegurar el cumplimiento de las políticas, procesos y procedimientos internos definidos.
- Las partes interesadas externas son las responsables de declarar las necesidades de protección de información (leyes, normas, decretos, oficios), así como también de fiscalizar el cumplimiento de las normativas o legislaciones aplicables a la entidad.
- La empresa auditora implementará las medidas de seguridad necesarias para proteger la confidencialidad, integridad y disponibilidad de la información privada, incluyendo:
    - Controles de acceso: Controles para restringir el acceso a la información a las personas autorizadas.
    - Controles de seguridad física: Controles para proteger la información de daños físicos o pérdida.

FIGURA 3.25: POLÍTICA DE SI (PARTE 6)

Fuente: Douglas Marín y César Medina

- Controles de seguridad lógica: Controles para proteger la información de accesos no autorizados o alteraciones.

- Se resguardará la confidencialidad de la información personal de clientes, así como información protegida por secreto de la empresa, mediante controles y procesos adecuados.
- El incumplimiento de esta Política tendrá como consecuencia la aplicación de sanciones, de acuerdo con el Reglamento Interno de la organización.

- La Subgerencia de TI será responsable de la aplicación de esta política y de mantener el Sistema de Gestión de Seguridad de la Información.

- Se realizarán auditorías y evaluaciones periódicas para garantizar el cumplimiento de esta Política.

VI. ROLES Y RESPONSABILIDADES

Con el propósito de la aplicación de la Política de Seguridad de la Información, se describen a continuación los roles y responsabilidades de los participantes para el funcionamiento del SGSI.

Rol	Responsabilidad
Dirección	Descripción: El nivel ejecutivo más alto de la organización y el grupo responsable de establecer la dirección estratégica y los objetivos generales de la empresa. Responsabilidades: a) Colaborar en la implementación del SGSI y la adopción de la Política de Seguridad.
Comité de Ciberseguridad	Descripción: Grupo de especialistas y líderes dentro de la organización encargado de supervisar y guiar las iniciativas relacionadas con la ciberseguridad. Responsabilidades: a) Desplegar las funciones de supervisión y asesoramiento en temas de ciberseguridad. b) Es responsable de la supervisión y el control del SGSI. c) Se reúne periódicamente para revisar el desempeño del SGSI y tomar decisiones sobre las medidas de seguridad.
Gerente General	Descripción: El Gerente General es el responsable ejecutivo de la organización y es responsable de la seguridad de la información en última instancia. Es el líder principal de la organización, responsable de la gestión global y la toma de decisiones estratégicas.

FIGURA 3.26: POLÍTICA DE SI (PARTE 7)

Fuente: Douglas Marín y César Medina

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 8 de 8

	Responsabilidades: a) Es responsable de la seguridad de la información en la organización. b) Aprueba la Política de Seguridad de la Información y los objetivos de seguridad. c) Proporciona los recursos necesarios para la implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
Subgerente de Cumplimento y auditoría interna	Descripción: Encargada de planificar, coordinar y supervisar las actividades de auditoría interna para garantizar el cumplimiento de políticas y normativas. Responsabilidades: a) Asegurar el cumplimiento de políticas, procesos y procedimientos internos. b) Realizar auditorías internas periódicas del SGSI. c) Garantizar que el SGSI sea efectivo y que se cumplan los objetivos de seguridad. d) Reporta los resultados de las auditorías a la alta dirección. e) Propone recomendaciones para mejorar el SGSI.
Especialista de Seguridad de la Información	Descripción: Encargado de garantizar el desarrollo, implementación y cumplimiento de las políticas y prácticas de seguridad de la información en la organización. Responsabilidades: a) Liderar y coordinar los esfuerzos de seguridad de la información en toda la organización. b) Dirige la implementación de las medidas de seguridad. c) Desarrollar e implementar políticas, procedimientos e instrucciones de seguridad, y brindar orientación y apoyo a la primera línea de defensa. d) Brinda orientación y apoyo a la primera línea de defensa. e) Analiza las amenazas cibernéticas. f) Responder y gestionar los incidentes de seguridad de la información.
Subgerente de TI	Descripción: Responsable de la gestión de los sistemas y servicios de TI de la organización. La Dirección de TI debe trabajar con la Dirección de Seguridad de la Información para garantizar que los sistemas y servicios de TI sean seguros. Responsabilidades: a) Gestiona los aspectos tecnológicos y de sistemas de información. b) Garantizar la disponibilidad y continuidad de las operaciones de la organización.

FIGURA 3.27: POLÍTICA DE SI (PARTE 8)

Fuente: Douglas Marín y César Medina

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 9 de 8

Oficial de Cumplimiento	Descripción: Responsable técnico de garantizar que la organización cumpla con las leyes y regulaciones aplicables a la seguridad de la información. El Oficial de Cumplimiento debe trabajar con la Dirección de Seguridad de la Información para garantizar que la organización cumpla con sus obligaciones legales y reglamentarias. Responsabilidades: a) Garantizar que la organización cumpla con sus obligaciones legales y reglamentarias.
Especialista TIC's	Descripción: Responsable de la detección, prevención, respuesta y recuperación ante ciberataques. La Gerencia de Ciberataque debe trabajar con la Dirección de Seguridad de la Información para desarrollar e implementar un plan de respuesta a incidentes de ciberseguridad. Responsabilidades: a) Gestionar la prevención, detección y respuesta a los ciberataques b) Cumplir el procedimiento de gestión de incidentes de seguridad de la información c) Proteger la infraestructura digital de la organización contra amenazas y ataques cibernéticos. d) Cumplir el procedimiento de gestión de incidentes de seguridad de la información e) Supervisa las estrategias y medidas de seguridad cibernética para proteger la información y los activos digitales. f) Apoyar y participar en la ejecución del plan de seguridad de la información de la organización.
Subgerente de Operaciones	Descripción: Responsable de garantizar que la organización pueda continuar operando en caso de un incidente de seguridad. La Gerencia de Continuidad del Negocio debe trabajar con la Dirección de Seguridad de la Información para desarrollar e implementar un plan de continuidad del negocio. Responsabilidades: a) Garantizar la continuidad de las operaciones. b) Desarrollar y mantener planes para garantizar la continuidad de las operaciones en situaciones de crisis o desastres.
Subgerente de Gestión Humana	Descripción: Responsable de la gestión del personal de la organización. La Gerencia de Recursos Humanos debe trabajar con la Dirección de Seguridad de la Información para garantizar que los empleados de la organización sean conscientes de la seguridad. Responsabilidades: c) Gestiona las funciones relacionadas con el personal, como contratación, capacitación, desarrollo y cumplimiento normativo. d) Apoya en el plan de concientización de seguridad de la información

FIGURA 3.28: POLÍTICA DE SI (PARTE 9)

Fuente: Douglas Marín y César Medina

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	COD POL-001 VER 1.0 PAG 10 de 8

Proveedores	Descripción: Empresas o personas que prestan servicios a una organización. Los proveedores pueden ser responsables del almacenamiento, el procesamiento o la transmisión de información confidencial de la organización. Por lo tanto, es importante que los proveedores tengan un buen programa de seguridad de la información. Responsabilidades: a) Garantizar el cumplimiento de esta política y de los procesos y procedimientos necesarios para preservar la confidencialidad, integridad y disponibilidad de la información de acuerdo con los requerimientos que el Banco posea b) Cumplir con los requisitos de seguridad de la información de la organización. c) Implementar medidas de seguridad adecuadas para proteger la información de la organización. d) Notificar a la organización de cualquier incidente de seguridad que pueda afectar a su información.
Partes Externas Interesadas	Descripción: Son personas u organizaciones que no son parte de la organización, pero que pueden verse afectadas por la seguridad de la información de la organización. Responsabilidades: a) Declarar las necesidades de protección de información (leyes, normas, decretos, oficios) b) Fiscalizar el cumplimiento de las normativas o legislaciones aplicables a la entidad.

VII. REFERENCIAS NORMATIVAS

- ISO 27001: Sistema de Gestión de la Seguridad de Información.
- ISO 27002: Prácticas para la gestión de la seguridad de la información.
- ISO 27003: Guía para la implementación de un Sistema de Gestión de Seguridad de la Información.
- ISO 27004: Medición de la Seguridad de la Información
- RAN 20-10: Recopilación Actualizada de Normas (RAN)
- Ley de Bancos de Alemania
- Ley de Seguridad de TI
- Ley General de Bancos

FIGURA 3.29: POLÍTICA DE SI (PARTE 10)

Fuente: Douglas Marín y César Medina

3.2.3 Identificación de activos

La identificación de activos en la empresa auditora es un proceso en el cual se tuvo que involucrar a personal de soporte TI para lograr obtener la información total proveniente de todos los departamentos de la empresa auditora. Estos activos pueden abarcar desde la información y datos sensibles hasta los dispositivos y sistemas que los almacenan y procesan. En la Figura 3.30, mostramos el tipo de activo identificado en la empresa con su respectivo código asociado:

Tipo de Activo	Codigo
Servicios	[S]
Datos	[D]
Aplicaciones	[SW]
Hardware	[HW]
Redes	[COM]
Soporte	[MEDIA]
Auxiliar	[AUX]
Instalaciones	[L]
Personal	[P]

FIGURA 3.30: IDENTIFICACIÓN DE ACTIVOS EN LA EMPRESA AUDITORA

Fuente: Douglas Marín y César Medina

[S] Servicios: Los servicios se diseñan con el propósito de atender las necesidades de los usuarios. Esta categoría abarca los servicios proporcionados por el sistema e incluye elementos como el sitio web, correo electrónico, servicio de FTP, intranet documental y sistemas de gestión de incidencias.

[D] Datos/Información: Los datos desempeñan un papel fundamental en el funcionamiento de una organización al permitir la prestación de sus servicios. La información, ya sea en forma de archivos o bases de datos, representa un activo abstracto que se guarda en dispositivos y medios de almacenamiento o se transfiere entre ubicaciones mediante métodos de transmisión de datos.

[SW] Aplicaciones: Aplicaciones informáticas, también conocidas como programas o aplicaciones, se refieren a procesos automatizados destinados a ejecutarse en un equipo informático. Estas aplicaciones tienen la función de gestionar, analizar y transformar datos, posibilitando así la explotación de la información para ofrecer servicios.

[HW] Hardware: Engloba todos los recursos materiales y físicos diseñados para respaldar, de manera directa o indirecta, los servicios proporcionados por la organización. Estos recursos son utilizados para almacenar datos, ejecutar aplicaciones informáticas y llevar a cabo el procesamiento o transmisión de información. Este conjunto de elementos incluye servidores físicos, computadoras (de escritorio y portátiles), teléfonos (tanto móviles como de escritorio), impresoras, escáneres, dispositivos electrónicos, switches y routers.

[COM] Redes: Esta categoría abarca tanto las instalaciones exclusivas como los servicios de comunicación externalizados a terceros. Dentro de este conjunto se encuentran las infraestructuras de red, el servicio ADSL, las redes inalámbricas y las redes locales.

[MEDIA] Soportes: En este apartado se contemplan dispositivos tangibles que posibilitan la retención de información de manera duradera, o al menos, por largos

lapsos. Este conjunto de activos incluye discos duros externos, memorias USB (pendrives) y CD/DVD.

[AUX] Auxiliar: En esta categoría se incluyen otros dispositivos que proporcionan respaldo a los sistemas de información, sin tener una conexión directa con los datos. Los activos comprendidos en este grupo abarcan generadores eléctricos, fuentes de alimentación, sistemas de climatización, mobiliario esencial y la infraestructura de cableado para las redes de comunicación.

[L] Instalaciones: En este segmento se localizan los sistemas de información y comunicación, incluyendo edificaciones de sedes, salas con los equipos informáticos principales y vehículos destinados exclusivamente al transporte del personal del departamento de Tecnologías de la Información y Comunicación.

[P] Personal: Esta sección hace referencia a las personas vinculadas con los sistemas de información, como operadores y administradores. Asimismo, se han considerado otros dos tipos de personal, empleados y usuarios generales, para evaluar sus respectivos riesgos.

3.2.3.1 Clasificación del tipo de activo

En la empresa auditora, los autores han decidido clasificar los activos según su tipo, por lo que se ha decidido utilizar los siguientes:

- **Servicios:** En esta categoría agrupamos los activos que correspondan a servicios propios o contratados a terceros.

Tipo Activo	Clasificación del Tipo de Activo
Servicios	[anon] anónimo (sin requerir identificación del usuario)
Servicios	[pub] al público en general (sin relación contractual)
Servicios	[ext] a usuarios externos (bajo una relación contractual)
Servicios	[int] interno (usuarios y medios de la propia organización)
Servicios	[cont] contratado a terceros (se presta con medios ajenos)
Servicios	[www] world wide web
Servicios	[telnet] acceso remoto a cuenta local
Servicios	[email] correo electrónico
Servicios	[file] almacenamiento de ficheros
Servicios	[ftp] transferencia de ficheros
Servicios	[edi] intercambio electrónico de datos
Servicios	[dir] servicio de directorio
Servicios	[idm] gestión de identidades
Servicios	[ipm] gestión de privilegios
Servicios	[pki] PKI - infraestructura de clave pública

FIGURA 3.31: CLASIFICACIÓN DE ACTIVOS POR TIPO SERVICIO

Fuente: Douglas Marín y César Medina

- **Datos:** Se agrupan los activos que corresponden a la información comercial y privada de la empresa.

Datos	[vr] datos vitales (vital records)
Datos	[com] datos de interés comercial
Datos	[adm] datos de interés para la administración pública
Datos	[int] datos de gestión interna
Datos	[voice] voz
Datos	[multimedia] multimedia
Datos	[source] código fuente
Datos	[exe] código ejecutable
Datos	[conf] datos de configuración
Datos	[log] registro de actividad (log)
Datos	[test] datos de prueba

FIGURA 3.32: CLASIFICACIÓN DE ACTIVOS POR TIPO DATOS

Fuente: Douglas Marín y César Medina

- **Aplicaciones:** Los activos relacionados con las aplicaciones desarrolladas o contratadas a terceros están dentro de esta categoría.

Aplicaciones	[prp] desarrollo propio (in house)
Aplicaciones	[sub] desarrollo a medida (subcontratado)
Aplicaciones	[std] estándar (off the shelf)
Aplicaciones	[browser] navegador web
Aplicaciones	[www] servidor de presentación
Aplicaciones	[app] servidor de aplicaciones
Aplicaciones	[email_client] cliente de correo electrónico
Aplicaciones	[file] servidor de ficheros
Aplicaciones	[dbms] sistema de gestión de bases de datos
Aplicaciones	[tm] monitor transaccional
Aplicaciones	[office] ofimática
Aplicaciones	[av] anti virus
Aplicaciones	[os] sistema operativo
Aplicaciones	[ts] servidor de terminales
Aplicaciones	[backup] sistema de backup

FIGURA 3.33: CLASIFICACIÓN DE ACTIVOS POR TIPO APLICACIONES

Fuente: Douglas Marín y César Medina

- **Hardware:** Todo el equipamiento que abarca desde puestos de trabajo hasta firewalls está incluidos en este grupo.

Hardware	[host] grandes equipos
Hardware	[mid] equipos medios
Hardware	[pc] informática personal
Hardware	[mobile] informática móvil
Hardware	[pda] agendas electrónicas
Hardware	[easy] fácilmente reemplazable
Hardware	[data] que almacena datos
Hardware	[peripheral] periféricos
Hardware	[print] medios de impresión
Hardware	[scan] escáneres
Hardware	[crypto] dispositivos criptográficos
Hardware	[network] soporte de la red
Hardware	[modem] módems
Hardware	[hub] concentradores
Hardware	[switch] conmutadores
Hardware	[router] encaminadores
Hardware	[bridge] pasarelas
Hardware	[firewall] cortafuegos
Hardware	[wap] punto de acceso wireless
Hardware	[pabx] centralita telefónica

FIGURA 3.34: CLASIFICACIÓN DE ACTIVOS POR TIPO HARDWARE

Fuente: Douglas Marín y César Medina

- **Redes de comunicación:** A esta categoría corresponden los componentes de networking que conforman la infraestructura de la empresa.

Redes de comunicación	[PSTN] red telefónica
Redes de comunicación	[ISDN] rdsi (red digital)
Redes de comunicación	[X25] X25 (red de datos)
Redes de comunicación	[ADSL] ADSL
Redes de comunicación	[pp] punto a punto
Redes de comunicación	[radio] red inalámbrica
Redes de comunicación	[sat] por satélite
Redes de comunicación	[LAN] red local
Redes de comunicación	[MAN] red metropolitana
Redes de comunicación	[Internet] Internet

FIGURA 3.35: CLASIFICACIÓN DE ACTIVOS POR TIPO REDES DE COMUNICACIÓN

Fuente: Douglas Marín y César Medina

- **Soporte de información:** Toda unidad, sea física o virtual, donde se pueda almacenar información entran en esta categoría.

Soporte de Información	[electronic] electrónicos
Soporte de Información	[disk] discos
Soporte de Información	[san] almacenamiento en red
Soporte de Información	[disquette] disquetes
Soporte de Información	[cd] cederrón (CD-ROM)
Soporte de Información	[usb] dispositivos USB
Soporte de Información	[dvd] DVD
Soporte de Información	[tape] cinta magnética
Soporte de Información	[mc] tarjetas de memoria
Soporte de Información	[ic] tarjetas inteligentes
Soporte de Información	[non_electronic] no electrónicos
Soporte de Información	[printed] material impreso
Soporte de Información	[tape] cinta de papel
Soporte de Información	[film] microfilm
Soporte de Información	[cards] tarjetas perforadas

FIGURA 3.36: CLASIFICACIÓN DE ACTIVOS POR TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

- **Equipamiento auxiliar:** La infraestructura eléctrica, mecánica, inmobiliaria están dentro de esta categoría.

Equipamiento Auxiliar	[power] fuentes de alimentación
Equipamiento Auxiliar	[ups] sistemas de alimentación ininterrumpida
Equipamiento Auxiliar	[gen] generadores eléctricos
Equipamiento Auxiliar	[ac] equipos de climatización
Equipamiento Auxiliar	[cabling] cableado
Equipamiento Auxiliar	[robot] robots
Equipamiento Auxiliar	[tape] ... de cintas
Equipamiento Auxiliar	[disk] ... de discos
Equipamiento Auxiliar	[supply] suministros esenciales
Equipamiento Auxiliar	[destroy] equipos de destrucción de soportes de información
Equipamiento Auxiliar	[furniture] mobiliario: armarios, etc
Equipamiento Auxiliar	[safe] cajas fuertes

FIGURA 3.37: CLASIFICACIÓN DE ACTIVOS POR TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

- **Instalaciones:** En esta categoría entran los bienes de la empresa utilizados para brindar servicios.

Instalaciones	[site] emplazamiento
Instalaciones	[building] edificio
Instalaciones	[local] local
Instalaciones	[mobile] plataformas móviles
Instalaciones	[car] vehículo terrestre: coche, camión, etc.
Instalaciones	[plane] vehículo aéreo: avión, etc.
Instalaciones	[ship] vehículo marítimo: buque, lancha, etc.
Instalaciones	[shelter] contenedores
Instalaciones	[channel] canalización

FIGURA 3.38: CLASIFICACIÓN DE ACTIVOS POR TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

- **Personal:** Corresponde a cada individuo que forma parte del ciclo transaccional de la empresa.

Personal	[ue] usuarios externos
Personal	[ui] usuarios internos
Personal	[op] operadores
Personal	[adm] administradores de sistemas
Personal	[com] administradores de comunicaciones
Personal	[dba] administradores de BBDD
Personal	[des] desarrolladores
Personal	[sub] subcontratas
Personal	[prov] proveedores

FIGURA 3.39: CLASIFICACIÓN DE ACTIVOS POR TIPO PERSONAL

Fuente: Douglas Marín y César Medina

3.2.3.2 Levantamiento de los activos dentro del alcance

Se realizo el levantamiento de activos que están dentro del alcance del PDS y se recolecto 66 activos agrupado de la siguiente manera, los cuales serán analizados juntos a la directiva para determinar cuáles son críticos:

• [S] Servicios: 6 activos

· [D] Datos: 7 activos

· [SW] Aplicaciones: 12 activos

· [HW] Hardware: 17 activos

· [COM] Redes: 3 activos

· [MEDIA] Soportes: 4 activos

· [AUX] Auxiliar: 5 activos

· [L]Instalaciones: 3 activos

· [P] Personal: 9 activos

Como observamos en las siguientes ilustraciones, también se detalla cada grupo de activos dentro del alcance:

SERVICIOS			
CODIGO	NOMBRE	RESPONSABLE	DESCRIPCIÓN
S1	E-commerce	Administrador de E-commerce	Pagina web para ventas de joyeria
S2	Correo Electronico	Coordinador TI	Correo coorporativo
S3	ERP	Coordinador TI	Software Informativo para las areas administrativas
S4	Core	Coordinador TI	Software Informativo para las areas operativas
S5	Aula Virtual	Implementador de proyectos	Aula virtual para capacitaciones usuarios internos de la empresa y clientes
S6	Red interta	Coordinador TI	Servicio para el almacenamiento y compartición de datos para uso de usuarios internos

FIGURA 3.40: GRUPO DE ACTIVOS CLASIFICADOS COMO SERVICIOS

Fuente: Douglas Marín y César Medina

DATOS			
CODIGO	NOMBRE	RESPONSABLE	DESCRIPCIÓN
D1	Ficheros de configuración	Coordinador TI	Ficheros guardados para configuraciones de aplicaciones y servidores
D2	Codigo fuente de los Sistemas	Coordinador Proyectos	Codigo fuente de aplicaciones del ERP y Core de la empresa
D3	Datos almacenados en Equipos coporativos	Coordinador TI	Datos almacenados en equipos PC, Laptops, Tablet
D4	Datos almacenados en Servidores Locales	Coordinador TI	Datos almacenados en servidores como Logs de los sistemas
D5	Datos almacenados en NAS	Coordinador TI	Datos almacenados de información de toda empresa
D6	Copia de seguridad en Discos duros externos	Coordinador TI	Copia de alamacenamiento de los NAS locales
D7	Ficheros en la Nube	Subgerente TI	Imágenes de ecommers, scanners, archivos compartidos entre departamentos, entidades externas.

FIGURA 3.41: GRUPO DE ACTIVOS CLASIFICADOS COMO DATOS

Fuente: Douglas Marín y César Medina

APLICACIONES / SOFTWARE			
CODIGO	NOMBRE	RESPONSABLE	DESCRIPCIÓN
S1	Antiphishing & Antispam	Coordinador TI	Antiphishing & Antispam para correo electrónico corporativos
S2	Endpoint	Coordinador TI	Antivirus para Servidores y equipos laptops y PC
S3	Ofimáticas	Coordinador TI	Aplicación Ofimática para usuarios internos
S4	Gestión de Backup	Coordinador TI	Mueve copias de seguridad a los NAS

S5	Administrador de correo	Coordinador TI	Administración de correos corporativos
S6	S.O Windows 10	Coordinador TI	Sistema Operativo para Laptops y PC de usuarios internos y externos
S7	S.O Windows 11	Coordinador TI	Sistema Operativo para Laptops y PC de usuarios internos y externos
S8	S.O Windows Server	Coordinador TI	Sistema operativo para servidores internos
S9	S.O Linux Ubuntu	Coordinador TI	Sistema Operativo para Laptops y PC de usuarios internos y externos
S10	Proxmox	Coordinador TI	Contenedor virtual de los sistemas operativos
S11	Despliegue de servicios	Coordinador TI	Contenedor que distribuye los servicios en ambientes de producción o prueba.
S12	Gestión de Base de Datos	Coordinador de Proyectos	Interfaz que permite instanciar base de datos

FIGURA 3.42: GRUPO DE ACTIVOS CLASIFICADOS COMO APLICACIONES/SOFTWARE

Fuente: Douglas Marín y César Medina

HARDWARE			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
HW1	PC de escritorio	Coordinador TI	Dispositivo utilizado en los puestos de trabajo de los empleados
HW2	Laptops de empleados	Coordinador TI	Dispositivo móvil utilizado por los empleados dentro de la empresa para trabajo
HW3	Servidores	Coordinador TI	En este grupo están considerados los servidores principales de la empresa auditora
HW4	Switch	Coordinador TI	Dispositivo que permite la conexión a la red local de la empresa y distribuye a los endpoints
HW5	Router	Coordinador TI	Dispositivo encargado del enrutamiento de red para poder alcanzar los servicios necesarios a los empleados
HW6	Access Points	Coordinador TI	Dispositivo conectado a la red que permite la conexión inalámbrica de los endpoints
HW7	Impresoras	Coordinador TI	Dispositivos de impresión utilizado por los empleados. Están ubicados en varios departamentos de la empresa
HW8	Firewall	Coordinador TI	Dispositivo conectado a la red que se encarga de la seguridad informática, cuya función es impedir ataques cibernéticos
HW9	Tablet	Coordinador TI	Dispositivo inalámbrico utilizado por los empleados para cumplir sus funciones dentro de la empresa
HW11	Proyectores	Coordinador TI	Dispositivo utilizado principalmente en las reuniones con la Dirección
HW12	Cámaras	Proveedor	Dispositivo utilizado en las salas de reuniones, cuarto de servidores y puestos de trabajo para vigilancia

HW13	NAS	Coordinador TI	Almacenar información de la empresa
HW14	Modem	Proveedor	Provee el acceso a internet en todo el edificio
HW15	Monitores	Coordinador TI	Equipo entregado para visualizar información proveniente de los equipos PC, utilizados para clientes y usuarios internos
HW16	Teclados	Coordinador TI	Periférico de PC usado para clientes y usuarios internos
HW17	Mouse	Coordinador TI	Periférico de PC usado para clientes y usuarios internos

FIGURA 3.43: GRUPO DE ACTIVOS CLASIFICADOS COMO HARDWARE

Fuente: Douglas Marín y César Medina

REDES DE COMUNICACIÓN			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
COM1	Red LAN cableada	Coordinador TI	Red de comunicación enlazada a través de los switches interconectados en la empresa
COM2	Red WLAN Inalámbrica	Coordinador TI	Red de comunicación inalámbrica, la cual se brinda a través de los access points de la empresa
COM3	Red de telefonía móvil	Subgerente TI	Red telefónica móvil a través de la cual los empleados internos de la empresa se comunican entre si

FIGURA 3.44: GRUPO DE ACTIVOS CLASIFICADOS COMO REDES DE COMUNICACION

Fuente: Douglas Marín y César Medina

SOPORTE DE INFORMACIÓN			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
MEDIA1	Scanner	Coordinador TI	Dispositivos en el cual se escanea toda la papelería física
MEDIA2	Memorias USB	Coordinador TI	Dispositivo portátil utilizado para guardar y pasar información entre usuarios
MEDIA3	Material impreso	Usuarios Internos	Los documentos impresos relevantes para los empleados están dentro de esta categoría
MEDIA4	Discos duros externos	Coordinador TI	Discos duros utilizados para guardar información y realizar copias de seguridad

FIGURA 3.45: GRUPO DE ACTIVOS CLASIFICADOS COMO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

EQUIPAMIENTO AUXILIAR			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
AUX1	Generador Eléctrico	Coordinador TI	Fuentes de alimentación utilizados por los diferentes equipos informáticos de la empresa
AUX2	Cableado UTP	Coordinador TI	Sistema de cableado estructurado que permite la comunicación entre los puestos de trabajo y servidores

AUX3	UPS	Coordinador TI	Sistema de poder no interrumpido que permite la continuidad del flujo eléctrico para los diferentes equipos informáticos de la empresa
AUX4	Climatización	Coordinador TI	Constituye todo el sistema de enfriamiento distribuido en la empresa, el cual se concentra en uno o varios cuartos
AUX5	Armarios y gabinetes	Coordinador TI	Espacio destinado al almacenamiento de material importante para la empresa como servidores y switches

FIGURA 3.46: GRUPO DE ACTIVOS CLASIFICADOS COMO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

INSTALACIONES			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
L1	Cuarto de servidores	Coordinador TI	Espacio donde se encuentra los servidores y switch
L2	Cuarto de Mantenimiento	Especialista Hardware y Software	Espacio para mantenimiento de equipos PC y servidores
L3	Puesto de trabajo	Coordinador TI	Todo el espacio ocupado por los

			diferentes departamentos de la empresa que tengan puntos de red

FIGURA 3.47: GRUPO DE ACTIVOS CLASIFICADOS COMO INSTALACIONES

Fuente: Douglas Marín y César Medina

PERSONAL			
CODIGO	**NOMBRE**	**RESPONSABLE**	**DESCRIPCIÓN**
P1	Subgerente TI	No Aplica	Encargado del departamento de TI
P2	Administrador Ecommerce	No Aplica	Personal del departamento de Comercial encargado de la administración de la página de ecommerce
P3	Coordinador TI	No Aplica	Personal del departamento TI encargado del área de gestión Tics y Especialista de Hardware y Software
P4	Coordinador de Proyectos	No Aplica	Personal del departamento TI encargado del área de Proyectos e implementador de proyectos
P5	Especialista Hardware y Software	No Aplica	Equipo encargado de soporte a los usuarios internos y clientes, también encargado de los activos de hardware para el uso de los usuarios
P6	Implementador de Proyectos	No Aplica	Personal encargado de implementar los proyectos tecnológicos de la empresa para sus clientes

P7	Usuarios Internos	No Aplica	Usuarios internos pertenecientes a la empresa
P8	Usuarios externos	No Aplica	Usuarios internos de Empresas que son clientes de la organización
P9	Proveedor	No Aplica	Proveedores de servicios subcontratados

FIGURA 3.48: GRUPO DE ACTIVOS CLASIFICADOS COMO PERSONAL

Fuente: Douglas Marín y César Medina

3.2.4 Responsables de la gestión de los activos

Los activos están a cargo de ciertos usuarios que serán responsables de su confidencialidad, integridad y disponibilidad acorde a rol que tengan dentro de la empresa. En la ilustración 52 se detalla específicamente cada uno de ellos:

NOMBRE	DESCRIPCIÓN
Subgerente TI	Encargador del departamento de TI
Administrador Ecommers	Personal del departamento de Comercial encargado de la administraciones de la pagina de ecommers
Coordinador TI	Personal del departamenti TI encargado del area de gestión Tics y Especialista de Hardware y Sofware
Coordinador de Proyectos	Personal del departamenti TI encargado del area de Proyectos e implmentador de proyectos
Especialista Hardware y Software	Equipo encargado de soporte a los usuarios internos y clientes, tambien encargado de los activos de hardware para el uso de los usuarios
Implementador de Proyectos	Personal encargado de implementar los proyectos tecnologicos de la empresa para sus clientes
Usuarios Internos	Usuarios internos pertenecientes a la empresa
Clientes	Clientes de la empresa
Proveedor	Proveedores de servicios subcontratados

FIGURA 3.49: RESPONSABLES DE LA GESTIÓN DE ACTIVOS DENTRO DE LA EMPRESA

Fuente: Douglas Marín y César Medina

CAPITULO IV.

MATRIZ DE RIESGO

4.1 Valoración de activos

La valoración de activos es un proceso en el cual se determina el valor de los recursos de una organización, considerando tanto su aspecto financiero como su relevancia para los objetivos y el funcionamiento de la entidad. En materia de gestión de riesgos en seguridad de la información, esta evaluación es crucial para comprender qué activos son críticos para la organización y, por tanto, requieren una protección y atención específicas.

4.1.1 Definición de Confiabilidad, Integridad y Disponibilidad (CID)

Para la empresa auditora, el cuidado de sus activos es crucial para la operación, ya que esto garantiza a los clientes que las plataformas estarán disponibles, seguras e invulnerables.

En el ámbito de la confiabilidad, la misión de la empresa auditora es garantizar que la información esté protegida contra accesos no autorizados, asegurando que solo aquellos con permisos específicos pueden acceder a ella. En la Figura 4.1 observamos el concepto de confidencialidad dentro de la empresa auditora.

Confidencialidad	Descripción	Ejemplos/Consideraciones
ALTO	Información disponible sólo para procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.	- Planes Estrategicos - Datos comerciales (BD de clientes, ventas, productos, portafolio) - Datos Financieros (EEFF, ingresos, centros de costos) - PII (salud, privacidad, intimidad) - Datos Tecnologicos (sistemas, configuraciones, passwords)
MEDIO	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por los funcionarios de la entidad para realizar labores propias de los procesos en los que participa, pero no puede ser conocida por terceros sin autorización del propietario.	- Datos Operacionales - Datos Personales (nombre, rut, dirección...)
BAJO	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.	- Información pública contenida en sitios web - Publicidad - Politicas de carácter público - Información comercial pública (productos, modelos de ventas)

FIGURA 4.1: CONFIDENCIALIDAD DENTRO DE LA EMPRESA AUDITORA

Fuente: Douglas Marín y César Medina

La integridad de la información garantiza que los datos sean precisos y confiables. Si los clientes perciben que la información de la empresa es precisa y segura, aumenta la confianza en los servicios y productos de la empresa auditora. Muchas industrias tienen regulaciones estrictas sobre la precisión y la integridad de los datos, como las leyes de privacidad. Los procesos de la empresa auditora dependen de datos precisos, por lo que la integridad asegura que las transacciones, registros y

operaciones se realicen de manera eficiente y sin errores con consecuencias. En la Figura 4.2 observamos el concepto de integridad dentro de la empresa auditora.

Intergridad	Descripción	Ejemplos/Consideraciones
ALTO	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen/reputación de la entidad.	- Información estrategica - Información operacional - Información administrada de terceros - Acceso o configuraciones en infraestructura, sistemas y aplicativos - Cumplimiento de controles normativos
MEDIO	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a procesos internos y/o funcionarios de la entidad.	- Información interna vinculada a procesos operacionales y administrativos - La perdida de integridad genera efectos internos, sin daño en imagen ni cumplimiento normativo.
BAJO	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.	- Información interna no vinculada a procesos operacionales ni administrativos de fácil recuperación y/o restauración del proceso normal.

FIGURA 4.2: INTEGRIDAD DENTRO DE LA EMPRESA AUDITORA

Fuente: Douglas Marín y César Medina

La disponibilidad de la información es crucial para el funcionamiento efectivo de una empresa, ya que garantiza que los datos críticos estén accesibles en todo momento. Esto es esencial para mantener la continuidad de las operaciones, especialmente en situaciones de emergencia o interrupciones inesperadas. Los clientes esperan acceso rápido a la información y servicios. La disponibilidad de datos garantiza una experiencia fluida para los clientes, lo que contribuye a la satisfacción del cliente y

fortalece la reputación de la empresa. En la Figura 4.3 observamos el concepto de disponibilidad dentro de la empresa auditora.

Disponibilidad	Ejemplos/Consideraciones	Ejemplos/Consideraciones
ALTO	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos. La no disponibilidad no puede superar las 4 horas.	- Activos que soportan procesos criticos - Activos cuyo RTO es menor a 4 horas - Activos con requisitos de terceros
MEDIO	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad. La no disponibilidad no puede superar las 12 horas.	- Activos que soportan procesos criticos - Activos cuyo RTO es entre 4 a 12 horas - Activos con requisitos de terceros
BAJO	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. La no disponibilidad no puede superar las 24 horas.	- Activos que soportan procesos no criticos - Activos cuyo RTO es mayor a 24 horas

FIGURA 4.3: DISPONIBILIDAD DENTRO DE LA EMPRESA AUDITORA

Fuente: Douglas Marín y César Medina

4.1.2 Estimación de Confiabilidad, Integridad y Disponibilidad (CID)

La estimación de confidencialidad, integridad y disponibilidad de la información de la empresa auditora implica evaluar y asignar los niveles de importancia y riesgo a estos tres aspectos cruciales de la seguridad de la información. El análisis de esta estimación se basará en la combinación de los riesgos asociados a la confidencialidad, integridad y disponibilidad. La estimación de estos tres aspectos contribuirá a la implementación efectiva de controles y políticas de seguridad de la información dentro de la empresa auditora. Es fundamental realizar este análisis de manera periódica para adaptarse a los cambios del entorno empresarial y las amenazas emergentes. Este enfoque integral contribuye a una gestión efectiva de riesgos que puedan afectar la seguridad de la información de la empresa. En la Figura 4.4 definimos las combinaciones posibles de la estimación de riesgos.

Combinación	Confidencialidad	Intergridad	Disponibilidad	Analisis
ALTOALTOALTO	ALTO	ALTO	ALTO	ALTO
ALTOALTOMEDIO	ALTO	ALTO	MEDIO	ALTO
ALTOALTOBAJO	ALTO	ALTO	BAJO	ALTO
ALTOMEDIOALTO	ALTO	MEDIO	ALTO	ALTO
ALTOMEDIOMEDIO	ALTO	MEDIO	MEDIO	ALTO
ALTOMEDIOBAJO	ALTO	MEDIO	BAJO	ALTO
ALTOBAJOALTO	ALTO	BAJO	ALTO	ALTO
ALTOBAJOMEDIO	ALTO	BAJO	MEDIO	ALTO
ALTOBAJOBAJO	ALTO	BAJO	BAJO	ALTO
MEDIOALTOALTO	MEDIO	ALTO	ALTO	ALTO
MEDIOALTOMEDIO	MEDIO	ALTO	MEDIO	ALTO
MEDIOALTOBAJO	MEDIO	ALTO	BAJO	ALTO
MEDIOMEDIOALTO	MEDIO	MEDIO	ALTO	ALTO
MEDIOMEDIOMEDIO	MEDIO	MEDIO	MEDIO	MEDIO
MEDIOMEDIOBAJO	MEDIO	MEDIO	BAJO	MEDIO
MEDIOBAJOALTO	MEDIO	BAJO	ALTO	ALTO
MEDIOBAJOMEDIO	MEDIO	BAJO	MEDIO	MEDIO
MEDIOBAJOBAJO	MEDIO	BAJO	BAJO	BAJO
BAJOALTOALTO	BAJO	ALTO	ALTO	ALTO
BAJOALTOMEDIO	BAJO	ALTO	MEDIO	ALTO
BAJOALTOBAJO	BAJO	ALTO	BAJO	ALTO
BAJOMEDIOALTO	BAJO	MEDIO	ALTO	ALTO
BAJOMEDIOMEDIO	BAJO	MEDIO	MEDIO	MEDIO
BAJOMEDIOBAJO	BAJO	MEDIO	BAJO	BAJO
BAJOBAJOALTO	BAJO	BAJO	ALTO	ALTO
BAJOBAJOMEDIO	BAJO	BAJO	MEDIO	BAJO
BAJOBAJOBAJO	BAJO	BAJO	BAJO	BAJO

Criticidad
Bajo
Medio
Alto

FIGURA 4.4: COMBINACIONES POSIBLES DE LA ESTIMACIÓN DE RIESGOS ASOCIADOS A LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Fuente: Douglas Marín y César Medina

4.1.3 Valoración de los activos críticos

En la valoración de activos nos enfocaremos en los considerados críticos para la organización, según la información brindada por la Dirección y la estimación de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información de la empresa.

En las ilustraciones siguientes, se muestran los resultados:

IDENTIFICACIÓN DE ACTIVOS – VALORACIÓN DE CRITICIDAD DE ACTIVOS									
Cod.	ACTIVO DE INFORMACIÓN	TIPO	SUB TIPO	TOS PERSONAL	C	I	D	IVEL CRITICIDA	JUSTIFICACIÓN CRITICIDAD
S1	Pagina web de Ecommerce	Servicios	[pub] al público en general (sin relación contractual)	MEDIO	MEDIO	MEDIO	ALTO	ALTO	Posee información personal de los clientes
S2	Correo Electronico Coorporativo	Servicios	[email] correo electrónico	ALTO	ALTO	ALTO	ALTO	ALTO	Posee información de usuarios internos, externos y empresariales
S3	ERP administrativa	Servicios	[ext] a usuarios externos (bajo una relación contractual)	MEDIO	MEDIO	ALTO	MEDIO	ALTO	Posee información personal moderada de clientes en trasacciones
S4	Sistema Core de trasacciones	Servicios	[ext] a usuarios externos (bajo una relación contractual)	ALTO	ALTO	ALTO	ALTO	ALTO	Posee información personal alta de clientes y de sus trasacciones
S5	Pagina web del Aula Virtual	Servicios	[ext] a usuarios externos (bajo una relación contractual)	MEDIO	ALTO	BAJO	BAJO	ALTO	Posee información vital para la capacitacion del personal de la organización
S6	Red interta corporativa	Servicios	[int] interno (usuarios y medios de la propia organización)	ALTO	ALTO	ALTO	ALTO	ALTO	Posee información cooperativa de alta confidencialidad de la empresa

FIGURA 4.5: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO SERVICIOS

Fuente: Douglas Marín y César Medina

D1	Ficheros de configuración	Datos	[com] datos de interés comercial	No Aplica	ALTO	ALTO	ALTO	ALTO	información de configuración para aplicaciones y servidores
D2	Codigo fuente de los Sistemas	Datos	[com] datos de interés comercial	No Aplica	ALTO	ALTO	ALTO	ALTO	información de codigo fuente de aplicaciones del ERP y Core de la empresa
D3	Datos almacenados en Equipos coporativos	Datos	[com] datos de interés comercial	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	Datos almacenados en equipos como documentos personales, trasaciones.
D4	Datos almacenados en Servidores Locales	Datos	[com] datos de interés comercial	BAJO	ALTO	ALTO	ALTO	ALTO	Datos almacenados en servidores como Logs de los sistemas
D5	Datos almacenados en NAS	Datos	[com] datos de interés comercial	ALTO	ALTO	ALTO	ALTO	ALTO	Datos almacenados de información de toda empresa y de clientes.
D6	Copia de seguridad en Discos duros externos	Datos	[com] datos de interés comercial	ALTO	ALTO	ALTO	ALTO	ALTO	Copia de alamacenamiento de los NAS locales.
D7	Ficheros en la Nube	Datos	[com] datos de interés comercial	ALTO	ALTO	ALTO	ALTO	ALTO	Imágenes de ecommers, scanners, archivos compartidos entre

FIGURA 4.6: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

SW6	S.O Windows 10	Aplicaciones	[os] sistema operativo	No Aplica	BAJO	BAJO	ALTO	ALTO	No Aplica
SW7	S.O Windows 11	Aplicaciones	[os] sistema operativo	No Aplica	BAJO	BAJO	BAJO	BAJO	No Aplica
SW8	S.O Windows Server	Aplicaciones	[os] sistema operativo	No Aplica	BAJO	BAJO	BAJO	BAJO	No Aplica
SW9	S.O Linux Ubuntu	Aplicaciones	[os] sistema operativo	No Aplica	BAJO	BAJO	BAJO	BAJO	No Aplica
SW10	Proxmox	Aplicaciones	[os] sistema operativo	No Aplica	BAJO	BAJO	BAJO	BAJO	No Aplica
SW11	Despliegue de servicios	Aplicaciones	[app] servidor de aplicaciones	No Aplica	ALTO	ALTO	ALTO	ALTO	Los servicios interactuan con los clientes y usuarios intercambiando información
SW12	Gestión de Base de Datos	Aplicaciones	[dbms] sistema de gestión de bases de datos	ALTO	ALTO	ALTO	ALTO	ALTO	Las base de datos almacenan información sencible

FIGURA 4.7: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO SOFTWARE

Fuente: Douglas Marín y César Medina

HW1	PC de escritorio	Hardware	[pc] informática personal	ALTO	ALTO	ALTO	ALTO	ALTO	Posee información personal y corporativa
HW2	Laptops de empleados	Hardware	[mobile] informática móvil	ALTO	ALTO	ALTO	ALTO	ALTO	Posee información corporativa
HW3	Servidores	Hardware	[host] grandes equipos	MEDIO	MEDIO	ALTO	ALTO	ALTO	Los servidores almacenan información sensible para la operación
HW4	Switch	Hardware	[network] soporte de la red	BAJO	MEDIO	MEDIO	MEDIO	MEDIO	El switch permite la comunicación entre usuarios
HW5	Router	Hardware	[network] soporte de la red	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	El router conecta la red lan de PC´s con la de servidores
HW6	Access Points	Hardware	[network] soporte de la red	BAJO	BAJO	BAJO	MEDIO	BAJO	No Aplica
HW7	Impresoras	Hardware	[print] medios de impresión	MEDIO	MEDIO	BAJO	BAJO	BAJO	No Aplica
HW8	Firewall	Hardware	[network] soporte de la red	ALTO	ALTO	ALTO	ALTO	ALTO	Las políticas del firewall permiten la comunicación a las redes públicas
HW9	Tablets	Hardware	[mobile] informática móvil	ALTO	ALTO	ALTO	ALTO	ALTO	Cada tablet posee informacion importante de la empresa
HW13	NAS	Hardware	[host] grandes equipos	ALTO	ALTO	ALTO	ALTO	ALTO	El almacenamiento conectado a la red contiene información de los clientes y

FIGURA 4.8: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

COM1	Red LAN cableada	Redes	[LAN] red local	ALTO	ALTO	ALTO	ALTO	ALTO	Dentro de la red LAN se encuentran todas las PC´S
COM2	Red WLAN Inalámbrica	Redes	[radio] red inalámbrica	ALTO	ALTO	ALTO	ALTO	ALTO	En la red inalámbrica están las laptos, tables y celulares de la empresa

FIGURA 4.9: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO REDES DE COMUNICACIÓN

Fuente: Douglas Marín y César Medina

MEDIA1	Scaner	Soporte	[electronic] electrónicos	MEDIO	MEDIO	BAJO	BAJO	BAJO	No Aplica
MEDIA2	Memorias USB	Soporte	[usb] dispositivos USB	ALTO	ALTO	ALTO	ALTO	ALTO	Pueden contener material sensible de la empresa
MEDIA3	Material impreso	Soporte	[printed] material impreso	ALTO	ALTO	ALTO	BAJO	ALTO	El material impreso puede quedar olvidado en las impresoras o mal
MEDIA4	Discos duros externos	Soporte	[disk] discos	ALTO	ALTO	ALTO	ALTO	ALTO	Debido a su gran capacidad de almacenamiento, podrían contener

FIGURA 4.10: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

AUX1	Generador Electrico	Auxiliar	[gen] generadores eléctricos	No Aplica	BAJO	BAJO	BAJO	BAJO	No aplica
AUX2	Cableado UTP	Auxiliar	[cabling] cableado	No Aplica	BAJO	BAJO	BAJO	BAJO	No aplica
AUX3	UPS	Auxiliar	[power] fuentes de alimentación	No Aplica	BAJO	BAJO	BAJO	BAJO	No aplica
AUX4	Climatización	Auxiliar	[ac] equipos de climatización	No Aplica	BAJO	BAJO	BAJO	BAJO	No aplica
AUX5	Armarios y gabinetes	Auxiliar	[furniture] mobiliario: armarios, etc	MEDIO	ALTO	BAJO	MEDIO	ALTO	Almacenan papeleria que tienen información de la empresa y de usuarios

FIGURA 4.11: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

L1	Cuarto de servidores	Instalaciones	[building] edificio	No Aplica	ALTO	BAJO	ALTO	ALTO	Almacena los servidores y switche
L2	Cuarto de Mantenimiento	Instalaciones	[building] edificio	No Aplica	BAJO	BAJO	BAJO	BAJO	No aplica
L3	Puesto de trabajo	Instalaciones	[building] edificio	MEDIO	ALTO	BAJO	MEDIO	ALTO	Almacenan papeleria impresa

FIGURA 4.12: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

P7	Usuarios Internos	Personal	[ui] usuarios internos	No Aplica	ALTO	ALTO	MEDIO	ALTO	Tienen conocomiento e informaicón de la empresa
P8	Usuarios Externos	Personal	[ue] usuarios externos	No Aplica	ALTO	ALTO	MEDIO	ALTO	Tienen conocomiento del negocio de la organización
P9	Proveedor	Personal	[prov] proveedores	ALTO	ALTO	BAJO	ALTO	ALTO	Tienen conocomiento e informaicón de la empresa

FIGURA 4.13: VALORACIÓN DE CRITICIDAD DE ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

4.2 Análisis y Evaluación de los Riesgos

El análisis y evaluación de los riesgos para la empresa auditora es un proceso integral que implica identificar amenazas potenciales, evaluar su probabilidad y el impacto resultante de los activos críticos de una organización. Este proceso permite priorizar los riesgos en función de su importancia y establecer estrategias de mitigación efectivas. Este enfoque sistemático es esencial para garantizar la seguridad de la información y proteger la continuidad de esta. La evaluación ayuda a priorizar los riesgos, establecer estrategias de mitigación y desarrollar controles efectivos para proteger la información empresarial. Esto es un proceso continuo que se adapta a los cambios en el entorno de seguridad, garantizando una gestión proactiva de la seguridad de la información para la empresa auditora.

4.2.1 Estimación de la Probabilidad

De manera general, la estimación de probabilidad en el contexto de la gestión de riesgos implica evaluar la posibilidad de que ocurra un evento adverso o una amenaza especifica. Este proceso busca asignar un valor numérico o cualitativo que refleje la chance de que se materialice un riesgo. Para la organización, la estimación de probabilidad se basa en la consideración de factores como la frecuencia histórica de eventos similares, la presencia de controles preventivos, y el análisis de las condiciones y contextos actuales. En la Figura 4.14 observamos la estimación de la probabilidad basada en categorías.

Categoría	Valor	Amenaza	Vulnerabilidad
Muy Alto	5	- El adversario tiene un nivel de experiencia muy sofisticado, cuenta con buenos recursos y que capacidades que puede generar oportunidades para soportar múltiples ataques exitosos, continuos y coordinados. - El adversario busca obstaculizar gravemente o destruir la función principal del negocio, explotando los sistemas de información de la organización o infraestructura. - Los efectos del tercero, error, accidente o acto de la naturaleza son devastadores e involucran a prácticamente todos los usuarios, sistemas, infraestructura y /o servicios de la organización.	- La vulnerabilidad está expuesta y es explotable, y su explotación podría resultar en impactos severos. - Es casi certeza que un tercero, error, accidente o acto de la naturaleza pueda explotar esta vulnerabilidad diariamente.
Alto	4	- El adversario tiene un nivel sofisticado de experiencia, con capacidades y oportunidades para soportar múltiples ataques coordinados exitosos - El adversario busca impedir aspectos críticos de una función principal del negocio o colocarse en una posición para hacerlo en el futuro, manteniendo una presencia en los sistemas de información o la infraestructura de la organización. - Los efectos del tercero,error, accidente o acto de la naturaleza son extensos e involucran a la mayoría de los usuarios, sistemas, infraestructura y /o servicios de la organización.	- La vulnerabilidad es de gran preocupación, basada en la exposición de la vulnerabilidad y la facilidad de explotación y / o sobre la gravedad de los impactos que pudieran resultar de su explotación. - Es muy probable que un tercero, un error, accidente o acto de la naturaleza pueda explotar esta vulnerabilidad mensualmente.
Medio	3	- El adversario tiene recursos, experiencia y oportunidades moderados para respaldar múltiples ataques. - El adversario busca obtener o modificar información crítica o sensible específica o usurpar los recursos cibernéticos de la organización estableciendo un punto de apoyo en la información de la organización sistemas o infraestructura. - Los efectos del tercero,error, accidente o acto de la naturaleza son de amplio alcance e involucran una parte significativa de los usuarios, sistemas, infraestructura y /o servicios de la organización.	- La vulnerabilidad es una preocupación moderada, basada en la exposición de la vulnerabilidad y la facilidad de explotación y / o sobre la gravedad de los impactos que pudieran resultar de su explotación. - Es algo probable que un tercero,un error, accidente o acto de la naturaleza pueda explotar esta vulnerabilidad al menos una vez por año.
Bajo	2	- El adversario tiene recursos, experiencia y oportunidades limitados para respaldar un ataque exitoso. - El adversario busca activamente obtener información crítica o sensible, interrumpiendo el uso de recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección. - Los efectos del tercero,error, accidente o acto de la naturaleza son son limitados e involucran a algunos de los usuarios, sistemas, infraestructura y /o servicios de la organización.	- La vulnerabilidad es una preocupación menor, pero la efectividad de la remediación podría mejorarse. - Es improbable que un tercero,un error, accidente o acto de la naturaleza pueda explotar esta vulnerabilidad al menos una vez en los últimos 5 año.
Muy Bajo	1	- El adversario tiene recursos, experiencia y oportunidades muy limitados para respaldar un ataque. - El adversario busca usurpar, interrumpir o desfigurar los recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección de ataques. - Los efectos del tercero,error, accidente o acto de la naturaleza son son mínimos, y afectan a pocos o ninguno de los los usuarios, sistemas, infraestructura y /o servicios de la organización.	- La vulnerabilidad no es motivo de preocupación. -Es muy improbable que un tercero,un error, accidente o acto de la naturaleza pueda explotar esta vulnerabilidad o ocurre despues de cada 5 años o más

FIGURA 4.14: ESTIMACIÓN DE LA PROBABILIDAD

Fuente: Douglas Marín y César Medina

4.2.2 Cálculo de Probabilidad

Para la empresa auditora, es vital priorizar los activos críticos para darles una atención y cuidado personalizados, y para esto es importante conocer el cálculo de probabilidad. En el contexto de la gestión de riesgos, el cálculo de la probabilidad de un riesgo se realiza evaluando la posibilidad de que un evento adverso especifico ocurra. Es importante recordar que la estimación de probabilidad en la gestión de riesgos para la empresa auditora no siempre se basa en datos exactos y puede variar según la naturaleza del riesgo y la información disponible. En la Figura 4.15 nos enfocamos en el cálculo de probabilidad.

Combinación	Nivel de Amenaza	Nivel de Probabilidad	Valor	Severidad	Valor
55	5	5	25	Casi Certeza	5

Casi Certeza

54	5	4	20	Casi Certeza	5
53	5	3	15	Probable	4
52	5	2	10	Probable	4
51	5	1	5	Moderado	3
45	4	5	20	Casi Certeza	5
44	4	4	16	Casi Certeza	5
43	4	3	12	Probable	4
42	4	2	8	Moderado	3
41	4	1	4	Improbable	2
35	3	5	15	Casi Certeza	5
34	3	4	12	Casi Certeza	5
33	3	3	9	Probable	4
32	3	2	6	Moderado	3
31	3	1	3	Improbable	2
25	2	5	10	Casi Certeza	5
24	2	4	8	Probable	4
23	2	3	6	Moderado	3
22	2	2	4	Improbable	2
21	2	1	2	Muy Improbable	1
15	1	5	5	Probable	4
14	1	4	4	Probable	4
13	1	3	3	Moderado	3
12	1	2	2	Improbable	2
11	1	1	1	Muy Improbable	1

Probable
Moderado
Improbable
Muy Improbable

FIGURA 4.15: CÁLCULO DE PROBABILIDAD

Fuente: Douglas Marín y César Medina

4.2.3 Estimación del Impacto

La estimación del impacto en la gestión de riesgo en la empresa auditora que estamos analizando se refiere a la evaluación de las consecuencias potenciales que tendría la

materialización de un evento adverso o riesgo en la empresa. Esta evaluación ayuda a comprender la magnitud de los daños o perdidas que podrían ocurrir. Para esto es importante la identificación de las consecuencias, la asignación de valores a cada una de las consecuencias identificadas, la evaluación de la severidad y la integración con la probabilidad de ocurrencia del riesgo. La reputación de la empresa auditora podría verse comprometida si es que no se realiza una adecuada estimación del impacto.

En la Figura 4.16 se observa cómo se categoriza la estimación del impacto.

Categoría	Valor	General	Financiero	Operacional	Reputacional	Normativo
Catastrofico	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en la organización y/o comprometen totalmente la imagen de la organización.	Superior $50.000.000	- Suspensión de operaciones claves generalizada por más de 4 horas - Perdida de operación en más del 50% de los procesos claves - Perdida de continuidad operativa en procesos claves o de soporte, superando el RTO establecido	- Cobertura negativa generalizada en medios masivos y redes sociales (>+1 semana) - Comentarios negativos de Stakeholders claves - Comentarios negativos a nivel sectorial - Caida en las acciones (>10%) - Perdida de empleados (>10%) - Perdida de clientes (>10%)	- Riesgo de incumplimiento muy alto con reguladores y/o clientes con consecuencias muy graves en caso de incumplimiento (sanciones económicas, cese definitivo, pérdida de licencia, restricción financiera, juicios). - Resolución judicial con determinación de sanciones y multas. -Multas o costos superiores a $25.000.000
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en la organización y/o comprometen fuertemente la imagen de la organización.	Entre $25.000.000 y $49.999.999	- Suspensión de operaciones claves generalizada por más de 2 horas - Perdida de operación en más del 30% de los procesos claves - Perdida de continuidad operativa en procesos claves o de soporte, superando el RTO establecido	- Cobertura negativa generalizada en medios masivos y redes sociales (Entre 6 a 3 días) - Comentarios negativos de Stakeholders - Comentarios negativos a nivel empresarial - Caida en las acciones (Entre un 5% y 10%) - Perdida de empleados (Entre un 5% y 10%) - Perdida de clientes (Entre un 5% y un 10%)	- Riesgo de incumplimiento alto con reguladores y/o clientes con consecuencias graves en caso de incumplimiento (sanciones económicas, cese definitivo, pérdida de licencia, restricción financiera, juicio, sanciones administrativas). - Resolución judicial con determinación de sanciones y multas. -Multas o costos entre $10.000.000 y hasta $25.000.000
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en ela organización y/o comprometen moderadamente la imagen de la organización	Entre $5.000.000 y $24.999.999	- Suspensión de operaciones claves generalizada por más de 1 horas - Perdida de operación en más del 10% de los procesos claves - Perdida de continuidad operativa en procesos claves o de soporte, superando el RTO establecido	- Cobertura negativa generalizada en medios masivos y redes sociales (Entre 2 a 3 días) - Caida en las acciones (Entre un 2% y 4%) - Perdida de empleados (Entre un 2% y 4%) - Perdida de clientes (Entre un 2% y un 4%)	- Riesgo de incumplimiento con reguladores y/o clientes con consecuencias en oficios o reclamos formales - Procesos judiciales o prejudiciales con potencial de acuerdo -Multas o costo entre $2.000.000 y hasta $5.000.000
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en la organización y/o comprometen de forma menor la imagen de la organización	Entre $1.000.000 y $4.999.999	- Perdida de operación en menos del 10% de los procesos claves - Suspensión de operaciones de procesos de soporte por más de 1 horas - Perdida de continuidad operativa en procesos de soporte, superando el RTO establecido	- Cobertura aislada y menciones esporadicas en medios masivos y redes sociales (menor a 2 días) - Caida en las acciones (Menor al 2%) - Perdida de empleados (Menor al 2%) - Perdida de clientes (Menor al 2%)	- Riesgo de incumplimiento con reguladores y/o clientes con consecuencias en amonestaciones formales o reclamos informales - Acuerdos formales de reparación dentro de lo establecido en regulación o contractualmente -Multas o costos menor a $2.000.000
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen de la organización.	Menor a $1.000.000	- Suspensión de operaciones de procesos de soporte por menos de 1 horas - Perdida de continuidad operativa en procesos de soporte, superando el RTO establecido	- Cobertura negativa limitada en redes sociales (escasos comentarios), sin menciones en otros medios masivos.	- Riesgo de incumplimiento sin efectos en reguladores o clientes. - Sin multa o costo economico relacionado.

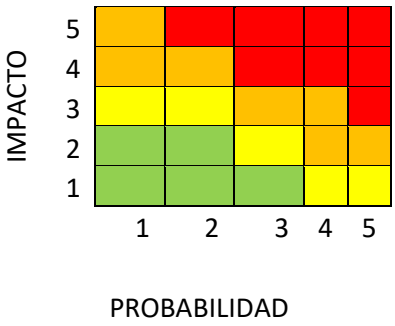
FIGURA 4.16: ESTIMACIÓN DEL IMPACTO

Fuente: Douglas Marín y César Medina

4.2.4 Apetito de Riesgo

El apetito de riesgo asociado a la empresa auditora se refiere al nivel de tolerancia que la organización está dispuesta a aceptar en cuánto a la exposición a riesgos. Es una declaración formal que establece los limites dentro de los cuales la empresa está dispuesta a operar en términos de riesgos. El apetito de riesgo se alinea con los

objetivos estratégicos empresariales y la cultura organizativa, y sirve como guía para la toma de decisiones en la gestión de riesgos. En base a lo expuesto, la organización establece los límites de riesgo aceptables y ayuda a equilibrar los riesgos y las oportunidades en busca de un rendimiento empresarial óptimo. En el caso de la empresa auditora, el apetito de riesgo está definido según la Figura 4.17.



Nivel de Probabilidad	Nivel de Impacto	Valor	Severidad
5	5	25	Extremo
5	4	20	Extremo
5	3	15	Extremo
5	2	10	Alto
5	1	5	Alto
4	5	20	Extremo
4	4	16	Extremo
4	3	12	Alto
4	2	8	Alto
4	1	4	Moderado
3	5	15	Extremo
3	4	12	Extremo
3	3	9	Alto
3	2	6	Moderado
3	1	3	Bajo
2	5	10	Extremo
2	4	8	Alto
2	3	6	Moderado
2	2	4	Bajo
2	1	2	Bajo
1	5	5	Alto
1	4	4	Alto
1	3	3	Moderado
1	2	2	Bajo
1	1	1	Bajo

FIGURA 4.17: APETITO DE RIESGO

Fuente: Douglas Marín y César Medina

4.2.5 Análisis de Riesgos de los activos críticos

En este punto la Dirección de la empresa, en conjunto con personal de Seguridad de la Información identifico los activos críticos fundamentales para los objetivos y operaciones de la empresa. Así mismo, se identificó las amenazas y vulnerabilidades que podrían afectar a estos activos críticos y las vulnerabilidades asociadas, considerando factores internos y externos. Este análisis de riesgo proporciona una base sólida para la toma de decisiones informada en la protección de activos críticos por parte de la Dirección de la empresa auditora, contribuyendo a la seguridad y la continuidad operativo de la empresa.

En las ilustraciones a continuación, se muestran los resultados:

	ANALISIS DE RIESGOS				
Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMEN
S1	Materialización de un ataque cibernético	Adversarios con recursos, experiencia y oportunidades moderados.	Ataque Cibernético	Alto	4
S2	Intento de phishing e Ingenieria Social	Atacantes con experiencia en Ingeneria Social y Ataque DOS	Phishing	Alto	4
S3	Materialización de un ataque cibernético	Adversarios con recursos, experiencia y oportunidades Altos.	Ataque Cibernético	Alto	4
S4	Indisponibilidad del Servicio	Recursos no aptos para la disponibilidad del sistema	Corte de energia, colapso de recursos de hardware	Muy Alto	5
S5	Materialización de un ataque cibernético	Adversarios con recursos, experiencia y oportunidades moderados.	Ataque Cibernético, implmentando phishing o ingeneria social.	Alto	4
S6	Ataque cibernetico	Usuario interno o externo mal intencionado	Extracion de informacion, filtración de malware.	Muy Alto	5

FIGURA 4.18: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO SERVICIO

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
D1	Modificaciones y eliminación de la información de las configuraciones	Usuario administrador	administradores modifican o eliminan configuraciones de	Medio	3
D2	Materialización de un ataque cibernetico	Adversarios con recursos, experiencia y oportunidades elevadas	SQL Injection,XSS (Cross Site Scripting),	Alto	4
D3	Exportación de información valiosa de la empresa y clientes	Usuarios interno.	Extracción de información	Alto	4
D4	Materialización de un ataque cibernetico	Adversarios con recursos, experiencia y oportunidades elevadas	Vulneración de puertos accesibles	Alto	4
D5	Daño en los discos duros de alamcenamiento	Final de vida util	Daños de los HDD	Bajo	2
D6	Daño en los discos duros de alamcenamiento	Final de vida util	Daños de los HDD	Bajo	2
D7	Robo de cuenta administrador	Ciberatacante	Phishing	Muy Bajo	1

FIGURA 4.19: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
SW6	Uso de Sistema operativo sin licencia genera vulnerabilidades de seguridad.	Instalaciónde programas que incluyan virus o algún tipo de malware	Captura de la información por ransowere o algun	Muy Alto	5
SW7	Uso de Sistema operativo sin licencia genera vulnerabilidades de seguridad.	Instalaciónde programas que incluyan virus o algún tipo de malware	Captura de la información por ransowere o algun	Muy Alto	5
SW8	Uso de Sistema operativo sin licencia genera vulnerabilidades de seguridad.	Ataque cibernetico por brechas de seguridad, puerto abiertos, falta de actualización	Ciberdelincuentes encuentran brechas de seguridad.	Muy Alto	5
SW9	No se realiza actualización de Sistema operativo automatico	Ataque cibernetico por brechas de seguridad, puerto abiertos, falta de actualización	Ciberdelincuentes encuentran brechas de seguridad.	Medio	3
SW10	No se realizan actualizaciones del S.O el cual Open source.	Ataque cibernetico por brechas de seguridad, puerto abiertos, falta de actualización	Ciberdelincuentes encuentran brechas de seguridad.	Muy Alto	5
SW11	Descarga de imaganes de docker alteradas	Descarga por el administrador imágenes no oficiales	Despliegue de imágenes con servicios irregulares	Bajo	2
SW12	Procedimeintos no documentados	Mal manejo de la gestión de las base de datos	Usuarios y contraseñas por defecto	Alto	4

FIGURA 4.20: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO SOFTWARE

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
AUX1	Fallas tecnicas	Daño por falta de mantenimiento	No realizar mantenimientos periodicos	Bajo	2
AUX2	Corte de cableado	Animales ruedores	Ratas o ratones podrian causar corte de cables UTP	Medio	3
AUX3	Daños por fallas tecnicas	FIlas tecnicas	Daño de bateria antes de su tiempo de vida util	Bajo	2
AUX4	Fallas tecnicas	Daño por falta de mantenimiento	Daño de aire que se encuentra en el datacenter	Medio	3
AUX5	Catastrofe Natural	Incendios	Perdida de información por fuego	Bajo	2

FIGURA 4.21: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
L1	Acceso al data center sin restriccion	Ciberatacante	Ingreso de personal no autorizado	Alto	4
L2	Acceso al data center sin restriccion	Ciberatacante	Robo de Disco duro	Alto	4
L3	Perdida o robo de información	Ciberatacante	Tecnica de ingeneria social para robo de información y	Alto	4

FIGURA 4.22: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
P7	Robo o destrucción de información	Usuarios Internos	Usuario con malas intenciones de perjudicar a la	Medio	3
P8	Robo o destrucción de información	Usuarios Externo	Usuario con malas intenciones de perjudicar a la	Medio	3
P9	Incumplimiento de contractuales	Proveedor	Incumplimeinto de sus deberes contractuales a la organización	Medio	3

FIGURA 4.23: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
HW1	Ataque cibernetico	Ciberatacante	Robo de información de la empresa	Alto	4
HW2	Ataque cibernetico	Ciberatacante	Robo de información de la empresa	Alto	4
HW3	Ataque de DDOS	Ciberatacante	Robo de información de la empresa	Alto	4
HW4	Bloqueo o pérdida de información de los puertos	Mala administración del dispositivo	Puertos mal configurados	Medio	3
HW5	Ataque cibernetico	Ciberatacante	Ataque de Fuerza Bruta para acceder al equipo	Alto	4
HW6	Acceso no autorizado	Usuario interno	Obtención de contraseña a red Wi-Fi	Bajo	2
HW7	Mal uso de dispositivo	Usuario interno	Imprimir documentos de otro usuario	Bajo	2
HW8	Cambio de políticas que puedan exponer al equipo a ataque cibernetico	Ciberatacante	Ciberdelincuentes encuentran brechas de seguridad.	Alto	4
HW9	Mal uso de dispositivo	usuario interno	Traspaso de información no autorizada	Medio	3
HW13	Perdida o robo de información	Ataque cibernetico dirigido al NAS	Perdida de información sensible debido a ataque cibernetico	Alto	4

FIGURA 4.24: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
COM1	Daño físico en el cableado	Falta de mantenimiento en la red cableada	Roedores en la ducteria de datos	Medio	3
COM2	Indisponibilidad del Servicio WLAN	Mala administración del dispositivo	Configuración de contraseña vulnerable	Medio	3

FIGURA 4.25: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO REDES DE COMUNICACIONES

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DEL RIESGO	FUENTE DE AMENAZA	EVENTO DE AMENAZA	NIVEL DE AMENAZA	VALOR AMENAZA
MEDIA1	Mal uso de dispositivo	usuario interno	Usuarios escaneando información sensible	Muy Bajo	1
MEDIA2	Transferencia de información no autorizada	Usuario interno o externo mal intencionado	La información de un usuario pasa a otro sin autorización	Alto	4
MEDIA3	Mal uso de información	Usuario interno	Fuga de información sensible	Medio	3
MEDIA4	Transferencia de información no autorizada	Usuario interno o externo mal intencionado	La información de un usuario para a otro sin autorización	Alto	4

FIGURA 4.26: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

	EVALUACIÓN DE RIESGOS												
Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABLIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
S1	Desarrollado con tecnología no actualizada.	Alto	4	Casi Certeza	5	4	3	5	1	5	Catastrofico	25	Extremo
S2	Personal con falta de concientización en seguridad de la información.	Alto	4	Casi Certeza	5	3	5	2	1	5	Catastrofico	25	Extremo
S3	Reconocimientos de Vulnerabilidades web.	Medio	3	Probable	4	2	4	2	1	4	Mayores	16	Extremo
S4	Los recursos de hardware no de adaptan a las exigencias del sistema.	Muy Alto	5	Casi Certeza	5	5	5	5	1	5	Catastrofico	25	Extremo
S5	Acceso al aula virtual por atacantes por medio del correo personal de la victma	Muy Alto	5	Casi Certeza	5	1	2	4	1	4	Mayores	20	Extremo
S6	Puertos USB no bloqueados en los equipos PC	Muy Alto	5	Casi Certeza	5	4	5	5	5	5	Catastrofico	25	Extremo

FIGURA 4.27: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO SERVICIO

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABIL IDAD	VALOR PROBABILI DAD	NIVEL DE PROBABILI DAD	CALCULO DE PROBABILI	IMPACT O FINACI	IMPACTO OPERACI ONAL	IMPACTO REPUTACI ONAL	IMPACTO NORMATI VO	CALCU LO IMPAC	NIVEL DE IMPACT	SEVERIDAD DEL RIESGO	DESCRIP CIÓN SEVERID
D1	No existen procedimientos documentados	Alto	4	Casi Certeza	5	3	5	3	1	5	Catastrofic	25	Extremo
D2	No se lleva acabo una metodologia de desarrollo seguro.	Alto	4	Casi Certeza	5	5	5	4	1	5	Catastrofic	25	Extremo
D3	No se cuenta con la proteccion o deteccion de la exportacion de la	Alto	4	Casi Certeza	5	3	3	5	5	5	Catastrofic	25	Extremo
D4	Los servidores cuentan con puertos no utilizados accesibles	Muy Alto	5	Casi Certeza	5	5	5	3	4	5	Catastrofic	25	Extremo
D5	Ninguna	Muy Bajo	1	Muy Improbable	1	1	1	1	1	1	significante	1	Bajo
D6	Ninguna	Muy Bajo	1	Muy Improbable	1	1	1	1	1	1	significante	1	Bajo
D7	Ninguna	Muy Bajo	1	Muy Improbable	1	1	1	1	1	1	significante	1	Bajo

FIGURA 4.28: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
SW6	Sistema Operativo no licenciado	Muy Alto	5	Casi Certeza	5	5	5	3	1	5	Catastrofico	25	Extremo
SW7	Sistema Operativo no licenciado	Muy Alto	5	Casi Certeza	5	5	5	3	1	5	Catastrofico	25	Extremo
SW8	Sistema Operativo no licenciado	Muy Alto	5	Casi Certeza	5	5	5	5	1	5	Catastrofico	25	Extremo
SW9	No existe actualización de S.O automatico	Medio	3	Probable	4	3	3	2	1	3	Moderadas	12	Alto
SW10	No existe actualización de S.O	Muy Alto	5	Casi Certeza	5	5	5	4	1	5	Catastrofico	25	Extremo
SW11	Desconocimeinto de administrador	Bajo	2	Improbable	2	2	2	2	1	2	Menores	4	Bajo
SW12	Procedimientos y politicas no definidas	Alto	4	Casi Certeza	5	4	4	5	5	5	Catastrofico	25	Extremo

FIGURA 4.29: ANÁLISIS DE RIESGO DE ACTIVOS DEL TIPO SOFTWARE

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
AUX1	No existe planificacion de mantenimiento periodico	Bajo	2	Improbable	2	5	4	1	1	5	Catastrofico	10	Extremo
AUX2	plan periodico de descontaminación en el edificio	Muy Bajo	1	Improbable	2	2	3	1	1	3	Moderadas	6	Moderado
AUX3	No existe planificacion de mantenimiento periodico	Bajo	2	Improbable	2	1	3	1	1	3	Moderadas	6	Moderado
AUX4	No existe planificacion de mantenimiento periodico	Medio	3	Probable	4	3	1	1	1	3	Moderadas	12	Alto
AUX5	sistema de protección contra incendio y permisos adecuados	Muy Bajo	1	Muy Improbable	1	5	5	1	1	5	Catastrofico	5	Alto

FIGURA 4.30: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
L1	No existe sistema bloqueo en ingreso al datacenter	Alto	4	Casi Certeza	5	4	5	4	1	5	Catastrofico	25	Extremo
L2	No existe sistema bloqueo en ingreso al cuarto de mantenimiento	Alto	4	Casi Certeza	5	1	1	1	4	4	Mayores	20	Extremo
L3	No existe políticas puesto de trabajo	Alto	4	Casi Certeza	5	3	4	4	1	4	Mayores	20	Extremo

FIGURA 4.31: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
P7	No existe un reglamento de acuerdo de confidencialidad y	Alto	4	Casi Certeza	5	2	2	5	5	5	Catastrofico	25	Extremo
P8	No existe un reglamento de acuerdo de confidencialidad y	Alto	4	Casi Certeza	5	2	2	5	5	5	Catastrofico	25	Extremo
P9	No existe política de seguridad de la información expuestas a	Alto	4	Casi Certeza	5	4	4	5	5	5	Catastrofico	25	Extremo

FIGURA 4.32: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
HW1	No existe un reglamento de acuerdo de confidencialidad y	Alto	4	Casi Certeza	5	3	4	4	1	4	Mayores	20	Extremo
HW2	No existe un reglamento de acuerdo de confidencialidad y	Alto	4	Casi Certeza	5	3	4	4	1	4	Mayores	20	Extremo
HW3	No existe un reglamento de acuerdo de confidencialidad y	Medio	3	Probable	4	4	4	4	1	4	Mayores	16	Extremo
HW4	Falta de experticia en configuración de equipos de networking	Medio	3	Probable	4	2	3	2	1	3	Moderadas	12	Alto
HW5	No existe un metodo robusto de autentiación en el equipo	Alto	4	Casi Certeza	5	3	3	3	1	3	Moderadas	15	Alto
HW6	No existe una política de control de acceso a redes inlamabricas	Bajo	2	Improbable	2	2	2	2	1	2	Menores	4	Bajo
HW7	No existe bloqueo de impresión por usuario	Bajo	2	Improbable	2	2	4	3	1	4	Mayores	8	Alto
HW8	No existe MFA para ingresar al Firewall	Alto	4	Casi Certeza	5	4	4	5	1	5	Catastrofico	25	Extremo
HW9	No existe un reglamento de acuerdo de confidencialidad y	Alto	4	Casi Certeza	5	2	3	3	1	3	Moderadas	15	Alto
HW13	No existe protección suficiente aplicada al NAS contra ataques	Muy Alto	5	Casi Certeza	5	4	4	5	1	5	Catastrofico	25	Extremo

FIGURA 4.33: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
COM1	Parte del cableado de datos no pasa por ducteri a y está espuesto	Medio	3	Probable	4	2	4	2	1	4	Mayores	16	Extremo
COM2	No existe una política de uso y seguimiento de contraseñas	Medio	3	Probable	4	2	4	2	1	4	Mayores	16	Extremo

FIGURA 4.34: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO REDES DE COMUNICACIONES

Fuente: Douglas Marín y César Medina

Cod.	DESCRIPCIÓN DE VULNERABILIDAD	NIVEL DE VULNERABILIDAD	VALOR PROBABILIDAD	NIVEL DE PROBABILIDAD	CALCULO DE PROBABILIDAD	IMPACTO FINACIERO	IMPACTO OPERACIONAL	IMPACTO REPUTACIONAL	IMPACTO NORMATIVO	CALCULO IMPACTO	NIVEL DE IMPACTO	SEVERIDAD DEL RIESGO	DESCRIPCIÓN SEVERIDAD
MEDIA1	No existe bloqueo de escaneo por usuario	Bajo	2	Improbable	2	2	2	3	1	3	Moderadas	6	Moderado
MEDIA2	Puertos USB no bloqueados en las PC´s y laptops	Alto	4	Casi Certeza	5	4	3	3	1	4	Mayores	20	Extremo
MEDIA3	No existe una política de almacenamiento de material sensible	Medio	3	Probable	4	4	4	4	1	4	Mayores	16	Extremo
MEDIA4	Puertos USB no bloqueados en las PC´s y laptops	Alto	4	Casi Certeza	5	4	3	3	1	4	Mayores	20	Extremo

FIGURA 4.35: EVALUACIÓN DE RIESGO DE ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

4.3 Descripción del tratamiento de riesgo

El tratamiento de riesgo es un proceso dinámico y continuo que requiere revisiones periódicas para adaptarse a los cambios en el entorno empresarial y en la naturaleza de los riesgos. La elección de estrategias dependerá de la naturaleza del riesgo, los recursos disponibles y los objetivos de la empresa. Es fundamental seleccionar estrategias de tratamiento basadas en la naturaleza del riesgo, los recursos disponibles y los objetivos organizacionales, lo que contribuirá a una toma de decisiones más segura y sostenible.

En la actualidad, el tratamiento de riesgo se ha vuelto más sofisticado, orientado por la tecnología y adaptado para abordar los desafíos emergentes en un entorno empresarial dinámico y cambiante. La gestión efectiva de riesgos sigue siendo esencial para la supervivencia y el crecimiento sostenible de las organizaciones.

4.3.1 Opciones de tratamiento

Para el tratamiento de riesgos, existen cuatro posibles opciones:

- **Evitar:** Implementar medidas para eliminar por completo la exposición al riesgo. Implica abstenerse de ciertas actividades que podrían dar lugar al riesgo identificado.
- **Aceptar:** Reconocer la existencia del riesgo y decidir no tomar medidas activas para cambiar su probabilidad de ocurrencia o su impacto.
- **Transferir:** Externalizar el riesgo a terceros, mediante la compra de seguros u otras formas de contrato. La responsabilidad financiera y operativa se traslada a otra entidad.

- **Mitigar:** Implementar medidas para reducir la probabilidad de ocurrencia de un riesgo para minimizar su impacto en caso de materializarse.

4.3.2 Tratamiento de los activos críticos

Para la empresa auditora, el tratamiento de los activos críticos es esencial con respecto a la continuidad operativa de la empresa, la protección de la información sensible, la ciberseguridad, el cumplimiento normativo, la gestión de riesgos y la reputación de la empresa. El tratamiento adecuado de los activos críticos de la empresa es esencial para garantizar la seguridad, la continuidad operativa y la resiliencia de la organización.

En las ilustraciones a continuación, se muestran los resultados:

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
S1	Mitigar	Migración de la página web a nuevas tecnologías actualizadas
S2	Mitigar	Realizar Capacitaciones a los usuarios que usen el servicio de correo y simulacro de phishing
S3	Mitigar	Servicio de Pentesting web
S4	Mitigar	Migración del servicio a un Hosting
S5	Mitigar	Implementar Doble factor de Autenticidad

S6	Mitigar	Control de los puertos USB por endpoint

FIGURA 4.36: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO SERVICIO

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
D1	Mitigar	Documentar procesos y procedimientos de todas las configuraciones y que sean accesibles por roles autorizados.
D2	Mitigar	Usar un Framework de Marco desarrollo seguro de software y buenas practicas
D3	Mitigar	Incorporación de un DLP
D4	Mitigar	Realizar Hardening en los servidores
D5	Aceptar	Se revisan periódicamente el estado de los HDD
D6	Aceptar	Se revisan periódicamente el estado de los HDD
D7	Aceptar	Las credenciales las conserva solo el Subgerente de TI con copia de Gerente general.

FIGURA 4.37: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
SW6	Mitigar	Compra de licencias de Sistema Operativo Windows 10 pro
SW7	Mitigar	Compra de licencias de Sistema Operativo Windows 11 pro
SW8	Mitigar	Compra de licencias de Sistema Operativo Windows Server 2022
SW9	Mitigar	Realizar actualizaciones de seguridad en los sistemas operativos
SW10	Aceptar	Al actualizar se ha verificado que afecta a las máquinas virtuales
SW11	Aceptar	Se cuenta con profesionales capacitados e informados con estos sucesos
SW12	Mitigar	Realizar políticas y procedimientos de la gestión de Bases de Datos

FIGURA 4.38: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO SOTFWARE

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
AUX1	Mitigar	Realizar planificación anual para mantenimiento de generador del edificio
AUX2	Aceptar	Ya existe planes de descontaminación
AUX3	Mitigar	Realizar planificación anual para mantenimiento de los UPS
AUX4	Mitigar	Realizar planificación anual para mantenimiento de los aires acondicionados
AUX5	Aceptar	Ya existe planes sobre sistema de protección contra incendio y permisos adecuados

FIGURA 4.39: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
L1	Mitigar	Instalación de reconocimiento por tarjeta a personal autorizado con Cámara
L2	Mitigar	Instalación de reconocimiento por tarjeta a personal autorizado con Cámara
L3	Mitigar	Realizar políticas de puesto de trabajo y concientización sobre ellas

FIGURA 4.40: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
P7	Mitigar	Realizar acuerdo de confidencialidad y privacidad
P8	Mitigar	Realizar acuerdo de confidencialidad y privacidad
P9	Mitigar	Realizar política de Seguridad de la información para la organización en general

FIGURA 4.41: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
HW1	Mitigar	Reforzar las políticas y controles en el antivirus de la PC

HW2	Mitigar	Reforzar las políticas y controles en el antivirus de las laptops
HW3	Mitigar	Reforzar la seguridad en el Firewall Perimetral
HW4	Aceptar	Tenemos un plan de capacitación a personal de TI para reforzar conocimientos
HW5	Mitigar	Reforzar la seguridad en el Firewall Perimetral
HW6	Mitigar	Reforzar las contraseñas de ingreso a los Access Points
HW7	Mitigar	Crear el bloque de impresión por usuario mediante contraseña personal
HW8	Mitigar	Adquisición de un NGFW que cumpla las necesidades de la empresa
HW9	Mitigar	Agregar el reglamento de acuerdo de confidencialidad al reglamento interno de la empresa
HW13	Mitigar	Adquisición de un NGFW para protección del NAS

FIGURA 4.42: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
COM1	Mitigar	Reforzar el cableado estructurado siguiendo las mejores prácticas

COM2	Aceptar	Ya existe un plan de acción para el uso de contraseñas

FIGURA 4.43: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO REDES DE COMUNICACIONES

Fuente: Douglas Marín y César Medina

Cod.	OPCION DE TRATAMIENTO	DESCRIPCIÓN DEL TRATAMIENTO
MEDIA1	Mitigar	Crear el bloque de escaneo por usuario mediante contraseña personal
MEDIA2	Mitigar	Bloqueo de puertos USB a personal de la empresa, y solo habilitar en casos excepcionales
MEDIA3	Mitigar	Adecuar un gabinete para guardar todo el material impreso
MEDIA4	Mitigar	Bloqueo de puertos USB a personal de la empresa, y solo habilitar en casos excepcionales

FIGURA 4.44: DESCRIPCIÓN DEL TRATAMIENTO DE ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

4.4 Cálculo de riesgo residual

El cálculo del riesgo residual en una empresa implica evaluar el riesgo que queda después de haber implementado medidas de tratamiento de riesgos.

Se puede expresar de la siguiente manera:

$$Riesgo\ Residual = Riesgo\ Inicial - Efectividad\ de\ las\ Medidas\ de\ Tratamiento$$

Donde el riesgo inicial es la evaluación del riesgo antes de implementar cualquier medida de tratamiento y la efectividad de las medidas de tratamiento representa la reducción del riesgo lograda por las acciones de tratamiento implementadas.

El resultado es el riesgo residual, que es el riesgo que la empresa aún enfrenta después de haber aplicado medidas para mitigar o gestionar el riesgo inicial.

En la Figura 4.45 observamos el cálculo del riesgo residual.

Oportunidad de Aplicación	Periodicidad de Aplicación	Automatización del Control
PREVENTIVO	PERMANENTE	AUTOMATIZADO
CORRECTIVO	PERIODICO	SEMI-AUTOMATIZADO
DETECTIVO	OCASIONAL	MANUAL

FIGURA 4.45: CÁLCULO DEL RIESGO RESIDUAL

Fuente: Douglas Marín y César Medina

4.4.1 Tipos de efectividad de tratamiento de riesgo

La efectividad del tratamiento de riesgo puede manifestarse de diversas maneras, como la reducción de la probabilidad y mitigación del impacto. Puede medirse por la eliminación total del riesgo, la transferencia eficaz mediante seguros, el cumplimiento normativo y la resiliencia organizativa. La mejora continua también es clave, evaluando la capacidad de adaptarse y aprender de la experiencia para ajustar estrategias. Estos tipos de efectividad reflejan la gestión integral de riesgos, buscando minimizar las amenazas y fortalecer la capacidad de la organización para enfrentar y recuperarse de eventos adversos en un entorno empresarial cambiante. En la Figura 4.46 se presentan las diferentes combinaciones que puede tener la efectividad de tratamiento de riesgo.

Combinación	Oportunidad de Aplicación	Periodicidad de Aplicación	Automatización del Control	Efectividad del Control	Nivel de efectividad
PREVENTIVOPERMANENTEAUTOMATIZADO	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5
PREVENTIVOPERMANENTESEMI-AUTOMATIZADO	PREVENTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	5
PREVENTIVOPERMANENTEMANUAL	PREVENTIVO	PERMANENTE	MANUAL	ÓPTIMO	5
CORRECTIVOPERMANENTEAUTOMATIZADO	CORRECTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5
CORRECTIVOPERMANENTESEMI-AUTOMATIZADO	CORRECTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	5
CORRECTIVOPERMANENTEMANUAL	CORRECTIVO	PERMANENTE	MANUAL	ÓPTIMO	5
DETECTIVOPERMANENTEAUTOMATIZADO	DETECTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5
DETECTIVOPERMANENTESEMI-AUTOMATIZADO	DETECTIVO	PERMANENTE	SEMI-AUTOMATIZADO	BUENO	4
DETECTIVOPERMANENTEMANUAL	DETECTIVO	PERMANENTE	MANUAL	BUENO	4
PREVENTIVOPERIODICOAUTOMATIZADO	PREVENTIVO	PERIODICO	AUTOMATIZADO	BUENO	4
PREVENTIVOPERIODICOSEMI-AUTOMATIZADO	PREVENTIVO	PERIODICO	SEMI-AUTOMATIZADO	BUENO	4
PREVENTIVOPERIODICOMANUAL	PREVENTIVO	PERIODICO	MANUAL	BUENO	4
CORRECTIVOPERIODICOAUTOMATIZADO	CORRECTIVO	PERIODICO	AUTOMATIZADO	BUENO	4
CORRECTIVOPERIODICOSEMI-AUTOMATIZADO	CORRECTIVO	PERIODICO	SEMI-AUTOMATIZADO	MAS QUE REGULAR	3
CORRECTIVOPERIODICOMANUAL	CORRECTIVO	PERIODICO	MANUAL	MAS QUE REGULAR	3
DETECTIVOPERIODICOAUTOMATIZADO	DETECTIVO	PERIODICO	AUTOMATIZADO	MAS QUE REGULAR	3
DETECTIVOPERIODICOSEMI-AUTOMATIZADO	DETECTIVO	PERIODICO	SEMI-AUTOMATIZADO	MAS QUE REGULAR	3
DETECTIVOPERIODICOMANUAL	DETECTIVO	PERIODICO	MANUAL	MAS QUE REGULAR	3
PREVENTIVOOCASIONALAUTOMATIZADO	PREVENTIVO	OCASIONAL	AUTOMATIZADO	REGULAR	2
PREVENTIVOOCASIONALSEMI-AUTOMATIZADO	PREVENTIVO	OCASIONAL	SEMI-AUTOMATIZADO	REGULAR	2
PREVENTIVOOCASIONALMANUAL	PREVENTIVO	OCASIONAL	MANUAL	REGULAR	2
CORRECTIVOOCASIONALAUTOMATIZADO	CORRECTIVO	OCASIONAL	AUTOMATIZADO	REGULAR	2
CORRECTIVOOCASIONALSEMI-AUTOMATIZADO	CORRECTIVO	OCASIONAL	SEMI-AUTOMATIZADO	REGULAR	2
CORRECTIVOOCASIONALMANUAL	CORRECTIVO	OCASIONAL	MANUAL	DEFICIENTE	1
DETECTIVOOCASIONALAUTOMATIZADO	DETECTIVO	OCASIONAL	AUTOMATIZADO	DEFICIENTE	1
DETECTIVOOCASIONALSEMI-AUTOMATIZADO	DETECTIVO	OCASIONAL	SEMI-AUTOMATIZADO	DEFICIENTE	1
DETECTIVOOCASIONALMANUAL	DETECTIVO	OCASIONAL	MANUAL	DEFICIENTE	1
NO DETERMINADONO DETERMINADONO DETERMINADO	NO DETERMINADO	NO DETERMINADO	NO DETERMINADO	INEXISTENTE	0

FIGURA 4.46: TIPOS DE EFECTIVIDAD DE TRATAMIENTO DE RIESGO

Fuente: Douglas Marín y César Medina

4.4.2 Niveles de exposición al riesgo

Para la empresa auditora, los niveles de exposición al riesgo abarcan diversas áreas. El financiero se vincula con la gestión económica y financiera. La operación eficiente y la cadena de suministro global introducen el riesgo operacional. En entornos regulados, el riesgo regulatorio surge de cambios normativos. La ciberseguridad es crítica para proteger datos y sistemas contra amenazas digitales. La reputación de la empresa auditora puede estar en juego ante la crisis de relaciones públicas. La sostenibilidad y la responsabilidad social corporativa abordan riesgos ambientales y sociales. La gestión integral de estos riesgos es esencial para la resiliencia empresarial. En la Figura 4.47 presentamos los niveles de exposición al riesgo, dependiendo del riesgo residual.

RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
< 7	MENOR
< 13	MEDIA
< 19	MAYOR
<= 25	NO ACEPTADO

FIGURA 4.47: NIVELES DE EXPOSICIÓN AL RIESGO

Fuente: Douglas Marín y César Medina

4.4.3 Cálculo del riesgo residual usando la efectividad de los controles en los activos críticos

Se realizo la valoración de los controles a los activos tratados para su mitigación de riesgos, dándonos un resultado de riesgo residual. Este cálculo es esencial para evaluar la eficiencia de las medidas de seguridad implementadas.

En las siguientes ilustraciones, se muestran los resultados:

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
S1	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
S2	PREVENTIVO	PERIODICO	SEMI-AUTOMATIZADO	BUENO	6,25	MENOR
S3	CORRECTIVO	OCASIONAL	AUTOMATIZADO	REGULAR	8	MEDIA
S4	CORRECTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
S5	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	4	MENOR
S6	CORRECTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR

FIGURA 4.48: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO SERVICIOS

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
D1	PREVENTIVO	PERMANENTE	MANUAL	ÓPTIMO	5	MENOR
D2	PREVENTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	5	MENOR
D3	DETECTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
D4	CORRECTIVO	PERIODICO	MANUAL	MAS QUE REGULAR	8,333333333	MEDIA

FIGURA 4.49: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
SW6	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
SW7	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
SW8	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
SW9	PREVENTIVO	PERIODICO	MANUAL	BUENO	3	MENOR
SW12	PREVENTIVO	PERIODICO	MANUAL	BUENO	6,25	MENOR

FIGURA 4.50: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO SOFTWARE

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
AUX1	PREVENTIVO	PERIODICO	MANUAL	BUENO	2,5	MENOR
AUX3	PREVENTIVO	PERIODICO	MANUAL	BUENO	1,5	MENOR
AUX4	PREVENTIVO	PERIODICO	MANUAL	BUENO	3	MENOR

FIGURA 4.51: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
L1	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
L2	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	4	MENOR
L3	PREVENTIVO	PERIODICO	MANUAL	BUENO	5	MENOR

FIGURA 4.52: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
P7	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
P8	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR
P9	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	5	MENOR

FIGURA 4.53: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
HW1	CORRECTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	4	MENOR
HW2	CORRECTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	4	MENOR
HW3	PREVENTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	3,2	MENOR
HW5	PREVENTIVO	PERIODICO	AUTOMATIZADO	BUENO	3,75	MENOR
HW6	PREVENTIVO	PERMANENTE	AUTOMATIZADO	ÓPTIMO	0,8	MENOR
HW7	CORRECTIVO	PERIODICO	MANUAL	MAS QUE REGULAR	2,666666667	MENOR
HW8	CORRECTIVO	PERMANENTE	MANUAL	ÓPTIMO	5	MENOR
HW9	CORRECTIVO	PERMANENTE	MANUAL	ÓPTIMO	3	MENOR
HW13	CORRECTIVO	PERMANENTE	MANUAL	ÓPTIMO	5	MENOR

FIGURA 4.54: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
COM1	PREVENTIVO	PERIODICO	MANUAL	BUENO	4	MENOR

FIGURA 4.55: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO REDES DE COMUNICACIONES

Fuente: Douglas Marín y César Medina

Cod.	OPORTUNIDAD DE APLICACIÓN	PERIODICIDAD DE APLICACIÓN	AUTOMATIZACIÓN DEL CONTROL	EFECTIVIDAD DEL CONTROL	RIESGO RESIDUAL	NIVEL DE EXPOSICIÓN AL RIESGO
MEDIA1	CORRECTIVO	PERIODICO	MANUAL	MAS QUE REGULAR	2	MENOR
MEDIA2	PREVENTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	4	MENOR
MEDIA3	CORRECTIVO	PERMANENTE	MANUAL	ÓPTIMO	3,2	MENOR
MEDIA4	PREVENTIVO	PERMANENTE	SEMI-AUTOMATIZADO	ÓPTIMO	4	MENOR

FIGURA 4.56: CÁLCULO DEL RIESGO RESIDUAL USANDO LA EFECTIVIDAD DE LOS CONTROLES EN LOS ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

4.5 Cálculo basado en probabilidad e impacto residual

En este segmento se calcula la probabilidad y el impacto que genera el riesgo residual en los activos que fueron tratados, también se define la justificación de la implementación de los controles implementados para la reducción de los riesgos.

En las siguientes ilustraciones, se muestran los resultados:

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
S1	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se aplica la actualización a nuevas tecnologias para descartar brechas de seguridad.
S2	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se activan las capacitciones a todos los usuarios que usen el servicio asi prevenir estafaz, captura de credenciales y ataques DOS
S3	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se realiza el control para corregir posibles brechas de seguridad
S4	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se contrata un hosting para el alojamiento del servicio para asegurar su disponibilidad 24/7
S5	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Implementación de MFA para acceso seguro por parte de usuarios.
S6	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Implementacion de bloqueo de Puertos USB para cuidar la información de cualquier ataque

FIGURA 4.57: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO SERVICIOS

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
D1	Muy Bajo	1	**Menores**	**2**	**Bajo**	**2**	Disminución por documentación de procesos y procedimientos de las configuraciones que manejan los
D2	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Con la implementación de este marco de desarrollo seguro disminuye las brechas y seguridad en el ciclo de vida
D3	Muy Bajo	1	**Menores**	**2**	**Bajo**	**2**	Dectar y bloquear la salida de información sencible
D4	Medio	3	**Menores**	**2**	**Moderado**	**6**	Se realiza hardening para reforzar la seguridad de los servidores en puertos abiertos sin utilizar.

FIGURA 4.58: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO DATOS

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
SW6	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implanta licenciamiento de S.O para actualizaciones de Seguridad.
SW7	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implanta licenciamiento de S.O para actualizaciones de Seguridad.
SW8	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implanta licenciamiento de S.O para actualizaciones de Seguridad.
SW9	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Planificación de actualización en los sistemas operativos de Linux para reforzar brechas de seguridad.
SW12	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa politicas y procedimeinto para el uso correcto de la base de datos.

FIGURA 4.59: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO SOFTWARE

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
AUX1	Bajo	2	**Insignificantes**	**1**	**Bajo**	**2**	Se realiza la planificacion anual para mantenimiento del generador y asi evitar fallas futuras.
AUX3	Bajo	2	**Insignificantes**	**1**	**Bajo**	**2**	Se realiza la planificacion anual para mantenimiento de los UPS y asi evitar fallas futuras.
AUX4	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se realiza la planificacion anual para mantenimiento de los equipos de climatización y asi evitar fallas futuras.

FIGURA 4.60: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO EQUIPAMIENTO AUXILIAR

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
L1	Bajo	2	**Menores**	**2**	**Bajo**	**4**	se implementa control para la restriccion de personal no autorizado
L2	Bajo	2	**Menores**	**2**	**Bajo**	**4**	se implementa control para la restriccion de personal no autorizado
L3	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa para que los usuarios tomen conciencia de los peligros de la ingeneria social.

FIGURA 4.61: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO INSTALACIONES

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
P7	Medio	3	**Menores**	**2**	**Moderado**	**6**	Se implementa para asegurar medidas legales contra el empleado en caso de que suceda
P8	Medio	3	**Menores**	**2**	**Moderado**	**6**	Se implementa para asegurar medidas legales contra el empleado en caso de que suceda
P9	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa para asegurar medidas legales contra el proveedor en caso de que suceda

FIGURA 4.62: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO PERSONAL

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
HW1	Medio	3	**Menores**	2	**Moderado**	6	Se implementa para evitar ataques ciberneticos e infoecciones de virus, gusanos, troyanos, etc
HW2	Medio	3	**Menores**	2	**Moderado**	6	Se implementa para evitar ataques ciberneticos e infoecciones de virus, gusanos, troyanos, etc
HW3	Medio	3	**Menores**	2	**Moderado**	6	Se implementa para garantizar la integridad de la información del activo
HW5	Bajo	2	**Menores**	2	**Bajo**	4	Se implementa para garantizar la integridad de la información del activo
HW6	Bajo	2	**Insignificantes**	1	**Bajo**	2	Se realiza el reforzamiento de contraseñas para evitar accesos no autorizados
HW7	Bajo	2	**Insignificantes**	1	**Bajo**	2	Se implementa para asegurar que cada usuario sea responsable de su trabajo de impresión
HW8	Bajo	2	**Menores**	2	**Bajo**	4	Se implementa por la necesidad de cambiar el Firewall actual
HW9	Bajo	2	**Menores**	2	**Bajo**	4	Se refuerza la confidencialidad de la información
HW13	Bajo	2	**Menores**	2	**Bajo**	4	Se implementa para reforzar la ciberseguridad del activo

FIGURA 4.63: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO HARDWARE

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
COM1	Bajo	2	**Insignificantes**	1	**Bajo**	2	Se realiza debido a buenas prácticas

FIGURA 4.64: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO REDES DE COMUNICACIONES

Fuente: Douglas Marín y César Medina

Cod.	NIVEL DE PROBABILIDAD	VALOR PROBABLIDAD	NIVEL DE IMPACTO	CALCULO IMPACTO	RIESGO RESIDUAL	RIESGO RESIDUAL	JUSTIFICACIÓN DEL TRATAMIENTO
MEDIA1	Bajo	2	**Insignificantes**	**1**	**Bajo**	**2**	Se implementa para asegurar que cada usuario sea responsable de su trabajo de escaneo
MEDIA2	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa por control de acceso a periféricos
MEDIA3	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa un lugar seguro para almacenar información sensible
MEDIA4	Bajo	2	**Menores**	**2**	**Bajo**	**4**	Se implementa por control de acceso a periféricos

FIGURA 4.65: CÁLCULO BASADO EN PROBABILIDAD E IMPACTO RESIDUAL EN LOS ACTIVOS DEL TIPO SOPORTE DE INFORMACIÓN

Fuente: Douglas Marín y César Medina

CAPITULO V.

DEFINICIÓN DE PDS

5.1 Conocer la estratégica de la organización

Para esta etapa del proyecto se realizó varias reuniones con la directiva de la empresa y los responsables de los activos dentro del alcance, esto para conocer la estrategia corporativa actual y conocer los proyectos actuales y los de largo plazo.

Se estableció que la empresa tiene prevista seguir prestando los servicios en varias áreas al grupo de la joyería, atendiendo sus necesidades y preparándose para la apertura de varias joyerías a nivel nacional.

También como proyecto actual esta prestar los servicios tecnológicos y de infraestructura TIC a joyerías internacionales perteneciente al mismo grupo tales como: España (Sistema Core de transacciones, servicio de correo corporativo), Perú (Sistema Core de tracciones), Panamá (Sistema Core de tracciones). Los servicios TIC estarán centralizados en el edificio de la empresa.

5.2 Definición de proyectos

La definición de los proyectos se basa en tener en cuenta todos los tratamientos de los activos críticos que fueron mitigados en la matriz de gestión de riesgo, haciendo de ellos proyectos individuales para presentarlos como posibles soluciones a la severidad de los riesgos.

A continuación, se presenta los proyectos acordes a los tratamientos realizados en los activos críticos:

ID	Proyecto	Descripción
01	Desarrollar e implementar políticas y procedimientos.	Seguridad de la información, Administración de red, configuraciones de servicios y aplicaciones, hardening, actualizaciones de S.O, Gestión de Base de Datos, Protección puesto de trabajo, BYOD, controles de acceso endpoint, copias de seguridad
02	Migración de Ecommerce	Actualización de nuevas tecnologías para página web
03	Servicio de Pentesting	Servicio de pentesting para ERP
04	Servicio de Hosting	Servicio de hosting para Sistema Core de transacciones
05	MFA	Implementación MFA para Aula virtual
06	Restricción de Puertos	Restricción de puertos en Equipos dentro de la red corporativa
07	Plataforma de Capacitación y Phishing Simulado	Realizar Capacitaciones a los usuarios que usen el servicio de correo y simulacro de phishing
08	DLP	DLP para control de envió y extracción de información
09	Licencias Sistemas Operativos	Licenciamiento de Sistema Operativo Windows 10, Windows 11pro y Windows Server 2022
10	Planificación de Mantenimiento Anual	Para equipos tecnológicos, generadores, UPS, climatización
11	Control de accesos Físico	Control de accesos para Data Center, cuarto de Mantenimiento y gabinete de documentos físicos por medio de tarjeta de control.
12	Implementación RGPD	Adaptar RGPD en la organización y cubrir leyes de confidencialidad para usuario y proveedores
13	Seguridad perimetral	Adquisición de firewall NGFW, reforzar contraseñas de ingreso con identificación.

Tabla 3: Definición de proyectos

Fuente: Douglas Marín y César Medina

5.3 Clasificar y priorizar proyectos

En este punto se clasifican y priorizan los proyectos antes mencionados acorde a la criticidad de los riesgos, coste de iniciativa económica y nivel de importancia de los activos acorde al impacto de perdida de generen.

Es importante saber que este punto está expuesto a cambios por parte de la dirección una vez presentado el proyecto.

Hemos clasificado y priorizado los proyectos según se observa en la Figura 5.1:

ID	Proyecto	Tiempo de Implementación Meses	Prioridad	Costo	Frecuencia	Justificación
01	Desarrollar e implementar politicas y procedimientos.	12	MEDIA	$0,00	Anual	La implementación de las politicas y procedimientos se realizará por los especialistas responsables de cada activo.
02	Migración de Ecommerce	6	ALTA	$0,00	Anual	La migración de las nuevas tecnologias OpenSource las realizará los especialista responable de los activos
03	Servicio de Pentesting	1	MEDIA	$5.000,00	Anual	Servicio focalizado a pentesting web, para identificar vulnerabilidades en el desarrollo y seguridad del ERP
04	Servicio de Hosting	1	ALTA	$1.000,00	Mensual	Servicio de Hosting para continuidad del servicio Core
05	MFA	1	ALTA	$0,00	Permanente	Implementación por especialistas con herrameinta gratuitas
06	Restricción de Puertos	1	ALTA	$0,00	Permanente	Implementación por especialistas con herrameinta gratuitas
07	Plataforma de Capacitación y Phishing Simulado	1	MEDIA	$3.500,00	Anual	Servicio para capacitaciones a los usuarios que usen el servicio de correo y simulacro de phishing
08	DLP	2	BAJA	$4.000,00	Anual	DLP para control de envio y extracción de información
09	Licencias Sistemas Operativos	3	ALTA	$5.000,00	Permanente	Licenciamiento de Sistema Operativo Windows 10, Windows 11pro y Windows Server 2022
10	Planificación de Mantenimiento Anual	1	MEDIA	$500,00	Anual	Para equipos tecnologicos, generadosres, UPS, climatización
11	Control de accesos Fisicos	1	MEDIA	$1.000,00	Permanente	Control de accesos para Data Center, cuarto de Mantenimiento y gabinete de documentos fisicos por medio de tarjetas con autorización
12	Implementación RGPD	6	MEDIA	$5.500,00	Permanente	Adaptar RGPD en la organización y cubrir leyes de confidencialidad para usuario y proveedores
13	Seguridad perimetral	2	ALTA	$500,00	Mensual	Servicio de firewall NGFW, reforzar contraseñas de ingreso con identificación.

FIGURA 5.1: CLASIFICACIÓN Y PRIORIZACIÓN DE PROYECTOS

Fuente: Douglas Marín y César Medina

5.4 Presentación de PDS a la Directiva

Una vez realizado la clasificación y priorización de los proyectos se planificará una reunión con la directiva para presentar los resultados del Plan director de seguridad, mostrándole diferentes opciones a escoger, para que según su criterio puedan aprobar la mejor opción e invertir en los proyectos expuestos.

Cada opción de Plan director de Seguridad abarcara diferentes presupuestos como plan de acción máximo, plan de acción medio y plan acción mínimo. Es importante comunicar a la directiva que no todos los planes contarán con todos los proyectos y dependerá mucho del presupuesto asignado.

Los riesgos que no se mitiguen con los proyectos propuestos serán responsabilidad de la directiva y plasmado en un documento.

Es importante saber que una vez aprobado los proyectos la dirección debe respaldar y comunicar el Plan director de seguridad a todos los empleados para que entienda la importancia de este mismo y que toda la organización pueda colaborar con su implementación.

Primer año - Acción Máxima				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**
01	Desarrollar e implementar políticas y procedimientos.	12	MEDIA	$0,00

13	Seguridad perimetral	2	ALTA	$500,00
02	Migración de Ecommerce	6	ALTA	$0,00
03	Servicio de Pentesting	1	MEDIA	$5.000,00
04	Servicio de Hosting	1	ALTA	$1.000,00
05	MFA	1	ALTA	$0,00
06	Restricción de Puertos	1	ALTA	$0,00
09	Licencias Sistemas Operativos	3	ALTA	$5.000,00
11	Control de accesos Físicos	1	MEDIA	$1.000,00
10	Planificación de Mantenimiento Anual	1	MEDIA	$500,00
			Total, presupuesto:	$13.000,00

Segundo año - Acción Máxima				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**
07	Plataforma de Capacitación y Phishing Simulado	1	MEDIA	$3.500,00
08	DLP	2	BAJA	$4.000,00
12	Implementación RGPD	6	MEDIA	$5.500,00
			Total, presupuesto:	$13.000,00

*** Los valores de costo $ 0 están justificados en la sección 5.3 Ilustración 118**

Tabla 4: Priorización de proyectos Acción Máxima

Fuente: Douglas Marín y César Medina

Primer año - Acción Media				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**
01	Desarrollar e implementar políticas y procedimientos.	12	MEDIA	$0,00
13	Seguridad perimetral	2	ALTA	$500,00
02	Migración de Ecommerce	6	ALTA	$0,00
04	Servicio de Hosting	1	ALTA	$1.000,00
05	MFA	1	ALTA	$0,00
06	Restricción de Puertos	1	ALTA	$0,00
09	Licencias Sistemas Operativos	3	ALTA	$5.000,00
11	Control de accesos Físicos	1	MEDIA	$1.000,00
10	Planificación de Mantenimiento Anual	1	MEDIA	$500,00

			Total, presupuesto:	$8.000,00
Segundo año - Acción Media				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**
07	Plataforma de Capacitación y Phishing Simulado	1	MEDIA	$3.500,00
12	Implementación RGPD	6	BAJA	$5.500,00
			Total, presupuesto:	$9.000,00
Acciones que no se llevarían acabo				
08	DLP	2	BAJA	$4.000,00
03	Servicio de Pentesting	1	BAJA	$5.000,00

*** Los valores de costo $ 0 están justificados en la sección 5.3 Ilustración 118**

Tabla 5: Priorización de proyectos Acción Media

Fuente: Douglas Marín y César Medina

Primer año - Acción Mínima				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**

01	Desarrollar e implementar políticas y procedimientos.	12	MEDIA	$0,00
13	Seguridad perimetral	2	ALTA	$500,00
02	Migración de Ecommerce	6	ALTA	$0,00
04	Servicio de Hosting	1	ALTA	$1.000,00
05	MFA	1	ALTA	$0,00
06	Restricción de Puertos	1	ALTA	$0,00
09	Licencias Sistemas Operativos	3	ALTA	$5.000,00
10	Planificación de Mantenimiento Anual	1	MEDIA	$500,00
			Total, presupuesto:	$7.000,00
Segundo año - Acción Mínima				
ID	**Proyecto**	**Tiempo de Implementación Meses**	**Prioridad**	**Costo**
12	Implementación RGPD	6	MEDIA	$5.500,00
			Total, presupuesto:	$5.500,00
Acciones que no se llevarían acabo				
08	DLP	2	BAJA	$4.000,00
03	Servicio de Pentesting	1	MEDIA	$5.000,00
11	Control de accesos Físicos	1	MEDIA	$1.000,00

07	Plataforma de Capacitación y Phishing Simulado	1	MEDIA	$3.500,00

*** Los valores de costo $ 0 están justificados en la sección 5.3 Ilustración 118**

Tabla 6: Priorización de proyectos Acción Mínima

Fuente: Douglas Marín y César Medina

CONCLUSIONES

1. La alta dirección eligió los activos y procesos de criticidad, escogidos según la operatividad de negocio y los aspectos que afecten a la capacidad de lograr resultados.
2. Se determinó cuál era el nivel actual en seguridad de la información en la organización y, con base en lo propuesto con la implementación de PDS, se determinó objetivos para mejorarla.
3. Se determino la necesidad de una política de seguridad de la información a nivel organizativo, la cual fue realizada en el proceso de este trabajo.
4. La empresa auditora no posee un historial de ataques cibernéticos, por lo que establecer las amenazas se vuelve difícil. Por lo tanto, para identificar las amenazas se tuvo en cuenta los riesgos comunes a los que está expuesta una empresa.
5. El resultado del riesgo residual de los activos críticos de la empresa estuvo dentro del rango esperado por la Dirección.
6. La elaboración de la matriz de riesgos es fundamental para establecer el enfoque de seguridad y la priorización de proyectos por parte de la Dirección.
7. Al contar con los activos críticos de la empresa definidos por la Dirección, debidamente identificados, facilitó el análisis y la evaluación de riesgo del presente trabajo.
8. Se determinó que la definición de los proyectos se realizó en base a los riesgos encontrados en los activos y procesos críticos que están dentro del alcance

9. Los diferentes planes de seguridad facilito la toma de decisiones de la Dirección General para poder invertir en proyectos en seguridad de la información.
10. La priorización de los proyectos se basa en las prioridades, necesidades y costos de implementación en la organización.

RECOMENDACIONES

1. La implementación del PDS en la empresa auditora contiene tareas que deben llevarse a cabo con cierta periodicidad porque los avances tecnológicos no cesan y estamos cada vez más expuestos a nuevas amenazas/vulnerabilidades.
2. Se debe dar a conocer a todos los usuarios de la organización la política de seguridad de la información realizada.
3. La concientización a los usuarios de la empresa auditora es vital para evitar que los activos críticos se vean vulnerados por engaños, fraudes o ingeniería social. Esto debe realizarse de manera continua y programada usando también simuladores de phishing.
4. Los activos críticos de la empresa auditora que pasarán a analizarse en la matriz de riesgos deben ser debidamente seleccionados para canalizar debidamente los esfuerzos del personal de seguridad informática al momento de analizar los riesgos expuestos.
5. Si la Alta dirección de la organización requiere modificar algún aspecto del alcance, debe comunicarse con tiempo al equipo de seguridad de la información para que puedan reestructurar el PDS si este lo necesitara.
6. Los riesgos que sean aceptados, eliminados o transferidos deben ser justificados, documentados y firmados por la alta dirección.
7. Establecer un programa de monitoreo y auditoría continua para evaluar el cumplimiento de las políticas, procedimientos y controles de seguridad establecidos en el PDSI.

8. Realizar evaluaciones de seguridad de forma regular, como pruebas de penetración, análisis de vulnerabilidades y pruebas de intrusión, con el objetivo de detectar y mitigar posibles debilidades en la seguridad de la información.
9. Fomentar la cooperación y coordinación entre los distintos departamentos y áreas de la organización para asegurar la implementación exitosa del Plan de Seguridad de la Información (PDSI).
10. Obtener y mantener el compromiso y apoyo de la alta dirección para asegurar la asignación de recursos y la implementación efectiva del PDSI en toda la organización.

BIBLIOGRAFÍA

[1] J. A. Montero Valencia, «Desarrollo del Plan Director de Seguridad para la Asociación APSA», 2019.

[2] G. B. Maldonado y J. A. O. Cano, «Metodología de la seguridad de la información como medida de protección en pequeñas empresas.», *Cuaderno activa*, vol. 6, pp. 71-77, 2014.

[3] G. Martínez-Ubierna de Evan y others, «Plan director de seguridad», 2018.

[4] H. de la Cruz, «¿Por qué necesita un Plan Director de Seguridad?», PMG SSI - ISO 27001. Accedido: 28 de septiembre de 2023. [En línea]. Disponible en: https://www.pmg-ssi.com/2022/05/por-que-necesitas-un-plan-director-de-seguridad/

[5] J. D. Evans, «Modelo de Seguridad de la Información Gobierno de Seguridad».

[6] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, «La seguridad informática y la seguridad de la información», *Polo del conocimiento*, vol. 2, n.º 12, pp. 145-155, 2018.

[7] I. Piera Cebrián, «Desarrollo de un SGSI para un grupo empresarial», 2021.

[8] R. Baldecchi y G. C. de Calidad, «Implementación efectiva de un SGSI ISO 27001», *Internet:(http://www. isaca. org/chapters8/Montevideo/cigras/Documents/CIGRAS2014% 20-% 20Exposici% C3% B3n% 202% 20CIGRAS% 20ISO% 2027001% 20-% 20rbq. pdf)*, 2014.

[9] G. Solutions, «¿Qué es la norma ISO 27001 y para qué sirve?», GlobalSuite Solutions. Accedido: 3 de diciembre de 2023. [En línea]. Disponible en:

https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

[10] NQA, «Certificación ISO 27001 - Sistema de seguridad de la información | NQA». Accedido: 3 de diciembre de 2023. [En línea]. Disponible en: https://www.nqa.com/es-mx/certification/standards/iso-27001

[11] D. Romo Villafuerte y J. Valarezo Constante, «Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil», B.S. thesis, 2012.

[12] Labbo, «ISO27002:Buenas prácticas para gestión de la seguridad de la información», OSTEC | Segurança digital de resultados. Accedido: 3 de diciembre de 2023. [En línea]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/

[13] INCIBE, «Plan director de Seguridad».

[14] M. A. Tejena-Macías, «Análisis de riesgos en seguridad de la información», *Polo del conocimiento*, vol. 3, n.º 4, pp. 230-244, 2018.

[15] C. A. Ortega Mora, «Análisis de riesgo de seguridad de la información de la infraestructura informática de la empresa" Cerámica y Ferreteria Ángel Tapia" del cantón Simón Bolívar», B.S. thesis, BABAHOYO: UTB, 2021, 2021.

[16] M. A. Castillo Palma, J. K. Molina Jiménez, y C. Freire, «Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005», Master’s Thesis, ESPOL. FIEC, 2020.

[17] Linkedin, «Las 5 claves para entender y aplicar la ISO/IEC 27005:2022». Accedido: 3 de diciembre de 2023. [En línea]. Disponible en: https://es.linkedin.com/pulse/las-5-claves-para-entender-y-aplicar-la-isoiec