ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TRABAJO DE TITULACIÓN

"DISEÑO DE UN ESQUEMA INTEGRAL DE SEGURIDAD PERIMETRAL BASADO EN UN ANÁLISIS DE RIESGO PARA UNA MEDIANA EMPRESA UBICADA EN LA CIUDAD DE GUAYAQUIL"

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. REINA AZUCENA LÓPEZ MASABANDA

ING. DANIEL FABRICIO PISFIL JORDAN

Guayaquil – Ecuador

2024

AGRADECIMIENTO

A mis maestros, por compartir sus amplios conocimientos con ética y profesionalismo.

A mi tutor de tesis, Ing. Lenin Freire, por su valiosa guía y asesoramiento en las diversas etapas del desarrollo del proyecto.

A mi amigo y compañero de tesis, Daniel Pisfil por su constante respaldo y colaboración durante el desarrollo de este proyecto. Su compromiso y trabajo en equipo fueron fundamentales para superar los desafíos y alcanzar los resultados deseados.

Ing. Reina Azucena López Masabanda.

En primer lugar, a Dios, mi familia y amigos, quienes han sido mi principal fuente de apoyo y motivación. Sus palabras alentadoras y comprensión han sido fundamentales durante este nuevo desafiante viaje académico.

Mi reconocimiento también se extiende a mis compañeros de clase y colaboradores de investigación en especial a mi amiga y compañera de tesis, Reina López. Trabajar codo a codo con ustedes ha enriquecido mi experiencia académica y ha contribuido de manera significativa al éxito de este proyecto.

A mi tutor de tesis, Ing. Lenin Freire, por su valiosa aportación de conocimientos y experiencias en las diversas etapas no tan solo del desarrollo del proyecto sino también en los conocimientos compartidos en su catedra.

Este logro no es solo mío, sino de todos aquellos que, han sido parte de este emocionante viaje académico. Gracias a todos por ser parte de este capítulo en mi vida.

Ing. Daniel Fabricio Pisfil Jordán

DEDICATORIA

A Dios por ser la guía en esta etapa académica y darme la fortaleza necesaria para continuar aun en los momentos más difíciles.

A mis queridos padres Reina y Eliaquín, mi más sincero agradecimiento, ya que gracias a su amor incondicional y apoyo inquebrantable no me permitieron rendirme. A través de su ejemplo, dedicación y sacrificio me han inspirado a perseguir mis metas y sueños con determinación, esfuerzo y trabajo duro.

A mis queridas hermanas, Margarita, Andrea y Laura, por su infinita paciencia y amor incondicional. Su apoyo constante ha sido un recordatorio invaluable de la importancia de celebrar los logros junto a la familia.

En memoria de mi querida abuela Margarita.

Ing. Reina Azucena López Masabanda.

A Dios y mis padres, Manuel Pisfil y Esther Jordán, cuyo amor incondicional y sacrificios han sido mi fuente constante de inspiración. Sus valores y correcciones han sido la fuerza impulsora detrás de cada logro en mi vida.

A mi esposa, Jessenia Burgos, por ser mi compañera constante en este viaje. Tu amor, paciencia, aliento y comprensión han hecho posible superar los desafíos académicos.

A mis hijos, Daniela, Danna y Daniel, quienes, a pesar de mi ausencia en muchos momentos, siempre han sido mi razón para esforzarme por ser mejor.

Esta tesis es el resultado de la contribución de muchas personas que han dejado una marca permanente en mi viaje académico como lo es mi amiga y compañera Reina López. A todos ustedes, mi más profundo agradecimiento y dedicación.

Ing. Daniel Fabricio Pisfil Jordán

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO
FREIRE COBO

M.SC. LENIN EDUARDO FREIRE COBO

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA
PLUA

M.SC. JUAN CARLOS GARCÍA PLÚA

REVISOR

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

(Reglamento de graduación de la ESPOL)

Firmado electrónicamente por:
REINA AZUCENA LOPEZ MASABANDA

ING. REINA AZUCENA LÓPEZ MASABANDA

Firmado electrónicamente por:
DANIEL FABRICIO PISFIL JORDAN

ING. DANIEL FABRICIO PISFIL JORDÁN

RESUMEN

El presente trabajo de titulación se centra en el diseño de un esquema integral de seguridad perimetral para una mediana empresa ubicada en la ciudad de Guayaquil, donde se busca desarrollar una estrategia de seguridad robusta y adaptada a las necesidades específicas de la empresa, basada en un análisis de riesgo.

Este análisis incluye la identificación de amenazas tanto internas como externas, así como la evaluación de vulnerabilidades en la infraestructura física y digital de la empresa. Al abordar estos aspectos, este trabajo de titulación busca proporcionar una solución integral que no solo proteja los activos de la empresa, sino que también garantice la continuidad operativa y la confianza de los clientes y empleados. Además, explora el impacto económico de implementar estas medidas de seguridad y cómo se puede lograr un equilibrio entre costos y beneficios para asegurar una inversión sostenible en la protección de la empresa.

También se pretende establecer una cultura de seguridad dentro de la organización, donde todos los niveles del personal estén conscientes de las políticas y procedimientos de seguridad, y sean capaces de actuar de manera proactiva ante cualquier incidente.

ÍNDICE GENERAL

ABREVIATURAS Y SÍMBOLOS

ISO Organización Internacional de Estandarización, en inglés International Organization for Standarization.

IEC Comisión electrotécnica internacional, en inglés International Electrotechnical Comission.

SGSI Sistema de Gestión de Seguridad de la Información.

DDoS ataque distribuido de denegación de servicio, en ingles Distributed Denial of Service

IDS Sistema de detección de intrusos, en inglés Intrusion Detection System.

IPS Sistema de prevención de intrusos, en ingles Intrusion Prevention System.

ISP Proveedor de Servicio de Internet, en inglés Internet Service Provider.

MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

De acuerdo con la era tecnológica en la actualidad, las empresas por más pequeñas que sean necesitan estar interconectados con el mundo exterior, tanto así que se ha vuelvo dependiente de la tecnología. Al existir estas necesidades de conexiones externas hace que desarrolladores de amenazas cibernéticas también se acrecienten, lo que exige a todos los campos a desarrollar e implementar estrategias de seguridad que ayuden a salvaguardar los activos que ellos poseen.

En este sentido, el presente estudio aborda el desafío específico de diseñar un esquema integral de seguridad perimetral, basado en un análisis de riesgo, destinado a fortalecer la postura de seguridad de una mediana empresa ubicada en la ciudad de Guayaquil reconociendo la singularidad de su entorno operativo. A través de un análisis detallado de los riesgos a los que se enfrenta, se buscará no solo identificar las amenazas potenciales, sino también comprender las vulnerabilidades específicas que podrían ser explotadas por actores malintencionados.

La seguridad perimetral, entendida como la defensa de los límites físicos y lógicos de una red, se posiciona como un componente fundamental en la protección contra amenazas externas; sin embargo, el diseño de un enfoque integral y adaptado a las características específicas de una empresa mediana requiere una comprensión profunda de los riesgos inherentes a su operación.

La importancia de una gestión de riesgos eficiente en el ámbito de la seguridad informática no puede subestimarse. La realidad empresarial contemporánea enfrenta amenazas que evolucionan constantemente, desde ciberataques sofisticados hasta la vulnerabilidad inherente a los sistemas

tecnológicos. Es por este motivo que el diseño de un esquema integral de seguridad perimetral para una mediana empresa en Guayaquil se presenta como una respuesta estratégica para mitigar estos riesgos y proteger la integridad, confidencialidad y disponibilidad de la información crítica.

La gestión de riesgos no solo se traduce en la reducción de la probabilidad de pérdida, robo o corrupción de datos, sino que también implica salvaguardar la continuidad operativa de la empresa. La disponibilidad constante de la información es esencial para garantizar la ejecución fluida de los procesos del negocio, así como para mantener la confianza de los clientes y socios comerciales.

Además, la investigación se orientará hacia la proposición de estrategias de mitigación prácticas y efectivas que se alineen con las necesidades y recursos de la empresa en cuestión. La implementación de un esquema de seguridad perimetral no solo se considerará como una barrera de defensa, sino como una inversión estratégica para fortalecer la resiliencia de la empresa frente a los desafíos cibernéticos emergentes.

En resumen, este estudio se posiciona como un aporte significativo al campo de la seguridad informática, no solo al proponer un marco integral de seguridad perimetral, sino al hacerlo con un enfoque adaptado a las condiciones específicas de una mediana empresa en Guayaquil. La gestión de riesgos se convierte así en un elemento clave para el desarrollo sostenible de las operaciones empresariales en un entorno digitalmente desafiante.

CAPITULO I

GENERALIDADES

1.1. Antecedentes

En el actual entorno empresarial altamente digitalizado, caracterizado por una exposición constante a una variedad de amenazas cibernéticas, la implementación de un sólido esquema de seguridad perimetral se convierte en una necesidad imperativa. Las empresas, independientemente de su tamaño, se enfrentan a una creciente diversidad de amenazas cibernéticas que pueden causar un daño significativo a sus operaciones y su reputación. A menudo, estas empresas almacenan información crítica y valiosa que resulta atractiva para ciberdelincuentes, lo que hace que la protección de estos activos sea esencial para garantizar la continuidad de las operaciones. La constante evolución de las amenazas cibernéticas, como el malware, la suplantación de identidad y los ataques de “ransomware”, exige una respuesta proactiva en la gestión de la seguridad de la información [1]. En este contexto, un sólido esquema

de seguridad perimetral desempeña un papel fundamental al actuar como un escudo protector en torno a la infraestructura empresarial, previniendo, detectando y mitigando amenazas cibernéticas. Además de asegurar la continuidad de las operaciones, también protege la reputación de la empresa y fomenta la confianza de los clientes al demostrar un firme compromiso con la seguridad de la información.

Para enfrentar todas estas amenazas, es fundamental que las empresas protejan sus activos críticos siguiendo estándares y mejores prácticas internacionalmente reconocidos en la gestión de la seguridad de la información, como es el caso de la norma ISO 27001 [2]. Esta norma, con su enfoque en el análisis de riesgos, se convierte en un pilar esencial para el desarrollo de un esquema de seguridad perimetral eficaz. Al adoptar un enfoque sistemático y estructurado para aplicar el análisis de riesgo basado en ISO 27001, se logra una comprensión profunda y precisa de las amenazas específicas que acechan a la empresa, así como de las vulnerabilidades presentes en su infraestructura perimetral. Esto, a su vez, permite la toma de decisiones informadas y la selección de elementos de seguridad perimetral adecuados, como firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones y filtros de contenido, que resultarán eficaces en la mitigación de los riesgos. De esta manera, se logra una infraestructura de seguridad perimetral que responde a las necesidades y amenazas específicas de la organización, contribuyendo a la salvaguardia de activos críticos, al mantenimiento de la confidencialidad y la integridad de los datos, y a la continuidad de las operaciones en un entorno empresarial en constante digitalización y con amenazas cibernéticas en evolución.

La aplicación del análisis de riesgo basado en la norma ISO 27001 implica una evaluación minuciosa de las amenazas, vulnerabilidades y activos críticos de la organización, lo que permite la identificación precisa de los riesgos que podrían poner en peligro la seguridad de la información [3]. Esto garantiza que la infraestructura de seguridad perimetral se ajuste a las necesidades y

amenazas específicas de la organización, lo que, a su vez, contribuye a la protección de activos críticos, la preservación de la confidencialidad y la integridad de los datos, y la garantía de la continuidad de las operaciones en un entorno empresarial que está experimentando una creciente digitalización y una constante evolución de las amenazas cibernéticas.

En resumen, este proyecto propone a los directivos de la organización realizar un análisis de riesgo para establecer procesos y políticas sólidas de seguridad, evitando que las amenazas detectadas se materialicen y permitiendo reducir el impacto de los riesgos detectados o mantenerlos bajo control. Un adecuado esquema de seguridad perimetral es de vital importancia para cualquier organización en la era digital, ya que actúa como la primera línea de defensa contra una amplia gama de amenazas cibernéticas, protegiendo activos críticos y mitigando amenazas como ataques de denegación de servicio, intrusiones maliciosas y suplantación de identidad, además de garantizar la continuidad de las operaciones y salvaguardar la reputación de la organización [4].

1.2. Descripción del Problema

Una mediana empresa ubicada en la ciudad de Guayaquil, especializada en la comercialización de materiales de construcción, ha experimentado un crecimiento constante durante sus 15 años en el mercado. Sin embargo, la falta de procesos y políticas sólidas de seguridad ha dejado a la organización vulnerable a diversas amenazas.

Actualmente la empresa no cuenta con procesos de seguridad establecidos, los cuales puede dejar a la organización vulnerable a amenazas cibernéticas. Sin controles adecuados, existe un mayor riesgo de sufrir brechas de seguridad, ataques de “malware”, robo de datos y otros incidentes. Adicional no se cuenta con un plan de actualización continua de equipos

pertenecientes a la infraestructura de seguridad, esto los expone a posibles vulnerabilidades existentes pudiendo dejar el dispositivo vulnerable a “exploits” conocidos.

Además de poner en riesgo la integridad de la empresa, la falta de sólidos procesos de seguridad también desmejora la confianza de los clientes y disminuye su reputación en el mercado. Esto conlleva la posibilidad de perder a clientes existentes y enfrentar dificultades para atraer nuevos. Proteger la información sensible y garantizar la confidencialidad de los datos de los clientes son pilares esenciales en la gestión de cualquier empresa.

1.3. Solución Propuesta

La realización de un análisis de riesgo como un modelo que ofrece la posibilidad de prevenir costos innecesarios, asociados a medidas de seguridad que resultan de una evaluación subjetiva de riesgos [5]. Este enfoque disminuye el tiempo requerido por un experto en seguridad de la información al contar con un método establecido de análisis.

Este estudio tiene como objetivo principal llevar a cabo un análisis de riesgo para identificar las vulnerabilidades y amenazas relacionadas con los procesos internos de la empresa. Para realizar este análisis de riesgo, hemos optado por la norma ISO 27001:2013. Esta elección se basa en su reconocimiento internacional y respeto en el campo de la seguridad de la información, así como en su capacidad para cumplir con normativas y expectativas globales, lo que puede ser atractivo si la empresa tiene como objetivo futuro extender sus operaciones con clientes en el extranjero. Además, este estándar proporciona un enfoque integral para la gestión de la seguridad de la información, abarcando no solo aspectos técnicos, sino también organizativos, de personal y procesos, lo que garantiza una gestión completa de la seguridad.

Después de recopilar la información necesaria utilizando la norma ISO 27001:2013, procederemos a elaborar el análisis de riesgo siguiendo un proceso que analizará el estado actual de la empresa:

- Establecimiento del contexto
- Identificación de activos
- Identificación de amenazas
- Evaluación de vulnerabilidades
- Evaluación de riesgos
- Tratamiento de riesgos
- Documentación

A partir de este análisis de riesgo, desarrollaremos un diseño de seguridad perimetral con el objetivo de abordar y minimizar las brechas de seguridad identificadas. Un esquema de seguridad perimetral sólido y bien diseñado es fundamental para proteger a una empresa de las amenazas cibernéticas y asegurar su continuidad operativa, reputación y relaciones comerciales. Este enfoque proactivo en la seguridad informática permitirá a la empresa fortalecer sus procesos internos, garantizando la confidencialidad, integridad y disponibilidad de la información y protegerá los intereses tanto de la empresa como de sus clientes.

Mantener un esquema de seguridad perimetral es esencial en el entorno actual debido al aumento constante de las amenazas cibernéticas y la necesidad de salvaguardar los activos de información y sistemas de una organización.

1.4. Objetivo General

Diseñar un esquema de seguridad perimetral en base a los estándares y normas de calidad 27001:2013 por medio de un análisis de riesgo, para una mediana empresa dentro de la ciudad de Guayaquil.

1.5. Objetivo Específico

- Identificar las vulnerabilidades y amenazas en los activos de información críticos de la empresa.
- Evaluar los riesgos en base a los hallazgos obtenidos durante la identificación de vulnerabilidades y amenazas.
- Diseñar esquema de seguridad y políticas de seguridad perimetral para proteger los activos críticos y mitigar los riesgos cibernéticos

1.6. Metodología

Para este trabajo se efectuará un estudio no experimental transversal basado en entrevista e información documentada. Se realizará un muestreo por conveniencia debido a que es necesario entrevistar a las personas involucradas en el proceso de facturación y ventas.

Como instrumentos se utilizarán entrevistas semiestructuradas presenciales a los participantes para obtener información más detallada del proceso. Adicional, el presente documento será respaldado con información documentada proporcionada por los directivos de la organización.

Con los datos recopilados efectuaremos un análisis cualitativo de la información obtenida para poder conocer cómo se efectúan los procesos de manera actual.

Una vez finalizada la etapa de entrevistas y levantamiento de información, con todos los datos obtenidos se espera identificar los activos, las amenazas y las vulnerabilidades a la cual está expuestos actualmente, es decir en este punto ya tendremos una visión más amplia de las posibles brechas de seguridad existentes.

Luego se efectuará el cálculo de los riesgos ya plenamente identificados, dando como resultado una matriz de riesgos que clasifica los riesgos en función de su gravedad. Obteniendo la matriz procederemos a priorizar los riesgos en función de su nivel de riesgo, lo que ayuda a determinar cuáles necesitan una atención inmediata.

Finalmente, seleccionaremos las medidas de control pertinentes que pueden mitigar, reducir o eliminar los riesgos.

Posterior al análisis de riesgo efectuado, se diseñará en esquema de seguridad perimetral tomando en consideración todas las brechas de seguridad ya detectadas en el análisis previo buscando proteger los activos y la infraestructura de una organización de amenazas externa.

CAPÍTULO II

MARCO TEÓRICO

2.1. Introducción a la Seguridad Informática

La seguridad informática desempeña un papel esencial en la actualidad, especialmente para las medianas empresas que, a pesar de su tamaño, se enfrentan a una creciente cantidad de amenazas cibernéticas que pueden tener un impacto devastador en sus operaciones y su reputación. Estas empresas, al igual que las grandes corporaciones, almacenan datos e información valiosa que resulta atractiva para los ciberdelincuentes. En este contexto altamente digitalizado, la implementación de un sólido esquema de seguridad informática se ha vuelto de vital importancia.

La creciente complejidad de las amenazas, como el “malware”, la suplantación de identidad y los ataques de “ransomware”, exige que las empresas adopten enfoques proactivos en la gestión de la seguridad de la información. Un esquema de seguridad informática efectivo actúa como un

escudo protector alrededor de la infraestructura de la empresa, previniendo, detectando y mitigando amenazas cibernéticas. Además, contribuye a garantizar la continuidad de las operaciones, protege la reputación de la empresa y fomenta la confianza de los clientes al demostrar un compromiso con la seguridad de la información.

En un entorno empresarial en constante evolución, las medianas empresas no pueden permitirse pasar por alto la importancia de la seguridad informática. Este factor se ha convertido en un elemento crítico para el éxito y la supervivencia de las organizaciones en la era digital. Este informe abordará en detalle la relevancia de la seguridad informática en el contexto de las medianas empresas y explorará cómo estas organizaciones pueden implementar medidas efectivas para proteger su infraestructura y datos contra las crecientes amenazas cibernéticas.

2.1.1. Definiciones

Vulnerabilidad. - se define como una debilidad o falla en el diseño, sistema, aplicación, red, procedimientos o recursos, no anticipada durante el desarrollo de la solución existente, que puede ser aprovechada por agentes malintencionados para comprometer la integridad, confidencialidad o disponibilidad de la información [6].

La detección tardía de una vulnerabilidad proporciona a las amenazas la oportunidad de materializarse, afectando así al sistema involucrado. El tratamiento adecuado de las vulnerabilidades es de vital importancia para garantizar la seguridad y la integridad de los sistemas de información. Tratar de manera proactiva estas debilidades, no solo reduce el riesgo de ataques cibernéticos, sino que también protege la confidencialidad de la información, preserva la integridad de los datos y asegura la disponibilidad continua de los recursos críticos.

Amenaza. - se refiere a cualquier circunstancia, evento o entidad que tiene el potencial de comprometer la seguridad de un sistema, red, aplicación o información. Las amenazas pueden ser diversas y pueden incluir desde ataques cibernéticos perpetrados por hackers, virus informáticos, y malware, hasta factores externos como desastres naturales o fallas en el hardware. Identificar y comprender las amenazas es crucial para desarrollar estrategias efectivas de seguridad, ya que permite implementar medidas preventivas y de mitigación para proteger los activos digitales y garantizar la continuidad operativa [6].

Riesgo. - Se refiere a la posibilidad de que eventos no deseados o amenazas afecten la confidencialidad, integridad o disponibilidad de los sistemas de información. Este riesgo es el resultado de la interacción entre las amenazas, las vulnerabilidades presentes en un sistema y los impactos potenciales de un incidente de seguridad.

Las amenazas en seguridad informática pueden incluir ataques cibernéticos, malware, accesos no autorizados, pérdida de datos y otros eventos que podrían comprometer la seguridad de la información. Las vulnerabilidades son debilidades en sistemas, aplicaciones o procesos que podrían ser explotadas por amenazas para llevar a cabo ataques [6].

2.1.2. Pilares de la Seguridad

La información constituye un activo crítico que permite el funcionamiento de las organizaciones en la era digital. Su gestión y protección adecuadas no solo son esenciales

para el desarrollo continuo de las operaciones internas, sino que también influyen directamente en la confianza de clientes, proveedores y directivos. La confidencialidad, asegurando que la información sensible esté resguardada contra accesos no autorizados; la integridad, que garantiza la exactitud y coherencia de los datos; y la disponibilidad, asegurando que la información esté accesible cuando sea requerida, constituyen los pilares fundamentales de la seguridad de la información. Estos principios no solo buscan prevenir amenazas y ataques, sino que también se orientan a establecer un entorno de confianza, donde la información actúa como un recurso fiable y valioso para respaldar las decisiones estratégicas y operativas. En este entorno digital dinámico, la protección de estos pilares se convierte en un imperativo para preservar la integridad de la organización y fortalecer su posición en un mundo empresarial altamente competitivo y digitalizado.

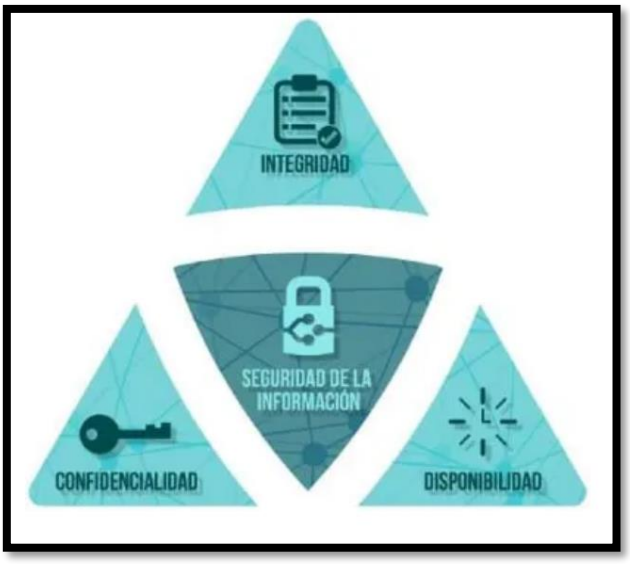


Figura 1: Pilares de la seguridad de la información [7]

En la figura 1 podemos observar los pilares de la seguridad informática los cuales serán descritos de manera detallada a continuación:

Confidencialidad. – Se refiere a proteger y restringir el acceso a información sensible o confidencial del uso indebido. Su principal objetivo es asegurar que la información sólo esté disponible para que el personal autorizado pueda efectuar sus funciones [8].

Para garantizar la confidencialidad se pueden aplicar diversas estrategias como autenticar acceso a plataformas para llevar trazabilidad de los accesos a sistemas, gestionar usuarios con privilegios específicos, desarrollar políticas de privacidad claras sobre manejo, almacenamiento y distribución de información confidencial, implementar medidas de acceso físico a lugares donde se encuentre información sensible, como por citar diversas medidas que se pueden aplicar para garantizar la confidencialidad.

Integridad. – Implica mantener la coherencia, precisión y confiabilidad de la información y los datos durante todo su ciclo de vida. Se define como el mecanismo que garantiza que el intruso no pueda modificar los datos que son enviados a través de la red [8].

Es importante considerar que para garantizar una información integra es necesario un monitoreo constante para descubrir posibles intrusos en la red e implementar políticas internas para poder manejar una trazabilidad de los sistemas [9].

La integridad es esencial para la toma de decisiones informada y la confianza en la información crítica. Al mantener la integridad, una organización puede garantizar la precisión y confiabilidad de sus datos, lo que contribuye a operaciones eficientes y toma de decisiones acertadas.

Disponibilidad. – Su principal objetivo es garantizar que los recursos de información y sistemas asociados se encuentren accesibles y operativos cuando los usuarios que cuenten con los permisos adecuados lo necesiten [8]. La disponibilidad es una característica fundamental para una implementación exitosa de sistemas digitales y redes. Los equipos

o software de seguridad adicionales, como firewalls y servidores proxy, pueden proteger contra tiempos de inactividad y datos, información y programas inalcanzables debido a actividades maliciosas, como ataques cibernéticos de denegación de servicio (DoS) e intrusiones en la red [9].

2.2. Sistema de Gestión de Seguridad de da Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque integral y sistemático diseñado para la administración integral de la seguridad de la información en una empresa. Su principal propósito consiste en asegurar la confidencialidad, integridad y disponibilidad de la información. En relación con su metodología, busca gestionar de manera efectiva los riesgos vinculados a la seguridad de la información mediante la implementación de políticas, procedimientos y controles pertinentes. Este sistema proporciona un marco estructurado que no solo aborda la protección de activos críticos, sino que también aborda dinámicamente los desafíos y riesgos en constante evolución en el ámbito de la seguridad cibernética, asegurando la confianza de las partes interesadas.

La tecnología mejora los procesos internos de manera que estos sean eficientes y se logre una comunicación más interactiva entre una empresa y sus clientes a través del uso de nuevas tendencias tecnológicas. Hace que surja la necesidad de aplicar políticas de controles y procedimientos a seguir, teniendo en cuenta los dos enfoques importantes dentro de toda organización que es la cara ante el cliente externo y el cliente interno, de cómo la tecnología cada vez avanza y con ello también las amenazas [10].

2.2.1. ISO 27001

ISO/IEC 27001, reconocido como el estándar más destacado a nivel mundial para los sistemas de gestión de seguridad de la información (SGSI), establece los requisitos que debe cumplir un SGSI. Este estándar brinda orientación a empresas de diversos tamaños y sectores para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información (SGSI). Obtener la conformidad con ISO/IEC 27001 indica que una organización ha implementado un sistema para manejar los riesgos asociados con la seguridad de los datos que posee o gestiona, asegurando así el cumplimiento de las mejores prácticas y principios establecidos en esta Norma Internacional.

Adicional la ISO 27001, brinda información relevante que puede ayudar al momento de estudiar o implementar, en el cual realiza una introducción muy importante desde su punto de vista, hoy en día como sabemos la ciberdelincuencia cada vez se fortalece haciéndose más severa y sofisticada acrecentándose conforme avanza la tecnología, desarrollando técnicas de cibercrimen muchas veces más avanzadas y difíciles de acaparar [11].

2.2.2. Estadísticas incidentes de seguridad

En el primer informe destacado de la Perspectiva Global de Ciberseguridad se identifica las tendencias y examina los próximos desafíos de ciberseguridad a corto plazo. La rápida transición al trabajo remoto durante la pandemia de COVID-19, combinada con los recientes ciberataques de alto perfil, ha situado la ciberseguridad en el centro de las

preocupaciones de los líderes de toma de decisiones tanto en organizaciones como en naciones [12].

A pesar de los avances, aún queda un trecho por recorrer para alcanzar una comprensión compartida sobre cómo fortalecer la resiliencia cibernética. Tal como se observa en la figura 2, el propósito fundamental de ese informe es proporcionar un análisis exhaustivo de los desafíos que enfrentan los líderes de seguridad, los enfoques que están adoptando para mantenerse a la vanguardia de los ciberdelincuentes y las medidas que están implementando para fortalecer la resiliencia cibernética, no solo dentro de sus propias organizaciones, sino también en el contexto más amplio del ecosistema cibernético.

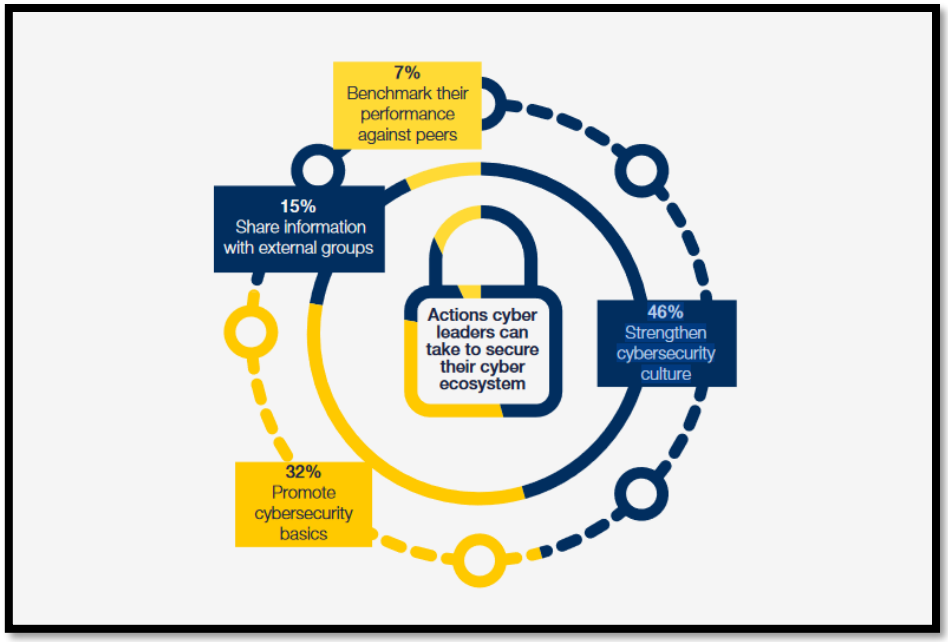


Figura 2: Acciones para un ecosistema seguro en seguridad informática [12].

Cada individuo que forma parte de un sistema cibernético posee la capacidad tanto de contribuir positivamente como de causar daño, debilitando o fortaleciendo el conjunto del

ecosistema digital en el que está inmerso. Se hace imperativo que cada miembro reconozca su papel específico dentro de este entorno, considerando su posición y responsabilidades, con el fin de minimizar las posibilidades y riesgos asociados con interrupciones. Esto implica no solo la protección de los activos digitales, sino también la influencia en la cultura laboral, promoviendo valores que nutran la confianza y la transparencia.

La construcción de confianza y transparencia no solo es esencial para la colaboración efectiva dentro del ecosistema, sino que también constituye la piedra angular de la resiliencia. Al fomentar una cultura donde la confianza sea mutua y la información se comparta de manera transparente, se sientan las bases para que el sistema cibernético sea capaz de resistir y recuperarse de posibles amenazas o eventos disruptivos. En última instancia, la conciencia colectiva de la importancia de estos principios y su aplicación en cada acción individual fortalecerá la seguridad y estabilidad del ecosistema cibernético en su conjunto.

El foro de ISO también da a conocer el reporte sobre Perspectivas de Ciberseguridad Globales del Foro Económico Mundial señala un aumento del 125% en los ciberataques a nivel global durante el año 2021, con indicios que sugieren una tendencia al alza hasta el año 2022. En este contexto de rápida evolución, es crucial que los líderes adopten un enfoque estratégico frente a los riesgos cibernéticos [11].

2.3. Seguridad Perimetral Informática

En el ámbito de la tecnología y la gestión de la información, la Seguridad Perimetral Informática desempeña un papel crucial al establecer la primera línea de defensa contra las amenazas

cibernéticas externas. Este enfoque estratégico implica la implementación de medidas y controles específicos diseñados para proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos desde el perímetro de la red de una organización.

En un entorno empresarial altamente digitalizado y expuesto a diversas amenazas cibernéticas, la implementación de un sólido esquema de seguridad perimetral es esencial. Este enfoque no solo busca prevenir la entrada de amenazas, sino también detectar y mitigar posibles intrusiones y ataques antes de que alcancen los sistemas internos y que causen daño significativo. Además, el análisis de riesgos basado en estándares reconocidos, como la norma ISO 27001, desempeña un papel fundamental en el diseño efectivo de estrategias de seguridad perimetral, asegurando una respuesta proactiva a las amenazas en constante evolución. La seguridad perimetral, por lo tanto, se convierte en una parte integral de la estrategia general de seguridad de la información de una organización, contribuyendo a la protección de activos críticos, la preservación de la confidencialidad y la integridad de los datos, y garantizando la continuidad operativa. Este enfoque estratégico no solo protege los activos digitales críticos, sino que también contribuye a mantener la confianza de los usuarios y clientes al garantizar un entorno en línea seguro y protegido.

2.3.1. Objetivo de la Seguridad Perimetral Informática

La Seguridad Perimetral Informática engloba las acciones y protocolos establecidos para resguardar la red y sistemas de una organización desde su límite exterior o perímetro. Se trata de la primera barrera defensiva ante amenazas externas, como posibles ataques provenientes de Internet o redes externas. La principal finalidad de la seguridad perimetral es prevenir o minimizar ataques potenciales antes de que alcancen a afectar los sistemas

internos, salvaguardando la infraestructura tecnológica de una organización desde sus límites exteriores.

Al establecer barreras efectivas en el perímetro de la red, se busca prevenir, detectar y mitigar posibles amenazas cibernéticas que podrían comprometer la integridad, confidencialidad y disponibilidad de la información. Esta defensa proactiva implica la implementación de firewalls, sistemas de detección de intrusiones, filtrado de contenido y otras medidas para crear un escudo protector alrededor de los activos digitales.

Además de proteger contra ataques externos, la Seguridad Perimetral Informática contribuye a fortalecer la postura general de seguridad de una organización. Al abordar las vulnerabilidades desde el inicio, se minimiza el riesgo de brechas de seguridad y se fomenta un entorno digital más seguro. Este enfoque integral no solo protege la infraestructura tecnológica, sino que también respalda la reputación de la organización al demostrar un compromiso sólido con la seguridad de la información.

Es de vital importancia que las organizaciones se encuentren en continua investigación y actualización para protegerse de las diversas amenazas en constante evolución en el entorno digital. Los ataques cibernéticos evolucionan rápidamente, y las organizaciones deben estar preparadas para enfrentar diversas formas de amenazas. Una de las amenazas más persistentes es la presencia de malware, que puede ingresar a través de correos electrónicos maliciosos, descargas no seguras o sitios web comprometidos [13]. Estos programas maliciosos pueden eludir las defensas perimetrales tradicionales, lo que destaca la importancia de contar con soluciones avanzadas de detección y prevención.

Otro tipo de amenaza importante es la suplantación de identidad, donde los atacantes buscan engañar a los sistemas perimetrales haciéndose pasar por usuarios legítimos. Esto

puede conducir a accesos no autorizados y comprometer la integridad de la información. Además, los ataques de denegación de servicio (DDoS) representan una amenaza significativa al abrumar los recursos de red y afectar la disponibilidad de los servicios [14]. Los atacantes pueden aprovechar la complejidad de la red para ejecutar ataques coordinados y dificultar la mitigación.

La seguridad perimetral también enfrenta riesgos asociados con vulnerabilidades en dispositivos y sistemas. La falta de actualizaciones, parches de seguridad o configuraciones inadecuadas puede dejar puntos de entrada abiertos para los atacantes. Es crucial que las organizaciones implementen medidas proactivas, como análisis de vulnerabilidades y políticas de parches, para fortalecer la seguridad en el perímetro y mitigar las amenazas emergentes.

2.3.2. Plataformas de Seguridad Perimetral Informática

Son conjuntos integrales de herramientas y tecnologías diseñadas para salvaguardar la red y los sistemas de una organización desde su borde exterior. Estas plataformas están diseñadas para proporcionar una defensa robusta contra una amplia variedad de amenazas cibernéticas provenientes del exterior. Incluyen funcionalidades como firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, filtros de contenido y otras medidas de seguridad que trabajan en conjunto para prevenir, detectar y mitigar posibles ataques.

La integración de estas plataformas en la arquitectura de red de una organización permite establecer una primera línea de defensa eficaz, protegiendo la infraestructura interna contra amenazas como *malware*, ataques de denegación de servicio (DDoS), intrusiones

maliciosas y otros riesgos potenciales. Estas plataformas se configuran y personalizan según las necesidades específicas de la organización, proporcionando una estrategia de seguridad coherente y adaptada a sus requisitos particulares. Con la evolución constante de las amenazas cibernéticas, las plataformas de seguridad perimetral informática desempeñan un papel crucial en la protección proactiva de los activos digitales de una organización.

A continuación, se detallan algunos elementos que integran las soluciones de seguridad perimetral.

Firewalls. - Juegan un papel importante en cada sistema de gestión de red para monitorear y definir reglas de seguridad. Un *firewall* correctamente configurado es una herramienta fundamental para fortalecer la postura de seguridad de una red, mitigar riesgos y proteger activos críticos contra amenazas cibernéticas. El firewall actúa como un escudo protector al regular y controlar el tráfico de datos, permitiendo únicamente el acceso autorizado y bloqueando actividades maliciosas potenciales. Esta capacidad es esencial para prevenir intrusiones no deseadas y salvaguardar la integridad de la red frente a amenazas externas.

VPN. - Es una tecnología que permite establecer conexiones seguras y cifradas entre dispositivos a través de una red pública, como Internet. El principal objetivo de una VPN es garantizar la privacidad y seguridad de la comunicación, especialmente cuando se accede a recursos en línea desde ubicaciones remotas. Al utilizar protocolos de cifrado robustos, una VPN crea un "túnel" seguro que protege la información transmitida, impidiendo que terceros no autorizados accedan o intercepten los datos. Una VPN

proporciona un alto nivel de seguridad al cifrar el tráfico de datos, lo que resulta fundamental al transmitir información confidencial o acceder a redes empresariales desde lugares externos. La implementación de una VPN es una estrategia efectiva para garantizar la seguridad, privacidad y accesibilidad en las comunicaciones digitales.

Sistemas De Detección y/o Prevención De Intrusión (IDS/IPS). - son herramientas fundamentales en la seguridad informática que se encargan de monitorear y analizar el tráfico de red en busca de actividades sospechosas o comportamientos maliciosos. El IDS identifica posibles amenazas y emite alertas cuando detecta patrones de actividad que podrían indicar un ataque, mientras que el IPS tiene la capacidad adicional de tomar medidas preventivas, como bloquear o filtrar el tráfico malicioso. Estos sistemas pueden identificar patrones de comportamiento anómalos o firmas específicas de ataques conocidos, permitiendo una respuesta rápida y proactiva ante posibles amenazas. Además, al contar con capacidades de prevención, los IPS pueden bloquear automáticamente el tráfico malicioso, protegiendo la red contra ataques en tiempo real. En resumen, la implementación de sistemas IDS/IPS fortalece la postura de seguridad de una organización al brindar detección temprana y medidas preventivas contra posibles intrusiones.

Control de Acceso y autenticación adaptiva. - Se traduce en una experiencia de inicio de sesión personalizada para usuarios con distintos niveles de riesgo [15]. Aquellos con riesgo bajo simplemente utilizan la autenticación de dos factores (2FA) mediante un código SMS o correo electrónico. En cambio, los usuarios de riesgo alto acceden a sus cuentas a través

de un escáner biométrico, elevando así el nivel de seguridad y asegurando que se adapte de manera flexible a la evaluación de riesgo, garantizando una protección adecuada para cada usuario.

La autenticación adaptiva esta es configurada como un enfoque altamente versátil para la implementación de la autenticación de dos factores (2FA) y la autenticación de múltiples factores (MFA). Este método se distingue por su capacidad para adaptar los niveles de seguridad a los riesgos específicos a los que un usuario puede estar expuesto.

En lugar de depender de un conjunto estático de factores de autenticación, la autenticación adaptativa evalúa y ajusta dinámicamente los métodos de verificación según las variables de riesgo asociadas al comportamiento y contexto del usuario.

Mediante la autenticación adaptativa, los sistemas de seguridad pueden personalizar la experiencia de autenticación para cada individuo, aprovechando diversos factores, como la ubicación geográfica, el dispositivo utilizado o el historial de acceso. Esta flexibilidad no solo optimiza la seguridad, sino que también garantiza una experiencia de usuario más fluida al adaptarse de manera inteligente a las condiciones específicas, asegurando así un equilibrio eficiente entre protección y comodidad.

Anti DDOS. - Los ataques de denegación de servicio (DoS) representan una amenaza significativa en la actualidad de Internet, siendo los (DDoS) los más preocupantes en el ámbito informático debido a su capacidad para causar daños severos. Estos ataques pueden agotar rápidamente los recursos de computación y comunicación de sus objetivos sin previo aviso de manera que estos podrían volverse inoperantes durante dichos

ataques. Para abordar este problema, se han propuesto diversos mecanismos de defensa que ayuden de alguna manera a poder contrarrestarlos.

En la figura 3 se observa el flujo de un ataque DDoS o de denegación de servicio distribuido, este tipo de ciberataque busca inutilizar un sitio web o recurso de red inundándolo con tráfico malicioso, impidiendo su funcionamiento adecuado. En este tipo de ataque, el agresor abruma el objetivo con tráfico no deseado de Internet, bloqueando el acceso del tráfico legítimo a su destino previsto. En términos más detallados, se puede comparar a un ataque DDoS o DoS con un congestionamiento de tráfico repentino causado por numerosas solicitudes falsas generadas a partir de un ataque. Aunque estas solicitudes parecen legítimas no son más que un engaño que provocan la pérdida del flujo correcto de tráfico.

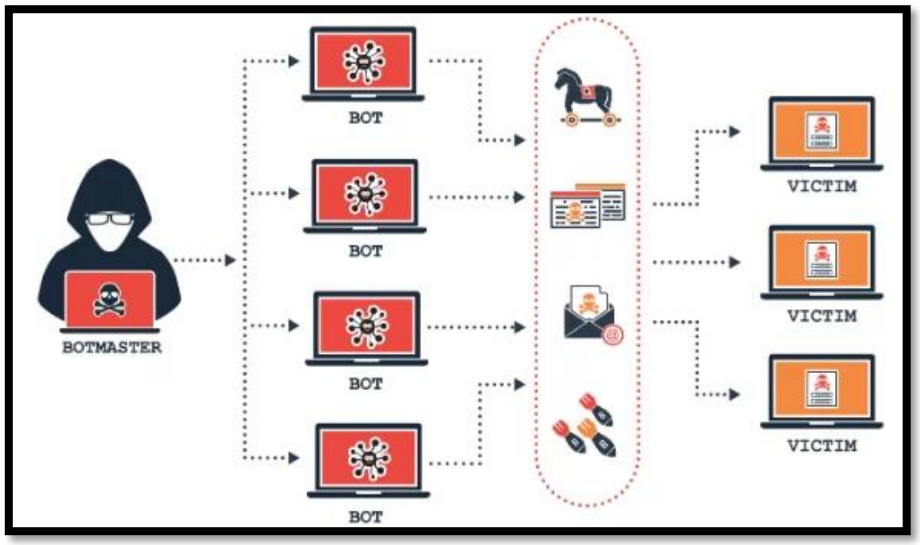


Figura 3: Descripción ataque DDos [16]

Antivirus/Antispam. **-** Un antivirus, ya sea en forma de programa o dispositivo, es una herramienta esencial para salvaguardar la integridad de computadoras y otros dispositivos

al prevenir posibles amenazas de virus que podrían comprometer tanto el software como el hardware de un dispositivo, poniendo en riesgo la información almacenada en el mismo. La función principal de un antivirus es la detección de posibles virus, incluso aquellos que han sido diseñados para evadir detección, con el objetivo de evitar su infiltración en los sistemas de usuarios. El antivirus busca impedir que estos agentes maliciosos accedan a los equipos, alteren archivos y generen errores en el sistema operativo de los dispositivos mediante la identificación proactiva de operaciones potencialmente perjudiciales para la integridad de la información o del propio dispositivo.

Un programa de ciberseguridad conocido como Antispam se encarga de resguardar los sistemas informáticos contra virus que buscan ingresar al sistema operativo mediante correos electrónicos no solicitados, comúnmente llamados Spam. Es necesario la implementación de filtros Antispam que permita evaluar cualquier intento que desee perjudicar o causar daño, el propósito será el prevenir que un dispositivo se vea afectada por virus maliciosos o se vean abrumadas por grandes volúmenes de correos electrónicos no deseados, los cuales pueden contener contenido perjudicial y puedan ser eficientemente eliminados para evitar los daños mencionados.

El SPAM se define como el envío masivo de correos electrónicos no solicitados, comúnmente conteniendo publicidad de productos, servicios, o páginas web [17]. También menciona que, en la actualidad, se estima que entre el 60% y el 80% de los correos electrónicos enviados se clasifican como SPAM, una cifra que destaca la magnitud de esta práctica intrusiva. Esta forma de comunicación no deseada no solo afecta la experiencia del usuario, sino que también tiene repercusiones negativas para las empresas que la emplean, ya que la saturación de bandejas de entrada y la irritación de los receptores pueden dañar la reputación de la marca y reducir la efectividad de las

campañas de marketing legítimas. En consecuencia, el SPAM no solo representa un inconveniente para los destinatarios, sino también un riesgo y una desventaja para aquellos que recurren a esta táctica de forma indiscriminada.

Tal como se observa en la figura 4, en el transcurso del año 2022, se observó una reducción en los incidentes y vulnerabilidades dentro de la industria de ISP y Carrier, así como en los ámbitos de comercio y servicios [18]. Este declive puede atribuirse a las medidas de gestión de incidentes y vulnerabilidades implementadas por los proveedores de servicios en beneficio de sus suscriptores. No obstante, las pequeñas y medianas empresas (pymes) continúan presentando la mayor cantidad de vulnerabilidades, lo que resulta en un aumento de los incidentes. Esta tendencia se explica principalmente por la falta de personal especializado en seguridad y ciberseguridad en estas empresas, a diferencia de las organizaciones de mayor tamaño.

Figura 4: Reporte de Tráfico malicioso, aumento de ataques DoS en 2022 [18]

CAPÍTULO III

LEVANTAMIENTO DE INFORMACIÓN

3.1. Establecimiento del contexto de la organización.

Para el desarrollo de este estudio se ha trabajado con una organización dedicada a la comercialización de materiales de construcción, debido a la naturaleza de su operación la organización maneja información delicada proveniente tanto de clientes como de proveedores.

A través de una entrevista con el Gerente de la empresa, se ha definido claramente el alcance de este análisis de riesgo. Se ha acordado que el estudio se enfocará de manera exclusiva en todos los componentes de la red, abarcando tanto hardware como software, que forman parte de la seguridad perimetral en la infraestructura actual de la empresa. Se establece que los clientes, tanto internos como externos, son considerados partes interesadas en este análisis de riesgo.

3.2. Identificación de activos de información de la empresa

En el proceso de identificación de activos de información, se realizaron entrevistas al personal del departamento de sistemas. De forma conjunta, se ha determinado los elementos de la Tabla 1 los que constituyen activos de información y están directa o indirectamente vinculados a aspectos relacionados con la seguridad perimetral de la empresa.

Tabla 1: Activos de la empresa.

TIPO DE ACTIVO	DESCRIPCIÓN	CANTIDAD
HW	Equipo de cómputo	12
HW	Cámara IP	8
HW	Teléfono análogo	8
HW	Switch Tplink interno 16 puertos	3
HW	Router propiedad del ISP	2
HW	Router WIFI	1
HW	Firewall interno Fortigate 100D	1
HW	Server Linux base de datos	1
HW	Server Linux correo electrónico	1
HW	Impresora	1
HW	NVR Hikivision	1
HW	PBX análogo	1
	TOTAL	**40**

3.3. Identificación de amenazas a las cuales están expuestas actualmente

En el proceso de identificación de amenazas, vulnerabilidades y valoración de riesgos, se ha empleado la metodología MAGERIT. Esta metodología se destaca como una de las más ampliamente utilizadas en la administración de riesgos de activos de información. Proporciona un enfoque estructurado y orientación para implementar las mejores prácticas en términos de gestión de riesgos en las organizaciones.

A través de la utilización del catálogo de amenazas de MAGERIT, hemos identificado las posibles amenazas que podrían impactar los activos pertenecientes a la seguridad perimetral de la

organización. Es crucial tener en cuenta que no todas las amenazas tienen el mismo potencial de afectar a todos los activos, y esta consideración ha sido parte integral del análisis efectuado.

En la Tabla 2 podemos verificar todas las amenazas a las cuales se encuentran expuestas los activos de la empresa.

Tabla 2: Matriz de amenazas.

ORIGEN	AMENAZA
De origen industrial	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
Errores y fallos no intencionados	[E.3] Errores de monitorización
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Ataques Intencionados	[A.3] Manipulación de los registros de actividad
	[A.4] Manipulación de la configuración
	[A.11] Acceso no autorizado
	[A.22] Manipulación de los equipos
	[A.23] Manipulación de los equipos
	[A.25] Robo

Para verificar el desglose detallado de las amenazas que podrían afectar a cada activo dirigirse al Anexo C.

3.4. Identificación de vulnerabilidades

Una vez identificadas las amenazas a las cuales están expuestas los activos, en conjunto con los propietarios de estos, se ha detallado las vulnerabilidades a las cuales están expuestos a cada uno de los activos inventariados.

Estas vulnerabilidades fueron identificadas a través de entrevistas realizadas al personal dueño del activo, así como al personal del departamento de sistemas. Durante este proceso, se validaron los controles actualmente implementados y se identificaron las brechas de seguridad existentes.

Para verificar el desglose detallado de las vulnerabilidades que podrían afectar a cada activo dirigirse al Anexo D.

3.5. Identificación de riesgos

La identificación de riesgos en una empresa es un paso fundamental para comprender y gestionar los posibles eventos que puedan afectar sus operaciones y objetivos. Para identificar los riesgos a los cuáles están expuestos bajo la infraestructura actual, se ha efectuado una evaluación sistemática de los activos críticos, las amenazas potenciales y las vulnerabilidades existentes. Durante las entrevistas y el proceso de recopilación de información, se detectaron posibles riesgos entre los diversos componentes de la red, a raíz de las vulnerabilidades identificadas los cuales están detallados en la Tabla 3.

Estos hallazgos acentúan la importancia de abordar proactivamente las debilidades en la infraestructura, permitiendo la implementación de medidas de seguridad efectivas para mitigar estos riesgos potenciales.

Tabla 3: Hallazgo en red interna

N°	DISPOSITIVO	HALLAZGOS
1	Firewall interno Fortigate 100D	No existe almacenamiento de logs ante eventos de seguridad. Usuarios de administración genéricos. Políticas de seguridad obsoletas o no identificadas. Firmware desactualizado. Equipo fuera de soporte.
2	Switch Tplink interno 16 puertos	Equipo no administrable sin posibilidad de configuración de *port security*. Todos los puertos habilitados. Equipo sin respaldo eléctrico
3	Router WIFI	No existe segmentación entre red de servidores, usuarios internos y visitantes. Políticas de seguridad no configuradas adecuadamente. SSID único para todos los usuarios
4	Server Linux base de datos	No poseen políticas de gestión de usuarios y contraseñas. No poseen política de verificación de parches de seguridad y actualizaciones disponibles Usuarios LAN, WIFI e invitados con conectividad ICMP. Sucursal con conexión remota insegura a server. No existe almacenamientos de logs ante eventos de seguridad. Política de seguridad configuradas para server en el firewall débiles para restringir el tráfico entrante y saliente. No existen copias de seguridad recientes ni políticas de respaldo definida. Copias de seguridad accesibles y sin encriptación.
5	Server Linux correo electrónico	No poseen políticas de gestión de usuarios y contraseñas. No poseen política de verificación de parches de seguridad y actualizaciones disponibles Usuarios LAN, WIFI e invitados con conectividad ICMP. No existe almacenamientos de logs ante eventos de seguridad. No existen copias de seguridad recientes ni políticas de respaldo definida. Copias de seguridad accesibles y sin encriptación.
6	Equipo de cómputo	Licencias de sistema operativo expiradas o no licenciados. Antivirus no licenciado. Máquinas sin contraseña. Bloqueo de pantalla ante inactividad no configurado. Puertos USB habilitados a todos los usuarios. Aplicaciones no autorizadas. Usuarios con privilegios de administrador. Máquinas desatendidas por usuarios.

N°	DISPOSITIVO	HALLAZGOS
7	Cámara IP	Cámara accesible para todos los usuarios desde la LAN interna. Usuario por defecto aun habilitado. Firmware desactualizado. Varios equipos descontinuados por la marca. (End of life) Equipos con fecha y hora incorrecta.
8	NVR Hikivision	NVR accesible desde el mundo. Claves por default habilitadas. No existe política de cambio de clave. Usuarios no autorizados con acceso a NVR. No existe política de acceso a NVR. Ubicación física de NVR inadecuada. Usuarios locales con acceso al NVR. Equipo NVR descontinuado por la marca (End of life)
9	Impresora	Todos los usuarios tienen acceso a la impresora.
10	PBX análogo	No existe almacenamiento de logs ante eventos de seguridad.
11	Teléfono análogo	Usuarios con privilegios de llamadas internacionales.
12	Router propiedad del ISP	Puertos disponibles con salida a internet

Al realizar entrevistas con personal clave, revisar procesos y evaluar el entorno empresarial, se obtuvo el siguiente análisis de brecha el cual permite identificar escenarios de riesgo actuales, desde ciber amenazas, hasta factores externos como eventos. En la figura 5 tenemos el resumen del análisis de brecha donde se visualiza el estatus actual de con respecto a la norma 27001:2013, de acuerdo con los controles actualmente identificados se estableció los porcentajes de cumplimiento respectivos en base a la Tabla 4.

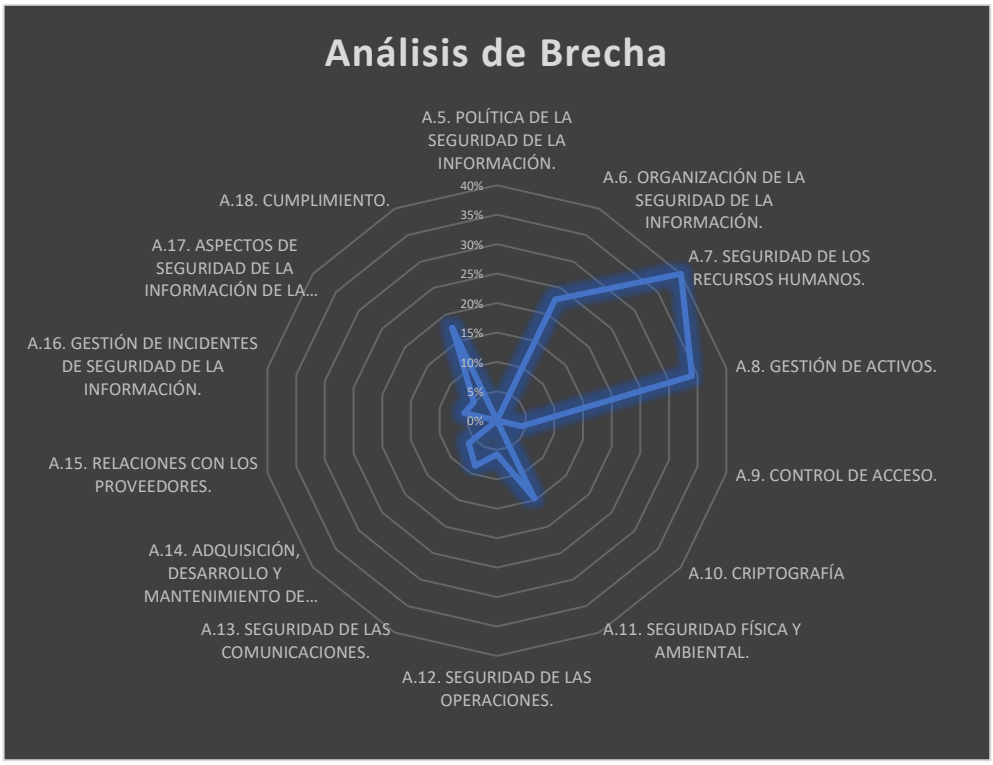


Figura 5: Análisis de brecha

Tabla 4: Criterios de calificación del nivel de cumplimiento para el análisis de brecha

ANÁLISIS DE BRECHA DE LA EMPRESA	
RESUMEN	**CALIFICACIÓN**
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	0%
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	23%
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	40%
A.8. GESTIÓN DE ACTIVOS.	34%
A.9. CONTROL DE ACCESO.	4%
A.10. CRIPTOGRAFÍA	0%
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	15%
A.12. SEGURIDAD DE LAS OPERACIONES.	6%
A.13. SEGURIDAD DE LAS COMUNICACIONES.	9%
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	6%
A.15. RELACIONES CON LOS PROVEEDORES.	0%
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	6%
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	5%
A.18. CUMPLIMIENTO.	18%
CALIFICACIÓN TOTAL	**12%**

CAPÍTULO IV

ANÁLISIS DE RIESGOS

4.1. Evaluación de impacto y probabilidad de materialización de las amenazas

El inicio del análisis de probabilidad e impacto requiere, de manera fundamental, la comprensión del valor asociado a cada activo examinado en el contexto organizacional. La evaluación del valor de un activo surge de la necesidad de proteger lo que se considera más crítico para una empresa. En este sentido, se otorga una mayor protección a los activos que poseen un valor significativo para el funcionamiento y desarrollo de las actividades de una organización. Para calcular las posibles consecuencias de la materialización de una amenaza, se recurre a las dimensiones de seguridad, que son atributos que confieren valor a un activo. El resultado de esta valoración proporciona una medida del potencial daño que podría afectar a la organización en caso de que un activo sufra algún perjuicio. Las dimensiones de seguridad utilizadas para valorar los activos de información son cruciales en este proceso. En la Tabla 5 se encuentra la escala de valoración que se ha definido para este estudio.

Tabla 5: Escala de valoración de activo de información.

VALORACIÓN DE ACTIVO		
ESCALA	**NOMENCLATURA**	**DEFINICIÓN**
MUY ALTO	MA	Deterioro muy significativo
ALTO	A	Deterioro significativo
MEDIO	M	Deterioro importante
BAJO	B	Deterioro menor
MUY BAJO	MB	Deterioro depreciable

En la Tabla 6 la valoración que se ha brindado a cada uno de los activos los cuales forman parte de la seguridad. Para mayor sobre como cada elemento fue evaluado dirigirse al Anexo F.

Tabla 6: Valoración activos de información.

ACTIVO	DESCRIPCIÓN	VALORACION
RT	Router propiedad del ISP	MUY ALTO
FW	Firewall interno Fortigate 100D	MUY ALTO
PC	Equipo de cómputo	MUY ALTO
SRV	Server Linux correo electrónico	ALTO
SVR	Server Linux base de datos	ALTO
SW	Switch Tplink interno 16 puertos	MEDIO
RT	Router WIFI	MEDIO
NVR	NVR Hikivision	MEDIO
CAM	Cámara IP	MEDIO
PBX	PBX análogo	BAJO
IMP	Impresora	MUY BAJO
TLF	Teléfono análogo	MUY BAJO

La evaluación del impacto y la probabilidad de la materialización de amenazas juega un papel fundamental en la gestión de riesgos. En este contexto, la probabilidad representa la medida de la posibilidad de que ocurra un evento no deseado, mientras que la amenaza es la entidad o situación que podría desencadenar dicho evento. Esta evaluación proporciona una visión integral

para determinar la magnitud potencial de un riesgo y la probabilidad asociada a su ocurrencia. Comprender tanto la probabilidad como la amenaza es esencial para identificar, priorizar y abordar eficazmente los riesgos en un entorno operativo. Al considerar estos factores, se establece una sólida base que permite priorizar la implementación de medidas de mitigación efectivas, posibilitando así una gestión proactiva y eficiente de los riesgos identificados en el entorno operativo.

Para el desarrollo puntual de este análisis de riesgo se han definido escalas personalizadas de impacto y probabilidad tomando en consideración el modelo de negocio y la naturaleza de las operaciones de la empresa, así como también los factores tanto internos como externos que puedan afectar la operación.

Para la escala de impacto la cual la podemos ver en la Tabla 7, se han definido 5 niveles en base a criterios de afectación económica, reputación e incumplimientos contractuales. A mayor nivel de impacto se tendrá mayor afectación en dichos factores.

Tabla 7: Escala de Impacto

ESCALA DE IMPACTO			
MA	5	CRÍTICO	Pérdida económica y de reputación grave. Incumplimientos contractuales
A	4	ALTO	Pérdida económica y de reputación considerable. Probablemente cause retrasos en obligaciones contractuales
M	3	MODERADO	Pérdida económica moderada sin daños considerables a la reputación. Poca probabilidad de incumplimiento contractual.
B	2	BAJO	Pérdida económica bajo sin daños a la reputación o incumplimientos contractuales.
D	1	DESPRECIABLE	No existe impacto financiero, reputación o contractual.

Por otro lado, la escala de probabilidad la cual observamos en la Tabla 8, se ha definido el nivel más alto una ocurrencia diaria, a medida que la probabilidad de ocurrencia disminuye también disminuye su valoración en la escala definida.

Tabla 8: Escala de Probabilidad

ESCALA DE PROBABILIDAD			
MP	5	MUY PROBABLE	Ocurrencia diaria
P	4	PROBABLE	Ocurrencia mensual
M	3	MODERADO	Ocurrencia semestral
PP	2	POCO PROBABLE	Ocurrencia anual
D	1	DEPRECIABLE	Ocurrencia mayor a 5 años

4.2. Análisis cuantitativo y cualitativo de riesgos

Para este estudio se ha llevado a cabo un análisis de riesgos de manera cuantitativa y cualitativa, ambas metodologías ofrecen enfoques distintos para evaluar y gestionar los riesgos.

Un análisis cualitativo de riesgos ofrece un enfoque el cual se centra en descripciones cualitativas y evaluaciones subjetivas de los riesgos para expresar la magnitud del riesgo. Este tipo de análisis proporciona una comprensión general y rápida de los riesgos.

Un análisis cualitativo de riesgos utiliza datos numéricos y estadísticas para cuantificar el impacto y la probabilidad de los riesgos. Este tipo de análisis proporciona resultados más cuantificables y precisos.

Para definir el nivel de riesgo asociado se ha definido una matriz de riesgo, la cual es una herramienta utilizada en la gestión de riesgos para categorizar y comunicar el grado de riesgo asociado a un evento o situación específica. Esta escala puede adaptarse según la terminología y los parámetros específicos de la organización o proyecto. En la Tabla 9 y Tabla 10 podemos observar los parámetros que se han definido para este estudio.

Tabla 9: Matriz de Riesgo

RIESGO		PROBABILIDAD				
		D	PP	M	P	MP
		1	2	3	4	5
IMPACTO						
MA	5	5	10	15	20	25
A	4	4	8	12	16	20
M	3	3	6	9	12	15
B	2	2	4	6	8	10
D	1	1	2	3	4	5

Tabla 10: Matriz de Riesgo

RIESGO		PROBABILIDAD				
		D	PP	M	P	MP
		1	2	3	4	5
IMPACTO	MA 5	MEDIO	ALTO	CRÍTICO	CRÍTICO	CRÍTICO
	A 4	BAJO	MEDIO	ALTO	CRÍTICO	CRÍTICO
	M 3	BAJO	MEDIO	MEDIO	ALTO	CRÍTICO
	B 2	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	D 1	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO

Por medio de esta matriz es posible de una forma rápida y visual de evaluar y priorizar los riesgos. Los riesgos ubicados en las categorías de impacto y probabilidad más altos generalmente requieren una atención más inmediata y medidas de mitigación más robustas.

4.3. Mapas de calor

Los mapas de calor es una representación gráfica que utiliza colores para visualizar la distribución de datos en una matriz bidimensional, proporcionan una representación visual de la distribución y la intensidad de los riesgos dentro de la organización. Este método de representación permite identificar riesgo de una manera rápida y visual. Un mapa de calor puede ser utilizado para destacar las áreas con mayor riesgo en una matriz, donde los colores más intensos señalan los riesgos más significativos, facilitando así la identificación y priorización visual de los elementos vulnerables de la red como es el caso de este estudio.

Durante el desarrollo de este análisis de riesgo se elaboraron mapas de calor para cada uno de los activos pertenecientes a la seguridad perimetral, donde permitió visualizar de manera gráfica el nivel de riesgo para cada una de sus amenazas asociadas.

Tabla 11: Mapa de calor activo

Activo: *Firewall* interno Fortigate 100D

Responsable: Jefe de sistemas

RIESGO		PROBABILIDAD				
		D 1	PP 2	M 3	P 4	MP 5
IMPACTO	MA 5		*I5* *A23*	*A4* *A11*		
	A 4			*E21*		
	M 3		*E3*			
	B 2					
	D 1					

En la Tabla 11 podemos observar los mapas de calor elaborados. Para mayor detalle sobre cada de uno de los mapas de calor desarrollados para cada uno de los activos de información identificados de la empresa, dirigirse al Anexo G, Mapas de calor.

CAPITULO V

TRATAMIENTOS DE RIESGOS

5.1. Priorización de riesgos

Basándonos en la priorización de riesgos realizada en los capítulos anteriores, se han evaluado aquellos que presentan los mayores niveles de riesgo. La identificación de elementos con riesgos más significativos destaca la necesidad de un tratamiento especial y, en algunos casos, intervenciones inmediatas. Estos activos críticos e importantes desempeñan un papel fundamental en la seguridad perimetral, subrayando la importancia de abordar de manera proactiva los riesgos asociados con ellos.

Para el análisis de riesgo efectuado a esta empresa, en conjunto con los directivos se ha determinado que es necesario establecer los controles respectivos a los riesgos identificados como Alto y Críticos. En la Tabla 12 podemos observar el detalle de los activos sobre los cuales se elaborará la propuesta de mejora. Para mayor detalle acerca de la identificación del nivel de riesgo asignado a cada activo dirigirse al Anexo H, Impacto Vs Probabilidad

Tabla 12: Activos identificados como Altos – Críticos.

N°	CÓDIGO	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	RIESGO
1	FW001	Firewall interno Fortigate 100D	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	12
				[I.5] Avería de origen físico o lógico	10
				[A.4] Manipulación de la configuración	15
				[A.11] Acceso no autorizado	15
				[A.23] Manipulación de los equipos	10
2	SW001 SW002 SW003	Switch Tplink interno 16 puertos	Jefe de sistemas	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	15
				[I.5] Avería de origen físico o lógico	10
				[I.7] Condiciones inadecuadas de temperatura o humedad	10
3	RT003	Router WIFI	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	12
4	SRV001	Server Linux correo electrónico	Jefe de sistemas	[E.3] Errores de monitorización	12
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	12
				[E.21] Errores de mantenimiento / actualización de programas (software)	12
				[E.24] Caída del sistema por agotamiento de recursos	12
				[A.11] Acceso no autorizado	12
5	SVR002	Server Linux base de datos	Jefe de sistemas	[E.3] Errores de monitorización	12
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	12
				[E.21] Errores de mantenimiento / actualización de programas (software)	12
				[E.24] Caída del sistema por agotamiento de recursos	12
				[A.11] Acceso no autorizado	12
6	PC001 PC002 PC003 PC004 PC005 PC006 PC007 PC008 PC009 PC010 PC011 PC012	Equipo de cómputo	Gerencia General Secretaria de gerencia Jefe de cobranzas Jefe de cobranzas Jefe de cobranzas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de sistemas Jefe de sistemas	[A.11] Acceso no autorizado	12
				[A.23] Manipulación de los equipos	12

5.2. Asignación de controles de seguridad a los riesgos priorizados.

Usando la norma 27001:2013 se ha establecido los controles de los riesgos priorizados como altos y críticos los cuales podemos observar en la Tabla 13.

Tabla 13: Controles de riesgos definidos

DESCRIPCIÓN	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
Firewall interno Fortigate 100D	12	Mitigar	Prevención/Monitorización	Gestión de las vulnerabilidades técnicas
	10	Evitar	Prevención	Política de Control de Acceso.
	15	Mitigar	Prevención	Acceso a redes y a servicios en red.
	15	Mitigar	Detección/Eliminación	Política de Control de Acceso. Restricción de acceso a información
	10	Evitar	Prevención	Política de Control de Acceso.
Switch Tplink interno 16 puertos	15	Evitar	Prevención/Monitorización	Gestión de las vulnerabilidades técnicas
	10	Mitigar	Prevención/Monitorización	Política de Control de Acceso.
	10	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red.
Router WIFI	12	Mitigar	Monitorización	Aseguramiento de la disponibilidad.
Server Linux correo electrónico	12	Transferir	Monitorización	Política de Control de Acceso. Restricción de acceso a información
	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
	12	Mitigar	Prevención/Monitorización/Eliminación	Mantenimiento de equipos.
	12	Mitigar	Prevención	Política de Control de Acceso. Restricción de acceso a información
Server Linux base de datos	12	Mitigar	Monitorización	Política de Control de Acceso. Restricción de acceso a información
	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
	12	Mitigar	Prevención/Monitorización/Eliminación	Mantenimiento de equipos.
	12	Mitigar	Prevención	Política de Control de Acceso. Restricción de acceso a información

DESCRIPCIÓN	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
Equipo de cómputo	12	Mitigar	Detección/Elimi nación	Política de Control de Acceso. Restricción de acceso a información
	12	Evitar	Prevención	Política de Control de Acceso. Avería de origen físico o lógico

Para mayor detalle acerca de los controles asignados a cada activo dirigirse al Anexo I, Controles de Riesgo.

5.3. Propuesta de implementación de los controles a los riesgos

- ***Firewall interno Fortigate 100D***

  - Solicitar al proveedor un cronograma regular de actualización tecnológica que contemple la renovación de licencias, implementación de redundancias en caso de fallos eléctricos, reemplazo de dispositivos en caso de daños físicos en los dispositivos y soporte de fabrica vigente.

    Responsable: Jefe de Sistemas - Gerente General

    Tiempo: 3 meses

  - Establecer una política interna para revisión y control de las actualizaciones, parches de seguridad y vulnerabilidades documentadas por parte del fabricante.

    Responsable: Jefe de Sistemas

    Tiempo: 3 meses

- Establecer una política de mantenimientos preventivos periódicos.

  Responsable: Jefe de Sistemas

  Tiempo: 3 meses

- Implementar un cuarto de rack equipos con respaldos eléctricos, condiciones de temperatura óptimas y un acceso restringido.

  Responsable: Jefe de Sistemas - Gerente General

  Tiempo: 6 meses

- Desarrollar e integrar un sistema de autenticación destinado a la gestión del firewall con el propósito de administrar los permisos de los administradores de red.

  Responsable: Jefe de Sistemas - Gerente de General

  Tiempo: 6 meses

- ***Switch Tplink interno 16 puertos***

  - Reemplazar switches existentes por equipo switch administrable con interfaces de 1G, con soporte por parte del fabricante vigente, que permite la implementación de portsecurity, configuración de vlans.

    Responsable: Jefe de Sistemas - Gerente General

    Tiempo: 3 meses

- Implementar un cuarto de rack equipos con respaldos eléctricos, condiciones de temperatura óptimas y un acceso restringido.

  Responsable: Jefe de Sistemas - Gerente de General

  Tiempo: 6 meses

- Desarrollar e integrar un sistema de autenticación destinado a la gestión del firewall con el propósito de administrar los permisos de los administradores de red.

  Responsable: Jefe de Sistemas - Gerente de General

  Tiempo: 6 meses

- ***Router WIFI***

  - Reemplazar router WIFI por uno con soporte por parte del fabricante vigente.

    Responsable: Jefe de Sistemas - Gerente de General

    Tiempo: 6 meses

  - Establecer una política interna para revisión y control de las actualizaciones, parches de seguridad y vulnerabilidades documentadas por parte del fabricante.

    Responsable: Jefe de Sistemas

    Tiempo: 3 meses

- ***Server Linux correo electrónico***

  - Implementación de una herramienta gratuita para el monitoreo de los recursos de red.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 3 meses

  - Implementación de una herramienta gratuita para generar backup automáticos y periódicos.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 3 meses

  - Asignar una VLAN específica para servidores, segregada dentro de la red LAN.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 6 meses

  - Implementar un sistema para habilitar la autenticación remota con doble factor mediante un servidor remoto de autenticación.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 6 meses

- Implementar políticas de acceso que asocien a los usuarios con los correspondientes permisos de acceso al servidor.

- Implementar políticas en firewall para limitar los puertos de acceso remoto.

- Implementar una conexión remota al servidor mediante una VPN SSL.

  Responsable: Jefe de Sistemas y Gerencia General

  Tiempo: 3 meses

- ***Server Linux base de datos***

  - Implementación de una herramienta gratuita para el monitoreo de los recursos de red.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 3 meses

  - Implementación de una herramienta gratuita para generar backup automáticos y periódicos.

    Responsable: Jefe de Sistemas y Gerencia General

    Tiempo: 3 meses

  - Asignar una VLAN específica para servidores, segregada dentro de la red LAN.

Responsable: Jefe de Sistemas y Gerencia General

Tiempo: 6 meses

- Implementar un sistema para habilitar la autenticación remota con doble factor mediante un servidor remoto de autenticación.

  Responsable: Jefe de Sistemas y Gerencia General

  Tiempo: 6 meses

- Implementar políticas de acceso que asocien a los usuarios con los correspondientes permisos de acceso al servidor.
- Implementar políticas en firewall para limitar los puertos de acceso remoto.
- Implementar una conexión remota al servidor para la sucursal de Machala mediante una VPN IPSEC.
- Implementar una conexión remota al servidor mediante una VPN SSL.

  Responsable: Jefe de Sistemas y Gerencia General

  Tiempo: 3 meses

- ***Equipo de cómputo***

  - Verificar la factibilidad de emplear un sistema (EDR) Endpoint Detection and Response para la gestión centralizada de dispositivos y la respuesta inmediata ante incidentes de seguridad.

    Responsable: Jefe de Sistemas - Gerente General

    Tiempo: 3 meses

  - Activar actualizaciones automáticas en los dispositivos de cómputos.

    Responsable: Jefe de Sistemas

    Tiempo: 1 meses

  - Gestionar que todos los equipos de cómputo posean las licencias del sistema operativo vigente.

    Responsable: Jefe de Sistemas - Gerente General

    Tiempo: 3 meses

  - Implementación de un servidor de autenticación para la administración centralizada, manejo de autorización y autenticación de usuarios en equipos de cómputo.

    Responsable: Jefe de Sistemas - Gerente General

    Tiempo: 6 meses

- Elaboración de política interna para gestión responsable de equipos de cómputo e información sensible almacenada en ellos.

  Responsable: Jefe de Sistemas

  Tiempo: 3 meses

5.4. Arquitectura seguridad

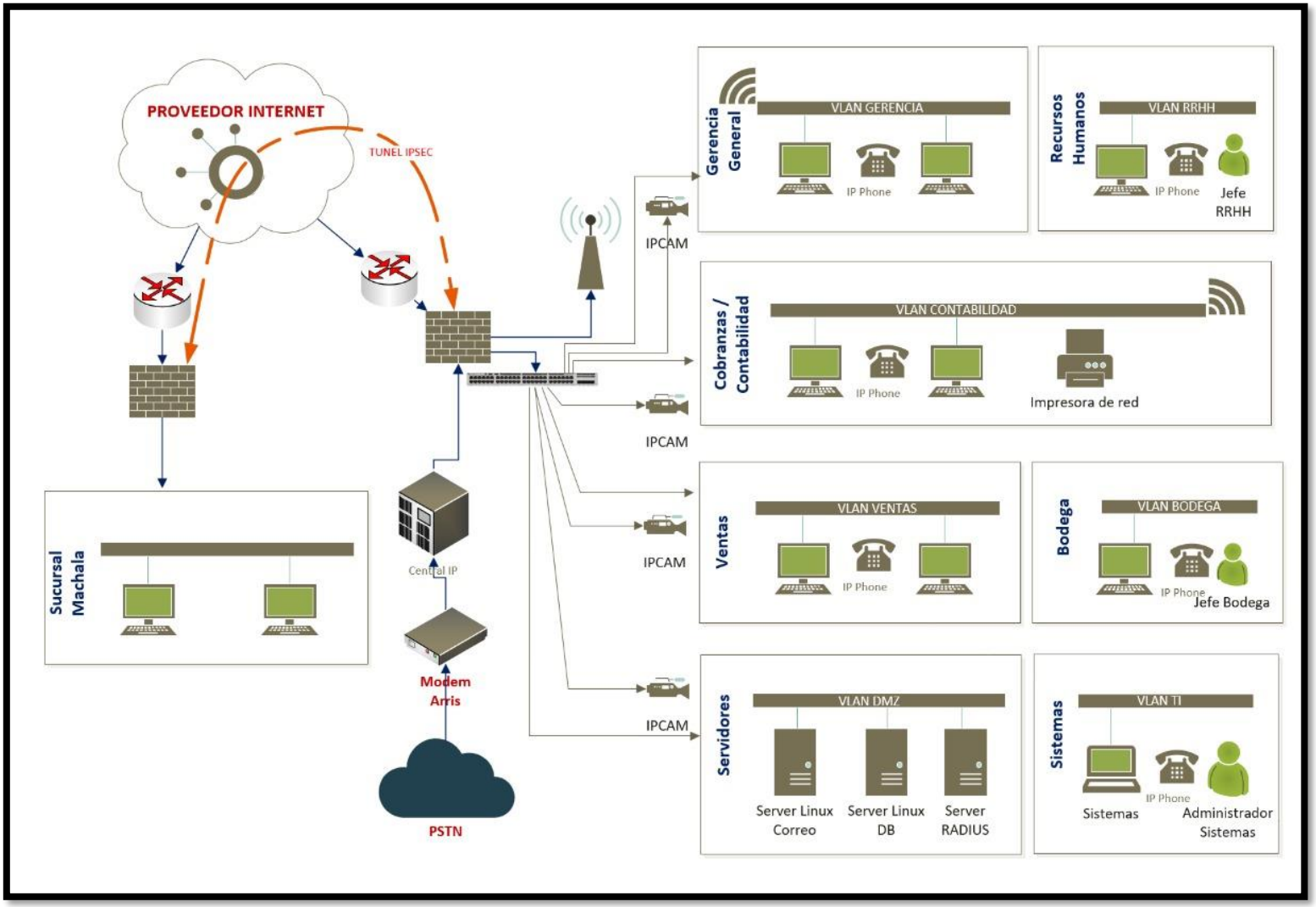


Figura 6: Propuesta de nueva arquitectura de red

En la arquitectura antes expuesta se propone lo siguiente:

Switch

- Equipo switch actual no permite administración remota ni segmentación por vlan, se recomienda el reemplazo por equipo administrable y que permita la configuración de VLANs
- Separar por VLANs cada uno de los departamentos de la empresa, de manera que los dispositivos de una red perteneciente a un departamento no tengan conectividad directa con otra red de otro departamento, sin antes pasar por el filtrado efectuado por el Firewall, para ello se enlistan las VLANs sugeridas.
    - ***VLAN MACHALA*** → Esta red pertenecerá a la sucursal Machala.
    - ***VLAN DMZ*** → Esta red pertenecerá a los servidores.
    - ***VLAN TI*** → Esta red pertenecerá a los administradores de la red.
    - ***VLAN BODEGA*** → Esta red pertenecerá al personal encargado de los despachos de bodega.
    - ***VLAN VENTAS*** → Esta red pertenecerá al personal encargado de la gestión de ventas.
    - ***VLAN CONTABILIDAD*** → Esta red pertenecerá al área de contabilidad.
    - ***VLAN RRHH*** → Esta red es de uso exclusivo para personal de Recursos Humanos.
    - ***VLAN GERENCIA*** → Esta red es de uso exclusivo para la alta Gerencia.

Firewall

- El equipo Firewall actual ha tenido su tiempo de vida útil, por lo que la recomendación es su cambio inmediato, evitando que nuevas vulnerabilidades no afecten la operación de la compañía.

Central Telefónica

- Se recomienda la renovación tecnológica de dicho equipo por motivo de obsolescencia en la que ya se encuentra dicha central, en la era tecnológica actual se está trabajando con telefonía IP dada las mejoras que han existido en este tipo de tecnología.

Comunicación de Datos sobre Internet:

- Para una comunicación más segura se propone levantar una comunicación encriptada mediante VPN IPSEC; de manera que el tráfico que se genere desde la matriz hacia su sucursal pase encriptado evitando así que sea interceptado por algún tipo de hacker mal intencionado.

Red Inalámbrica

- Implementar una conexión inalámbrica exclusiva para clientes y que esta sea aislada de las redes corporativa.

CONCLUSIONES

La investigación destaca la necesidad crítica de implementar un esquema de seguridad perimetral dentro de las empresas medianas, como la estudiada en este trabajo de titulación dentro de la ciudad de Guayaquil. La creciente complejidad de las amenazas cibernéticas subraya la importancia de proteger los límites físicos y lógicos de toda la red para preservar la integridad y confidencialidad de la información pudiendo ofrecer confianza entre los clientes.

Este proyecto fue concebido con la firme determinación de alcanzar el objetivo fundamental de disminuir el nivel de riesgo en el caso de que una amenaza se materialice. Este propósito se logró mediante una exhaustiva evaluación de riesgos que abarcó los activos que forman parte de la seguridad perimetral.

La implementación de medidas de seguridad perimetral, guiada por los resultados del análisis de riesgos, no solo buscaba cuantificar y cualificar las amenazas, sino también diseñar e implementar estrategias prácticas y efectivas. El objetivo primordial consistía en fortalecer la seguridad en el perímetro, garantizando la integridad, confidencialidad y disponibilidad de los activos de información relacionados a la comercialización de materiales de construcción.

RECOMENDACIONES

Recomendamos la incorporación de un proceso continuo de análisis de riesgos que se adapte a la evolución del entorno operativo y las amenazas cibernéticas. La evaluación periódica permitirá identificar nuevas vulnerabilidades y ajustar estrategias de seguridad perimetral de manera proactiva.

Sugerimos llevar a cabo evaluaciones periódicas dentro del tiempo que se considere pertinente de las herramientas de seguridad utilizadas dentro del entorno, asegurándose de que estén actualizadas y alineadas con las necesidades específicas de la empresa. La tecnología de seguridad perimetral debe evolucionar juntamente con las amenazas para mantener su efectividad al momento de que se llegasen a necesitar de manera automatizada.

Con respecto a Servidores y equipamiento, destacamos la importancia de implementar un sólido plan de respaldo y recuperación de datos. Realizar copias de seguridad regulares y probar la capacidad de recuperación, estas son acciones fundamentales para asegurar la continuidad del negocio en caso de un incidente.

Es esencial invertir en programas de formación continua para el personal, enfocándose en la concientización y el conocimiento actualizado en el ámbito de la seguridad informática. Un personal bien informado representa una defensa fundamental contra tácticas de ingeniería social y otras amenazas potenciales.

Se aconseja de manera enfática la implementación y configuración adecuada de un Directorio Activo (AD) como parte integral de la infraestructura de seguridad de la empresa. El Directorio Activo, proporcionado

por Microsoft, ofrece un conjunto robusto de servicios de directorio que desempeñan un papel esencial en la administración centralizada de identidades, autorizaciones y recursos en un entorno de red. Permitiendo la centralización de la administración de identidades y permisos en toda la red. Esto permite un control eficiente sobre los usuarios, grupos y recursos, simplificando la gestión de accesos y mejorando la seguridad al reducir la complejidad de la administración de cuentas individuales.

BIBLIOGRAFIA

[1] E. G. Little y G. L. Rogova, «An Ontological Analysis of Threat and Vulnerability», en *2006 9th International Conference on Information Fusion*, 2006, pp. 1-8. doi: 10.1109/ICIF.2006.301716.

[2] ISO/IEC 27001:2013, «Information technology - Security techniques - Information security management systems - Requirements». 2013. [En línea]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[3] M. N. Aleksandrov, V. A. Vasiliev, y S. V. Aleksandrova, «Implementation of the Risk-based Approach Methodology in Information Security Management Systems», en *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 137-139. doi: 10.1109/ITQMIS53292.2021.9642767.

[4] M. A. Roumani, C. C. Fung, y P. Choejey, «Assessing economic impact due to cyber attacks with System Dynamics approach», en *2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2015, pp. 1-6. doi: 10.1109/ECTICon.2015.7207084.

[5] Z. Alimzhanova, A. Tleubergen, S. Zhunusbayeva, y D. Nazarbayev, «Comparative Analysis of Risk Assessment During an Enterprise Information Security Audit», en *2022 International Conference on Smart Information Systems and Technologies (SIST)*, 2022, pp. 1-6. doi: 10.1109/SIST54437.2022.9945804.

[6] A. Hapon, V. Fedorchenko, V. Martovytskyi, V. Rykun, O. Sievierinov, y I. Oleshko, «Measuring Vulnerabilities in Threat Modelling with Risk Matrix», en *2021 IEEE 8th International Conference on*

Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 617-619. doi: 10.1109/PICST54195.2021.9772211.

[7] G. Castro Arica, «Introducción a la Ciberseguridad», *2021*, abril de 2021. [En línea]. Disponible en: https://gerardokaztro.medium.com/introducci%C3%B3n-a-la-ciberseguridad-ff67eb3dff12

[8] D. P. F. Möller, H. Vakilzadian, y R. E. Haas, «Cybersecurity Certificate in Digital Transformation», en *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, pp. 556-561. doi: 10.1109/eIT53891.2022.9813932.

[9] L. Gashi, A. Luma, y A. Aliu, «A comprehensive review of cybersecurity perspective for Wireless Sensor Networks», en *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 2022, pp. 392-395. doi: 10.1109/ISMSIT56059.2022.9932788.

[10] N. Ismail, «What is digital transformation in business: everything you need to know», *2020*, abril de 2020. [En línea]. Disponible en: https://www.information-age.com/what-is-digital-transformation-in-business-12365/

[11] «ISO/IEC 27001: What's new in IT security?», *25/10/2022*, 2022.

[12] J. Jurgens y K. Bissell, «Global Cybersecurity Outlook 2022», enero de 2022.

[13] R. R. Branco y G. N. Barbosa, «Distributed malware analysis scheduling», en *2011 6th International Conference on Malicious and Unwanted Software*, 2011, pp. 34-41. doi: 10.1109/MALWARE.2011.6112324.

[14] I. Sumantra y S. Indira Gandhi, «DDoS attack Detection and Mitigation in Software Defined Networks», en *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, 2020, pp. 1-5. doi: 10.1109/ICSCAN49426.2020.9262408.

[15] F. Trishan, «¿Qué es la autenticación adaptativa y cuáles son sus retos y desafíos?» [En línea]. Disponible en: https://www.chakray.com/es/autenticacion-adaptativa-cuales-son-retos-desafios/

[16] A. Abrie, «¿Qué son los ataques DDoS y DoS?», 29 de septiembre de 2020. [En línea]. Disponible en: www.icm.es/2020/09/29/ddos-dos/

[17] Z. V. Altamirano Valarezo, Á. B. Pinto Astudillo, y J. D. C. Sánchez Guerrero, «Text mining aplicado a la clasificación y distribución automÁtica de correo electrónico y detección de correo SPAM», Escuela Superio Politecnica del Litoral, Guayaquil, 2007. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/3225/1/5744.pdf

[18] «Reporte de Tráfico Malicioso refleja aumento de ataques DoS en 2022», 19 de abril de 2023. [Https://itahora.com]. Disponible en: https://itahora.com/2023/04/19/reporte-de-trafico-malicioso-refleja-aumento-de-ataques-dos-en-2022/

ANEXOS

Anexo A: Resumen entrevista jefe de sistemas.

1. **A nivel de seguridad informática, ¿Cuál es el nivel de madurez que tiene la organización?**

   Con respecto a seguridad Informática, siempre los ingenieros tratamos de dar lo mejor en conocimientos y aplicarlos; pero, está demostrado que no siempre estamos del todo protegido, existen cada vez más herramientas potentes que hace que nuestros equipos o herramientas utilizadas para contrarrestar algún tipo de vulnerabilidad se vuelvan obsoleto por el ingenio que tienen los ciberdelincuentes para penetrar sistemas; entonces la madurez creo que es medida más porque por la experiencia, se mide por la actualización constante en temas de seguridad y temas afines.

2. **¿Se maneja algún tipo de inventario para la identificación de los activos que conforman la seguridad perimetral de la empresa?**

   Al hablar de seguridad perimetral hablamos de los equipos de perímetro o equipos de borde, por lo que no son tantos, tenemos un firewall, los routers del proveedor, una central telefónica, y el resto son equipos de cómputo que entre ellos tenemos los servidores.

3. **En los últimos 5 años, ¿ha experimentado un evento de seguridad que haya comprometido los activos de seguridad informática de la empresa?**

   Si, hemos presentado un ataque a nuestros servidores de DDoS que ocasionaron que nuestros equipos queden fuera de servicio lo que nos ocasiono un retraso en la operación de ventas, pero han sido

manejables se han tomado las acciones correctivas, pero como ya lo mencioné no siempre uno puede protegerse al 100%.

4. **Ante un evento de seguridad que comprometa la red interna incluyendo los equipos que integran la seguridad perimetral, ¿existen un protocolo para el manejo de estas?**

   Creo no poder dar una respuesta favorable, no tenemos un departamento de riesgos que pueda ayudarnos elaborando un protocolo que nos permita actuar de una manera oportuna; sin embargo, existe la iniciativa de comunicarles verbalmente los riesgos que existen al abrir un correo personal dentro de la organización, y/o traer un dispositivo extraíble.

5. **En sus procesos internos, ¿han implementado un protocolo de pruebas para evaluar la robustez de su infraestructura ante posibles eventos de seguridad?**

   No tenemos alguna herramienta o contrato con algún proveedor que pueda medir este tipo de riesgos.

6. **Dentro de sus procedimientos internos, ¿existen cronogramas de mantenimiento tanto a nivel de hardware como de software para preservar la integridad de los componentes de seguridad perimetral de la organización?**

   No, no tenemos un plan de mantenimiento, pero si se detecta que existen equipo que ameriten una limpieza sea de hardware o software, se procede a coordinarla y ejecutarla.

7. **Para asegurar la integridad y seguridad de las operaciones, ¿la empresa emplea software con licencia en todas sus aplicaciones y programas utilizados?**

Tenemos una licencia de firewall que es proporcionada por el proveedor y con lo que respecta a servidores tratamos de manejar software opensource, mientras que para las computadoras tenemos unas que vienen con software original.

8. **¿Cuáles son las estrategias y herramientas específicas que emplea para anticipar y gestionar posibles problemas de obsolescencia dentro de la infraestructura interna, asegurando al mismo tiempo la integridad y seguridad de la información en el ámbito de la ciberseguridad?**

   Mediante políticas de firewall realizamos la contención en lo posible del tráfico malicioso de entrada y salida; pero, para el equipamiento interno no hemos adquirido un antivirus nos regimos al antivirus que trae por defecto cada dispositivo.

9. **¿Cuáles son las medidas y mejores prácticas implementadas por la empresa en cuanto a la gestión de contraseñas y el control de acceso de usuarios para garantizar la seguridad de la información?**

   Las contraseñas son administradas por cada usuario, no tenemos un control ni un procedimiento de buenas prácticas, ya depende de cada usuario.

10. **¿Cuáles son las medidas y protocolos implementados por la empresa para garantizar la seguridad y prevenir posibles fugas de información en equipos desatendidos?**

    Para ser sinceros, no contamos con un protocolo que nos proteja de este tipo de riesgo, los usuarios tienen la responsabilidad de tener sus equipos protegidos con contraseñas propias y velar por la seguridad de dicho equipo, no puede dejar desatendido su equipo.

11. **¿La empresa cuenta con un sistema de registro de eventos de seguridad o logs, que le permita realizar un seguimiento y análisis de posibles incidentes de seguridad? En caso afirmativo, ¿podría proporcionar detalles sobre cómo se gestionan y almacenan estos registros?**

    Con respecto al firewall el proveedor tiene un analizador de eventos que guarda dicha información para posterior análisis, para el resto de los equipos no se tiene un servidor o un almacenamiento externo de LOGs.

12. **¿La empresa cuenta con políticas y procedimientos con respecto al uso de puertos USB para evitar eventos de seguridad o fuga de información? En caso de que se detecte un uso no autorizado de puertos USB, ¿existe algún protocolo de respuesta ante dicho incidente?**

    No, no contamos con un protocolo de respuesta ante este tipo de incidentes, tampoco tenemos un tipo de control en los puertos USB, el personal sabe que está prohibido el uso de estos dispositivos.

13. **¿La empresa actualmente utiliza algún sistema o gestor de administración centralizada para la autenticación y autorización de permisos en sus plataformas y sistemas? En caso afirmativo, ¿podría proporcionar más detalles sobre cómo se gestiona este proceso y qué herramientas específicas se emplean?**

    No, todos los dispositivos tienen claves locales, no administramos algún gestor centralizado.

14. **¿Cómo se gestiona actualmente el control de acceso a los NVR dentro de la infraestructura de la empresa?**

    El acceso se lo realiza mediante dispositivos Laptop/Tablet/IPPhone de los dueños de la compañía y quien les habla; es decir, las claves solo son conocidas por los antes ya mencionados, ningún colaborador tiene las claves de acceso.

Anexo B: Inventarios de activos

ACTIVOS DE INFORMACIÓN				
N°	**CÓDIGO**	**TIPO ACTIVO**	**DESCRIPCIÓN**	**RESPONSABLE**
1	RT001	HW	Router propiedad del ISP	Jefe de sistemas
2	RT002	HW	Router propiedad del ISP	Jefe de sistemas
3	FW001	HW	Firewall interno Fortigate 100D	Jefe de sistemas
4	SW001	HW	Switch Tplink interno 16 puertos	Jefe de sistemas
5	SW002	HW	Switch Tplink interno 16 puertos	Jefe de sistemas
6	SW003	HW	Switch Tplink interno 16 puertos	Jefe de sistemas
7	RT003	HW	Router WIFI	Jefe de sistemas
8	SRV001	HW	Server Linux correo electrónico	Jefe de sistemas
9	SVR002	HW	Server Linux base de datos	Jefe de sistemas
10	PBX001	HW	PBX análogo	Jefe de sistemas
11	NVR001	HW	NVR Hikivision	Jefe de sistemas
12	CAM01	HW	Cámara IP	Jefe de sistemas
13	CAM02	HW	Cámara IP	Jefe de sistemas
14	CAM03	HW	Cámara IP	Jefe de sistemas
15	CAM04	HW	Cámara IP	Jefe de sistemas
16	CAM05	HW	Cámara IP	Jefe de sistemas
17	CAM06	HW	Cámara IP	Jefe de sistemas
18	CAM07	HW	Cámara IP	Jefe de sistemas
19	CAM08	HW	Cámara IP	Jefe de sistemas
20	PC001	HW	Equipo de cómputo	Gerencia General
21	PC002	HW	Equipo de cómputo	Secretaria de gerencia
22	PC003	HW	Equipo de cómputo	Jefe de cobranzas
23	PC004	HW	Equipo de cómputo	Jefe de cobranzas
24	PC005	HW	Equipo de cómputo	Jefe de cobranzas
25	PC006	HW	Equipo de cómputo	Jefe de ventas
26	PC007	HW	Equipo de cómputo	Jefe de ventas
27	PC008	HW	Equipo de cómputo	Jefe de ventas
28	PC009	HW	Equipo de cómputo	Jefe de ventas
29	PC010	HW	Equipo de cómputo	Jefe de ventas
30	PC011	HW	Equipo de cómputo	Jefe de sistemas
31	PC012	HW	Equipo de cómputo	Jefe de sistemas
32	IMP001	HW	Impresora	Jefe de sistemas
33	TLF001	HW	Teléfono análogo	Jefe de sistemas
34	TLF002	HW	Teléfono análogo	Jefe de sistemas
35	TLF003	HW	Teléfono análogo	Jefe de sistemas
36	TLF004	HW	Teléfono análogo	Jefe de sistemas

ACTIVOS DE INFORMACIÓN				
N°	**CÓDIGO**	**TIPO ACTIVO**	**DESCRIPCIÓN**	**RESPONSABLE**
37	TLF005	HW	Teléfono análogo	Jefe de sistemas
38	TLF006	HW	Teléfono análogo	Jefe de sistemas
39	TLF007	HW	Teléfono análogo	Jefe de sistemas
40	TLF008	HW	Teléfono análogo	Jefe de sistemas

Anexo C: Identificación de amenazas

IDENTIFICACION DE AMENAZAS				
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**
1	HW	RT001 RT002	Router propiedad del ISP	[E.21] Errores de mantenimiento / actualización de programas (software)
				[I.5] Avería de origen físico o lógico
				[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
2	HW	FW001	Firewall interno Fortigate 100D	[E.3] Errores de monitorización
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[I.5] Avería de origen físico o lógico
				[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
3	HW	SW001 SW002 SW003	Switch Tplink interno 16 puertos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
				[I.5] Avería de origen físico o lógico
				[I.7] Condiciones inadecuadas de temperatura o humedad
4	HW	RT003	Router WIFI	[E.21] Errores de mantenimiento / actualización de programas (software)
				[I.5] Avería de origen físico o lógico
				[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos

IDENTIFICACION DE AMENAZAS				
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**
5	HW	SRV001	Server Linux correo electrónico	[E.3] Errores de monitorización
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[E.24] Caída del sistema por agotamiento de recursos
				[A.3] Manipulación de los registros de actividad
				[A.11] Acceso no autorizado
				[A.22] Manipulación de los equipos
6	HW	SVR002	Server Linux base de datos	[E.3] Errores de monitorización
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[E.24] Caída del sistema por agotamiento de recursos
				[A.3] Manipulación de los registros de actividad
				[A.11] Acceso no autorizado
				[A.22] Manipulación de los equipos
7	HW	PBX001	PBX análogo	[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
				[I.5] Avería de origen físico o lógico
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)
8	HW	NVR001	NVR Hikivision	[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
				[I.5] Avería de origen físico o lógico
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)

IDENTIFICACION DE AMENAZAS				
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**
9	HW	CAM01 CAM02 CAM03 CAM04 CAM05 CAM06 CAM07 CAM08	Cámara IP	[A.4] Manipulación de la configuración
				[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
				[I.5] Avería de origen físico o lógico
				[E.21] Errores de mantenimiento / actualización de programas (software)
10	HW	PC001 PC002 PC003 PC004 PC005 PC006 PC007 PC008 PC009 PC010 PC011 PC012	Equipo de cómputo	[A.11] Acceso no autorizado
				[A.23] Manipulación de los equipos
				[A.25] Robo
				[I.5] Avería de origen físico o lógico
				[E.8] Difusión de software dañino
				[E.20] Vulnerabilidades de los programas (software)
				[E.21] Errores de mantenimiento / actualización de programas (software)
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)
11	IMP001	IMP001	Impresora	[A.11] Acceso no autorizado
				[E.21] Errores de mantenimiento / actualización de programas (software)
12	HW	TLF001 TLF002 TLF003 TLF004 TLF005 TLF006 TLF007 TLF008	Teléfono análogo	[A.11] Acceso no autorizado

Anexo D: Identificación de vulnerabilidades

IDENTIFICACION DE VULNERABILIDADES					
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**	**VULNERABILIDAD**
1	HW	RT001 RT002	Router propiedad del ISP	[E.21] Errores de mantenimiento / actualización de programas (software)	Uso de software obsoletos con vulnerabilidades conocidas, provocando fallos de seguridades.
				[I.5] Avería de origen físico o lógico	Interrupción total del servicio
				[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos
				[A.11] Acceso no autorizado	Falta de listas de accesos de remotos permitidos.
				[A.23] Manipulación de los equipos	No utilización de espacios adecuados como gabinetes/racks cerrados con su debida protección.
2	HW	FW001	Firewall interno Fortigate 100D	[E.3] Errores de monitorización	Detección tardía de accesos a herramientas o aplicaciones no autorizados
				[E.21] Errores de mantenimiento / actualización de programas (software)	Uso de software obsoletos con vulnerabilidades conocidas, provocando fallos de seguridades.
				[I.5] Avería de origen físico o lógico	Interrupción total del servicio
				[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos
				[A.11] Acceso no autorizado	Manipulaciones en la configuración existente
				[A.23] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.
3	HW	SW001 SW002 SW003	Switch Tplink interno 16 puertos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad e inestabilidad en la red, afectando la comunicación entre los dispositivos de la red
				[I.5] Avería de origen físico o lógico	Interrupción total del servicio
				[I.7] Condiciones inadecuadas de temperatura o humedad	Pérdida de conectividad y daño físico a los componentes
4	HW	RT003	Router WIFI	[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad a dispositivos conectados. Pérdida de datos.
				[I.5] Avería de origen físico o lógico	Pérdida de conectividad de dispositivos conectados
				[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos
				[A.11] Acceso no autorizado	Manipulaciones en la configuración existente
				[A.23] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.

IDENTIFICACION DE VULNERABILIDADES					
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**	**VULNERABILIDAD**
5	HW	SRV001	Server Linux correo electrónico	[E.3] Errores de monitorización	Fallos en detección temprana de uso de recursos, ataques y accesos no autorizados
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.
				[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.
				[E.24] Caída del sistema por agotamiento de recursos	Problemas de rendimiento, interrupción del servicio
				[A.3] Manipulación de los registros de actividad	Detección tardía de actividades maliciosas.
				[A.11] Acceso no autorizado	Manipulaciones en la configuración existente
				[A.22] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.
6	HW	SVR002	Server Linux base de datos	[E.3] Errores de monitorización	Fallos en detección temprana de uso de recursos, ataques y accesos no autorizados
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.
				[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.
				[E.24] Caída del sistema por agotamiento de recursos	Problemas de rendimiento, interrupción del servicio
				[A.3] Manipulación de los registros de actividad	Detección tardía de actividades maliciosas.
				[A.11] Acceso no autorizado	Manipulaciones en la configuración existente
				[A.22] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.
7	HW	PBX001	PBX análogo	[A.4] Manipulación de la configuración	Modificación no autorizada de enrutamientos de llamadas, privilegios de usuarios u otras funciones.
				[A.11] Acceso no autorizado	Cambios no autorizados en ajustes críticos
				[A.23] Manipulación de los equipos	Cambios no autorizados en ajustes críticos
				[I.5] Avería de origen físico o lógico	Pérdida de equipo
				[E.21] Errores de mantenimiento / actualización de programas (software)	Daños en la configuración a causa de errores no detectados en los mantenimientos y/o actualizaciones.
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perdida de operatividad por manipulación inadecuada al momento de realizar trabajos en el equipo.

IDENTIFICACION DE VULNERABILIDADES					
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**	**VULNERABILIDAD**
8	HW	NVR001	NVR Hikivision	[A.4] Manipulación de la configuración	Intentos de eliminar/modificar o dañar grabaciones almacenadas.
				[A.11] Acceso no autorizado	Detección tardía de actividades maliciosas. Fuga de información.
				[A.23] Manipulación de los equipos	Detección tardía de actividades maliciosas. Fuga de información.
				[I.5] Avería de origen físico o lógico	Detección tardía de actividades maliciosas. Fuga de información.
				[E.21] Errores de mantenimiento / actualización de programas (software)	Perdida de operatividad por manipulación inadecuada.
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perdida de operatividad por manipulación inadecuada.
9	HW	CAM01 CAM02 CAM03 CAM04 CAM05 CAM06 CAM07 CAM08	Cámara IP	[A.4] Manipulación de la configuración	Cambios no autorizados en su funcionalidad como: cambio de contraseñas, desactivación de funciones de seguridad.
				[A.11] Acceso no autorizado	Detección tardía de actividades maliciosas. Fuga de información.
				[A.23] Manipulación de los equipos	Movimientos de enfoque en dispositivos con el objetivo de evadir algún punto de vista ciego al que se tenga monitoreo de cámaras.
				[I.5] Avería de origen físico o lógico	Daños la integridad del dispositivo.
				[E.21] Errores de mantenimiento / actualización de programas (software)	Perdida de configuraciones establecidas.
10	HW	PC001 PC002 PC003 PC004 PC005 PC006 PC007 PC008 PC009 PC010 PC011 PC012	Equipo de cómputo	[A.11] Acceso no autorizado	Instalación de software maliciosos, acceso a datos sensibles, Fuga de información, suplantación de identidad
				[A.23] Manipulación de los equipos	Manipulación de hardware, instalación de software maliciosos, acceso a datos sensibles, fuga de información, suplantación de identidad.
				[A.25] Robo	Acceso a datos sensibles, fuga de información.
				[I.5] Avería de origen físico o lógico	Pérdida de equipo e información sensible.
				[E.8] Difusión de software dañino	Suplantación de identidad, fuga de información, ataques a la red
				[E.20] Vulnerabilidades de los programas (software)	Softwares desactualizados, exposición a nuevos ataques
				[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de información, exposición a nuevos ataques.
				[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de información.

IDENTIFICACION DE VULNERABILIDADES					
N°	**TIPO ACTIVO**	**CÓDIGO**	**DESCRIPCIÓN**	**AMENAZAS**	**VULNERABILIDAD**
11	IMP001	IMP001	Impresora	[A.11] Acceso no autorizado	Fuga de información.
				[E.21] Errores de mantenimiento / actualización de programas (software)	Firmwares desactualizados, ataques de red
12	HW	TLF001 TLF002 TLF003 TLF004 TLF005 TLF006 TLF007 TLF008	Teléfono análogo	[A.11] Acceso no autorizado	Intercepción de información, Fuga de información.

Anexo E: Análisis de Brecha

ISO27001:2013			
OBJETIVOS DE CONTROL Y CONTROLES			**CALIFICACIÓN**
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	**A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.**	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	0%
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	0%
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	**A.6.1. Organización Interna.**	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	60%
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	40%
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	40%
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	0%
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	20%
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	0%
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	60%
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	40%
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	40%
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	40%
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	20%
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	40%
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.8. GESTIÓN DE ACTIVOS.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	40%
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	100%
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	20%
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	100%
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	40%
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	0%
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	0%
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	0%
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	20%
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	20%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.9. CONTROL DE ACCESO.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	20%
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	0%
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	0%
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	0%
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	0%
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	0%
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	0%
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	0%
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1. Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	0%
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.		
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	20%
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	0%
		A.9.4.3. Sistema de Gestión de Contraseñas.los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.9. CONTROL DE ACCESO.	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	0%
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.	20%
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	0%
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	0%
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	0%
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	20%
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	20%
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	0%
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	0%
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	20%
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	0%
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	0%
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	40%
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	60%
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	0%
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.	20%
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	20%
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	20%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	20%
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	0%
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	0%
		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	0%
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	20%
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	20%
	Objetivo. Proteger contra la pérdida de datos.		
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	20%
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	0%
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	0%
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	0%
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.		
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	0%
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	0%
	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	0%
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	40%
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	20%
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	0%
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	0%
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.2. Transferencia de información.	A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	0%
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	0%
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	0%
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	40%
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	20%
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	0%
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	0%
		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	20%
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	0%
		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	0%
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	0%
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	0%
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	0%
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	0%
	Objetivo. Asegurar la protección de los datos usados para ensayos.		
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	0%
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	0%
		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	0%
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	0%
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	0%
	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	0%
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	0%
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	20%
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	0%
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	20%
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	0%
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	0%
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	20%
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.2. Redundancia Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	0%
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	60%
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.	40%
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	40%
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	0%
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos	0%

OBJETIVOS DE CONTROL Y CONTROLES			CALIFICACIÓN
A.18. CUMPLIMIENTO.	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	0%
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	0%
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	0%

NIVEL DE CUMPLIMIENTO	
CALIFICACIÓN	**JUSTIFICACIÓN**
0%	El control no ha sido implementado. La Organización no ha reconocido que hay un problema a tratar
20%	La Organización reconoce que existe un problema que debe ser tratado. No existen procesos estandarizados sino procedimientos particulares aplicados a cosos individuales (ad hoc), es decir que la implementación de un control depende de cada individuo y es principalmente reactiva.
40%	Se desarrollan procesos dependientes de las personas y otras la siguen. No hay una comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos. Excesiva confianza en el conocimiento de los individuos, por tanto, los errores son comunes. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
60%	Los procesos se definen, documentan, y se comunican a través de un entrenamiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por sí mismos no son sofisticados, pero se formalizan las prácticas existentes.
80%	Existen mediciones y monitoreo sobre el cumplimiento de los procedimientos y es posible tomar medidas de acción donde los procesos no estén funcionando eficientemente. Los procedimientos están bajo constante mejoramiento y aportan a la calidad y productividad. Normalmente requiere de herramientas automatizadas para la medición
100%	Los procesos se depuran a nivel de buenas prácticas con baso en los resultados del mejoramiento continuo y los modelos de madurez de otras empresas. Normalmente, se cuenta con herramientas automatizadas e work flow que ayudan a la identificación de los elementos más débiles de los procesos. Se recoge evidencia numérica que se usa para justificar la aplicación, de tecnología en área críticas. Se realiza un riguroso análisis de causas y prevención de defectos.

Anexo F: Valoración de Activos

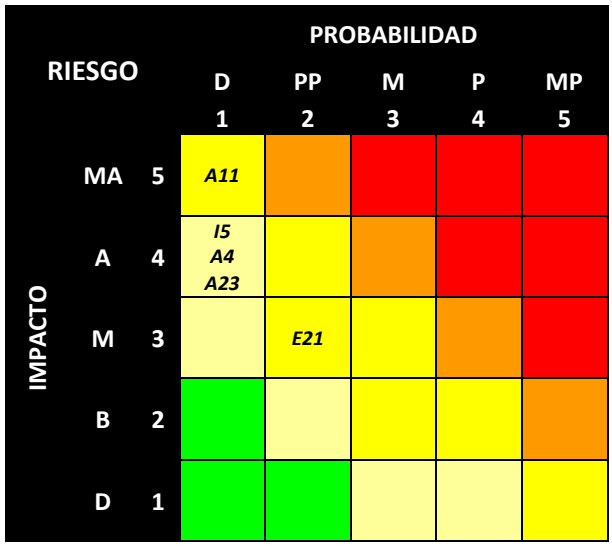
ACTIVOS DE INFORMACIÓN								
N°	**CÓDIGO**	**TIPO ACTIVO**	**DESCRIPCIÓN**	**RESPONSABLE**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**VALORACION**
1	RT001	HW	Router propiedad del ISP	Jefe de sistemas	X	X	X	MA
2	RT002	HW	Router propiedad del ISP	Jefe de sistemas	X	X	X	MA
3	FW001	HW	Firewall interno Fortigate 100D	Jefe de sistemas	X	X	X	MA
4	SW001	HW	Switch Tplink interno 16 puertos	Jefe de sistemas			X	M
5	SW002	HW	Switch Tplink interno 16 puertos	Jefe de sistemas			X	M
6	SW003	HW	Switch Tplink interno 16 puertos	Jefe de sistemas			X	M
7	RT003	HW	Router WIFI	Jefe de sistemas	X	X	X	M
8	SRV001	HW	Server Linux correo electrónico	Jefe de sistemas	X	X	X	A
9	SVR002	HW	Server Linux base de datos	Jefe de sistemas	X	X	X	A
10	PBX001	HW	PBX análogo	Jefe de sistemas	X	X	X	B
11	NVR001	HW	NVR Hikivision	Jefe de sistemas	X	X	X	M
12	CAM01	HW	Cámara IP	Jefe de sistemas	X	X	X	M
13	CAM02	HW	Cámara IP	Jefe de sistemas	X	X	X	M
14	CAM03	HW	Cámara IP	Jefe de sistemas	X	X	X	M
15	CAM04	HW	Cámara IP	Jefe de sistemas	X	X	X	M
16	CAM05	HW	Cámara IP	Jefe de sistemas	X	X	X	M
17	CAM06	HW	Cámara IP	Jefe de sistemas	X	X	X	M
18	CAM07	HW	Cámara IP	Jefe de sistemas	X	X	X	M
19	CAM08	HW	Cámara IP	Jefe de sistemas	X	X	X	M
20	PC001	HW	Equipo de cómputo	Gerencia General	X	X	X	MA
21	PC002	HW	Equipo de cómputo	Secretaria de gerencia	X	X	X	MA
22	PC003	HW	Equipo de cómputo	Jefe de cobranzas	X	X	X	MA
23	PC004	HW	Equipo de cómputo	Jefe de cobranzas	X	X	X	MA
24	PC005	HW	Equipo de cómputo	Jefe de cobranzas	X	X	X	MA
25	PC006	HW	Equipo de cómputo	Jefe de ventas	X	X	X	MA

N°	CÓDIGO	TIPO ACTIVO	DESCRIPCIÓN	RESPONSABLE	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALORACION
26	PC007	HW	Equipo de cómputo	Jefe de ventas	X	X	X	MA
27	PC008	HW	Equipo de cómputo	Jefe de ventas	X	X	X	MA
28	PC009	HW	Equipo de cómputo	Jefe de ventas	X	X	X	MA
29	PC010	HW	Equipo de cómputo	Jefe de ventas	X	X	X	MA
30	PC011	HW	Equipo de cómputo	Jefe de sistemas	X	X	X	MA
31	PC012	HW	Equipo de cómputo	Jefe de sistemas	X	X	X	MA
32	IMP001	HW	Impresora	Jefe de sistemas			X	MB
33	TLF001	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
34	TLF002	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
35	TLF003	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
36	TLF004	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
37	TLF005	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
38	TLF006	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
39	TLF007	HW	Teléfono análogo	Jefe de sistemas	X	X		MB
40	TLF008	HW	Teléfono análogo	Jefe de sistemas	X	X		MB

Anexo G: Mapas de calor

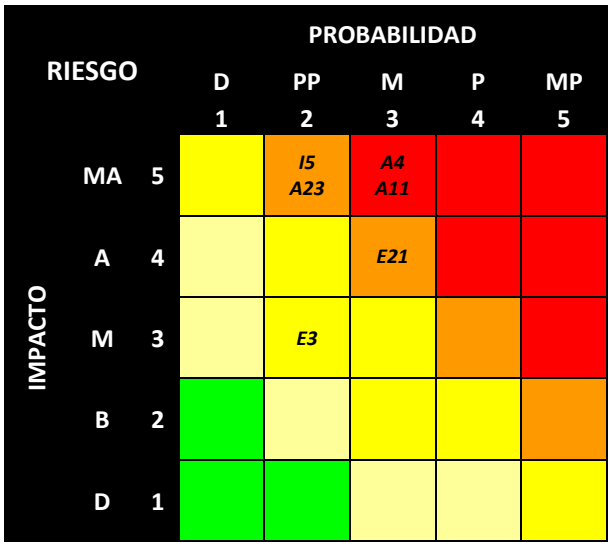
Activo: Router propiedad del ISP

Responsable: Jefe de sistemas



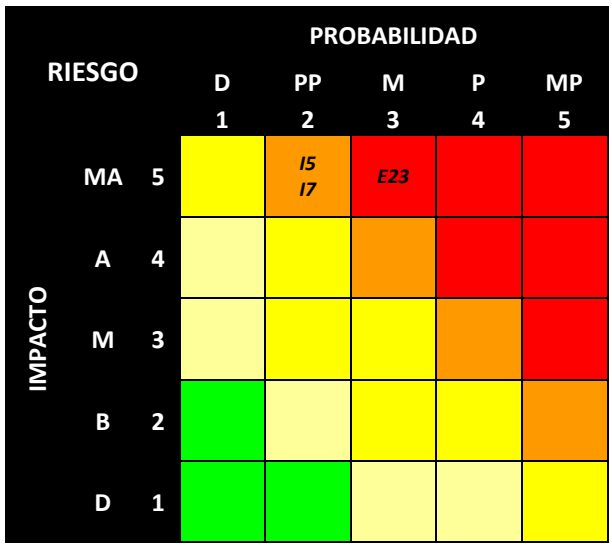
Activo: Firewall interno Fortigate 100D

Responsable: Jefe de sistemas



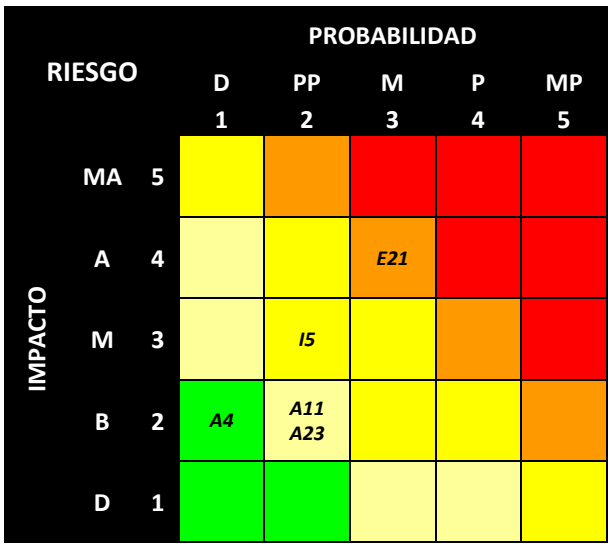
Activo: Switch Tplink interno 16 puertos

Responsable: Jefe de sistemas



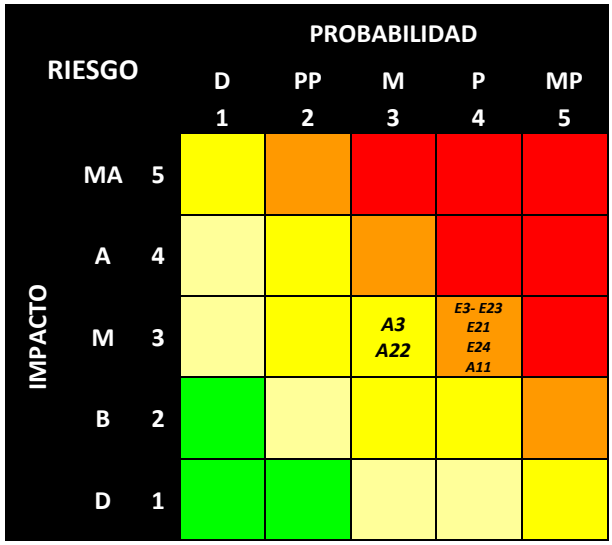
Activo: Router WIFI

Responsable: Jefe de sistemas



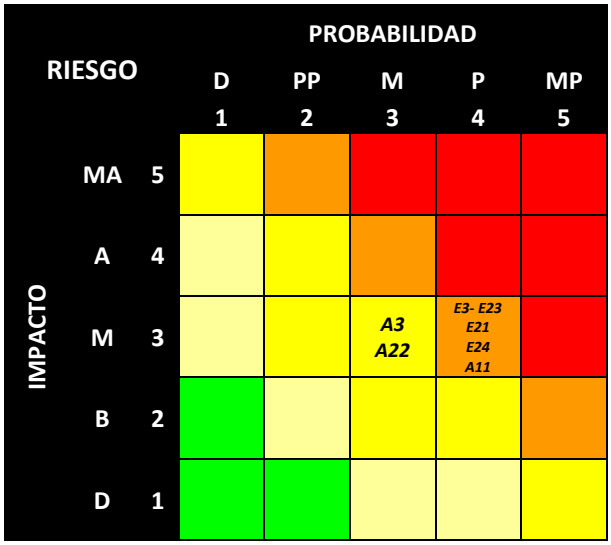
Activo: Server Linux correo electrónico

Responsable: Jefe de sistemas



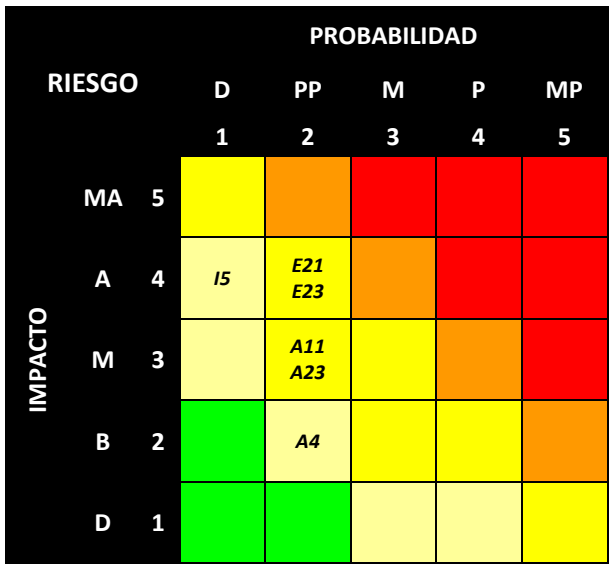
Activo: Server Linux base de datos

Responsable: Jefe de sistemas



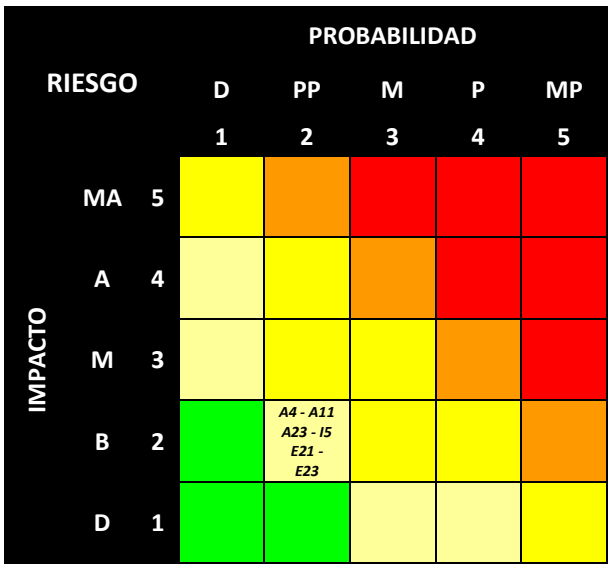
Activo: PBX análogo

Responsable: Jefe de sistemas



Activo: NVR Hikivision

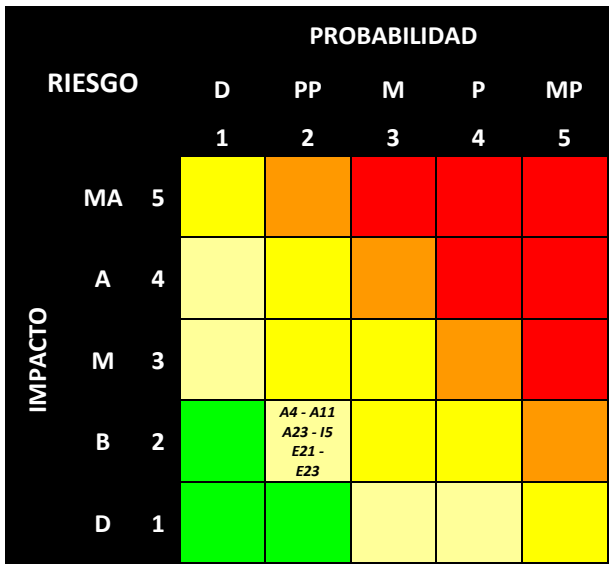
Responsable: Jefe de sistemas



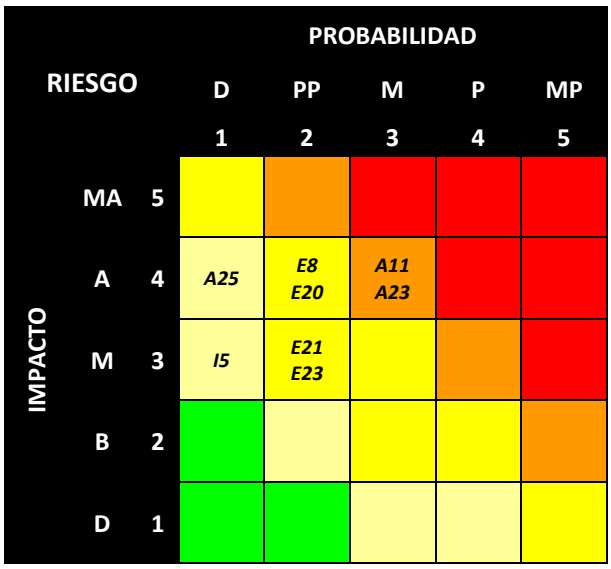
Activo: Cámara IP

Activo: Equipo de cómputo

Responsable: Jefe de sistemas

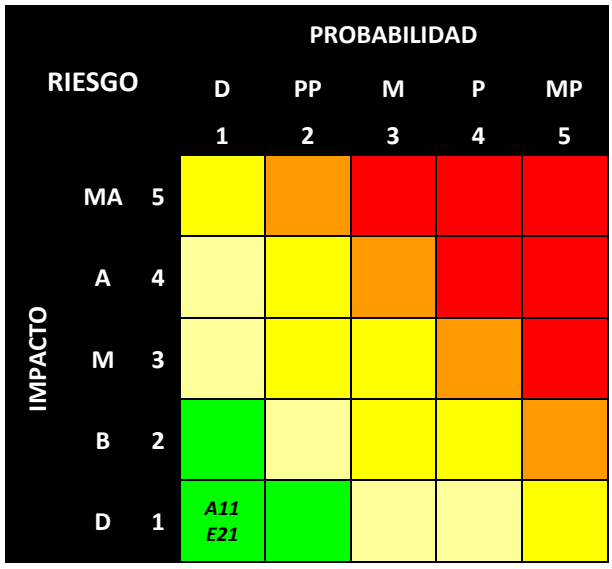


Responsable: Gerencia General, Secretaria de gerencia, Jefe de cobranzas, Jefe de ventas, Jefe de sistemas



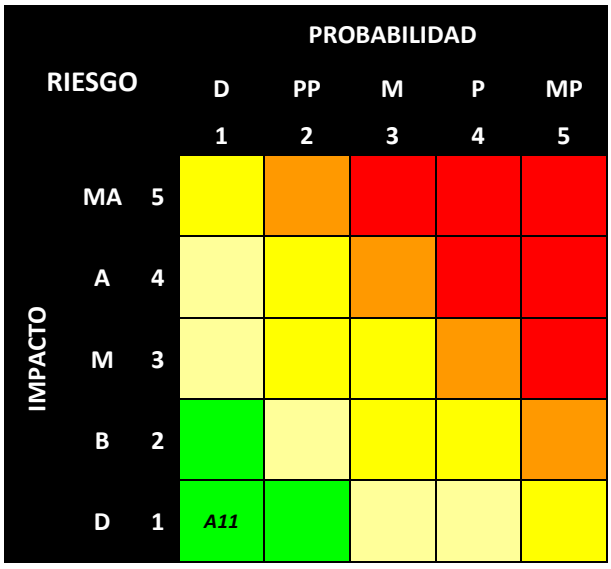
Activo: Impresora

Responsable: Jefe de sistemas



Activo: Teléfono análogo

Responsable: Jefe de sistemas



Anexo H: Impacto Vs Probabilidad

IMPACTO VS PROBABILIDAD						
N°	**DESCRIPCIÓN**	**RESPONSABLE**	**AMENAZAS**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
1	Router propiedad del ISP	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	2	3	6
			[I.5] Avería de origen físico o lógico	1	4	4
			[A.4] Manipulación de la configuración	1	4	4
			[A.11] Acceso no autorizado	1	5	5
			[A.23] Manipulación de los equipos	1	4	4
2	Firewall interno Fortigate 100D	Jefe de sistemas	[E.3] Errores de monitorización	3	2	6
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12
			[I.5] Avería de origen físico o lógico	2	5	10
			[A.4] Manipulación de la configuración	3	5	15
			[A.11] Acceso no autorizado	3	5	15
			[A.23] Manipulación de los equipos	2	5	10
3	Switch Tplink interno 16 puertos	Jefe de sistemas	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	15
			[I.5] Avería de origen físico o lógico	2	5	10
			[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	10
4	Router WIFI	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12
			[I.5] Avería de origen físico o lógico	2	3	6
			[A.4] Manipulación de la configuración	1	2	2

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
4	Router WIFI	Jefe de sistemas	[A.11] Acceso no autorizado	2	2	4
			[A.23] Manipulación de los equipos	2	2	4
5	Server Linux correo electrónico	Jefe de sistemas	[E.3] Errores de monitorización	3	4	12
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	12
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12
			[E.24] Caída del sistema por agotamiento de recursos	3	4	12
			[A.3] Manipulación de los registros de actividad	3	3	9
			[A.11] Acceso no autorizado	3	4	12
			[A.22] Manipulación de los equipos	3	3	9
6	Server Linux base de datos	Jefe de sistemas	[E.3] Errores de monitorización	3	4	12
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	12
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12
			[E.24] Caída del sistema por agotamiento de recursos	3	4	12
			[A.3] Manipulación de los registros de actividad	3	3	9
			[A.11] Acceso no autorizado	3	4	12
			[A.22] Manipulación de los equipos	3	3	9
7	PBX análogo	Jefe de sistemas	[A.4] Manipulación de la configuración	2	2	4
			[A.11] Acceso no autorizado	2	3	6
			[A.23] Manipulación de los equipos	2	3	6
			[I.5] Avería de origen físico o lógico	1	4	4
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	8
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	8

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
8	NVR Hikivision	Jefe de sistemas	[A.4] Manipulación de la configuración	2	2	4
			[A.11] Acceso no autorizado	2	2	4
			[A.23] Manipulación de los equipos	2	2	4
			[I.5] Avería de origen físico o lógico	2	2	4
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	4
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	2	4
9	Cámara IP	Jefe de sistemas	[A.4] Manipulación de la configuración	2	2	4
			[A.11] Acceso no autorizado	2	2	4
			[A.23] Manipulación de los equipos	2	2	4
			[I.5] Avería de origen físico o lógico	2	2	4
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	4
10	Equipo de cómputo	Gerencia General Secretaria de gerencia Jefe de cobranzas Jefe de cobranzas Jefe de cobranzas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de ventas Jefe de sistemas Jefe de sistemas	[A.11] Acceso no autorizado	3	4	12
			[A.23] Manipulación de los equipos	3	4	12
			[A.25] Robo	1	4	4
			[I.5] Avería de origen físico o lógico	1	3	3
			[E.8] Difusión de software dañino	2	4	8
			[E.20] Vulnerabilidades de los programas (software)	2	4	8
			[E.21] Errores de mantenimiento / actualización de programas (software)	2	3	6
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	6

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
11	Impresora	Jefe de sistemas	[A.11] Acceso no autorizado	1	1	1
			[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1
12	Teléfono análogo	Jefe de sistemas	[A.11] Acceso no autorizado	1	1	1

ANEXO I: Controles de Riesgo

CONTROLES DE RIESGOS								
N°	**DESCRIPCIÓN**	**RESPONSABLE**	**AMENAZAS**	**VULNERABILIDADES**	**RIESGO**	**TRATAMIENTO**	**TIPO DE CONTROL**	**CONTROLES**
1	Router propiedad del ISP	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	Uso de software obsoletos con vulnerabilidades conocidas, provocando fallos de seguridades.	6	Transferir	Prevención	Análisis de vulnerabilidades y parches.
			[I.5] Avería de origen físico o lógico	Interrupción total del servicio	4	Transferir	Prevención	Enlaces de contingencias.
			[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos	4	Transferir	Monitorización/Prevención	Registros de actividades, Logs.
			[A.11] Acceso no autorizado	Falta de listas de accesos de remotos permitidos.	5	Transferir	Prevención/Monitorización/Eliminación	Política de Control de Acceso.
			[A.23] Manipulación de los equipos	No utilización de espacios adecuados como gabinetes/racks cerrados con su debida protección.	4	Transferir	Prevención/Monitorización/Eliminación	Protección de equipos. Aseguramiento de disponibilidad.
2	Firewall interno Fortigate 100D	Jefe de sistemas	[E.3] Errores de monitorización	Detección tardía de accesos a herramientas o aplicaciones no autorizados	6	Mitigar	Monitorización/ Eliminación	Herramienta de monitorización
			[E.21] Errores de mantenimiento / actualización de programas (software)	Uso de software obsoletos con vulnerabilidades conocidas, provocando fallos de seguridades.	12	Mitigar	Prevención/Monitorización	Gestión de las vulnerabilidades técnicas
			[I.5] Avería de origen físico o lógico	Interrupción total del servicio	10	Evitar	Prevención	Política de Control de Acceso.
			[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos	15	Mitigar	Prevención	Acceso a redes y a servicios en red.
			[A.11] Acceso no autorizado	Manipulaciones en la configuración existente	15	Mitigar	Detección/Eliminación	Política de Control de Acceso. Restricción de acceso a información
			[A.23] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.	10	Evitar	Prevención	Política de Control de Acceso.

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	VULNERABILIDADES	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
3	Switch Tplink interno 16 puertos	Jefe de sistemas	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad y inestabilidad en la red, afectando la comunicación entre los dispositivos de la red	15	Evitar	Prevención/Monitorización	Gestión de las vulnerabilidades técnicas
			[I.5] Avería de origen físico o lógico	Interrupción total del servicio	10	Mitigar	Prevención/Monitorización	Política de Control de Acceso.
			[I.7] Condiciones inadecuadas de temperatura o humedad	Pérdida de conectividad y daño físico a los componentes	10	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red.
4	Router WIFI	Jefe de sistemas	[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad a dispositivos conectados. Pérdida de datos.	12	Mitigar	Monitorización	Aseguramiento de la disponibilidad.
			[I.5] Avería de origen físico o lógico	Pérdida de conectividad de dispositivos conectados	6	Aceptar	Prevención	Herramienta de monitoreo del estado de los recursos.
			[A.4] Manipulación de la configuración	Cambios no autorizados en ajustes críticos	2	Mitigar	Prevención	Política de Control de Acceso. Acceso a redes y a servicios en red.
			[A.11] Acceso no autorizado	Manipulaciones en la configuración existente	4	Mitigar	Prevención	Política de Control de Acceso. Restricción de acceso a información
			[A.23] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.	4	Transferir	Prevención	Control de accesos físicos. Mantenimiento de equipos.
5	Server Linux correo electrónico	Jefe de sistemas	[E.3] Errores de monitorización	Fallos en detección temprana de uso de recursos, ataques y accesos no autorizados	12	Transferir	Monitorización	Política de Control de Acceso. Restricción de acceso a información
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	VULNERABILIDADES	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
5	Server Linux correo electrónico	Jefe de sistemas	[E.24] Caída del sistema por agotamiento de recursos	Problemas de rendimiento, interrupción del servicio	12	Mitigar	Prevención/Monitorización/Eliminación	Mantenimiento de equipos.
			[A.3] Manipulación de los registros de actividad	Detección tardía de actividades maliciosas.	9	Evitar	Monitorización/ Eliminación	Herramienta de monitorización
			[A.11] Acceso no autorizado	Manipulaciones en la configuración existente	12	Mitigar	Prevención	Política de Control de Acceso. Restricción de acceso a información
			[A.22] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.	9	Mitigar	Prevención	Control de accesos físicos. Mantenimiento de equipos.
6	Server Linux base de datos	Jefe de sistemas	[E.3] Errores de monitorización	Fallos en detección temprana de uso de recursos, ataques y accesos no autorizados	12	Mitigar	Monitorización	Política de Control de Acceso. Restricción de acceso a información
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de conectividad, problemas de rendimiento, pérdida de datos, interrupción del servicio.	12	Mitigar	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
			[E.24] Caída del sistema por agotamiento de recursos	Problemas de rendimiento, interrupción del servicio	12	Mitigar	Prevención/Monitorización/Eliminación	Mantenimiento de equipos.
			[A.3] Manipulación de los registros de actividad	Detección tardía de actividades maliciosas.	9	Evitar	Monitorización/ Eliminación	Herramienta de monitorización
			[A.11] Acceso no autorizado	Manipulaciones en la configuración existente	12	Mitigar	Prevención	Política de Control de Acceso. Restricción de acceso a información
			[A.22] Manipulación de los equipos	Daños físicos de equipos por manipulación incorrecta.	9	Mitigar	Prevención	Control de accesos físicos. Mantenimiento de equipos.

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	VULNERABILIDADES	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
7	PBX análogo	Jefe de sistemas	[A.4] Manipulación de la configuración	Modificación no autorizada de enrutamientos de llamadas, privilegios de usuarios u otras funciones.	4	Transferencia	Prevención	Uso de utilidades con privilegios del sistema.
			[A.11] Acceso no autorizado	Cambios no autorizados en ajustes críticos	6	Transferencia	Prevención	Política de Control de Acceso.
			[A.23] Manipulación de los equipos	Cambios no autorizados en ajustes críticos	6	Transferencia	Prevención	Política de Control de Acceso.
			[I.5] Avería de origen físico o lógico	Pérdida de equipo	4	Evitar	Monitorización/ Eliminación	Seguridad de los equipos fuera de la instalación.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Daños en la configuración a causa de errores no detectados en los mantenimientos y/o actualizaciones.	8	Transferencia	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perdida de operatividad por manipulación inadecuada al momento de realizar trabajos en el equipo.	8	Transferencia	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
8	NVR Hikivision	Jefe de sistemas	[A.4] Manipulación de la configuración	Intentos de eliminar/modificar o dañar grabaciones almacenadas.	4	Mitigar	Monitorización/ Eliminación	Herramienta de monitorización.
			[A.11] Acceso no autorizado	Detección tardía de actividades maliciosas. Fuga de información.	4	Mitigar	Prevención/Monitorización/Eliminación	Protección de los registros de la organización.
			[A.23] Manipulación de los equipos	Detección tardía de actividades maliciosas. Fuga de información.	4	Mitigar	Prevención/Monitorización/Eliminación	Protección de los registros de la organización.
			[I.5] Avería de origen físico o lógico	Detección tardía de actividades maliciosas. Fuga de información.	4	Mitigar	Prevención/Monitorización/Eliminación	Protección de los registros de la organización.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Perdida de operatividad por manipulación inadecuada.	4	Transferencia	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perdida de operatividad por manipulación inadecuada.	4	Transferencia	Prevención/Monitorización	Acceso a redes y a servicios en red. Mantenimiento de equipos.

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	VULNERABILIDADES	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
9	Cámara IP	Jefe de sistemas	[A.4] Manipulación de la configuración	Cambios no autorizados en su funcionalidad como: cambio de contraseñas, desactivación de funciones de seguridad.	4	Mitigar	Prevención	Política de Control de Acceso. Acceso a redes y a servicios en red.
			[A.11] Acceso no autorizado	Detección tardía de actividades maliciosas. Fuga de información.	4	Mitigar	Prevención/Monitorización/Eliminación	Protección de los registros de la organización.
			[A.23] Manipulación de los equipos	Movimientos de enfoque en dispositivos con el objetivo de evadir algún punto de vista ciego al que se tenga monitoreo de cámaras.	4	Mitigar	Prevención/Monitorización/Eliminación	Registro de administración y operación. Restricción de acceso a información.
			[I.5] Avería de origen físico o lógico	Daños la integridad del dispositivo.	4	Mitigar	Prevención	Emplazamiento y protección de equipo.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Perdida de configuraciones establecidas.	4	Transferencia	Prevención/Monitorización	Políticas para la seguridad de la información.
10	Equipo de cómputo	Gerencia General Secretaria de gerencia Jefe de cobranzas Jefe de ventas Jefe de sistemas	[A.11] Acceso no autorizado	Instalación de software maliciosos, acceso a datos sensibles, Fuga de información, suplantación de identidad	12	Mitigar	Detección/Eliminación	Política de Control de Acceso. Restricción de acceso a información
			[A.23] Manipulación de los equipos	Manipulación de hardware, instalación de software maliciosos, acceso a datos sensibles, fuga de información, suplantación de identidad.	12	Evitar	Prevención	Política de Control de Acceso. Avería de origen físico o lógico
			[A.25] Robo	Acceso a datos sensibles, fuga de información.	4	Mitigar	Prevención/Monitorización/Eliminación	Perímetro de seguridad física.
			[I.5] Avería de origen físico o lógico	Pérdida de equipo e información sensible.	3	Mitigar	Prevención/Monitorización/Eliminación	Soportes físicos en tránsito. Retirada o reasignación de los derechos de acceso
			[E.8] Difusión de software dañino	Suplantación de identidad, fuga de información, ataques a la red	8	Evitar	Prevención/Eliminación	Acceso a redes y a servicios en red. Mantenimiento de equipos.

N°	DESCRIPCIÓN	RESPONSABLE	AMENAZAS	VULNERABILIDADES	RIESGO	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
10	Equipo de cómputo	Gerencia General Secretaria de gerencia Jefe de cobranzas Jefe de ventas Jefe de sistemas	[E.20] Vulnerabilidades de los programas (software)	Softwares desactualizados, exposición a nuevos ataques	8	Evitar	Prevención/Eliminación	Controles contra el código malicioso.
			[E.21] Errores de mantenimiento / actualización de programas (software)	Pérdida de información, exposición a nuevos ataques.	6	Transferencia	Prevención/Monitorización/Eliminación	Revisión de políticas para la seguridad de la información.
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Pérdida de información.	6	Transferencia	Prevención/Monitorización/Eliminación	Políticas para la seguridad de la información.
11	Impresora	Jefe de sistemas	[A.11] Acceso no autorizado	Fuga de información.	1	Evitar	Monitorización/ Eliminación	Herramienta de monitorización
			[E.21] Errores de mantenimiento / actualización de programas (software)	Firmwares desactualizados, ataques de red	1	Evitar	Monitorización/ Eliminación	Herramienta de monitorización
12	Teléfono análogo	Jefe de sistemas	[A.11] Acceso no autorizado	Intercepción de información, Fuga de información.	1	Evitar	Monitorización/ Eliminación	Herramienta de monitorización