UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

FACULTAD CIENCIAS DE LA VIDA Y TECNOLOGÍAS

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

"DISEÑO DE UNA ESTRATEGIA DE SEGURIDAD INFORMÁTICA EN ATAQUES DE RANSOMWARE PARA POTENCIAR EL ÁREA DE TI EN SARDIPAC"

AUTORA:

MIELES PITA SILVIA MARINA

TUTOR:

ING. JORGE HERRERA TAPIA, PhD.

MANTA – MANABÍ – ECUADOR

2025-2

CERTIFICACIÓN

En calidad de docente tutor(a) de la Facultad de Ciencias de la Vida y Tecnologías de la Carrera de Tecnologías de la Información de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de Integración Curricular bajo la autoría de la estudiante Mieles Pita Silvia Marina, legalmente matriculado/a en la carrera de Tecnologías de la Información, período académico 2025-2026, cumpliendo el total de 384 horas, cuyo tema del proyecto es **"DISEÑO DE UNA ESTRATEGIA DE SEGURIDAD INFORMÁTICA EN ATAQUES DE RANSOMWARE PARA POTENCIAR EL ÁREA DE TI EN SARDIPAC".**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad de este, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 04 de febrero de 2025

Lo certifico,

Firmado electrónicamente por:
JORGE SERGIO HERRERA TAPIA
Validar únicamente con FirmaEC

Ing. Jorge Herrera Tapia PhD

Docente Tutor

Área: Redes de comunicaciones

DECLARACIÓN EXPRESA DE AUTORÍA

Yo**, Mieles Pita Silvia Marina**, portadora de la cédula de ciudadanía N.º **131667007-2**, en calidad de autora de trabajo de titulación titulado:

"DISEÑO DE UNA ESTRATEGIA DE SEGURIDAD INFORMÁTICA EN ATAQUES DE RANSOMWARE PARA POTENCIAR EL ÁREA DE TI EN SARDIPAC"

Declaro que el presente trabajo es original y de mi autoría; que ha sido elaborado bajo mi responsabilidad y que he citado y referenciado correctamente todas las fuentes utilizadas, respetando las disposiciones legales vigentes en materia de derechos de autor.

Asimismo, autorizo a la **Universidad Laica "Eloy Alfaro de Manabí"** a utilizar este trabajo con fines académicos e investigativos, así como a publicarlo y difundirlo en su repositorio digital institucional, conforme a la normativa vigente.

En constancia de lo expuesto, firmo la presente declaración.

Firmado electrónicamente por:
SILVIA MARINA
MIELES PITA
Validar únicamente con FirmaEC

Mieles Pita Silvia Marina

CI:131667007-2

Dedicatoria

Le dedico este trabajo a Dios por ser mi guía y fortaleza a cada paso de este camino.

A mis padres, por su amor incondicional, su sacrificio y su apoyo constante, que hicieron posible alcanzar este logro.

Agradecimiento

A Dios por permitirme alcanzar este logro y guiar cada paso de mi camino.

A mis padres, por ser el pilar fundamental en mi vida. Gracias por acompañarme en todo este proceso, por su apoyo incondicional, por sus palabras de aliento y por enseñarme a no rendirme nunca.

A mis hermanos y a cada miembro de mi familia que estuvo presente durante mi formación universitaria, brindándome ánimo, confianza y cariño en cada etapa.

A mis tíos, especialmente a mi tía Maribel, por ser como una segunda mamá para mí, por su amor y su apoyo sincero.

A mis amigos, con quienes compartí esta etapa tan significativa, haciendo que cada desafío fuera más llevadero, cada día más alegre y cada recuerdo inolvidable.

A Maholy, mi primera amiga en la facultad con quien compartí mucho más que tareas y clases; vivimos intensamente cada momento de estos años que pasaron tan rápido. Esta amistad la llevaré siempre en mi corazón.

También quiero agradecerle a una persona especial que me acompañó durante gran parte de mi carrera. Incluso en la distancia, fue un apoyo invaluable, escuchando cada dificultad y cada inquietud. Siempre tuvo las palabras adecuadas y supo recordarme lo capaz que soy. Sin duda, este recorrido fue mucho mejor con su compañía.

Finalmente, agradezco a mi tutor, Ing. Jorge Herrera, por su orientación, sus valiosas observaciones y su apoyo constante a lo largo del desarrollo de este trabajo.

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

La digitalización ha traído consigo importantes cambios que han trascendido hasta el sector empresarial, pero a su vez ha significado un reto en términos de ciberseguridad debido a la exposición constante a vulnerabilidades tecnológicas como el ransomware, volviéndose una amenaza para la integridad y confidencialidad de la información. Con base en lo anterior, este trabajo tuvo como objetivo diseñar una estrategia de seguridad informática orientada a la prevención y respuesta ante ataques de ransomware, con el fin de fortalecer el área de Tecnologías de la Información en la empresa Sardipac. Para esto se utilizó una metodología de enfoque mixto, aplicando una encuesta a 13 colaboradores y una entrevista a 2 técnicos de seguridad informática que brindan soporte externo a la organización, posteriormente, con estos datos se realizó un análisis de riesgos bajo la metodología Magerit. Como resultados se pudo conocer que los datos internos, los dispositivos móviles y el personal son los activos que presentaron niveles más altos de riesgo ante incidentes como fugas de información, divulgación de información, acceso no autorizado, extorsión e ingeniería social. Con base en esto se diseñó una estrategia de seguridad informática basada en la prevención, detección temprana, respuesta y formación del personal ante ataques ransomware; esto permitió además establecer indicadores de evaluación medibles para comprobar la efectividad de la propuesta. Se pudo concluir que la empresa se enfrenta a riesgo constante de vulneración de información por lo que resulta efectivo efectuar evaluaciones constantes y adoptar medidas de control.

Palabras clave: Ransomware, ciberseguridad, Magerit, vulnerabilidades, phishing

Abstract

Digitization has brought about significant changes that have transcended the business sector, but at the same time, it has posed a challenge in terms of cybersecurity due to constant exposure to technological vulnerabilities such as ransomware, becoming a threat to the integrity and confidentiality of information. Based on the above, the objective of this work was to design an IT security strategy aimed at preventing and responding to ransomware attacks, in order to strengthen the Information Technology area at Sardipac. To this end, a mixed-method approach was used, applying a survey to 13 employees and an interview to two IT security technicians who provide external support to the organization. Subsequently, this data was used to perform a risk analysis using the Magerit methodology. The results showed that internal data, mobile devices, and personnel are the assets that presented the highest levels of risk in the event of incidents such as information leaks, information disclosure, unauthorized access, extortion, and social engineering. Based on this, an IT security strategy was designed based on prevention, early detection, response, and staff training in the event of ransomware attacks. This also made it possible to establish measurable evaluation indicators to verify the effectiveness of the proposal. It was concluded that the company faces a constant risk of information breaches, making it effective to carry out constant evaluations and adopt control measures.

Keywords: Ransomware, cybersecurity, Magerit, vulnerabilities, phishing

Introducción

Este trabajo de investigación indaga acerca de las acciones que pueden implementarse como parte de una estrategia de seguridad informática ante ataques de ransomware con lo que se busca potenciar el área de Tecnologías de la Información de la empresa Sardipac, ubicada en la vía Manta-Rocafuerte y cuyas operaciones principales se orientan al procesamiento de productos enlatados del mar. Con esto se ha buscado identificar criterios de vulnerabilidad en los que caben acciones de mejora con la finalidad de fomentar una cultura de ciberseguridad dentro de esta organización que maneja información sensible sobre sus clientes y operaciones.

En ese sentido, se debe mencionar que la ciberseguridad en las empresas ha tomado especial relevancia en los últimos años debido a la proliferación de modalidades de ataque a las infraestructuras informáticas cada vez más sofisticadas como el ransomware, el phishing y la ingeniería social, por ende resulta clave realizar análisis de riesgos que conlleven a identificar activos vulnerables a estos ataques, riesgos potenciales, niveles de amenaza, impactos y salvaguardas, esto por medio de acciones basadas en procedimientos estandarizados y normativa vigente como la ISO/IEC 27001. En ese sentido, este trabajo recoge los criterios de dichos procedimientos para evaluar la realidad institucional y proponer acciones que ayuden a prevenir, mitigar y reducir los impactos de estos ataques. Para ello se realiza una investigación contemplada en cuatro capítulos que se describen a continuación.

El capítulo 1 o planteamiento del problema, recoge la información disponible sobre la realidad estudiada dentro del contexto de interés, además en este se plantean los objetivos que guían la investigación, delimitando su alcance y resultados esperados al culminar el trabajo. El capítulo 2 o marco teórico, detalla el estado de arte o literatura disponible que ha abordado previamente temáticas similares a la de este documento, en este también se definen los principales términos ligados al tema de estudio y que brindan argumentación teórica a la investigación.

El capítulo 3 o metodología, explica a detalle el tipo de investigación realizada, los métodos empleados, la estrategia operacional para la recolección de datos y el análisis y resultados de los resultados, presentados de forma lógica y sistemática. Y finalmente, el capítulo 4 o propuesta recoge las acciones y estrategias que surgen de la fase diagnóstica, permitiendo describir los ejes de mejora, los recursos necesarios, las etapas de ejecución y los resultados al alcanzarse una vez se haya implementado lo formulado.

Capítulo I
Planteamiento del Problema

1.1 Planteamiento del problema

En el contexto digitalizado actual, las organizaciones se enfrentan a amenazas cibernéticas cada vez más avanzadas, siendo el ransomware una de las más peligrosas. Este ataque pone en riesgo la disponibilidad y la confidencialidad de la información, lo que impacta negativamente en la operatividad de los sistemas de las empresas. Según el informe State of Ransomware 2023 de Sophos, el 66% de las empresas encuestadas a nivel global, experimentaron al menos un ataque de ransomware durante ese año, donde en muchos casos, los delincuentes informáticos lograron cifrar los datos (Sophos, 2023).

De hecho, los costos asociados a estos ataques continúan incrementándose, pues según se reportó en el informe de IBM Security (2023), los incidentes de seguridad relacionados con ransomware pueden implicar pérdidas económicas superiores al millón de dólares por evento, sin contar el daño reputacional y la interrupción operativa. Además, la Agencia de Ciberseguridad de la Unión Europea (2022) destacó que una estrategia efectiva contra el ransomware debe incorporar medidas preventivas, entrenamiento constante del personal y planes de recuperación claramente definidos.

Sardipac, como empresa comprometida con el fortalecimiento continuo de su infraestructura tecnológica, reconoce la importancia de anticiparse a los riesgos asociados al ransomware. Este estudio se enfoca específicamente en el área de Tecnologías de la Información (TI), encargada de gestionar los sistemas informáticos y la seguridad digital de la empresa. Aunque actualmente se cuenta con medidas básicas de protección, la creciente sofisticación de las amenazas exige el diseño e implementación de una estrategia más especializada, orientada a mitigar los riesgos de ransomware, proteger los activos digitales clave y garantizar la continuidad operativa del negocio.

1.2 Formulación del problema

¿Cómo diseñar una estrategia de seguridad informática para prevenir y responder ante ataques de ransomware que contribuya a fortalecer el área de Tecnologías de la Información en la empresa Sardipac?

1.3 Objetivos

1.3.1 Objetivo General

Diseñar una estrategia de seguridad informática orientada a la prevención y respuesta ante ataques de ransomware, con el fin de fortalecer el área de Tecnologías de la Información en la empresa Sardipac.

1.3.2 Objetivos específicos

- Diagnosticar el estado actual de la seguridad informática en el área de TI de Sardipac.
- Identificar principales activos, vulnerabilidades y riesgos expuesto a riesgos frente a ataques de ransomware en la organización.
- Revisar estrategias y buenas prácticas en ciberseguridad implementadas por otras organizaciones similares.
- Diseñar una estrategia con un plan de acción que contemple medidas preventivas, de detección y respuesta frente a incidentes de ransomware.
- Establecer indicadores para evaluar la efectividad de la estrategia diseñada.

1.4 Justificación

El ransomware se ha convertido en una amenaza crítica para la ciberseguridad de las empresas, debido a que afecta directamente la operatividad, la reputación y los datos sensibles de estas entidades. Como indica el *Data Breach Investigations Report*, "aproximadamente un tercio de todas las filtraciones involucraron ransomware u otra técnica de extorsión" (Verizon Business, 2024) (*traducción propia*). En este contexto, las empresas requieren desarrollar estrategias de seguridad informática que integren mecanismos efectivos de prevención, detección y respuesta para minimizar el impacto de estos incidentes.

Ante esta realidad, se vuelve prioritario para Sardipac diseñar una estrategia específica de seguridad informática orientada a la prevención, detección y respuesta frente a este tipo de incidentes. Lo propuesto en este trabajo permitirá potenciar las capacidades del área de Tecnologías de la Información, anticiparse a amenazas emergentes y garantizar la continuidad de los procesos críticos del negocio. Las acciones propuestas aportarán valor al proporcionar un enfoque metodológico que facilite la identificación y mitigación de riesgos específicos, promoviendo una cultura organizacional orientada a la seguridad y la resiliencia tecnológica en un entorno dinámico y desafiante.

Capítulo II
Marco Teórico

2.1 Estado del Arte

Algunos estudios han tratado esta problemática desde diversas perspectivas, sugiriendo estrategias para prevenir, detectar y responder antes los ataques de ransomware. Esta tendencia no solo muestra un aumento en la frecuencia de estos ataques, sino también en su complejidad debido a que los cibercriminales utilizan técnicas más sofisticadas, como el cifrado de datos doble, ataques dirigidos y la explotación de vulnerabilidades en la cadena de suministro.

Por ejemplo, el informe "State of Ransomware 2023" de Sophos (2023) reveló que el 66% de las organizaciones encuestadas fueron víctimas de ataques en el año 2022, esto demuestra la creciente vulnerabilidad en la que incluso las empresas que cuentan con medidas de protección mínimas no están exentas de tener que enfrentarse a estas situaciones. El informe destaca que en el 76% de casos, los atacantes logran cifrar la información, y lo que resulta más preocupante es que el 46% de las empresas estuvieron dispuestas a pagar por el rescate, aunque esto no significó lamentablemente que recuperaran la mayoría de su información y datos, esta realidad evidencia la necesidad de establecer estrategias de seguridad integrales, así como el hecho de que pagar un rescate no es garantía de que se pueda recuperar la información sensible de una entidad.

En el estudio de Paniagua Soza (2022) titulado “Anatomía del ransomware”, el autor presenta y permite ver un análisis técnico y estructural del ransomware desde sus orígenes, explicando detalladamente cómo comenzó hasta cómo se fue dando su evolución, asimismo aborda con detalle la arquitectura interna de estos programas maliciosos, las tácticas utilizadas por los cibercriminales y los mecanismos de cifrado aplicados para extorsionar a las víctimas. Esta investigación destaca por su enfoque experimental, en el que se realiza un análisis de laboratorio de un tipo de ransomware en específico, permitiendo comprender su comportamiento, vectores de ataque y estrategias de propagación. Lo que es de ayuda y aporte para esta investigación porque brinda información sustancial para entender cómo funciona el ransomware, su historia y evolución.

Por otro lado, algo que se consideró importante agregar y mencionar, es la forma en que el impacto de este tipo de extorciones y amenaza se expanden alrededor de todo el mundo sin excepciones, respecto a ello Avila Niño (2023) analizó el aumento del ransomware en Latinoamérica en su trabajo “Ransomware, una amenaza latente en Latinoamérica”, por medio de este examina el crecimiento del ransomware desde 2015, destacando los países más

vulnerables a dichos ataques, las variantes más comunes de ransomware y las principales debilidades en la infraestructura de ciberseguridad que facilitan sus propagación.

Dentro de estos razonamientos cabe agregar que, el ransomware ha evolucionado en términos de complejidad y objetivos, generando distintas categorías que varían según su sofisticación, pues tal como detalla Paniagua Soza (2022), existen tres tipos principales de estas amenazas como son: el ransomware de cifrado, que bloquea los archivos del usuario y exige un rescate para obtener la clave de descifrado; el ransomware de bloqueo, que impide el acceso al sistema operativo; y el ransomware híbrido, que emplea ambos métodos para causar un mayor impacto en las victimas.

Asimismo, en reportes de ESET (2024) y Kaspersky (2025) se habla de los métodos de propagación, indicando que los principales vectores de infección incluyen correos electrónicos con archivos adjuntos maliciosos, enlaces fraudulentos (phishing), descargas desde sitios comprometidos, vulnerabilidades en servicios de escritorio remoto (RDP) y campañas de malvertising. Resaltan además que, los ataques se han vuelto cada vez más dirigidos, llegando a utilizar ingeniería social para engañar a empleados o usuarios específicos dentro de las organizaciones. En América Latina, las variantes más detectadas en los últimos años corresponden a familias como LockBit, Conti, BlackCat y Hive, que han afectado infraestructuras críticas y entidades públicas (Kaspersky, 2025). Comprender estas tipologías y métodos de propagación resulta esencial para el desarrollo de estrategias de defensa efectivas y políticas de prevención adaptadas a la realidad digital ecuatoriana, donde las brechas de seguridad continúan siendo un desafío significativo.

En el ámbito académico, estudios como el de Zapata Chasiguasin (2020), realizado en la Universidad Técnica de Ambato, proponen la implementación de sistemas de seguridad basados en normativas internacionales como ISO/IEC 27001 para fortalecer la infraestructura tecnológica y la gestión de la seguridad de la información en instituciones públicas. En su análisis se identifican como principales deficiencias la falta de capacitación del personal, el uso inadecuado de contraseñas y la ausencia de planes de recuperación ante desastres.

Otro trabajo relevante es el de Salas-Riega et al. (2025), quienes analizaron la eficacia de los marcos NIST para la prevención de ataques informáticos, concluyendo que la adopción de este tipo de estructuras mejora significativamente los tiempos de respuesta y recuperación ante incidentes. Estos investigadores proponen un enfoque práctico basado en las cinco

funciones del marco NIST: identificar, proteger, detectar, responder y recuperar, adaptadas a la realidad de empresas medianas.

Las acciones más implementadas en las empresas son la protección de datos sensibles (72%), la capacitación al personal (70%) y el despliegue de planes integrales de seguridad digital (67%). Estas iniciativas reflejan una evolución desde una visión reactiva hacia enfoques más preventivos y estructurados, aunque factores como la limitación presupuestaria (45%) y la escasez de talento especializado siguen siendo desafíos significativos (IT Ahora, 2025).

Asimismo, Trujillo Alvira (2024) planteó un plan de seguridad para la empresa de tecnología QWERTY S.A., de Colombia, para esto hizo una evaluación de riesgos bajo los lineamientos Magerit, diseñó una política se seguridad para la organización y ejecutó una serie de acciones que involucraron la gestión de riesgos identificados y capacitación del personal, con ello abordó el problema de la empresa desde un enfoque integral empelando procedimientos estandarizados y normativa vigente como la ISO 27001.

En ese mismo contexto, Duque Agudelo (2022) realizaron un plan de seguridad informática para la empresa de prestación de servicios automotrices Socia BPO, para esto realizaron una evaluación de riesgos bajo la norma ISO/IEC 27001, para posteriormente fijar acciones como el diseño de políticas de seguridad, creó MZ para granja de servidores, implementó Email Security Gateway, propuso la contratación de auditoría externa, incentivó a la capacitación del personal, estableció como prioridad el cifrado de equipos e implementó software antivirus.

En el contexto ecuatoriano, diversos proyectos de titulación han demostrado la utilidad de aplicar metodologías como MAGERIT para la evaluación de riesgos tecnológicos en pequeñas y medianas empresas, permitiendo una mejor priorización de activos y control de amenazas. La metodología facilita el análisis detallado de los activos de información, la identificación de vulnerabilidades y la asignación de controles adecuados según el nivel de riesgo (Guamán et al., 2023; Jácome Segovia et al., 2021; Paez y Portilla, 2024).

Dentro de este contexto, Sánchez y Andaluz (2024) llevaron a cabo un estudio con el cual buscaron identificar tecnologías que aporten a la seguridad de las empresas de la ciudad de Guayaquil, para ello realizaron un sondeo sobre la realidad de estas entidades dentro de la localidad encontrando importantes limitaciones, con base en esto propusieron la adopción de estrategias como la integración de tecnología avanzada de seguridad de equipos y sistemas,

capacitación en ciberseguridad y medidas de control de riesgos conforme con la realidad de cada organización.

Por otra parte, Moya Gavilanes (2023) realizó una propuesta para mejorar la seguridad informática de la empresa Municipal de Agua Potable y Alcantarillado de Ambato, para esto primero evaluó la situación de seguridad de esta institución a fin de identificar vulnerabilidades potenciales y en apego a la norma ISO 27001 propuso como estrategias de mejora, difundir la política de seguridad de la información entre los departamentos, asignar responsabilidades al personal encargado del área de seguridad informática, capacitación del personal y mejora continua del sistema de seguridad informática.

A pesar de que existen diversas investigaciones sobre el impacto y las estrategias de defensa contra el ransomware, la mayoría de los estudios llegan a conclusiones similares sobre la necesidad urgente de adoptar estrategias de seguridad cibernética más avanzadas y especializadas. Sin embargo, es evidente que hacen falta investigaciones profundas centradas en el diseño de estrategias específicas para mitigar este tipo de amenazas en empresas. La mayoría de las investigaciones existentes se enfocan en las generalidades del ransomware y su evolución, pero no abordan de manera detallada cómo estas estrategias pueden ser implementadas eficazmente en sectores empresariales específicos. Este vacío en la investigación justifica el propósito de este estudio, orientado a diseñar una estrategia de seguridad informática, con el fin de diagnosticar el estado actual de la seguridad, identificar vulnerabilidades y riesgos específicos y establecer un plan de acción que fortalezca el área de Tecnologías de la Información.

2.2 Definiciones conceptuales

2.2.1 Seguridad Informática

Con respecto a este tema Vega Briceño (2021) destaca que, la seguridad de la información se ha convertido en un aspecto fundamental en la sociedad actual, caracterizada por la alta conectividad, a tal nivel que la adopción masiva de tecnologías de información y comunicación ha trasformado profundamente la vida cotidiana. Sin embargo, esta integración de la tecnología también significa numerosos riesgos de seguridad, debido a que si los sistemas que almacenan información crítica, como las cuentas bancarias o los datos de los empleados, son vulnerables a ciberataques, las consecuencias pueden ser devastadoras. Estos riesgos incluyen la pérdida de fondos personales o pérdidas millonarias para las empresas, además de daños a su reputación y problemas legales debido a fallos de seguridad en sus sistemas, sobre

todo al considerar que la frecuencia de estos incidentes es cada vez mayor, que hace cinco, diez o veinte años atrás.

2.2.2 Ransomware

El Instituto Nacional de Ciberseguridad (2021) de España, define al ransomware como un “Malware cuya funcionalidad es «secuestrar» un dispositivo, equipo, o la información y datos que posee haciendo de esta forma que, si la víctima no está dispuesta a pagar un rescate económico, no podrá volver a acceder a su información” (p. 65). Incluso si las víctimas pagan el rescate, a veces siguen sin poder recuperar sus datos, lo cual se debe principalmente a que el atacante no ha cumplido su promesa o a que la víctima ha borrado accidentalmente el archivo con la clave de descifrado (Albshaier et al., 2024).

En adición a lo anterior, Kritika (2025) detalla que el ransomware es un malware en rápida evolución cuyo objetivo principal es cifrar los archivos de los dispositivos electrónicos para que no puedan utilizarse en el futuro. La aparición prematura de este tipo de ataque se remonta a 1989, cuando salió a la luz el malware troyano AIDS. Se ha demostrado que los recientes avances en este tipo de ataques se deben a vectores de amenaza más sofisticados con transfiguración multidimensional.

Esta se ha convertido en la modalidad de ataque más utilizada por los ciberdelincuentes alrededor del mundo, pues según detallan Albshaier et al. (2024), estos han ido en aumento desde la creación de Internet en 1989. Los autores explican que, el primer ataque de esta naturaleza se dio ese mismo año en el contexto de una conferencia de la OMS, llevado a cabo por el biólogo Joseph L. Popp originario de Ohio, este se denominó "Troyano del SIDA" (AIDS Trojan) o "PC Cyborg", la modalidad consistió en enviar 20,000 disquetes infectados a asistentes de dicha conferencia, y como rescate pidió el envío de 189 dólares estadounidenses a una oficina de correos de Panamá para liberar archivos cifrados.

A lo largo de las décadas, el ransomware se ha vuelto mucho más sofisticado y extendido, aprovechando todo el ecosistema de la ciberdelincuencia y la Dark Web. El auge de las criptomonedas en 2010 proporcionó a los delincuentes un método fácil para cobrar rescates y mantener un mayor anonimato, lo que permitió que este tipo de ciberdelincuencia se convirtiera en algo lucrativo. En 2013, CryptoLocker se convirtió en el primero de su clase, aprovechando no solo los pagos con Bitcoin, sino también el cifrado avanzado, con el troyano bancario Gameover ZeuS como mecanismo de distribución. Aunque la operación fue

desmantelada por el FBI estadounidense y los investigadores de CrowdStrike, no tardaron en aparecer clones y variaciones (Hansel y Silomon, 2024).

En esa misma línea de ideas, Nagar (2024) añaden que este ha ido evolucionando hasta encontrarse un ransomware de nueva generación que aplica un cifrado sofisticado, por lo que, sin pagar el rescate, los archivos no pueden ni deben recuperarse. También incorpora el modelo Ransomware-as-a-Service (RaaS), que hace que el ransomware sea accesible para cualquiera debido a su simplicidad de uso, sin necesidad de tener muchos conocimientos de piratería informática. Desde el punto de vista de este autor, la existencia de métodos como la doble extorsión, en la que, además de cifrar los datos, los roban y afirman que los liberarán, se están convirtiendo en algo habitual. Y también coincide en que, la situación se ha agravado con la aparición de criptomonedas como Bitcoin, que permiten a los atacantes alcanzar sus objetivos de otra manera, mediante el pago anónimo de rescates.

En ese contexto, Hansel y Silomon (2024) consideran que el sector privado es el objetivo predominante de estos ataques, aunque en los últimos años también se han dirigido a entidades del sector público involucrando infraestructuras críticas. Con respecto a ello, XYZ señalan que en 2021 se produjo un aumento considerable de ataques de ransomware, de casi más del 150 %, que afectaron a diversos sectores diferentes, como la sanidad, las finanzas y la administración pública (Albshaier et al., 2024).

Actualmente el ransomware se puede clasificar en tres tipos principales: locker, crypto y scareware. El scareware puede utilizar anuncios emergentes para manipular a los usuarios y hacerles creer que deben descargar determinado software, utilizando así técnicas de coacción para descargar malware, se aprovecha del miedo y su objetivo no es causar daño en el ordenador de la víctima sino bloqueas las funciones principales. El locker puede cifrar determinados archivos que bloquean la pantalla y/o el teclado del ordenador, pero por lo general es fácil de superar y a menudo se puede resolver reiniciando el equipo en modo seguro o ejecutando un escáner de virus bajo demanda. El crypto cifra los archivos confidenciales del usuario, pero no interfiere en las funciones básicas del ordenador, puede utilizar uno de estos tres esquemas de cifrado: simétrico, asimétrico o híbrido (Beaman et al., 2021).

2.2.3 Backup

Para el Instituto Nacional de Ciberseguridad (2021) de España, se trata de una copia de seguridad que se realiza en aplicaciones que están contenidas en un ordenador con el objetivo de poder recuperar la información en el caso de que el sistema sufra daños o perdidas no

deseadas y accidentales de los datos que se encuentran almacenados; en se sentido, se considera como una operación que busca salvaguardar los datos de una entidad evitando con ello consecuencias importantes para la infraestructura tecnológica y física.

Asimismo, Shaytura y Pitkevich (2022) explican que esta es una práctica que combina métodos y soluciones para el almacenamiento eficiente y económico de datos con el proceso de computación paralela, lo que da lugar a un efecto sinérgico. Los datos corporativos se copian en una o más ubicaciones con una frecuencia predeterminada y capacidades variables. Se puede configurar una operación de copia de seguridad flexible utilizando la arquitectura propia de la empresa o las soluciones disponibles, combinándolas con el almacenamiento local. Hoy en día existen muchas soluciones técnicas para el almacenamiento corporativo, que permiten a las empresas proteger los datos, evitar su pérdida, prevenir fugas y minimizar costes.

2.2.4 Cortafuegos

Según ha explicado el Instituto Nacional de Ciberseguridad (2021) de España, el cortafuegos se concibe como un:

> Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación. (p. 32)

De manera más detallada, Nabi et al. (2022) explican que, el cortafuegos es el mecanismo de defensa más común utilizado en la seguridad de las redes, el cual impone restricciones a los paquetes que entran o salen de la red privada. Todo el tráfico que sale del interior y viceversa debe pasar por el cortafuegos, pero solo permite el paso al tráfico autorizado, es decir que no da acceso a paquetes a menos que cumplan con una especificación de filtrado o que haya una negociación que implique algún tipo de autenticación.

2.2.5 Gestión de Riesgos

La gestión de riesgos en el ámbito de la seguridad de la información implica un análisis sistemático para identificar amenazas, evaluar vulnerabilidades y aplicar controles, siendo MAGERIT una metodología ampliamente usada para ello en países hispanohablantes. Según

el documento oficial de MAGERIT v3.0, “la gestión de riesgos es el proceso de tomar decisiones sobre la forma de tratar los riesgos, basado en los resultados de un análisis de riesgos. Implica seleccionar e implementar medidas para modificar el riesgo” (Amutio Gómez et al., 2012a).

En ese sentido, se puede argumentar que el hecho de gestionar correctamente los riesgos ayuda a alcanzar una visión global y selectiva de dichos riesgos, así como a la fijación de objetivos con base en la situación actual de la organización, esta “comprende tres tareas básicas esenciales que tienen por objetivo asegurar la continuidad de la empresa, garantizar su éxito a largo plazo y minimizar los costos. La gestión de riesgos influye y engloba todas las áreas de una empresa” (Rossetti y Quiroga, 2023, p. 23).

2.2.6 ISO/IEC 27001

La ISO/IEC 27001 es la norma más reconocida a nivel mundial para realizar la implementación de sistemas de gestión de la seguridad de la información. Esta norma establece los requisitos esenciales para la creación, implementación, y mejora continua de estos sistemas, con el objetivo de gestionar de manera efectiva los riesgos relacionados con la seguridad de los datos, garantizando que las organizaciones sigan buenas prácticas y principios internacionales. Sin importar el tamaño de la empresa o del sector, proporciona orientaciones para establecer, implantar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información.

Acerca de su aplicación en el contexto empresarial la norma describe que “la conformidad con la ISO/IEC 27001 implica que una organización ha implementado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee, respetando todas las buenas prácticas y principios contemplados en esta Norma Internacional” (ISO/IEC, 2022, párr. 3), es decir que su cumplimiento requiere de parámetros claramente definidos, ejecutables y medibles, que permitan corroborar su conformidad de acuerdo con los lineamientos que esta describe.

2.2.7 Ciclo de mejora continua

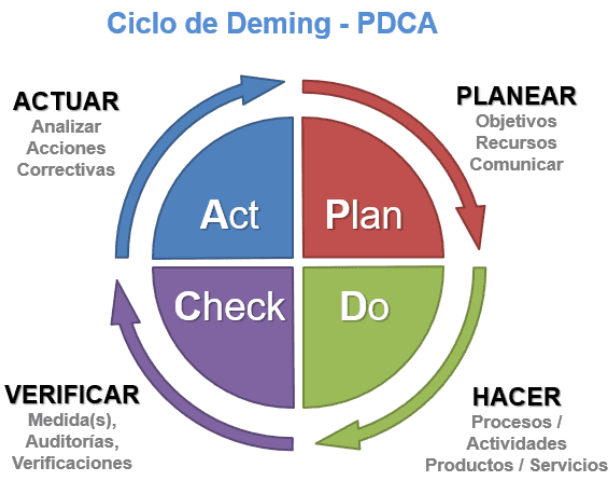
La norma ISO/IEC 27001 incluye un ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) o tambien llamado el Ciclo de Deming (PDCA), que asegura una revisión constante del Área de Tecnologías de la Información (TI), de acuerdo con Gorka y Popek (2025), este consta de cuatro etapas, que representan las siguientes acciones sucesivas:

1) Planificar: establecer y planificar acciones para alcanzar un objetivo determinado.
2) Hacer: llevar a cabo las acciones establecidas a modo de prueba.
3) Verificar: verificar si el plan implementado fue eficaz, si da resultados y cómo se puede mejorar el proceso.
4) Actuar: un proceso perfecto que ha demostrado o corregido errores en un proceso fallido.

En la figura a continuación se muestran cada una de las etapas previamente descritas y sus componentes:

Figura 1

Ciclo de Deming (PDCA)



Nota. Tomado de (Ingeniería de Calidad, 2020)

El uso del Ciclo Deming en organizaciones tecnológicas, educativas o industriales se ha consolidado como una estrategia eficaz para optimizar procesos internos, fomentar la toma de decisiones basada en datos y promover una cultura organizacional centrada en la calidad. En el contexto de la gestión de proyectos o sistemas de información, su aplicación permite reducir fallos, minimizar desperdicios y aumentar la eficiencia operativa a través de revisiones periódicas y adaptaciones constantes (The Deming Institute, 2017).

2.2.8 SGSI

Conforme con lo expuesto por el Instituto Nacional de Ciberseguridad (2021) de España, el SGSI es:

> Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI

es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. (p. 70)

2.3 Fundamentación legal

El diseño de una estrategia de seguridad informática orientada a prevenir y responder ante ataques de ransomware debe enmarcarse en un conjunto de normativas nacionales e internacionales que regulan el uso, protección y gestión de la información en las organizaciones.

2.3.1 Normas internacionales aplicadas

- ISO/IEC 27001: Proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).
- MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): Herramienta promovida por el gobierno español que permite identificar y valorar riesgos sobre activos tecnológicos.

Capítulo III
Metodología

Este capítulo describe el tipo de investigación, los métodos, las técnicas de recolección de datos y los procedimientos de análisis que fueron implementados para el diseño de una estrategia de seguridad informática orientada a la prevención y respuesta ante ataques de ransomware en el área de Tecnologías de la Información de la empresa de Sardipac, este apartado constituye un eje central del trabajo porque conllevó a la obtención de datos teóricos y empíricos esenciales para el desarrollo de una propuesta basada en la evidencia real del contexto analizado que para este caso corresponde a la entidad previamente mencionada.

3.1 Tipo de investigación

Esta investigación se llevó a cabo bajo un enfoque mixto, debido a que combinó métodos tanto cuantitativos como cualitativos. Esto, porque es necesario comprender y abordar de manera integral la problemática de seguridad informática, especialmente en relación con los ataques de ransomware, en el área de Tecnologías de la Información (TI) de la empresa Sardipac, lo que requiere del empleo de metodologías que ayuden a entender la realidad y a proponer acciones concretas apegadas a lo observado.

Investigación Bibliográfica: En esta fase se revisó literatura relevante sobre seguridad informática, ransomware y las estrategias de ciberseguridad que las organizaciones utilizan para protegerse de ataques. Esto permitió establecer una base sólida de teorías y mejores prácticas en la prevención de ransomware que sirvió como referencia para el diseño de la estrategia detallada en este documento.

Investigación empírica: Se recolectaron datos a través de entrevistas, encuestas y observación directa. Estos datos permitieron analizar el estado actual de la seguridad informática en Sardipac, identificando vulnerabilidades y áreas de mejora, elementos que fueron clave para el diseño de acciones propuestas que pueden ser implementadas como medidas de protección de esta entidad.

3.2 Métodos de investigación

3.2.1 Teóricos

Se utilizó un enfoque tanto deductivo como inductivo para el análisis y la aplicación de los conceptos teóricos en la práctica:

- **Deductivo:** Se utilizó un enfoque deductivo en el que se aplicaron teorías generales sobre seguridad Informática y gestión de riesgos a la estructura específica de TI de Sardipac. Esto incluyó la aplicación de normas

internacionales como ISO/IEC 27001:2022 y estrategias de protección contra ransomware.

- **Inductivo:** Se adoptó un enfoque inductivo al analizar los datos empíricos recolectados (encuestas, entrevista y observación) lo que ayudó a identificar patrones específicos dentro de Sardipac y a generar conclusiones sobre las vulnerabilidades y riesgos de seguridad informática frente a ransomware

3.2.2 Empíricos:

La investigación empírica en este trabajo se basó en el uso de análisis de casos para evaluar cómo otras organizaciones han implementado estrategias de seguridad efectivas para prevenir y mitigar los efectos de ransomware. Además, también se realizaron entrevistas con los encargados de TI en Sardipac para obtener información directa sobre las políticas de seguridad existentes y vulnerabilidades percibidas.

3.2.3 Técnicas:

Se emplearon las siguientes técnicas de recolección de datos:

- **Encuesta:** Se llevó a cabo para evaluar el nivel de conocimiento de los encargados del área de TI sobre ransomware y las prácticas de seguridad actuales en la empresa.
- **Entrevista:** Se realizaron entrevistas semiestructuradas con responsables de TI para obtener información más detallada y cualitativa sobre las políticas de seguridad, activos críticos y los riesgos actuales.
- **Observación:** Se llevó a cabo una observación directa de la infraestructura de TI de la empresa para identificar vulnerabilidades en redes, configuraciones de sistemas, políticas de seguridad, entre otros.

3.3 Estrategia Operacional para la Recolección de Datos

La estrategia operacional de recolección de datos se basó en un diseño de investigación que conllevó a obtener información completa y precisa sobre las políticas de seguridad y vulnerabilidades de la infraestructura de TI de Sardipac. La recolección se datos se realizó utilizando las siguientes técnicas:

- **Diagnóstico Inicial**
  - **Objetivo:** Identificar el estado actual de la seguridad informática en el área de TI de Sardipac.

- **Técnicas**: (1) Observación directa para revisión de políticas, configuraciones de red, respaldos y controles de acceso, y (2) entrevistas semiestructuradas con los encargaos de TI para conocer los procedimientos y protocolos vigentes.
- **Instrumentos:** Guía de observación y cuestionario de entrevista.

- **Fase 2: Evaluación de análisis y vulnerabilidades**
  - **Objetivo:** Detectar vulnerabilidades, riesgos y activos críticos frente a posibles ataques de ransomware.
  - **Técnicas:** (1) Encuestas estructuradas aplicadas al personal técnico, y (2) análisis documental de registros de seguridad y políticas internas
  - **Instrumento:** Cuestionario digital matriz de riesgos basada en MAGERIT.
- **Fase 3: Diseño de la estrategia**
  - **Objetivo:** Proponer una estrategia integral de seguridad informática que incluya medidas de prevención, detección, respuesta y recuperación.
  - **Técnicas:** (1) Análisis comparativo con buenas prácticas internacionales (ISO 27001), y (2) validación de la propuesta mediante entrevistas con expertos o asesores de seguridad.
  - **Instrumentos:** Matriz de acciones estratégicas y plan de implementación

3.3.1 Población – Segmentación – Técnica de muestreo – Tamaño de la muestra

Para la obtención de datos cualitativos, la población estuvo compuesta por los dos ingenieros externos que brindan soporte técnico a la empresa Sardipac. Ellos fueron seleccionados mediante un muestreo no probabilístico e intencional, debido a su conocimiento especializado sobre la infraestructura y los sistemas de la empresa. Este grupo proporcionó información técnica necesaria para el diagnóstico y detección de vulnerabilidades.

Mientras que, para la obtención de datos cuantitativos, la población estuvo conformada por 13 empleados administrativos y operativos de Sardipac que utilizan los sistemas informáticos en su trabajo diario. A este grupo se le aplicó una encuesta de 10 ítems para identificar el nivel de conocimiento, hábitos y prácticas en materia de seguridad y uso responsable de los recursos tecnológicos, quienes a su vez son los beneficiarios de las estrategias y medidas de seguridad informática propuestas al final de este trabajo.

3.3.2 Estructura de los instrumentos de recolección de datos aplicadas

Los instrumentos de recolección de datos para este caso fueron los medios utilizados para obtener la información necesaria dentro del cumplimiento de los objetivos de la investigación. Los instrumentos fueron diseñados de acuerdo con la naturaleza de la investigación y la población participante, enfocándose en la recopilación de datos cualitativos y técnicos que permitieron diagnosticar el estado actual. Los instrumentos principales utilizados fueron la entrevista semiestructurada y la guía de observación, mientras que la encuesta se consideró una herramienta complementaria, destinada a diagnosticar el nivel de conocimiento del personal administrativo previo a la implementación de la estrategia de capacitación.

Tabla 1

Técnicas e instrumentos de recolección de datos

Técnica	Instrumento	Propósito
Entrevista semiestructuturada	Cuestionario de 25 preguntas abiertas distribuidas en seis bloques temáticos	Obtener información cualitativa sobre la situación actual de la seguridad informática, las vulnerabilidades detectadas, las prácticas de respaldo y la cultura de ciberseguridad.
Guía de observación	Lista de verificación de políticas, controles y procedimientos	Contrastar la información de las entrevistas con la observación directa en las instalaciones, verificando la existencia de políticas y medidas de seguridad.
Encuesta	Cuestionario de 10 ítems de opción múltiple	Diagnosticar el nivel de conocimiento y conciencia del personal administrativo sobre buenas prácticas en seguridad informática.

Nota. Elaboración propia

a) Entrevista

La entrevista semiestructurada fue aplicada a los dos ingenieros externos responsables del soporte técnico y la administración de la infraestructura informática de la empresa. Su propósito fue obtener información detallada sobre las políticas de seguridad implementadas, las vulnerabilidades existentes y las medidas preventivas aplicadas frente a amenazas de tipo ransomware.

El instrumento constó de 25 preguntas abiertas, distribuidas en seis bloques temáticos, orientados a cubrir todos los aspectos relevantes del entorno de seguridad informática.

Bloques temáticos:

1) Información general del entrevistado: recoge datos sobre la experiencia, funciones, y relación con la empresa.
2) Estado actual de la seguridad informática: indaga sobre políticas, procedimientos, herramientas y controles aplicados.
3) Identificación de vulnerabilidades: analiza puntos débiles, riesgos, y amenazas presentes en la infraestructura tecnológica.
4) Prácticas de respaldo y recuperación: revisa los métodos de respaldo, almacenamiento y recuperación de datos.
5) Cultura de ciberseguridad: examina el nivel de cultura que tiene la empresa con respecto a la seguridad informática.
6) Propuestas de mejora: recopila las sugerencias técnicas y estratégicas para fortalecer la seguridad informática

El cuestionario dirigido al jefe del área de TI se enfocó en aspectos de gestión, políticas y toma de decisiones, mientras que el destinado al ingeniero de soporte técnico abordó tareas operativas, mantenimiento, control de accesos y procedimientos preventivos. Ambos instrumentos permitieron obtener una visión integral del estado actual de la seguridad informática y los riesgos específicos que enfrenta la empresa.

b) Guía de observación

Se utilizó para verificar de manera directa las condiciones reales de la infraestructura tecnológica de la empresa y contrastar la información suministrada durante las entrevistas. Este instrumento permitió identificar vulnerabilidades visibles y evaluar el nivel de cumplimiento de las medidas de seguridad existentes.

Los criterios que se buscaron observar fueron los siguientes:

- Existencia de políticas o procedimientos de seguridad informática documentados.
- Control de acceso físico y lógico a los sistemas y redes.
- Gestión de contraseñas y autenticación de usuarios.
- Frecuencia y método de copias de seguridad.
- Disponibilidad de planes de contingencia y recuperación ante desastres.
- Uso de herramientas de protección, como antivirus, firewall o filtros de seguridad en red.

La observación fue realizada por la investigadora en las instalaciones de la empresa Sardipac, registrando las evidencias en una lista de verificación elaborada previamente.

c) Encuesta

De manera complementaria, se diseñó una encuesta breve de 10 ítems de opción múltiple dirigida al personal administrativo y operativo de la empresa. Su objetivo fue diagnosticar el nivel de conocimiento, hábitos y prácticas en materia de seguridad y uso responsable de los recursos tecnológicos.

3.3.3 Plan de recolección de datos

Esta sección detalla los pasos efectuados durante la etapa de recolección de la información necesaria para el cumplimiento de los objetivos detallados al inicio de este trabajo, mediante el que se recurre al uso de instrumentos cualitativos y cuantitativos, con los que se buscó obtener información técnica y detallada sobre el estado actual de la seguridad informática de la empresa motivo de estudio.

Procedimiento para la recolección de Datos:

1) Selección de Participantes:

   - Entrevistas: Se realizó una entrevista semiestructurada a los ingenieros responsables del soporte técnico y administración de la infraestructura tecnológica de la empresa. Esta entrevista proporcionó información sobre las políticas de seguridad implementadas, las vulnerabilidades existentes y las medidas preventivas aplicadas frente a amenazas.
   - Encuesta: Se aplicó una encuesta a empleados administrativos y operativos de la empresa. El objetivo de esta técnica fue evaluar su conocimiento sobre las buenas prácticas en seguridad informática y la cultura organizacional en torno a la ciberseguridad.

2) Métodos y Técnicas:
   - Entrevista Semiestructurada: Se utilizó una entrevista de 25 preguntas abiertas distribuidas en 6 bloques temáticos, que abordaron la seguridad informática de manera integral.

- Guía de Observación: Se empleó una lista de verificación que permitió observar de forma directa las instalaciones y verificar la existencia de políticas y controles de seguridad en la infraestructura tecnológica.
- Encuesta: Se aplicó una encuesta de 10 ítems de opción múltiple al personal administrativo para diagnosticar su nivel de conocimiento sobre seguridad informática.

3) Cronograma de Recolección de Datos
   - Semana 1: Preparación y validación de los instrumentos de recolección.
   - Semana 2: Aplicación de entrevistas
   - Semana 3: Observación directa en las Instalaciones
   - Semana 4: Realización de Charla de concientización y encuesta al personal.

3.4 Análisis y Presentación de Resultados.

Los resultados obtenidos mediante las entrevistas, la observación y las encuestas son cruciales para el diagnóstico del estado actual de la seguridad informática en la empresa Sardipac. El análisis se realizó mediante la obtención de datos cualitativos y cuantitativos a fin de alcanzar una visión integral de la realidad estudiada y proponer acciones basadas en lo observado a lo largo del estudio.

3.4.1 Tabulación y análisis de datos

3.4.1.1 Resultados y análisis de la entrevista de seguridad.

La entrevista se aplicó con el objetivo de identificar vulnerabilidades técnicas, prácticas de respaldo y procedimientos de seguridad vigentes en infraestructura TI de la empresa. Para el tratamiento de la información cualitativa, se realizó un análisis por categorías, que consistió en agrupar las respuestas del entrevistado en dimensiones analíticas coherentes con el objetivo de la investigación. A continuación, se detallan las categorías abordadas, así como los resultados que se desprendieron de estas:

a) Identificación del rol y alcance del soporte técnico

El entrevistado mencionó que su función principal es brindar soporte a usuarios finales y revisar políticas del firewall dentro de la infraestructura de red. Esta respuesta permitió delimitar el alcance y confiabilidad de la fuente, puesto que el participante está vinculado directamente a la operación del perímetro de seguridad.

b) Criticidad de sistemas y plataformas

Se identificaron como sistemas críticos dentro de la infraestructura tecnológica dos elementos como son: Inforfish y Qbiz. La identificación de estos sistemas críticos constituye un insumo esencial para MAGERIT, porque orienta la priorización de activos y el enfoque en riesgos que afecten la continuidad operativa y la protección de la información.

c) Monitoreo y herramientas de diagnóstico

Como herramienta de monitoreo y diagnóstico se mencionó Fortinet (Firewall/seguridad perimetral). Esto sugiere que existe una estrategia de seguridad perimetral con capacidades de registro y detección relevante para el control de accesos y eventos de red.

d) Incidentes de seguridad y evidencia de intentos de intrusión

Se reportó la detección diaria de intentos de inicio de sesión fraudulento en el firewall. Este hallazgo es crítico porque evidencia una amenaza activa y recurrente que incrementa la probabilidad del riesgo asociado a accesos no autorizados.

e) Gestión de actualizaciones y control de cambios.

Se indicó que las actualizaciones se gestionan mediante un ambiente controlado virtualizado, y que adicionalmente Kasperky reporta equipos con problemas de actualización. Sobre esto se puede añadir que el análisis de la gestión controlada de actualizaciones reduce vulnerabilidades asociadas a software desactualizado, sin embargo, la existencia de equipos con fallos en actualización representa una superficie de ataque residual que debe observarse.

f) Registro de fallas recurrente/ endpoint security

Se afirmó que Kasperky registra los equipos o usuarios con fallas recurrentes. Como análisis este control respalda procesos de trazabilidad, respuesta y mejora continua, útil para correlacionar incidentes y fortalecer la detección.

g) Vulnerabilidades percibidas en la red

Se identificó como principal vulnerabilidad “las conexiones externas a servicios”. Este punto es central para el análisis de riesgos, el acceso desde el exterior (servicios expuestos o conectividad con terceros) tiende a elevar la probabilidad de amenazas como intrusión, explotación de vulnerabilidades y robo de credenciales.

h) Respaldo, almacenamiento y recuperación

Se indicó que las copias de bases de datos son diarias, cifradas y replicadas en nube, los respaldos de equipos son semanales y cifrados. Además, los respaldos se almacenan en NAS y en la nube, y se cuenta con plan de recuperación de desastres (backup del servidor completo). La integridad de copia se verifica periódicamente. Como análisis de este hallazgo se puede mencionar que, en términos MAGERIT, estas salvaguardias mitigan riesgos de disponibilidad e integridad, no obstante, debe analizarse el riesgo residual considerando dependencia tecnológica, accesos y procedimientos.

i) Medidas preventivas ante ransomware

Se realiza revisión periódica de vulnerabilidades mediante reportes diarios sobre infecciones y reportes diarios del firewall. En este caso se evidencia que existe monitoreo continuo, sin embargo, la eficacia depende de tiempos de respuesta, cobertura en endpoints y medidas de prevención complementarias (control de privilegios, segmentación, MFA, entre otros).

j) Políticas de autenticación y control de accesos

Existe política de contraseñas con combinación de mayúsculas, caracteres especiales y números. El acceso a administrador y a servidores lo posee únicamente el equipo de TI. Como análisis de este ítem se identifican controles de autenticación y restricción de privilegio. Estos reducen la probabilidad de accesos no autorizados, a pesar de que no elimina riesgos asociados a ataques de fuerza bruta, phishing o reutilización de contraseñas.

k) Capacitación y evaluación de conocimiento

Se reporta capacitación al menos tres veces al año. La evaluación del conocimiento se realiza mediante encuestas de satisfacción. Como análisis de este hallazgo se puede agregar que este componente aborda el factor humano (que es la causa más frecuente de incidentes). Sin embargo, la encuesta posterior debe realizarse para identificar brechas.

l) Mantenimiento preventivo

Se realiza mantenimiento preventivo bimensual de red y servidores. Sobre esto se puede mencionar que este tipo de acción mitiga riesgos técnicos por deterioro, fallas y configuraciones no revisadas a la disponibilidad.

m) Indicadores utilizados para evaluar seguridad

Se mencionaron indicadores como tasa de detección de amenazas, número de incidentes, tiempo promedio de detección, porcentaje de equipos actualizados, porcentaje de tráfico cifrado y número de vulnerabilidades críticas. Sobre esto se puede mencionar que, la existencia de KPIs sugiere un enfoque de seguimiento, lo cual es relevante para sustentar medición y control continuo dentro de la propuesta.

n) Limitaciones para mejorar la seguridad

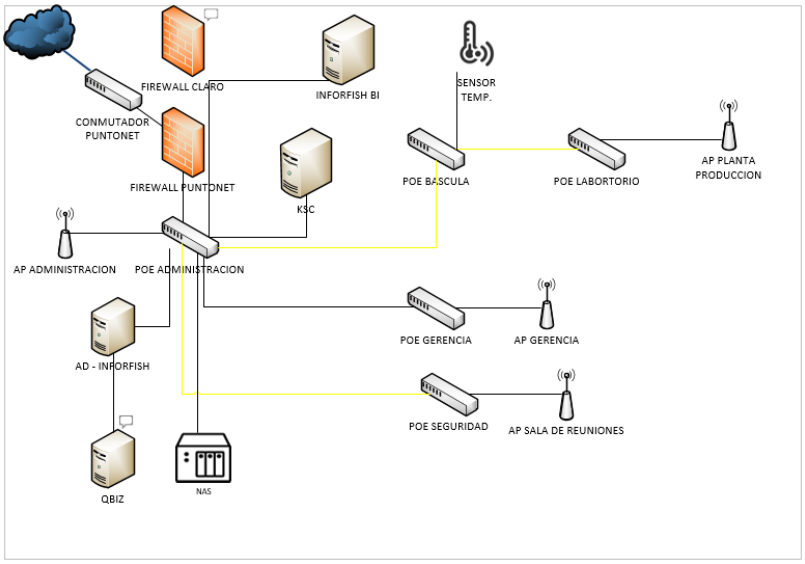
Se reportaron limitaciones presupuestarias, falta de políticas y procedimientos actualizados, y falta de concienciación del personal. En este caso, dichas limitaciones inciden directamente en el riesgo residual, pues afectan la capacidad de implementar salvaguardar y mantener controles vigentes.

3.4.1.2 Diagrama de red actual.

En esta subsección se explica la situación actual de la estructura tecnológica de la empresa, para ello se identifica en primera instancia el siguiente diagrama de red:

Figura 2

Diagrama de red



Nota. Por asuntos de seguridad se omiten las IP de las redes, pero el esquema del funcionamiento es idéntico

La topología de red de la empresa, como se muestra en la figura 2, está organizada para ofrecer conectividad y seguridad, pero también presenta algunas vulnerabilidades que deben ser abordadas.

Componentes de la infraestructura de red:

- **Firewall:** Estos protegen el perímetro de la red, sin embargo, si llegara a haber una configuración incorrecta o desactualizada de las reglas de filtrado podría permitir accesos no autorizados, esto incrementaría la exposición de la red.
- **Inforfish BI y QBIZ**: Servidores críticos de la empresa, cuyo acceso debe estar restringido para evitar riesgos de compromiso de datos. A pesar de estar en una red interna, la falta de controles adicionales podría hacerlos vulnerables a ataques internos
- **PoE (Power over Ethernet)**: Los dispositivos conectados mediante puntos de acceso, cámaras de seguridad, entre otros, son vulnerables a ataques físicos si no se toman medidas para proteger su acceso. La seguridad de los equipos es fundamental para mitigar esta vulnerabilidad.
- **NAS (Almacenamiento centralizado)**: El NAS almacena datos críticos de la empresa, y si no tiene las configuraciones de seguridad adecuadas, puede ser un punto vulnerable a ataque para la modificación o pérdida de datos. Especialmente en caso de un ransomware o ataques de malware.

Vulnerabilidades identificadas:

- Exposición del perímetro de la red: A pesar de los firewalls, el acceso continuo al perímetro de la red representa un riesgo si no se implementan reglas de seguridad específicas para cada tipo de tráfico.
- Riesgos de accesos no controlados a sistemas críticos: La falta de segmentación adecuada y control de acceso en servidores, como Inforfish BI y QBIZ deja abierta la posibilidad de accesos no autorizados a estos recursos.
- Vulnerabilidad de los puntos de acceso.
- Riesgos en el almacenamiento NAS, la falta de cifrado y políticas de acceso restringido en el NAS incrementa la probabilidad de datos sensibles sean comprometidos.

3.4.1.3 Resultados y análisis de la encuesta de seguridad.

Para la recolección de datos mediante la encuesta se aplicó un cuestionario basado en los fundamentos de ciberseguridad abordados mediante 10 ítems o preguntas orientadas a 13 colaboradores de la empresa Sardipac, esta se realizó mediante la plataforma Kahoot, la que permitió recolectar la información de manera sistemática y debidamente categorizada. Los resultados de este procedimiento se detallan a continuación.

1) ¿Qué debes hacer si recibes un correo con un enlace sospechoso?

Tabla 2

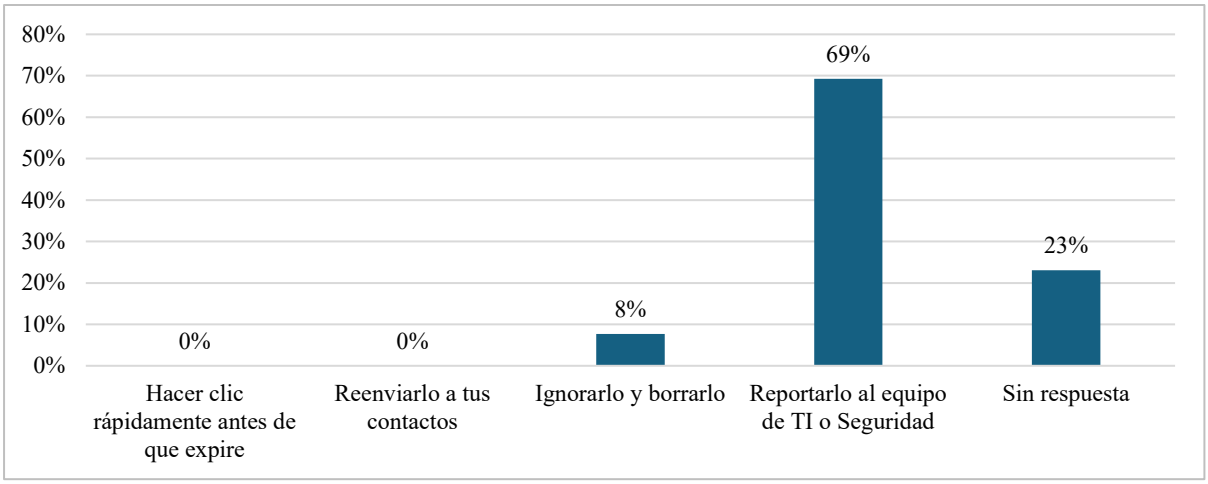
Acción ante un correo con un enlace sospechoso

Opción	Frecuencia	Porcentaje
Hacer clic rápidamente antes de que expire	0	0%
Reenviarlo a tus contactos	0	0%
Ignorarlo y borrarlo	1	8%
Reportarlo al equipo de TI o Seguridad	9	69%
Sin respuesta	3	23%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 3

Acción ante un correo con un enlace sospechoso



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: Al abordar sobre la acción correcta ante un correo con un enlace sospechoso se pudo conocer que, el 69% de los colaboradores manifestó que el procedimiento adecuado es reportarlo al equipo de TI o Seguridad, el 23% no pudo responder a esta interrogante y el 8% dio una respuesta incorrecta que fue ignorarlo y borrarlo. Para este caso se pudo notar que el 31% de los colaboradores no tiene conocimiento pleno sobre el procedimiento adecuado ante este tipo de incidente, siendo un aspecto de vulnerabilidad para la empresa.

2) ¿Cuál es una señal clara de un correo de phishing?

Tabla 3

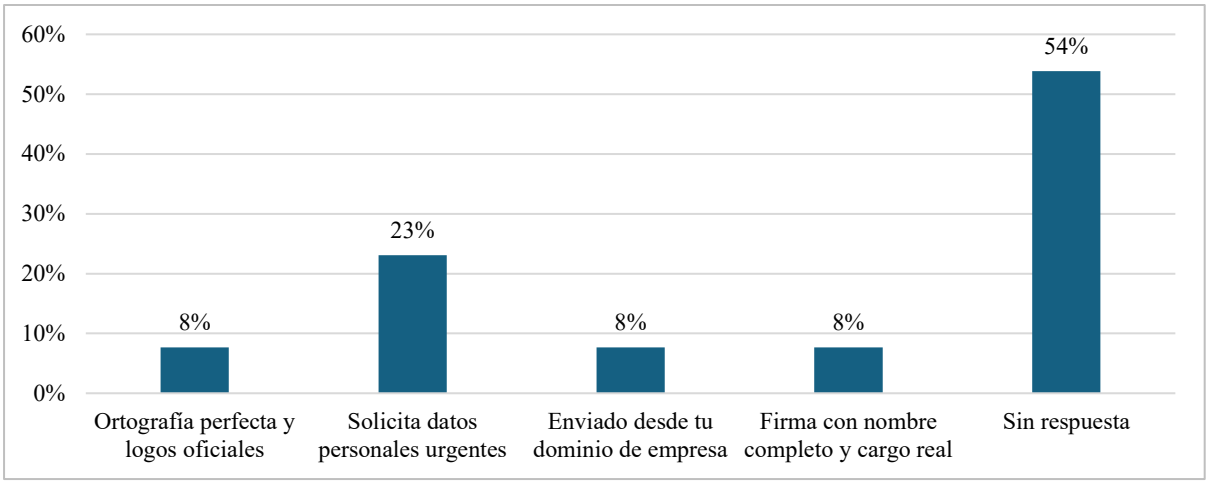
Conocimiento sobre señal clara de un correo phishing

Opción	Frecuencia	Porcentaje
Ortografía perfecta y logos oficiales	1	8%
Solicita datos personales urgentes	3	23%
Enviado desde tu dominio de empresa	1	8%
Firma con nombre completo y cargo real	1	8%
Sin respuesta	7	54%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 4

Conocimiento sobre señal clara de un correo phishing



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: Al preguntar sobre si con conocían la señal clara de un correo phishing se conoció que, el 54% de los colaboradores encuestados no pudo dar una respuesta, el 23% respondió que este tipo de ataque solicita datos personales urgentes, el 8% indicó que se caracteriza por ser enviado desde su dominio de empresa, el 8% dijo que se identifica por presentar ortografía perfecta y logos oficiales y otro 8% mencionó que presenta firma con nombre completo y cargo real. Para este caso se pudo notar que únicamente el 23% de los colaboradores conoce las características principales de un correo phishing, se observa además que la mayoría tiene nula o escasa capacidad para identificar esta modalidad de ataque, siendo un factor de vulnerabilidad considerable para la empresa debido a las implicaciones de confidencialidad y robo de datos que representa.

3) ¿Qué contraseña es más segura?

Tabla 4

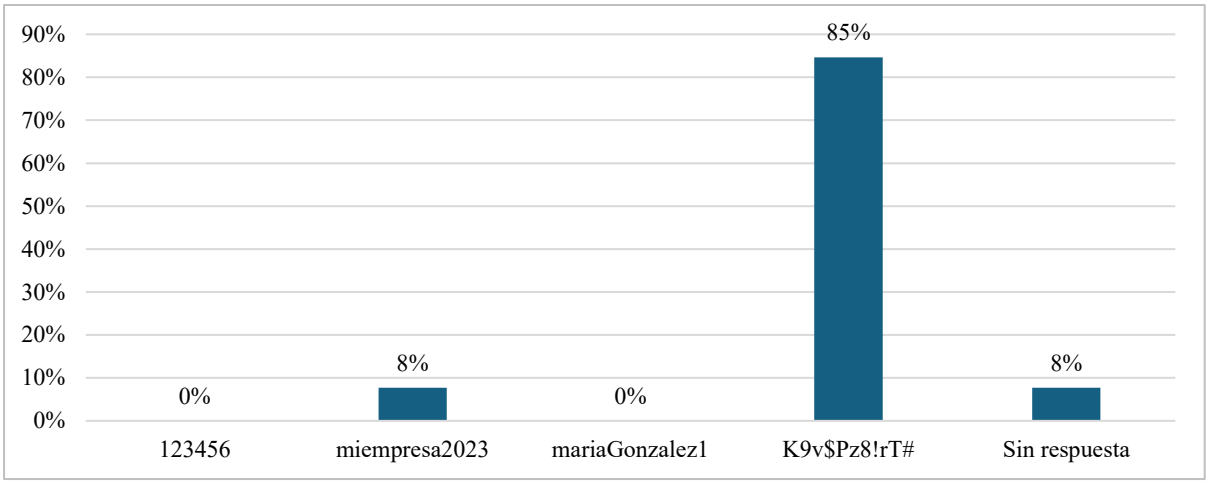
Conocimiento sobre contraseñas seguras

Opción	Frecuencia	Porcentaje
123456	0	0%
miempresa2023	1	8%
mariaGonzalez1	0	0%
K9v$Pz8!rT#	11	85%
Sin respuesta	1	8%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 5

Conocimiento sobre contraseñas seguras



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: Al indagar acerca de qué tipo de contraseña consideraban más segura, se pudo conocer que, el 85% de los colaboradores consideró de alta seguridad una contraseña que contiene mayúsculas, minúsculas, números y caracteres especiales; el 8% consideró como segura una contraseña compuesta por una palabra en minúsculas y números (año); el 8% restante no dio una respuesta cerca de esta interrogante. Estos resultados dejan ver que, la mayor parte del personal de la empresa tiene pleno conocimiento acerca del uso de contraseñas altamente seguras, aunque es importante hacer hincapié en el 16% de tiene escaso o nulo conocimiento en este aspecto, lo cual puede ser un factor de vulnerabilidad ante malwares que involucren el robo de cuentas y de información sensible.

4) ¿Qué es un malware?

Tabla 5

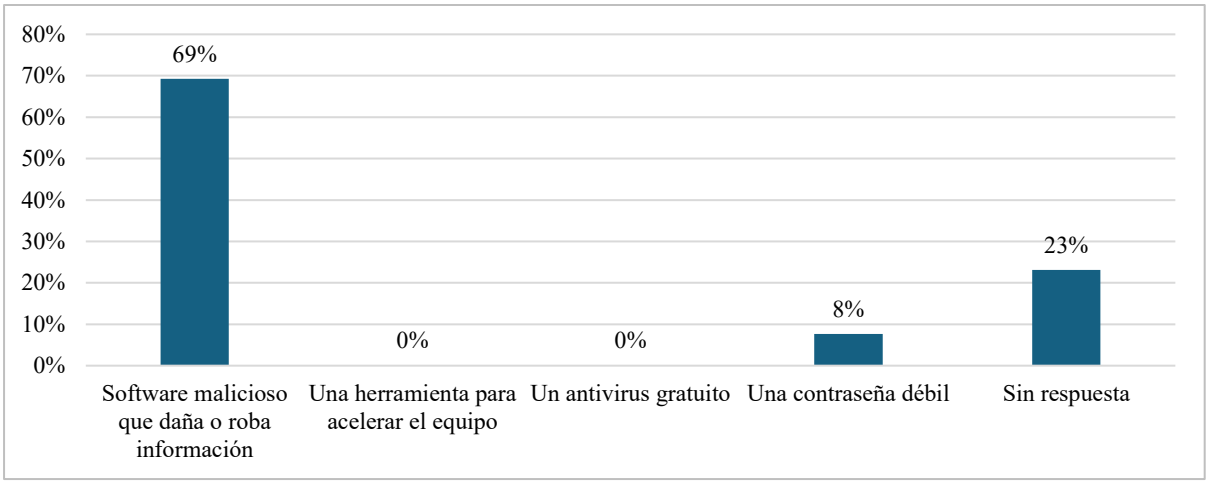
Conocimiento sobre malware

Opción	Frecuencia	Porcentaje
Software malicioso que daña o roba información	9	69%
Una herramienta para acelerar el equipo	0	0%
Un antivirus gratuito	0	0%
Una contraseña débil	1	8%
Sin respuesta	3	23%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 6

Conocimiento sobre malware



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: En torno al conocimiento sobre malware, se pudo conocer que, el 69% de los colaboradores encuestados dio una respuesta correcta indicando que se trata de un software malicioso que daña o roba información, el 23% no dio una respuesta al respecto y el 8% restante dio una respuesta equivocada señalando que se trata de una contraseña débil. Dentro de este ítem es importante mencionar que, a pesar de que la mayoría de los colaboradores tiene noción de este tipo de programa malicioso, existe un 31% que se encuentra vulnerable a estos ataques debido a su limitado conocimiento e identificación, lo que representa una vulnerabilidad considerable para la empresa, debido a que se puede caer fácilmente en esta modalidad de ciberataque, afectando la confidencialidad y e integridad de la información.

5) ¿Qué medida mejora la seguridad de tus cuentas en línea?

Tabla 6

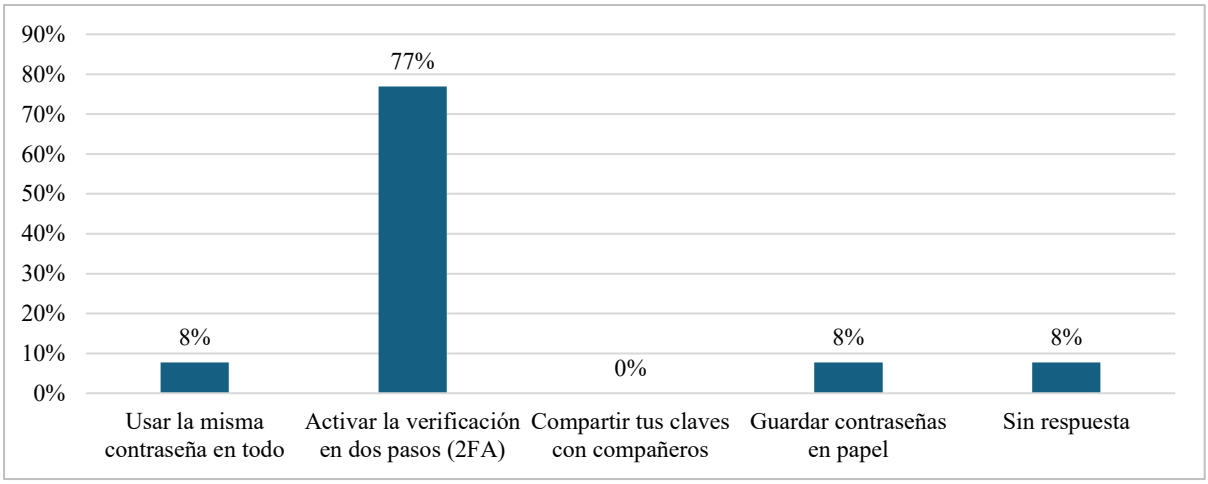
Conocimiento sobre medida que mejora seguridad de cuentas en línea

Opción	Frecuencia	Porcentaje
Usar la misma contraseña en todo	1	8%
Activar la verificación en dos pasos (2FA)	10	77%
Compartir tus claves con compañeros	0	0%
Guardar contraseñas en papel	1	8%
Sin respuesta	1	8%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 7

Conocimiento sobre medida que mejora seguridad de cuentas en línea



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: Al abordar sobre la medida que mejora la seguridad de sus cuentas en línea se pudo conocer que, el 77% de los colaboradores encuestados dio una respuesta correcta indicando que consiste en activar la verificación en dos pasos (2AF), el 8% manifestó indicó que la medida idónea es usar la misma contraseña en todo, el 8% indicó como opción confiable el guardar contraseñas en papel y el 8% restante no supo responder a esta interrogante. Mediante estos resultados se puede deducir un alto conocimiento acerca de medidas de prevención, sin embargo, todavía existe un 24% de colaboradores que presentan nula o escasa noción en este aspecto, lo que es también un aspecto de vulnerabilidad por la exposición a ataques maliciosos que buscan secuestrar o robar cuentas a través de distintas modalidades de ciberataque.

6) ¿Qué debes hacer si encuentras una memoria USB desconocida?

Tabla 7

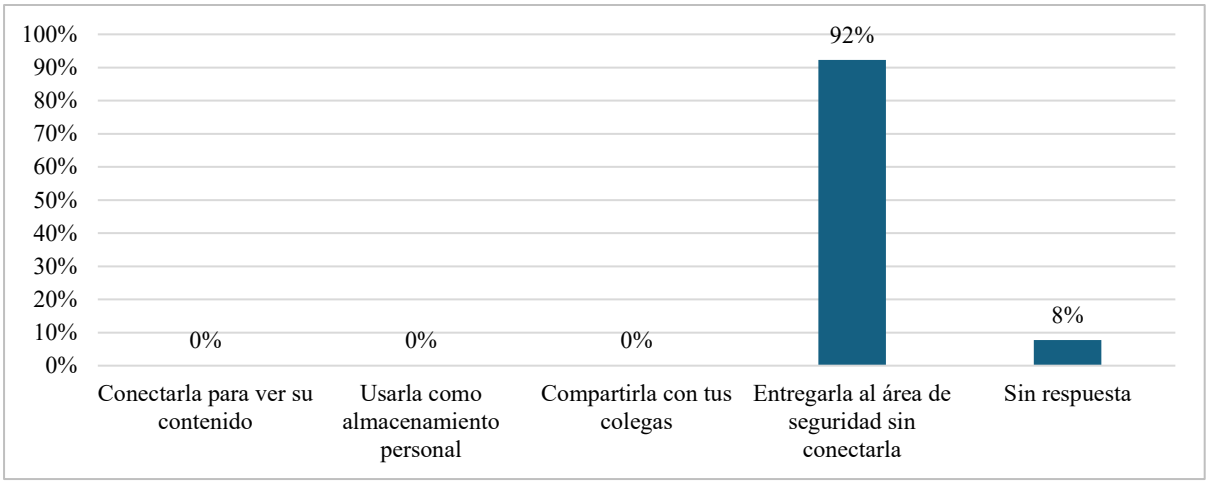
Conocimiento sobre acción al encontrar una memoria USB desconocida

Opción	Frecuencia	Porcentaje
Conectarla para ver su contenido	0	0%
Usarla como almacenamiento personal	0	0%
Compartirla con tus colegas	0	0%
Entregarla al área de seguridad sin conectarla	12	92%
Sin respuesta	1	8%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 8

Conocimiento sobre acción al encontrar una memoria USB desconocida



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis:

Al indagar sobre el procedimiento adecuado al encontrase una memoria USB desconocida se evidenció que, el 92% de los colaboradores dio una respuesta correcta indicando que debe entregarse al área de seguridad sin conectarla, mientras que el 8% restante no supo responder a esta interrogante. En este caso se observa un conocimiento generalizado sobre el protocolo a seguir ante este tipo de eventualidad, lo que resulta un factor de menor vulnerabilidad para la empresa, aunque es importante llevar a cabo acciones de refuerzo en concientización de protocolo y manejo de dispositivos de origen sospechoso y que pueden ser potencialmente maliciosos para el sistema de seguridad de la empresa.

7) ¿Qué tipo de ataque busca engañar al usuario usando sitios web falsos?

Tabla 8

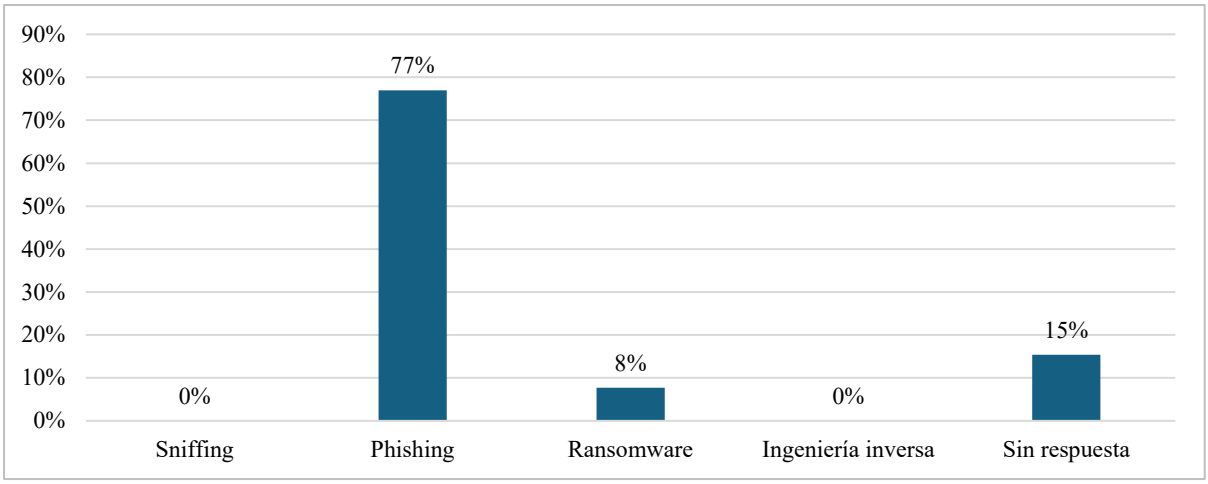
Conocimiento sobre ataque que busca engañar al usuario usando sitios web falsos

Opción	Frecuencia	Porcentaje
Sniffing	0	0%
Phishing	10	77%
Ransomware	1	8%
Ingeniería inversa	0	0%
Sin respuesta	2	15%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 9

Conocimiento sobre ataque que busca engañar al usuario usando sitios web falsos



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: Al momento de indagar sobre qué ataque busca engañar al usuario usando sitios web falsos, se pudo conocer que, el 77% de los colaboradores encuestados dio una respuesta correcta señalando que es el phishing, el 8% mencionó como respuesta el ransomware y el 15% restante no supo responder a esta interrogante. Para este caso se muestra que a pesar de que la mayor parte de los colaboradores conoce sobre la modalidad de este tipo de ciberataque, el 23% de estos presenta escaso o nulo conocimiento al respecto lo cual se considera un factor de vulnerabilidad para la empresa ante la limitada capacidad para conocer este tipo de ataque altamente utilizado para trasgredir infraestructura informática y como efecto la violación de datos sentibles.

8) ¿Cuál es el objetivo de un ataque de ingeniería social?

Tabla 9

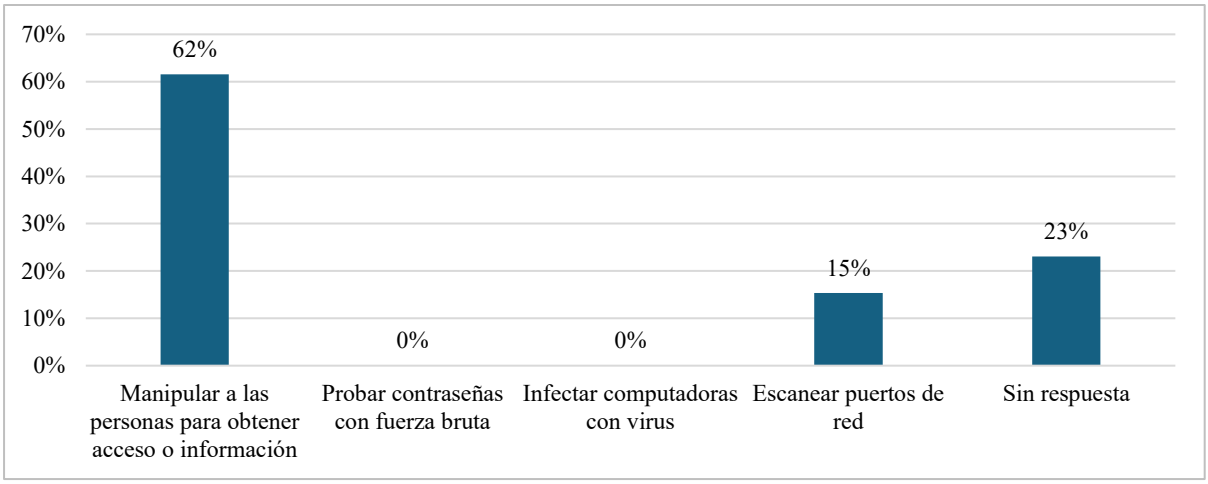
Conocimiento sobre objetivo de un ataque de ingeniería social

Opción	Frecuencia	Porcentaje
Manipular a las personas para obtener acceso o información	8	62%
Probar contraseñas con fuerza bruta	0	0%
Infectar computadoras con virus	0	0%
Escanear puertos de red	2	15%
Sin respuesta	3	23%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 10

Conocimiento sobre objetivo de un ataque de ingeniería social



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: En lo relacionado al objetivo de un ataque de ingeniería social se pudo conocer que, el 62% de los colaboradores encuestados dio una respuesta correcta señalando que este tiene como fin manipular a las personas para obtener acceso o información, el 23% no supo dar una respuesta a esta interrogante y el 15% restante manifestó que su fin es escanear puertos de red. Con base en estos datos se puede deducir que, aunque la mayor parte de los trabajadores de la empresa tiene noción sobre esta modalidad de ciberataque, no existe concientización generalizada, pues el 38% todavía desconoce estos procedimientos sofisticados de vulneración de datos, aspecto que puede comprometer la seguridad de la información sensible de la empresa y por ende su correcta operatividad.

9) ¿Qué puedes hacer para evitar el espionaje visual ("shoulder surfing")?

Tabla 10

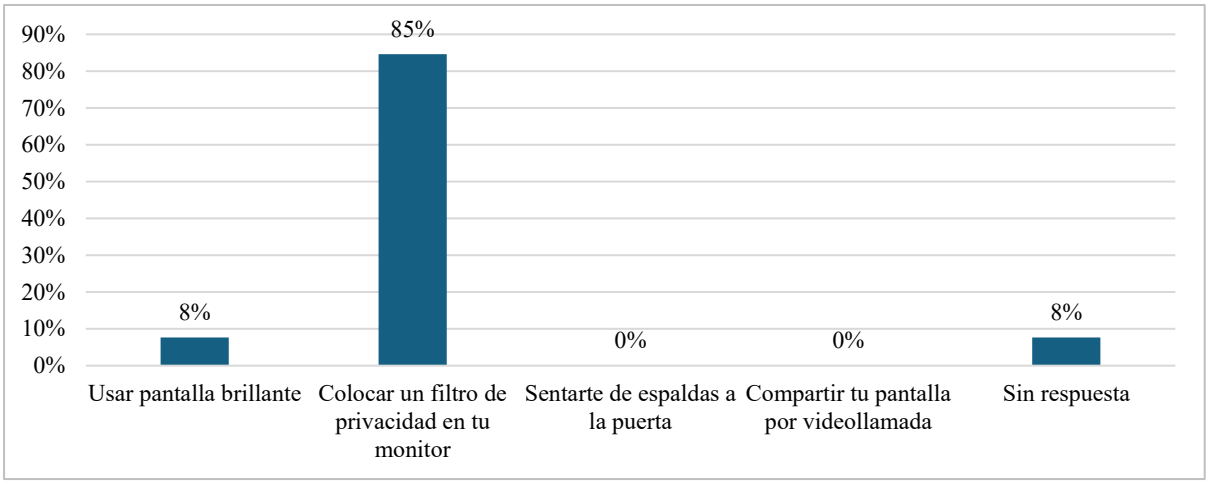
Conocimiento sobre acción para evitar el espionaje visual ("shoulder surfing")

Opción	Frecuencia	Porcentaje
Usar pantalla brillante	1	8%
Colocar un filtro de privacidad en tu monitor	11	85%
Sentarte de espaldas a la puerta	0	0%
Compartir tu pantalla por videollamada	0	0%
Sin respuesta	1	8%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 11

Conocimiento sobre acción para evitar el espionaje visual ("shoulder surfing")



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: En lo relacionado a las acciones para evitar el espionaje visual ("shoulder surfing"), se pudo conocer que, el 85% de los colaboradores encuestados dio una respuesta correcta señalando como acción colocar un filtro de privacidad en el monitor, el 8% dio una respuesta incorrecta indicando como medida usar pantalla brillante y el 8% restante no supo dar una respuesta a esta interrogante. Estos resultados reflejan la adherencia de una cultura organizacional para prevenir esta modalidad de acceso y vulneración a datos que pueden ser sensibles para la organización, sin embargo, es necesario reforzar la concientización sobre estos protocolos en una parte del personal con la finalidad de incentivar a entornos de mayor ciberseguridad en los puestos de trabajo.

10) ¿Cuál de estos elementos NO es parte de una buena práctica en ciberseguridad?

Tabla 11

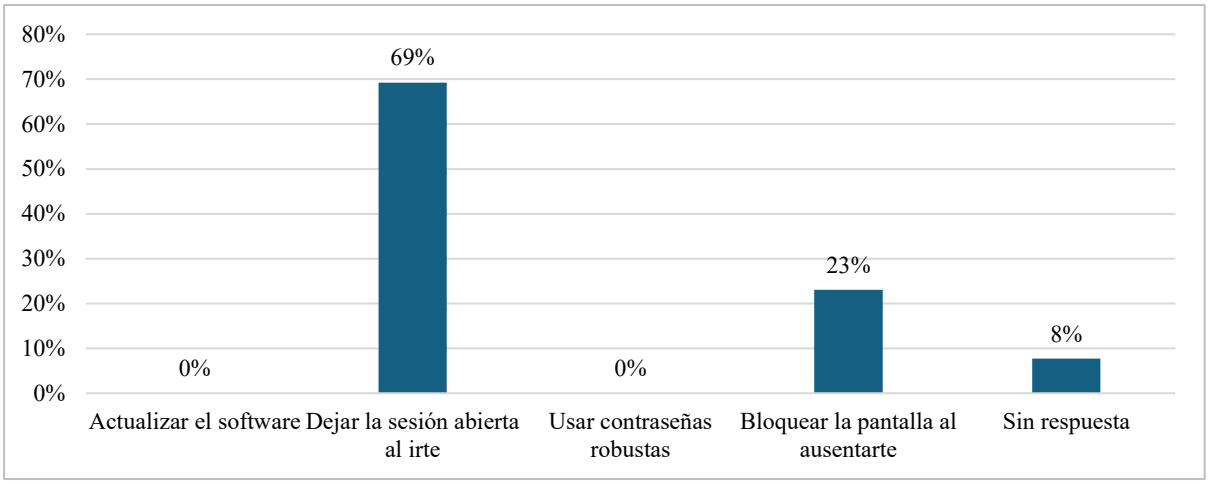
Identificación de elemento que no es parte de una buena práctica en ciberseguridad

Opción	Frecuencia	Porcentaje
Actualizar el software	0	0%
Dejar la sesión abierta al irte	9	69%
Usar contraseñas robustas	0	0%
Bloquear la pantalla al ausentarte	3	23%
Sin respuesta	1	8%
Total	**13**	**100%**

Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Figura 12

Identificación de elemento que no es parte de una buena práctica en ciberseguridad



Nota. Elaboración propia a partir de encuesta aplicada a colaboradores de Sardipac.

Análisis: En lo concerniente al elemento que no es parte de una buena práctica en ciberseguridad, se pudo conocer que, el 69% de los colaboradores dio una respuesta correcta indicando que un aspecto de vulnerabilidad es dejar la sesión abierta al irse, el 23% dio una respuesta incorrecta que fue bloquear la pantalla al ausentarse y el 8% restante no supo dar una respuesta a esta interrogante. Para este caso se observa que a pesar de que la mayor parte de los trabajadores conoce sobre este protocolo de ciberseguridad, todavía existe una 31% de estos que tiene escasa o nula noción al respecto, debido a ello es importante que se propongan acciones preventivas para reforzar los conocimientos de este tipo de prácticas, que, aunque parezcan inofensivas pueden desencadenar en acceso nos permitidos al sistema informativo de la empresa y por ende a la vulneración de su información sensible.

3.4.1.4 Resultados de análisis Magerit

Para el análisis bajo la metodología Magerit se llevaron a cabo cinco pasos, los que abordaron, primero la identificación de activos, a través de la cual se realizó un inventario de los activos ligados directamente al área de Tecnologías de la Información de la empresa Sardipac; segundo, se realizó la valoración de activos mediante tres categorías como fueron disponibilidad, integridad y confidencialidad; tercero, se determinaron las amenazas relacionadas con cada activo conforme con catálogo de elementos Magerit; cuarto, se analizaron los riesgos e impacto de cada amenaza; y quinto, se identificaron las salvaguardias para el control de cada amenaza. En ese sentido, se siguió un orden lógico tal como se muestra en la siguiente figura:

Figura 13

Proceso de metodología Magerit

Nota. Elaboración propia

Por medio de la primera fase se lograron identificar 18 activos relacionados con el área de Tecnologías de la Información de la empresa Sardipac, los que fueron debidamente codificados y clasificados conforme con la metodología Magerit. En este caso se observaron ocho tipos de activos como fueron: activos esenciales, datos/información, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, equipamiento auxiliar, el personal. Cada uno de estos activos se muestran de forma detallada en la siguiente tabla:

Tabla 12

Identificación de activos

Código	Activo	Tipo	Clasificación MAGERIT
AC-01	Datos de procesos	Activos esenciales	[ESSENTIAL] [ADM] datos de interés para la administración
AC-02	Datos de clientes, empleados y proveedores	Activos esenciales	[ESSENTIAL] [PER] datos de carácter personal
AC-03	Backups y servidores NAS	Datos / Información	[D] [BACKUP] copias de respaldo

AC-04	Acceso a servidores	Servicios	[S] [TELNET] acceso remoto a cuenta local
AC-05	Kaspersky (antivirus)	Aplicaciones (software)	[SW] [AV] antivirus
AC-06	Servidor de respaldo	Aplicaciones (software)	[SW] [BACKUP] sistema de backup
AC-07	Computadoras personales	Equipos informáticos (Hardware)	[HW] [PC] Informática personal
AC-08	Tablets	Equipos informáticos (Hardware)	[HW] [PC] Informática móvil
AC-09	Switch POE	Equipos informáticos (Hardware)	[HW[[SWITCH] conmutadores
AC-10	Firewall (Fortinet)	Equipos informáticos (Hardware)	[HW] [FIREWALL] cortafuegos
AC-11	Access Points (AP) /Puntos de Acceso	Equipos informáticos (Hardware)	[HW] [WAP] punto de acceso inalámbrico
AC-12	Equipo telefónico fijo	Redes de comunicaciones	[COM] [PSTN] red telefónica
AC-13	Conexión inalámbrica	Redes de comunicaciones	[COM] [WIFI] red inalámbrica
AC-14	Equipo telefónico móvil	Redes de comunicaciones	[COM] [MOBILE] telefonía móvil
AC-15	Red de área local	Redes de comunicaciones	[COM] [LAN] red local
AC-16	Conexión a internet	Redes de comunicaciones	[COM] [INTERNET] Internet
AC-17	UPS (Fuentes de alimentación)	Equipamiento auxiliar	[AUX] [UPS] sistemas de alimentación ininterrumpida
AC-18	Trabajadores / colaboradores	Personal	[P] [UI] usuarios internos

Nota. Elaboración propia a partir de (Amutio Gómez et al., 2012b)

Una vez identificados los activos se procedió a categorizarlos según su valoración, lo cual se realizó bajo tres parámetros como fueron: disponibilidad, integridad y confidencialidad. Para dicha valoración se utilizó una escala de 1 a 10 conforme con los siguientes criterios:

Tabla 13

Criterios de valoración de activos

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

Nota. Tomado de (Amutio Gómez et al., 2012b)

Para valorar la criticidad de cada activo se recurrió al uso de la siguiente fórmula:

$$Valor\ de\ activo = C + I + D$$

Cada elemento de la fórmula se abrevió de la siguiente manera:

- C = Confidencialidad
- I = Integridad
- D = Disponibilidad

Asimismo, para conocer y categorizar el nivel de riesgo de cada activo se tomó como referencia la siguiente escala:

Tabla 14

Escala de valoración de activos (C + I + D)

Rango	Calificación
1 a 3	Bajo
4 a 6	Medio
7 a 9	Alto
10 a 12	Muy Alto
13 a 15	Extremo

Nota. Tomado de (Guamán et al., 2023)

Bajo estos parámetros y criterios se procedió con la valoración respectiva, identificando siete (7) activos de riesgo extremo, cuatro (4) activos de riesgo muy alto, tres (3) activos de riesgo alto, un (1) activo de riesgo medio, y (3) tres activos de riesgo bajo. Resultados que dejan ver que, la mayor parte de estos activos tienen un valor importante a nivel de disponibilidad, integridad y confidencialidad, por lo que alcanzan valoraciones de alto riesgo si se materializan las amenazas. Em la siguiente tabla se muestran a detalle los valores previamente descritos:

Tabla 15

Valoración de activos

Tipo	Código	Activo	Disponibilidad	Integridad	Confidencialidad	Total
Activos esenciales	AC-01	Datos de procesos	5	5	5	15
	AC-02	Datos de clientes, empleados y proveedores	5	5	5	15
Datos / Información	AC-03	Backups y servidores NAS	5	5	5	15
Servicios	AC-04	Acceso a servidores	5	5	5	15
Aplicaciones (software)	AC-05	Kaspersky (antivirus)	3	4	3	10
	AC-06	Servidor de respaldo	5	5	5	15
	AC-07	Computadoras personales	4	5	5	14
Equipos informáticos (Hardware)	AC-08	Tablets	3	4	5	12
	AC-09	Switch POE	2	0	0	2
	AC-10	Firewall (Fortinet)	5	5	4	14
	AC-11	Access Points (AP) / Puntos de Acceso	3	4	3	10
	AC-12	Equipo telefónico fijo	1	1	1	3
Redes de comunicaciones	AC-13	Conexión inalámbrica	3	3	3	9
	AC-14	Equipo telefónico móvil	3	3	4	10
	AC-15	Red de área local	3	2	2	7
	AC-16	Conexión a internet	3	3	3	9

Tipo	Código	Activo	Disponibilidad	Integridad	Confidencialidad	Total
Equipamiento auxiliar	AC-17	UPS (Fuentes de alimentación)	2	1	0	3
Personal	AC-18	Trabajadores / colaboradores	4	1	1	6

Nota. Elaboración propia a partir de (Amutio Gómez et al., 2012b)

El siguiente paso correspondió a la determinación de las amenazas, para esto se utilizó el catálogo del segundo libro de la metodología Magerit, encontrando con ello un total de 64 amenazas relacionadas a los 18 tipos de activos identificados en el área de TI de la empresa Sardipac. Este paso resultó esencial para conocer los riesgos comunes asociados a las actividades de estos activos, pudiendo con ello valorarlos adecuadamente y realizar acciones de control posteriores. En la siguiente tabla se muestran a detalle las amenazas identificadas por cada tipo de activo:

Tabla 16

Determinación de amenazas

Código	Activo	Código Amenaza	Amenaza
AC-01	Datos de procesos	[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
		[A.15]	Modificación deliberada de la información
		[A.18]	Destrucción de información
		[A.19]	Divulgación de información
AC-02	Datos de clientes, empleados y proveedores	[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
		[A.15]	Modificación deliberada de la información
		[A.18]	Destrucción de información
		[A.19]	Divulgación de información
AC-03	Backups y servidores NAS	[E.15]	Alteración accidental de la información
		[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
		[A.15]	Modificación deliberada de la información
		[A.18]	Destrucción de información
		[A.19]	Divulgación de información
AC-04	Acceso a servidores	[A.7]	Uso no previsto
		[A.24]	Denegación de servicio
		[E.1]	Errores de los usuarios
		[E.2]	Errores del administrador
		[A.11]	Acceso no autorizado
AC-05	Kaspersky (antivirus)	[E.8]	Difusión de software dañino
		[A.7]	Uso no previsto
		[E.18]	Destrucción de información
		[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
AC-06	Servidor de respaldo	[E.8]	Difusión de software dañino
		[A.7]	Uso no previsto
		[E.18]	Destrucción de información
		[E.19]	Fugas de información
		[A.11]	Acceso no autorizado
AC-07	Computadoras personales	[E.25]	Pérdida de equipos

Código	Activo	Código Amenaza	Amenaza
		[A.23]	Manipulación de los equipos
		[A.25]	Robo
		[A.7]	Uso no previsto
		[A.11]	Acceso no autorizado
AC-08	Tablets	[E.25]	Pérdida de equipos
		[A.23]	Manipulación de los equipos
		[A.25]	Robo
		[A.7]	Uso no previsto
		[A.11]	Acceso no autorizado
AC-09	Switch POE	[A.23]	Manipulación de los equipos
		[A.11]	Acceso no autorizado
AC-10	Firewall (Fortinet)	[A.23]	Manipulación de los equipos
		[A.11]	Acceso no autorizado
AC-11	Access Points (AP) / Puntos de Acceso	[A.24]	Denegación de servicio
		[A.11]	Acceso no autorizado
AC-12	Equipo telefónico fijo	[A.14]	Interceptación de información (escucha)
AC-13	Conexión inalámbrica	[E.19]	Fugas de información
		[A.19]	Divulgación de información
		[A.11]	Acceso no autorizado
AC-14	Equipo telefónico móvil	[A.14]	Interceptación de información (escucha)
		[A.11]	Acceso no autorizado
AC-15	Red de área local	[A.24]	Denegación de servicio
		[A.11]	Acceso no autorizado
AC-16	Conexión a internet	[A.24]	Denegación de servicio
		[E.19]	Fugas de información
		[A.19]	Divulgación de información
		[A.11]	Acceso no autorizado
AC-17	UPS (Fuentes de alimentación)	[E.25]	Pérdida de equipos
		[A.23]	Manipulación de los equipos
AC-18	Trabajadores / colaboradores	[A.29	Extorsión
		[A.30]	Ingeniería social (picaresca)
		[E.19]	Fugas de información

Nota. Elaboración propia a partir de (Amutio Gómez et al., 2012b)

Conforme con estas amenazas se realizó el análisis de riesgos e impactos. Siguiendo los lineamientos de la metodología Magerit, para determinar el nivel de riesgo de cada activo es preciso considerar la probabilidad y el impacto en caso de la ocurrencia de dichas amenazas. Para establecer la probabilidad se utilizó una escala de 1 a 5 conforme con los siguientes criterios:

Tabla 17

Escala de probabilidad de la amenaza

Nivel de probabilidad	Detalle	Valor
Muy bajo	Es probable la materialización de la amenaza en un contexto actual o futuro previsible	1
Bajo	Hay circunstancias que podrían llevar a la materialización de la amenaza, pero no son raras	2
Medio	Hay circunstancias en las que es razonablemente posible la materialización de la amenaza	3

Nivel de probabilidad	Detalle	Valor
Alto	Es probable la materialización de la amenaza en circunstancias normales	4
Muy alto	Es casi segura la materialización de la amenaza en un futuro previsible, excepto porque se tomen medidas de prevención	5

Nota. Elaboración propia a partir de (Guamán et al., 2023)

Por otra parte, para estimar el impacto de las amenazas se utilizó también una escala de 1 a 5, considerando los siguientes criterios:

Tabla 18

Escala de impacto de la amenaza

Nivel de impacto	Detalle	Valor
Insignificante	El daño ocasionado a activos, operaciones o reputación de la empresa sería mínimo y de fácil manejo sin el uso de medidas correctivas especiales	1
Menor	El daño ocasionaría problemas menores y retrasos, aunque no incidiría significativamente a las operaciones y reputación de la empresa	2
Moderado	El daño ocasionaría una interrupción notable y causaría un efecto moderado en las operaciones o reputación de la empresa	3
Mayor	El daño ocasionaría una interrupción significativa en las operaciones u ocasionaría un efecto considerable en la reputación de la empresa	4
Catastrófico	El daño ocasionaría una interrupción grave en las operaciones u ocasionaría un efecto devastador en la reputación de la empresa	5

Nota. Elaboración propia a partir de (Guamán et al., 2023)

Habiendo fijado estos valores para cada amenaza, el nivel de riesgo se obtendrá al multiplicar la probabilidad por el impacto. Para establecer el nivel de riesgo se toman como referencia los parámetros de la siguiente tabla:

Tabla 19

Escala de valoración de riesgos

Riesgo	Detalle	Rango
Bajo	Riesgo aceptable	1 a 6
Medio	Riesgo tolerable	7 a 14
Alto	Riesgo inadmisible	15 a 25

Nota. Elaboración propia a partir de (Guamán et al., 2023)

Conforme con los parámetros anteriores se obtuvieron 7 riesgos de nivel alto, 13 riesgos de nivel medio y 44 riesgos de nivel bajo, siendo los de mayor criticidad aquellos relacionados con datos o información., acceso no autorizado a teléfonos móviles, y a aquellos asociados con los trabajadores, como extorsión, ingeniería social y fugas de información. En la siguiente tabla se muestran a detalle los riesgos y su respectiva valoración:

Tabla 20

Análisis de riesgos e impactos de los activos del área de TI de Sardipac

Activo	Código Amenaza	Amenaza	Impacto	Probabilidad	Riesgo
Datos de procesos	[E.19]	Fugas de información	5	2	10
	[A.11]	Acceso no autorizado	5	1	5
	[A.15]	Modificación deliberada de la información	5	2	10
	[A.18]	Destrucción de información	5	2	10
	[A.19]	Divulgación de información	5	3	15
Datos de clientes, empleados y proveedores	[E.19]	Fugas de información	5	3	15
	[A.11]	Acceso no autorizado	5	1	5
	[A.15]	Modificación deliberada de la información	5	2	10
	[A.18]	Destrucción de información	5	2	10
	[A.19]	Divulgación de información	5	3	15
Backups y servidores NAS	[E.15]	Alteración accidental de la información	4	2	8
	[E.19]	Fugas de información	5	2	10
	[A.11]	Acceso no autorizado	4	1	4
	[A.15]	Modificación deliberada de la información	5	1	5
	[A.18]	Destrucción de información	5	1	5
	[A.19]	Divulgación de información	5	2	10
Acceso a servidores	[A.7]	Uso no previsto	4	2	8
	[A.24]	Denegación de servicio	3	1	3
	[E.1]	Errores de los usuarios	3	1	3
	[E.2]	Errores del administrador	4	1	4
	[A.11]	Acceso no autorizado	4	2	8
Kaspersky (antivirus)	[E.8]	Difusión de software dañino	3	4	12
	[A.7]	Uso no previsto	3	1	3
	[E.18]	Destrucción de información	2	1	2
	[E.19]	Fugas de información	2	1	2
	[A.11]	Acceso no autorizado	3	1	3
Servidor de respaldo	[E.8]	Difusión de software dañino	4	3	12
	[A.7]	Uso no previsto	3	1	3
	[E.18]	Destrucción de información	4	1	4
	[E.19]	Fugas de información	4	1	4
	[A.11]	Acceso no autorizado	4	1	4
Computadoras personales	[E.25]	Pérdida de equipos	2	2	4
	[A.23]	Manipulación de los equipos	2	2	4
	[A.25]	Robo	3	1	3
	[A.7]	Uso no previsto	3	1	3
	[A.11]	Acceso no autorizado	3	1	3
Tablets	[E.25]	Pérdida de equipos	2	2	4
	[A.23]	Manipulación de los equipos	2	2	4
	[A.25]	Robo	3	1	3
	[A.7]	Uso no previsto	3	1	3
	[A.11]	Acceso no autorizado	3	1	3
Switch POE	[A.23]	Manipulación de los equipos	2	1	2
	[A.11]	Acceso no autorizado	2	1	2
Firewall (Fortinet)	[A.23]	Manipulación de los equipos	2	1	2
	[A.11]	Acceso no autorizado	2	1	2
Access Points (AP) / Puntos de Acceso	[A.24]	Denegación de servicio	3	2	6
	[A.11]	Acceso no autorizado	4	1	4
Equipo telefónico fijo	[A.14]	Interceptación de información (escucha)	4	2	8
Conexión inalámbrica	[E.19]	Fugas de información	4	1	4
	[A.19]	Divulgación de información	4	1	4
	[A.11]	Acceso no autorizado	4	1	4

Activo	Código Amenaza	Amenaza	Impacto	Probabilidad	Riesgo
Equipo telefónico móvil	[A.14]	Interceptación de información (escucha)	3	2	6
	[A.11]	Acceso no autorizado	4	4	16
Red de área local	[A.24]	Denegación de servicio	3	1	3
	[A.11]	Acceso no autorizado	3	1	3
Conexión a internet	[A.24]	Denegación de servicio	3	2	6
	[E.19]	Fugas de información	4	1	4
	[A.19]	Divulgación de información	4	1	4
	[A.11]	Acceso no autorizado	4	1	4
UPS (Fuentes de alimentación)	[E.25]	Pérdida de equipos	1	1	1
	[A.23]	Manipulación de los equipos	1	1	1
Trabajadores / colaboradores	[A.29	Extorsión	4	4	16
	[A.30]	Ingeniería social (picaresca)	4	5	20
	[E.19]	Fugas de información	4	5	20

Nota. Elaboración propia a partir de (Amutio Gómez et al., 2012b)

Como último punto y partiendo de los resultados anteriores, se procedió a la identificación de las salvaguardias o medidas de control para cada riesgo asociado a los activos del área de TI de la empresa Sardipac, mismas que se detallan en la siguiente tabla:

Tabla 21

Identificación de salvaguardas

Activo	Código Amenaza	Amenaza	Riesgo	Control
Datos de procesos	[E.19]	Fugas de información	10	Aseguramiento de la integridad
	[A.11]	Acceso no autorizado	5	Identificación y autenticación
	[A.15]	Modificación deliberada de la información	10	Protección de la Información
	[A.18]	Destrucción de información	10	Protección de la Información
	[A.19]	Divulgación de información	15	Aseguramiento de la integridad
Datos de clientes, empleados y proveedores	[E.19]	Fugas de información	15	Aseguramiento de la integridad
	[A.11]	Acceso no autorizado	5	Identificación y autenticación
	[A.15]	Modificación deliberada de la información	10	Protección de la Información
	[A.18]	Destrucción de información	10	Protección de la Información
	[A.19]	Divulgación de información	15	Aseguramiento de la integridad
Backups y servidores NAS	[E.15]	Alteración accidental de la información	8	Cifrado de la información
	[E.19]	Fugas de información	10	Cifrado de la información
	[A.11]	Acceso no autorizado	4	Identificación y autenticación
	[A.15]	Modificación deliberada de la información	5	Protección de la Información
	[A.18]	Destrucción de información	5	Protección de la Información
	[A.19]	Divulgación de información	10	Aseguramiento de la integridad
Acceso a servidores	[A.7]	Uso no previsto	8	Protección de los Servicios
	[A.24]	Denegación de servicio	3	Aseguramiento de la disponibilidad
	[E.1]	Errores de los usuarios	3	Gestión de cambios (mejoras y sustituciones)
	[E.2]	Errores del administrador	4	Gestión de cambios (mejoras y sustituciones)
	[A.11]	Acceso no autorizado	8	Protección de servicios y aplicaciones web

Activo	Código Amenaza	Amenaza	Riesgo	Control
Kaspersky (antivirus)	[E.8]	Difusión de software dañino	12	Protección de las Aplicaciones Informáticas
	[A.7]	Uso no previsto	3	Se aplican perfiles de seguridad
	[E.18]	Destrucción de información	2	Copias de seguridad (backup)
	[E.19]	Fugas de información	2	Cambios (actualizaciones y mantenimiento)
	[A.11]	Acceso no autorizado	3	Se aplican perfiles de seguridad
Servidor de respaldo	[E.8]	Difusión de software dañino	12	Protección de las Aplicaciones Informáticas
	[A.7]	Uso no previsto	3	Se aplican perfiles de seguridad
	[E.18]	Destrucción de información	4	Copias de seguridad (backup)
	[E.19]	Fugas de información	4	Cambios (actualizaciones y mantenimiento)
	[A.11]	Acceso no autorizado	4	Se aplican perfiles de seguridad
Computadoras personales	[E.25]	Pérdida de equipos	4	Protección de los Equipos Informáticos
	[A.23]	Manipulación de los equipos	4	Se aplican perfiles de seguridad
	[A.25]	Robo	3	Protección de los Equipos Informáticos
	[A.7]	Uso no previsto	3	Se aplican perfiles de seguridad
	[A.11]	Acceso no autorizado	3	Se aplican perfiles de seguridad
Tablets	[E.25]	Pérdida de equipos	4	Protección de los Equipos Informáticos
	[A.23]	Manipulación de los equipos	4	Se aplican perfiles de seguridad
	[A.25]	Robo	3	Protección de los Equipos Informáticos
	[A.7]	Uso no previsto	3	Se aplican perfiles de seguridad
	[A.11]	Acceso no autorizado	3	Se aplican perfiles de seguridad
Switch POE	[A.23]	Manipulación de los equipos	2	Se aplican perfiles de seguridad
	[A.11]	Acceso no autorizado	2	Se aplican perfiles de seguridad
Firewall (Fortinet)	[A.23]	Manipulación de los equipos	2	Se aplican perfiles de seguridad
	[A.11]	Acceso no autorizado	2	Se aplican perfiles de seguridad
Access Points (AP) / Puntos de Acceso	[A.24]	Denegación de servicio	6	Aseguramiento de la disponibilidad
	[A.11]	Acceso no autorizado	4	Se aplican perfiles de seguridad
Equipo telefónico fijo	[A.14]	Interceptación de información (escucha)	8	Protección de la centralita telefónica (PABX)
Conexión inalámbrica	[E.19]	Fugas de información	4	Protección de la integridad de los datos intercambiados
	[A.19]	Divulgación de información	4	Protección criptográfica de la confidencialidad de los datos intercambiados
	[A.11]	Acceso no autorizado	4	Seguridad Wireless (WiFi)
Equipo telefónico móvil	[A.14]	Interceptación de información (escucha)	6	Protección de la integridad de los datos intercambiados
	[A.11]	Acceso no autorizado	16	Terminación
Red de área local	[A.24]	Denegación de servicio	3	Aseguramiento de la disponibilidad
	[A.11]	Acceso no autorizado	3	Terminación
Conexión a internet	[A.24]	Denegación de servicio	6	Aseguramiento de la disponibilidad
	[E.19]	Fugas de información	4	Protección de la integridad de los datos intercambiados
	[A.19]	Divulgación de información	4	Protección criptográfica de la confidencialidad de los datos intercambiados

Activo	Código Amenaza	Amenaza	Riesgo	Control
	[A.11]	Acceso no autorizado	4	Terminación
UPS (Fuentes de alimentación)	[E.25]	Pérdida de equipos	1	Protección del cableado
	[A.23]	Manipulación de los equipos	1	Elementos Auxiliares
Trabajadores / colaboradores	[A.29	Extorsión	16	Formación y concienciación
	[A.30]	Ingeniería social (picaresca)	20	Formación y concienciación
	[E.19]	Fugas de información	20	Formación y concienciación

Nota. Elaboración propia a partir de (Amutio Gómez et al., 2012b)

Capítulo IV
Propuesta

4.1 Descripción de la propuesta

4.1.1 Fundamentación de la propuesta

La presente propuesta se centra en el diseño de una estrategia de seguridad informática en ataques de ransomware para potenciar el área de TI en Sardipac, ello partiendo desde los datos obtenidos a través del proceso diagnóstico de las amenazas potenciales que enfrenta esta área de la compañía. Esta estrategia fue concebida bajo cuatro capas o ejes de acción, tales como:

- A: Prevención
- B: Detección temprana
- C: Respuesta y recuperación
- D: Personas y gobierno

Para proponer las acciones correspondientes a cada eje, se consideraron en primera instancia los riesgos de mayor relevancia obtenidos a través de la metodología Magerit, mismos que se detallan en la siguiente tabla:

Tabla 22

Riesgos más relevantes de la estrategia

Riesgo	Nivel	Amenaza potencial
Extorsión	Crítico	Ransomware (cifrado + chantaje)
Fugas de información	Alto	Doble extorsión (cifrado y robo de datos)
Modificación deliberada de la información	Alto	Alteración de recetas, lotes, trazabilidad
Acceso no autorizado	Medio	Vector inicial del ataque
Denegación de servicio	Bajo	Paro de operaciones y pérdidas económicas.

Nota. Elaboración propia

Dentro de este tipo de amenazas se identifican como principales activos afectados los siguientes: Datos de procesos productivos, datos de clientes, empleados y proveedores, backups y servidores NAS, redes de comunicaciones, y personal (colaboradores internos). En torno a esto se formula una estrategia con base en cuatro capas o ejes alienados a Magerit y a la norma ISO/IEC 27001.

4.1.2 Objetivo de la propuesta

Establecer acciones de seguridad informática bajo los parámetros de Magerit y la norma ISO/IEC 27001 para garantizar la continuidad de las actividades productivas de la empresa

Sardipac, asimismo, proteger la información sensible y reducir al mínimo el impacto económico y operativo de ataques ransomware.

4.1.3 Beneficiarios de la propuesta

El desarrollo de la propuesta se centró en la consideración de los siguientes beneficiarios tanto directos como indirectos:

- Beneficiarios directos: Personal del área de TI, colaboradores
- Beneficiarios indirectos: Personal administrativo, accionistas, proveedores

4.1.4 Estrategia de la propuesta

Con base en lo mencionado previamente se proponen las siguientes acciones y estrategias alienadas a Magerit y la norma ISO/IEC 27001:

Tabla 23

Estrategias y acciones de la propuesta

Ejes	Estrategias	Acciones	Ámbito de acción
1 Prevención	Control de accesos y credenciales	Autenticación multifactor (MFA) en: - Correo electrónico - VPN - Accesos a servidores y NAS	Ayudan a mitigar acceso no autorizado y extorsión.
		Eliminación de cuentas genéricas en planta	
		Principio de mínimo privilegio (operarios ≠ administración)	
	Protección de endpoints y servidores	Antivirus/EDR con protección anti-ransomware	Ayuda a mitigar la modificación deliberada y acceso no autorizado.
		Bloqueo de: - Macros no firmadas - PowerShell no autorizado - Ejecución desde carpetas temporales	
		Parcheo periódico de sistemas y PLC conectados	
	Segmentación de red	Separar: - Red administrativa - Red de producción (OT) - Backups	Ayuda a mitigar propagación del ransomware.
		Firewalls internos entre segmentos	
		Sin acceso directo de internet a sistemas de planta	

	Ejes	Estrategias	Acciones	Ámbito de acción
2	Detección temprana	Monitorización y alertas	Logs centralizados (SIEM o equivalente): − Accesos anómalos − Cifrado masivo de archivos − Uso extraño de cuentas administrativas	Ayuda a reducir el impacto de extorsión y fuga de información.
			Alertas automáticas ante: − Cambios masivos en NAS − Actividad fuera de horario	
		Protección del correo electrónico	Filtro antiphishing	Ayuda a mitigar este vector de entrada de ransomware.
			Bloqueo de adjuntos ejecutables	
			Análisis de enlaces sospechosos	
3	Respuesta y recuperación	Backups robustos	Estrategia 3-2-1: − 3 copias − 2 medios distintos − 1 copia offline o inmutable	Mitiga directamente el riesgo.
			Pruebas periódicas de restauración	
			Backups separados de la red productiva	
		Plan de respuesta a incidentes	Procedimiento claro: 1) Aislar equipos infectados 2) Desconectar red afectada 3) Notificar responsables 4) Recuperar desde backups	Reduce el tiempo de parada de operaciones de la empresa.
			Contacto legal y autoridades	
4	Personas y gobierno	Concienciación del personal	Formación básica: − Phishing − USB desconocidos − Buenas prácticas en contraseñas	Prepara al personal para gestionar correctamente los riesgos potenciales.
			Simulacros de ataque	
		Políticas y gobierno de seguridad	Política de seguridad de la información	Alinea las políticas de seguridad informática con Magerit e ISO/IEC 270001
			Política de backups	
			Gestión de proveedores (riesgo de terceros)	

Nota. Elaboración propia

4.1.4.1 Plan de acción de la propuesta

Tabla 24

Plan de acción de la propuesta

Objetivos	Ejes	Estrategias	Acciones específicas	Responsables	Resultados esperados
Prevenir ataques ransomware mediante control de accesos y credenciales, protección de servidores y segmentación de red.	Prevención	Control de accesos y credenciales	Autenticación multifactor (MFA) en: • Correo electrónico • VPN • Accesos a servidores y NAS	Técnicos de seguridad informática	Se cuenta con capas de seguridad multifactor de alta confiabilidad.
			Eliminación de cuentas genéricas en planta	Técnicos de seguridad informática	Se logra depurar cuestas genéricas en planta.
			Principio de mínimo privilegio (operarios ≠ administración)	Técnicos de seguridad informática	Se ha brindado a los usuarios acceso mínimo a aplicaciones y sistemas.
		Protección de endpoints y servidores	Antivirus/EDR con protección anti-ransomware	Técnicos de seguridad informática	Los equipos se encuentran protegidos
			Bloqueo de: • Macros no firmadas • PowerShell no autorizado • Ejecución desde carpetas temporales	Técnicos de seguridad informática	Se han bloqueado recursos con riesgo potencial o que pueda alojar malwares.
			Parcheo periódico de sistemas y PLC conectados	Técnicos de seguridad informática	Se han corregido vulnerabilidades.
		Segmentación de red	Separar: • Red administrativa • Red de producción (OT) • Backups	Técnicos de seguridad informática	Se ha logrado separar las redes limitando propagación de ataques.
			Firewalls internos entre segmentos	Técnicos de seguridad informática	Se ha logrado controlar el tráfico de redes.
			Sin acceso directo de internet a sistemas de planta	Técnicos de seguridad informática	Se ha logrado aislar de la red a sistemas de planta.

Objetivos	Ejes	Estrategias	Acciones específicas	Responsables	Resultados esperados
Contar con mecanismos de detección temprana de ataques ransomware centrados en monitorización y alertas, y protección de correo electrónico.	Detección temprana	Monitorización y alertas	Logs centralizados (SIEM o equivalente): • Accesos anómalos • Cifrado masivo de archivos • Uso extraño de cuentas administrativas	Técnicos de seguridad informática	Se ha logrado recopilar y analizar eventos anómalos.
			Alertas automáticas ante: • Cambios masivos en NAS • Actividad fuera de horario	Técnicos de seguridad informática	Se han incorporado mecanismos de alerta ante eventos anómalos.
		Protección del correo electrónico	Filtro antiphishing	Técnicos de seguridad informática	Se cuenta con filtro antiphishing.
			Bloqueo de adjuntos ejecutables	Técnicos de seguridad informática	Se logran bloquear adjuntos ejecutables.
			Análisis de enlaces sospechosos	Técnicos de seguridad informática	Se tiene reporte de enlaces sospechosos.
Generar respuesta y atención oportuna a ataques ransomware mediante backups robustos y procedimientos bien definidos.	Respuesta y recuperación	Backups robustos	Estrategia 3-2-1: • 3 copias • 2 medios distintos • 1 copia offline o inmutable	Técnicos de seguridad informática	Se garantiza la disponibilidad de los datos mediante procesos rigurosos.
			Pruebas periódicas de restauración	Técnicos de seguridad informática	Se ha comprobado la disponibilidad.
			Backups separados de la red productiva	Técnicos de seguridad informática	Se logra aislar la red productiva de backups
		Plan de respuesta a incidentes	Procedimiento claro: 1) Aislar equipos infectados 2) Desconectar red afectada 3) Notificar responsables 4) Recuperar desde backups	Técnicos de seguridad informática	Los colaboradores cuentan con formación sobre los procedimientos a seguir ante eventos y amenazas ransomware.
			Contacto legal y autoridades	Gerente general	Apoyo de autoridades

Objetivos	Ejes	Estrategias	Acciones específicas	Responsables	Resultados esperados
Brindar a los colaboradores formación continua sobre las modalidades de ataques ransomware y contar con política institucional claramente definida.	Personas y gobierno	Concienciación del personal	Formación básica: • Phishing • USB desconocidos • Buenas prácticas en contraseñas	Gerente general Consultor externo Colaboradores	Los colaboradores están debidamente formados en identificación de amenazas y buenas prácticas de seguridad.
			Simulacros de ataque	Consultor externo	Se cuenta con reporte de los ataques simulados efectuados, tasa de víctimas potenciales y se ha concientizado al personal.
		Políticas y gobierno de seguridad	Política de seguridad de la información	Gerente general Comité de seguridad informática	Se cuenta con política institucional apegada a Magerit y la norma ISO/IEC 27001.
			Política de backups	Gerente general Técnicos de seguridad informática	Se cuenta con política clara de backups para la integridad y disponibilidad de los datos.
			Gestión de proveedores (riesgo de terceros)	Gerente general Técnicos de seguridad informática	Se ha efectuado una correcta gestión de proveedores para mitigar riesgos de terceros.

Nota. Elaboración propia. Los objetivos descritos en la tabla corresponden puntualmente a la propuesta.

4.2 Determinación de recursos

Dentro de esta estrategia también es importante definir los recursos necesarios para la puesta en marcha de las acciones descritas anteriormente, en ese sentido se evidencia la necesidad de contar con recurso humano, tecnológico y financiero para la correcta ejecución de los ejes propuestos. En la siguiente tabla se describen a detalle dichos recursos:

Tabla 25

Determinación de recursos de la propuesta

Ejes	Estrategias	Acciones	Recursos
Prevención	Control de accesos y credenciales	Autenticación multifactor (MFA) en: − Correo electrónico − VPN − Accesos a servidores y NAS	− Humano − Tecnológico
		Eliminación de cuentas genéricas en planta	− Humano − Tecnológico
		Principio de mínimo privilegio (operarios ≠ administración)	− Humano − Tecnológico
	Protección de endpoints y servidores	Antivirus/EDR con protección anti-ransomware	− Huma − Tecnológico − Financiero
		Bloqueo de: − Macros no firmadas − PowerShell no autorizado − Ejecución desde carpetas temporales	− Humano − Tecnológico
		Parcheo periódico de sistemas y PLC conectados	− Humano − Tecnológico
	Segmentación de red	Separar: − Red administrativa − Red de producción (OT) − Backups	− Humano − Tecnológico
		Firewalls internos entre segmentos	− Humano − Tecnológico − Financiero
		Sin acceso directo de internet a sistemas de planta	− Humano − Tecnológico
Detección temprana	Monitorización y alertas	Logs centralizados (SIEM o equivalente): − Accesos anómalos − Cifrado masivo de archivos	− Humano − Tecnológico

Ejes	Estrategias	Acciones	Recursos
		− Uso extraño de cuentas administrativas	
		Alertas automáticas ante: − Cambios masivos en NAS − Actividad fuera de horario	− Humano − Tecnológico
	Protección del correo electrónico	Filtro antiphishing	− Humano − Tecnológico − Financiero
		Bloqueo de adjuntos ejecutables	− Humano − Tecnológico
		Análisis de enlaces sospechosos	− Humano − Tecnológico
Respuesta y recuperación	Backups robustos	Estrategia 3-2-1: − 3 copias − 2 medios distintos − 1 copia offline o inmutable	− Humano − Tecnológico
		Pruebas periódicas de restauración	− Humano − Tecnológico
		Backups separados de la red productiva	− Humano − Tecnológico
	Plan de respuesta a incidentes	Procedimiento claro: 1) Aislar equipos infectados 2) Desconectar red afectada 3) Notificar responsables 4) Recuperar desde backups	− Humano − Tecnológico
		Contacto legal y autoridades	− Humano
Personas y gobierno	Concienciación del personal	Formación básica: − Phishing − USB desconocidos − Buenas prácticas en contraseñas	− Humano − Tecnológico − Financiero
		Simulacros de ataque	− Humano − Tecnológico − Financiero
	Políticas y gobierno de seguridad	Política de seguridad de la información	− Humano
		Política de backups	− Humano
		Gestión de proveedores (riesgo de terceros)	− Humano

Nota. Elaboración propia

4.3 Etapas de acción para el desarrollo de la propuesta

Para la puesta en marcha de la estrategia de seguridad informática descrita en este trabajo se propone un marco de ejecución de nueve (9) fases, que van desde la fijación del alcance hasta el cierre de la implementación, definiendo de esta forma plazos, responsables, resultados esperados y recursos a utilizar. Cada una de estas etapas se describen a detalle en los siguientes enunciados.

Fase 1: Fijación del alcance de la estrategia

En esta fase se reúne el gerente general, personal de seguridad informática y los técnicos externos para definir los ejes de trabajo de la estrategia, definiendo los recursos disponibles y aquellos que se deben implementar para la correcta puesta en marcha de las acciones. De esta fase se espera la aprobación de presupuestos, así como la asignación de recurso humano, tecnológico e institucional, y se llevará a cabo bajo los siguientes parámetros:

Tabla 26

Fijación del alcance de la estrategia

Resultado	Plazo límite	Recursos	Responsables
Se cuenta con aprobación de prepuesto y recursos necesarios para ejecución de la estrategia.	2 semana posterior a aprobación de la estrategia	Personal administrativo y técnico	Gerente general Personal de TI Técnicos asesores

Fase 2: Reunión de lanzamiento y partes interesadas de la estrategia de seguridad informática

Para esta reunión se integra a accionistas, personal administrativo, asesores tecnológicos externos y personal técnico interno con la finalidad de establecer los lineamientos de ejecución del plan, contemplando la disponibilidad de tiempo y recursos. De esta fase se espera haber socializado la estrategia de seguridad informática con los stakeholders, misma que se realizará considerando los siguientes parámetros:

Tabla 27

Reunión de lanzamiento y partes interesadas

Resultado	Plazo límite	Recursos	Responsables
Se ha socializado la estrategia con las partes interesadas.	2 semanas posterior a haberse fijado el alcance	Accionistas, personal administrativo y técnicos.	Gerente general Junta de accionistas

Fase 3: Implementación de las acciones de prevención de ataques ransomware

En esta fase se llevan a cabo las acciones relacionadas con las estrategias de prevención de ransomware, mismas que consisten primero en el control de accesos y credenciales, protección de endpoints y servidores, y segmentación de red. Esto con la finalidad de integrar protocolos que ayuden a blindar y proteger ante eventos potenciales a sistemas, equipos y personal de la empresa; para ello se consideran los siguientes parámetros:

Tabla 28

Implementación de acciones de prevención de ransomware

Resultado	Plazo límite	Recursos	Responsables
Se cuenta con protocolos y procesos de prevención de ataques ransomware.	2 semanas posterior a la reunión de lanzamiento	Recurso humano y tecnológico	Técnicos de seguridad informática

Fase 4: Implementación de las acciones de detección temprana de ransomware

Para esta fase se ponen en marcha las acciones relacionadas con la estrategia de detección temprana de ataques ransomware, mismas que tienen que ver con monitorización y alertas, y protección del correo electrónico. De esta etapa se espera contar con protocolos para la identificación a tiempo de ataques potenciales que puedan vulnerar datos, sistemas y personal de la empresa, mismas que se llevará a cabo bajo los siguientes parámetros:

Tabla 29

Implementación de acciones de detección de ransomware

Resultado	Plazo límite	Recursos	Responsables
Se han integrado acciones de detención temprana de ransomware.	8 semanas posterior a la estrategia de prevención	Recurso humano, tecnológico y financiero.	Técnicos de seguridad informática

Fase 5: Implementación de las acciones de respuesta y recuperación ante ataques ransomware

Durante esta fase se llevan a cabo las acciones planificadas que tienen que ver con respuesta y recuperación ante ataques ransomware, mismas que se centran en contar con backups robustos y con un plan de respuesta a incidentes. A través de estas acciones se espera asegurar la integridad y disponibilidad de los datos de la empresa y salvaguardar sistemas, dominios y personas. Para su ejecución se consideran los siguientes parámetros:

Tabla 30

Implementación de acciones de respuesta y recuperación de ransomware

Resultado	Plazo límite	Recursos	Responsables
Se cuenta con un plan claro de respuesta y recuperación ante ataques ransomware.	4 semanas posterior a la estrategia de detección temprana	Recurso humano, tecnológico y financiero.	Técnicos de seguridad informática

Fase 6: Implementación de las acciones ligadas a personas y gobierno organizacional

En esta última etapa se integrarán acciones relacionadas con las personas y política institucional, tales como concienciación del personal y políticas internas, ayudando a los colaboradores a identificar ataques como phishing e ingeniería social, y a su vez contar con política claras de seguridad que rijan las acciones presentes y futuras con respecto al manejo de riesgos informáticos. Para su ejecución se contemplan los siguientes parámetros:

Tabla 31

Implementación de acciones de personas y gobierno

Resultado	Plazo límite	Recursos	Responsables
Se ha formado al personal y se cuenta con políticas claras de manejo de riesgos informativos.	4 semanas posterior a la estrategia de respuesta	Recurso humano, tecnológico y financiero.	Técnicos de seguridad informática

Fase 7: Pruebas

Durante esta fase se revisan las estrategias y acciones ejecutadas, se evalúan los protocolos efectuados a fin de identificar mejoras que puedan corregirse a tiempo, siendo esencial para determinar la capacidad de prevención, detección y respuesta de la empresa ante ataques ransomware, asegurando la mejora continua con base en los lineamientos de Magerit y la norma ISO/IEC 27001. Para su puesta en marcha se consideran los siguientes parámetros:

Tabla 32

Pruebas posteriores a la ejecución de la estrategia

Resultado	Plazo límite	Recursos	Responsables
Se ha formado al personal y se cuenta con políticas claras de manejo de riesgos informativos.	4 semanas posterior a la estrategia personas y gobierno	Recurso humano, tecnológico y financiero.	Técnicos de seguridad informática

Fase 8: Levantamiento de documentación de la estrategia de seguridad informática

Una vez llevadas a cabo las distintas acciones de la estrategia de seguridad informática del área de Tecnologías de la Información de la empresa Sardipac, se procederá a levantar la documentación necesaria de respaldo que verifique el cumplimiento de cada uno de los ejes propuestos, además de los reportes surgidos a lo largo de la implementación, mismos que sirven para el replanteamiento de estas acciones y el mantenimiento de los protocolos de seguridad propuestos. Esta fase se desarrolla tomando en cuenta los siguientes parámetros:

Tabla 33

Levantamiento de documentación de la estrategia

Resultado	Plazo límite	Recursos	Responsables
Se logra recolectar toda la documentación que respalda la ejecución de la estrategia.	4 semanas posterior a la fase de pruebas	Recurso humano	Gerente Técnicos de seguridad informática

Nota. Elaboración propia

Fase 9:

Como último punto de la estrategia propuesta se considera el cierre de su ejecución, esto mediante la generación de reportes, resultados y firmas de responsabilidad del personal involucrado. Esta fase es importante porque ayuda a definir las metas alcanzadas, identificar limitaciones y a proponer mejoras conforme con los lineamientos de la política de seguridad informática de la empresa. Para su puesta en marcha se consideran los siguientes parámetros:

Tabla 34

Cierre de la implementación de la estrategia

Resultado	Plazo límite	Recursos	Responsables
Se logra dar cierre a la estrategia de seguridad dando cumplimiento a los resultados.	2 semanas posterior al levantamiento de documentación.	Recurso humano	Gerente Técnicos de seguridad informática

Nota. Elaboración propia

4.4 Presentación y análisis de resultados

Debido a que este trabajo se limita a proponer una estrategia de seguridad informática sin considerar su ejecución, en este apartado se describen los indicadores de cumplimiento de las acciones fijadas, los que servirán para verificar y evaluar los hitos alcanzados en cada eje relacionado con la prevención, detección, respuesta y formación del personal en lo relacionado

Ejes	Estrategias	Acciones	Indicadores de cumplimiento
Prevención	Control de accesos y credenciales	Autenticación multifactor (MFA) en: - Correo electrónico - VPN - Accesos a servidores y NAS	% de sistemas críticos con MFA habilitado % de usuarios con MFA activo sobre el total # de accesos bloqueados por fallo de MFA Tiempo promedio de despliegue de MFA (días)
		Eliminación de cuentas genéricas en planta	# de cuentas genéricas detectadas % de cuentas genéricas eliminadas % de usuarios con cuentas nominales % de incidencias asociadas a cuentas compartidas
		Principio de mínimo privilegio (operarios ≠ administración)	% de usuarios con permisos acordes a su rol # de accesos privilegiados no justificados % de revisiones de permisos realizadas en plazo # de incidentes por exceso de privilegios
	Protección de endpoints y servidores	Antivirus/EDR con protección anti-ransomware	% de equipos con EDR activo y actualizado # de amenazas bloqueadas automáticamente Tiempo medio de detección de malware % de endpoints sin protección (objetivo: 0%)
		Bloqueo de: - Macros no firmadas - PowerShell no autorizado - Ejecución desde carpetas temporales	% de políticas de restricción aplicadas # de intentos bloqueados por estas reglas % de equipos con hardening completo # de excepciones aprobadas vs solicitadas
		Parcheo periódico de sistemas y PLC conectados	% de sistemas (IT y PLC) parcheados dentro del plazo definido Tiempo medio de aplicación de parches críticos (MTTP) # de vulnerabilidades críticas sin parchear # de incidencias operativas causadas por actividades de parcheo
	Segmentación de red	Separar: - Red administrativa - Red de producción (OT) - Backups	% de activos correctamente segmentados # de accesos cruzados detectados Resultado de pruebas de aislamiento (OK / NOK) # de incidentes propagados entre segmentos
		Firewalls internos entre segmentos	% de segmentos de red protegidos por firewalls internos

			# de comunicaciones no autorizadas bloqueadas entre segmentos % de reglas de firewall revisadas y aprobadas según el calendario $ de incidentes de seguridad por fallas de segmentación
		Sin acceso directo de internet a sistemas de planta	# de sistemas OT con salida directa a internet % de tráfico OT bloqueado correctamente # de alertas por intento de conexión externa Cumplimiento de arquitectura definida (%)
Detección temprana	Monitorización y alertas	Logs centralizados (SIEM o equivalente): - Accesos anómalos - Cifrado masivo de archivos - Uso extraño de cuentas administrativas	% de sistemas enviando logs al SIEM # de eventos analizados por día % de fuentes críticas integradas Retención de logs (días vs objetivo)
		Alertas automáticas ante: - Cambios masivos en NAS - Actividad fuera de horario	# de alertas generadas % de alertas atendidas en SLA Tiempo medio de detección (MTTD) % de falsos positivos
	Protección del correo electrónico	Filtro antiphishing	% de correos maliciosos bloqueados # de correos de phishing entregados al usuario # de incidentes originados por email
		Bloqueo de adjuntos ejecutables	# de adjuntos bloqueados % de intentos de envío con malware # de excepciones autorizadas Incidentes asociados a adjuntos (ideal: 0)
		Análisis de enlaces sospechosos	# de enlaces analizados % de enlaces maliciosos bloqueados Tiempo de análisis promedio Incidentes por enlaces no detectados
Respuesta y recuperación	Backups robustos	Estrategia 3-2-1: - 3 copias - 2 medios distintos - 1 copia offline o inmutable	% de sistemas cubiertos por backup 3-2-1 # de fallos de copia de seguridad Cumplimiento de frecuencia de backup (%) # de backups verificados
		Pruebas periódicas de restauración	# de pruebas realizadas vs planificadas % de restauraciones exitosas Tiempo medio de recuperación (RTO)

			Desviación entre RTO real y objetivo
		Backups separados de la red productiva	% de backups aislados correctamente # de accesos no autorizados a backups Resultado de auditorías de aislamiento Incidentes de cifrado de backups (0 esperado)
	Plan de respuesta a incidentes	Procedimiento claro: 1) Aislar equipos infectados 2) Desconectar red afectada 3) Notificar responsables 4) Recuperar desde backups	% de incidentes gestionados según procedimiento Tiempo medio de respuesta (MTTR) # de incidentes sin documentación Resultado de revisiones post-incidente
		Contacto legal y autoridades	Tiempo de notificación tras incidente grave % de incidentes con escalamiento correcto Cumplimiento legal (sí/no)
Personas y gobierno	Concienciación del personal	Formación básica: - Phishing - USB desconocidos - Buenas prácticas en contraseñas	% de personal formado Resultados promedio de evaluaciones # de incidentes por error humano Frecuencia anual de formación
		Simulacros de ataque	# de simulacros realizados Tasa de detección por empleados Tasa de clic en correos simulados Tiempo de reacción del personal Mejora porcentual entre simulacros
	Políticas y gobierno de seguridad	Política de seguridad de la información	Política aprobada y vigente (sí/no) % de empleados que la conocen # de incumplimientos detectados
		Política de backups	Fecha de última revisión Cumplimiento de la política (%) # de desviaciones detectadas Frecuencia de revisión Incidentes por backup incorrecto
		Gestión de proveedores (riesgo de terceros)	% de proveedores evaluados en seguridad # de proveedores de alto riesgo % de contratos con cláusulas de seguridad Incidentes originados en terceros

a ataques ransomware; dicho esto, en la siguiente tabla se muestran las acciones con sus respectivos indicadores:

Tabla 35

Indicadores de cumplimiento de la propuesta

Nota. Elaboración propia

Conclusiones

Conforme con el análisis de este trabajo se pudo comprobar que la empresa Sardipac cuenta con personal externo para la asistencia técnica relacionado con la seguridad informática, quienes se encarga principalmente de dar soporte a los usuarios y revisar políticas del firewall, en este contexto se identificaron dos elementos críticos de infraestructura tecnológica como son Inforfish y Qbiz que contienen datos sensibles de personal, clientes, proveedores, entre otros; además se ha integrado a Fortinet como herramienta de monitoreo para contrarrestar ataques ransomware. A más de esto se pudo conocer que la entidad se enfrenta a continuos intentos de inicio de sesión inusuales, lo que evidentemente representan un riesgo para la integridad y confidencialidad de los datos.

Para identificar los activos de mayor vulnerabilidad y riesgo a ataques ransomware se realizó un análisis utilizando la metodología Magerit, esto permitió comprobar que los datos internos representan un elemento de alto riesgo para la compañía al igual que los dispositivos móviles y el personal, expuestos principalmente a vulnerabilidades como fugas de información, divulgación de información, acceso no autorizado, extorsión e ingeniería social; además de riesgos de nivel medio como difusión de software dañino, modificación deliberada de la información y destrucción de la información.

Al revisar las estrategias y buenas prácticas se encontró que las organizaciones suelen hacer uso continuo de evaluaciones de seguridad mediante la metodología Magerit que se encuentra apegada a la norma ISO/IEC 27001, dentro de esto se encontró que diversos autores realizan estrategias de seguridad informática asociada a la implementación de políticas se seguridad, gestión de riesgos, segmentación de servidores, protección de correo electrónico, cifrado de equipos y capacitaciones al personal en temas de ciberseguridad, siendo esta última la acción más mencionada en la literatura debido a la importancia de este activo y a la vulnerabilidad que presenta continuamente.

Debido a lo observado en la evaluación de riesgos de esta investigación, se propuso una estrategia de seguridad informática centrada en cuatro ejes: prevención, detección temprana, respuesta y recuperación, y personas y gobierno. El primero ayudó a establecer protocolos para reforzar la integridad de los datos de la compañía, el segundo permitió definir acciones para la prevención oportuna de ataques ransomware mediante mecanismos avanzados, el tercero permitió definir líneas de acción para responder a estos ataques siguiendo pasos claramente

detallados, y el cuarto ayudó a sugerir la integración de políticas de seguridad en la empresa, así como la formación del personal para la gestión adecuada de las vulnerabilidades.

Para el cumplimiento de las estrategias fue necesario definir indicadores de cumplimiento, por ello se formularon criterios de evaluación para cada acción propuesta, los que abarcan porcentajes de cumplimiento, número de incidentes, reportes de procedimientos efectuados, temporalidad y resultados de pruebas efectuadas. Se ha concluido que estas herramientas de medición son fundamentales para el seguimiento de la propuesta en su fase de ejecución, porque ayudan al personal técnico a generar reportes de efectividad y a realizar ajustes correctivos para reforzar la seguridad informática de la compañía.

Como resultado global de esta investigación se puede concluir que, el diseño de una estrategia de seguridad representa una alternativa pertinente para ser aplicada en el área de Tecnologías de la Información de la empresa Sardipac, debido a que actualmente las organizaciones privadas son el foco principal de la ciberdelincuencia, factor que presenta un riesgo potencial de vulneración de datos aspecto que puede conllevar a la afectación de las operaciones del negocio, por ende abordar esta situación desde una mirada integral resulta clave para prevenir y mitigar ataques ransomware en este contexto.

Recomendaciones

Realizar diagnósticos de seguridad informática de manera frecuente a fin de identificar aspectos de vulnerabilidad en la empresa, lo que permitirá establecer mecanismos de control acorde con las modalidades cada vez más sofisticadas de ataque ransomware, dichos diagnósticos deben realizarse mediante metodologías probadas y estandarizadas como Magerit, que conllevan a un análisis minucioso y confiable sobre los riesgos potenciales.

Evaluar de forma constante la vulnerabilidad de los activos de la compañía a fin de recategorizarlos según sus niveles de riesgo, ajustando a su vez las medidas de seguridad que ayuden a salvaguardar la integridad y confidencialidad de elementos sensibles como los datos internos, que ante ataques de ransomware podría verse comprometida la operatividad de la compañía.

Revisar constantemente las actualizaciones y nuevas estrategias de seguridad informática adoptada en el contexto empresarial, esto con la finalidad de mantenerse a la vanguardia de los protocolos basados en la normativa internacional, ayudando a crear entornos competitivos altamente seguros, principalmente en un contexto cada vez más digitalizado que facilita la proliferación de ataques ransomware que pueden llegar a afectar sectores productivos.

Ejecutar la estrategia de seguridad propuesta en este documento, apegándose a las directrices y lineamientos descritos en el plan de acción y fases de ejecución, lo que ayudará a la integración adecuada de las acciones de seguridad que abordan de manera integral y sistemática todos los ejes que conforman un sistema sólido de ciberseguridad como son la prevención, detección, respuesta y formación del personal.

Emplear los indicadores de evaluación descritos en este trabajo con la finalidad de dar seguimiento oportuno a las acciones propuestas, realizar acciones correctivas y mantener reportes continuos con todos los involucrados, esto permitirá comprobar el nivel de efectividad de la estrategia, conllevando a ser aplicada de manera sostenida como parte de la política de seguridad informática de la empresa Sardipac.

Bibliografía

Agencia de Ciberseguridad de la Unión Europea. (2022). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Albshaier, L., Almarri, S., y Rahman, M. M. H. (2024). Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. *Information*, *15*(8), 484. https://doi.org/10.3390/info15080484

Amutio Gómez, M. A., Candau, J., y Mañas, J. A. (2012a). *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I* (p. 127). Ministerio de Hacienda y Administraciones Públicas de España. https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html

Amutio Gómez, M. A., Candau, J., y Mañas, J. A. (2012b). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos* (p. 75). Ministerio de Hacienda y Administraciones Públicas de España. https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Avila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49), 92-119. https://doi.org/10.15517/isucr.v24i49.50765

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., y Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Duque Agudelo, D. A. (2022). *Plan de Seguridad Informática* [Tesis de Ingeniería, Universidad de Antioquia]. https://hdl.handle.net/10495/30458

ESET. (2024, diciembre 19). *Ransomware en 2024: Un año récord a nivel de impacto y ganancias*. https://www.eset.com/ec/acerca-de-eset/sala-de-prensa/comunicados-de-

prensa/articulos-de-prensa/ransomware-en-2024-un-ano-record-a-nivel-de-impacto-y-ganancias/

Gorka, A., y Popek, A. (2025). Attempt to Use the Deming Cycle (PDCA) in the Process of Implementing an Information Security Management System. *International Journal for Quality Research*, *19*(2), 371-386. https://doi.org/10.24874/IJQR19.02-01

Guamán, M., Zenteno, J. A. C., Urgilés, Cristhian Flores, Urgilés, Cristina Flores, y Egas, M. R. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*(49), 139-165. https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165

Hansel, M., y Silomon, J. (2024). Ransomware as a threat to peace and security: Understanding and avoiding political worst-case scenarios. *Journal of Cyber Policy*, *9*(2), 159-178. https://doi.org/10.1080/23738871.2024.2357092

IBM Security. (2023). *Cost of a data breach report 2023*. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf

Ingeniería de Calidad. (2020, febrero 8). *Ciclo de Deming: Metodología de mejora continua | PDCA - PHVA*. https://www.ingenieriadecalidad.com/2020/02/ciclo-de-deming.html

Instituto Nacional de Ciberseguridad. (2021). *Glosario de términos de ciberseguridad* (p. 82). INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ISO/IEC. (2022). *ISO/IEC 27001:2022. Sistemas de gestión de la seguridad de la información*. https://www.iso.org/es/norma/27001

IT Ahora. (2025, abril 16). *Ciberseguridad y Protección de Datos: Un desafío estratégico para las empresas en Ecuador*. https://itahora.com/2025/04/16/ciberseguridad-y-proteccion-de-datos-un-desafio-estrategico-para-las-empresas-en-ecuador/

Jácome Segovia, D., Castillo Fiallos, J., Mantilla Cabrera, C., y Vaca Barahona, B. E. (2021). Aplicación de MAGERIT para reducir riesgos en servicios Web en un contexto académico en Ecuador. *AlfaPublicaciones*, *3*(2.2), 66-82. https://doi.org/10.33262/ap.v3i2.2.60

Kaspersky. (2025, mayo 12). *Aumento sostenido de los ataques de ransomware en América Latina*. https://latam.kaspersky.com/about/press-releases/aumento-sostenido-de-los-ataques-de-ransomware-en-america-latina-kaspersky

Kritika, Er. (2025). A comprehensive literature review on ransomware detection using deep learning. *Cyber Security and Applications*, *3*, 100078. https://doi.org/10.1016/j.csa.2024.100078

Moya Gavilanes, C. A. (2023). *Propuesta de un plan de seguridad informático para la empresa E.P.-E.M.A.P.A.* [Tesis de Maestría, Pontificia Universidad Católica del Ecuador]. https://repositorio.puce.edu.ec/handle/123456789/9066

Nabi, A. U., Ahmed, M., y Abro, A. (2022). An Overview of Firewall Types, Technologies, and Functionalities. *International Journal of Computing and Related Technologies*, *3*(No 1), 10-16.

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *International Journal of Scientific Research and Management (IJSRM)*, *12*(06), 1282-1298. https://doi.org/10.18535/ijsrm/v12i06.ec09

Paez, M., y Portilla, D. (2024). La Metodología Magerit para la evaluación de riesgos de activos de información, caso Instituto Superior Tecnológico Nelson Torres: Evaluacion de Riesgos. *NEXOS CIENTÍFICOS - ISSN 2773-7489*, *8*(1), 1-11.

Paniagua Soza, R. J. (2022). *Anatomía del ransomware* [Tesis de Maestría, Universitat Oberta de Catalunya (UOC)]. https://hdl.handle.net/10609/145831

Rossetti, G. H., y Quiroga, O. D. (2023). Metodología de gestión de riesgos para el desarrollo de productos tecnológicos en una empresa multinacional. *Revista Tecnología en Marcha*. https://doi.org/10.18845/tm.v36i7.6856

Salas-Riega, J. L., Riega-Virú, Y., Ninaquispe-Soto, M., y Salas-Riega, J. M. (2025). Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats. *International Journal of Advanced Computer Science and Applications*, *16*(6). https://doi.org/10.14569/IJACSA.2025.0160672

Sánchez, F. P., y Andaluz, L. M. (2024). Tecnologías de seguridad para empresas en Guayaquil. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *6*(2), 250-263. https://doi.org/10.59169/pentaciencias.v6i2.1045

Shaytura, S. V., y Pitkevich, P. N. (2022). Data backup methods for mission-critical information systems. *Russian Technological Journal*, *10*(1), 28-34. https://doi.org/10.32362/2500-316X-2022-10-1-28-34

Sophos. (2023). *The State of Ransomware 2023*. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/CRN360/sophos-state-of-ransomware-2023-wp.pdf

The Deming Institute. (2017, agosto 27). PDSA Cycle (Plan-Do-Study-Act). *Https://Deming.Org/*. https://deming.org/explore/pdsa/

Trujillo Alvira, J. (2024). *Diseñar estrategias complementarias para mejorar la seguridad informática y de la información en la compañía QWERTY S.A. utilizando la norma ISO 27001* [Tesis de Licenciatura, Universidad Nacional Abierta y a Distancia UNAD]. http://repository.unad.edu.co/handle/10596/47673

Vega Briceño, E. (2021). *Seguridad de la Información* (1ra edición). Editorial 3Ciencia. http://hdl.handle.net/11056/19011

Verizon Business. (2024). *2024 Data Breach Investigations Report* (p. 100). Verizon. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Zapata Chasiguasin, K. B. (2020). *Sistema de gestión de seguridad de la información basado en las Normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato* [Tesis de Licenciatura, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos]. https://repositorio.uta.edu.ec/handle/123456789/30694

Anexos

Anexo 1: Resultados de encuesta a colaboradores

Fundamentos de Ciberseguridad

1 Quiz ¿Qué debes hacer si recibes un correo con un enlace sospechoso?

Correct answer(s)	Reportarlo al equipo de TI o Seguridad
Players correct (%)	69.23%
Question duration	20 seconds

Answer Summary

Answer options	▲ Hacer clic rápidamente antes de que expire	◆ Reenviarlo a tus contactos	● Ignorarlo y borrarlo	■ Reportarlo al equipo de TI o Seguridad	⬟	▼
Is answer correct?	✗	✗	✗	✓		
Number of answers received	0	0	1	9		
Average time taken to answer (seconds)	0.00	0.00	14.97	14.02		

Player Details

Player	Answer		Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓	Reportarlo al equipo de TI o Seguridad	800	800	7.83
Alex	✓	Reportarlo al equipo de TI o Seguridad	687	687	12.502
CINCC	-		0	0	20
Carmen	-		0	0	20
Cesar	-		0	0	20
Fabri	✓	Reportarlo al equipo de TI o Seguridad	574	574	17.043
Genesis	✓	Reportarlo al equipo de TI o Seguridad	612	612	15.534
Génesis F	✓	Reportarlo al equipo de TI o Seguridad	549	549	18.048
IRVING	✓	Reportarlo al equipo de TI o Seguridad	542	542	18.308
Julio	✓	Reportarlo al equipo de TI o Seguridad	507	507	19.701
Melissa	✓	Reportarlo al equipo de TI o Seguridad	606	606	15.773
Samanta	✓	Reportarlo al equipo de TI o Seguridad	757	757	9.709
Wilmer	✗	Ignorarlo y borrarlo	0	0	14.967

Fundamentos de Ciberseguridad

2Quiz ¿Cuál es una señal clara de un correo de phishing?

Correct answer/s	Solicitud de datos personales urgentes
Players correct (%)	23.08%
Question duration	20 seconds

Answer Summary

Answer options	▲ Ortografía perfecta y logos oficiales	◆ Solicita datos personales urgentes	■ Enviado desde tu dominio de empresa	● Firma con nombre completo y cargo real
Is answer correct?	✗	✓	✗	✗
Number of answers received	1	3	1	1
Average time taken to answer (seconds)	14,84	13,00	14,28	16,00

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✗ Enviado desde tu dominio de empresa	0	809	14,98
Alex	✓ Solicita datos personales urgentes	531	1218	18,778
CNCC	-	0	0	20
Carmen	✗ Firma con nombre completo y cargo real	0	0	16,032
Cesar	✗ Ortografía perfecta y logos oficiales	0	0	14,842
Fabi	✓ Solicita datos personales urgentes	714	1288	11,452
Gamaliel	-	0	812	20
Gamaliel F	✓ Solicita datos personales urgentes	781	1330	8,769
IPMNG	-	0	542	20
Julio	-	0	507	20
Melissa	-	0	808	20
Samanta	-	0	757	20
Wilmar	-	0	0	20

Fundamentos de Ciberseguridad

3 Quiz ¿Qué contraseña es más segura?

Correct answers	K9v$Pz8IrT#
Players correct (%)	84,62%
Question duration	20 seconds

Answer Summary

Answer options	▲ 123456	◆ miempresa2023	● mariaGonzalez1	■ K9v$Pz8IrT#	⬟	▼
Is answer correct?	✗	✗	✗	✓		
Number of answers received	0	1	0	11		
Average time taken to answer (seconds)	0,00	15,13	0,00	6,85		

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓ K9v$Pz8IrT#	891	1700	4,362
Alex	✓ K9v$Pz8IrT#	886	2104	4,562
CRCC	✗ miempresa2023	0	0	15,129
Carmen	✓ K9v$Pz8IrT#	681	681	12,775
Cesar	✓ K9v$Pz8IrT#	827	827	6,912
Fabri	✓ K9v$Pz8IrT#	886	2174	4,549
Genesis	✓ K9v$Pz8IrT#	849	1461	6,037
Génesis F	✓ K9v$Pz8IrT#	868	2198	5,294
IRVING	–	0	542	20
Julio	✓ K9v$Pz8IrT#	710	1217	11,594
Melissa	✓ K9v$Pz8IrT#	875	1481	4,987
Samanta	✓ K9v$Pz8IrT#	903	1660	3,893
Wilmer	✓ K9v$Pz8IrT#	740	740	10,382

Fundamentos de Ciberseguridad

4 Quiz ¿Qué es un malware?

Correct answers	Software malicioso que daña o roba información
Players correct (%)	69.23%
Question duration	20 seconds

Answer Summary

Answer options	Software malicioso que daña o roba información	Una herramienta para acelerar el equipo	Un antivirus molesto	Una contraseña débil
Is answer correct?	✓	✗	✗	✗
Number of answers received	9	0	0	1
Average time taken to answer (seconds)	10.36	0.00	0.00	16.87

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓ Software malicioso que daña o roba información	823	2523	7,071
Alex	✓ Software malicioso que daña o roba información	742	2848	10,311
CRCC	✗ Una contraseña débil	0	0	16,872
Carmen	✓ Software malicioso que daña o roba información	747	1428	10,113
Cesar	✓ Software malicioso que daña o roba información	711	1539	11,573
Fabri	✓ Software malicioso que daña o roba información	876	3050	4,977
Gerardo	✓ Software malicioso que daña o roba información	721	2182	11,169
Gerardo F	✓ Software malicioso que daña o roba información	828	2928	14,873
IRVING	-	0	542	20
Julio	-	0	1217	20
Melissa	✓ Software malicioso que daña o roba información	773	2254	9,034
Semanta	✓ Software malicioso que daña o roba información	849	2939	14,028
Wilmer	-	0	740	20

Fundamentos de Ciberseguridad

9 Quiz	¿Qué medida mejora la seguridad de tus cuentas en línea?
Correct answers	Activar la verificación en dos pasos. (2FA)
Players correct (%)	76,92%.
Question duration	20 seconds.

Answer Summary

Answer options	▲ Usar la misma contraseña en todo	◆ Activar la verificación en dos pasos. (2FA)	● Compartir fotos reales con compañeros	■ Guardar contraseñas en papel	▼
Is answer correct?	✗	✓	✗	✗	
Number of answers received	1	10	0	1	
Average time taken to answer (seconds)	8,53	11,40	0,00	13,15	

Player Details

Player	Answer		Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓	Activar la verificación en dos pasos. (2FA)	765	3369	8,569
Alex	✓	Activar la verificación en dos pasos. (2FA)	630	3169	14,49
CRCC	✗	Guardar contraseñas en papel	0	0	13,145
Carmen	✗	Usar la misma contraseña en todo	0	1128	8,534
Cesar	✓	Activar la verificación en dos pasos. (2FA)	753	2958	9,651
Fabri	✓	Activar la verificación en dos pasos. (2FA)	667	3417	5,327
Gabriela	✓	Activar la verificación en dos pasos. (2FA)	620	2902	15,199
Gabriela F	✓	Activar la verificación en dos pasos. (2FA)	618	3044	7,279
IRVING	-		0	512	20
Julio	✓	Activar la verificación en dos pasos. (2FA)	632	1849	14,71
Melissa	✓	Activar la verificación en dos pasos. (2FA)	719	2870	11,224
Samanta	✓	Activar la verificación en dos pasos. (2FA)	774	3069	9,025
Wilmer	✓	Activar la verificación en dos pasos. (2FA)	543	1969	18,266

Fundamentos de Ciberseguridad

Quiz ¿Qué debes hacer si encuentras una memoria USB desconocida?

Correct answers	Entregarla al área de seguridad sin conectarla
Players correct (%)	92.31%
Question duration	20 seconds

Answer Summary

Answer options	Conectarla para ver su contenido	Usarla como almacenamiento personal	Compartirla con tus colegas	Entregarla al área de seguridad sin conectarla
Is answer correct?	✗	✗	✗	✓
Number of answers received	0	0	0	12
Average time taken to answer (seconds)	0.00	0.00	0.00	9.47

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓ Entregarla al área de seguridad sin conectarla	666	4174	5.373
Alex	✓ Entregarla al área de seguridad sin conectarla	770	4254	9.247
CRCC	✓ Entregarla al área de seguridad sin conectarla	666	666	12.541
Carmen	✓ Entregarla al área de seguridad sin conectarla	664	3112	12.655
Cesar	✓ Entregarla al área de seguridad sin conectarla	713	3004	11.462
Fabi	✓ Entregarla al área de seguridad sin conectarla	901	4018	3.975
Gianela	✓ Entregarla al área de seguridad sin conectarla	759	3561	9.622
Gianela F	✓ Entregarla al área de seguridad sin conectarla	844	4168	6.227
IRVING	-	0	542	20
Julio	✓ Entregarla al área de seguridad sin conectarla	703	3552	11.86
Melissa	✓ Entregarla al área de seguridad sin conectarla	740	3719	10.157
Samanta	✓ Entregarla al área de seguridad sin conectarla	816	3699	7.362
Wilmer	✓ Entregarla al área de seguridad sin conectarla	671	1954	13.158

Fundamentos de Ciberseguridad

7 Quiz ¿Qué tipo de ataque busca engañar al usuario usando sitios web falsos?

Correct answers	Phishing
Players correct (%)	76,92%
Question duration	20 seconds

Answer Summary

Answer options	▲ Sniffing	◆ Phishing	● Ransomware	■ Ingeniería inversa	⬟	▼
Is answer correct?	✗	✓	✗	✗		
Number of answers received	0	10	1	0		
Average time taken to answer (seconds)	0,00	6,09	15,04	0,00		

Player Details

Player	Answer		Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓	Phishing	805	4979	7,815
Alex	✓	Phishing	936	5190	2,564
CRCC	✓	Phishing	851	1537	5,951
Carmen	✓	Phishing	840	2952	6,387
Cesar	✓	Phishing	836	3840	6,556
Fabri	✓	Phishing	893	5711	4,274
Genesis	✓	Phishing	842	4403	6,318
Génesis F	✓	Phishing	796	5284	8,155
IRVING	-		0	542	20
Julio	✓	Phishing	836	3388	6,565
Melissa	✗	Ransomware	0	3719	15,038
Samanta	✓	Phishing	841	4740	6,363
Wilmer	-		0	1954	20

Fundamentos de Ciberseguridad

8 Quiz ¿Cuál es el objetivo de un ataque de ingeniería social?

Correct answers	Manipular a las personas para obtener acceso o información
Players correct (%)	61,54%
Question duration	20 seconds

Answer Summary

Answer options	▲ Manipular a las personas para obtener acceso o información	◆ Probar contraseñas con fuerza bruta	● Infectar computadoras con virus	■ Escanear puertos de red	⬟	▼
Is answer correct?	✓	✗	✗	✗		
Number of answers received	8	0	0	2		
Average time taken to answer (seconds)	10,13	0,00	0,00	13,03		

Player Details

Player	Answer		Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓	Manipular a las personas para obtener acceso o información	781	5760	8,753
Alex	✓	Manipular a las personas para obtener acceso o información	835	6025	6,581
CROC	✓	Manipular a las personas para obtener acceso o información	613	2150	15,49
Carmen	✓	Manipular a las personas para obtener acceso o información	624	3578	15,025
Cesar	✓	Manipular a las personas para obtener acceso o información	728	4668	10,895
Fabri	✓	Manipular a las personas para obtener acceso o información	808	6519	7,881
Genesis	✓	Manipular a las personas para obtener acceso o información	814	5217	7,428
Génesis F	✓	Manipular a las personas para obtener acceso o información	771	6055	9,174
IRVING	-		0	542	20
Julio	-		0	3388	20
Melissa	-		0	3719	20
Samanta	✗	Escanear puertos de red	0	4740	7,179
Wilmer	✗	Escanear puertos de red	0	1954	18,279

Quiz	¿Qué puedes hacer para evitar el espionaje visual ("shoulder surfing")?
Correct answers	Colocar un filtro de privacidad en tu monitor
Players correct (%)	84.62%
Question duration	20 seconds

Answer Summary

Answer options	Usar pantalla brillante	Colocar un filtro de privacidad en tu monitor	Sentarte de espaldas a la puerta	Compartir tu pantalla por videoconferencia
Is answer correct?	✗	✓	✗	✗
Number of answers received	1	11	0	0
Average time taken to answer (seconds)	14.94	11.78	0.00	0.00

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✗ Usar pantalla brillante	0	5760	14,943
Alex	✓ Colocar un filtro de privacidad en tu monitor	535	6820	16,204
CROC	✓ Colocar un filtro de privacidad en tu monitor	843	2893	8,269
Carmen	✓ Colocar un filtro de privacidad en tu monitor	708	4284	11,875
Cesar	✓ Colocar un filtro de privacidad en tu monitor	711	5279	11,543
Fabri	✓ Colocar un filtro de privacidad en tu monitor	880	7339	4,733
Genesis	✓ Colocar un filtro de privacidad en tu monitor	564	5781	17,423
GénesisF	✓ Colocar un filtro de privacidad en tu monitor	797	6852	8,116
IRVING	-	0	542	20
Julio	✓ Colocar un filtro de privacidad en tu monitor	863	4051	13,492
Melissa	✓ Colocar un filtro de privacidad en tu monitor	857	4378	13,727
Samanta	✓ Colocar un filtro de privacidad en tu monitor	702	5442	11,931
Wilmer	✓ Colocar un filtro de privacidad en tu monitor	840	2594	14,397

Fundamentos de Ciberseguridad

10 ¿Cuál de estos elementos NO es parte de una buena práctica en ciberseguridad?

Correct answers	Dejar la sesión abierta al irte
Players correct (%)	69,23%
Question duration	20 seconds

Answer Summary

Answer options	Actualizar el software	Dejar la sesión abierta al irte	Usar contraseñas robustas	Bloquear la pantalla al ausentarte
Is answer correct?	✗	✓	✗	✗
Number of answers received	0	9	0	3
Average time taken to answer (seconds)	0,00	10,24	0,00	15,40

Player Details

Player	Answer	Score (points)	Current Total Score (points)	Answer time (seconds)
Ab	✓ Dejar la sesión abierta al irte	737	8557	8,103
Alex	✓ Dejar la sesión abierta al irte	708	7418	8,173
DNCC	✗ Bloquear la pantalla al ausentarte	0	2933	15,221
Carmen	✓ Dejar la sesión abierta al irte	529	4923	16,016
Cesar	✗ Bloquear la pantalla al ausentarte	0	5279	12,694
Fabi	✓ Dejar la sesión abierta al irte	737	8136	8,105
Gerardo	✓ Dejar la sesión abierta al irte	779	6560	8,256
Gerardo F	✓ Dejar la sesión abierta al irte	740	7502	10,394
INMG	-	0	542	20
Julio	✗ Bloquear la pantalla al ausentarte	0	4051	18,085
Melissa	✓ Dejar la sesión abierta al irte	874	5250	5,038
Samanta	✓ Dejar la sesión abierta al irte	751	6193	9,983
Wilmer	✓ Dejar la sesión abierta al irte	565	3159	17,418

Glosario

Ciberseguridad = Prácticas, procesos y controles para la protección de sistemas informáticos

Backup = Copia de seguridad o respaldo de datos, programas o archivos en un medio separado

BlackCat = Un tipo de ransomware que ataca principalmente a organizaciones

Conti = Operación de ransomware que realiza ataques agresivos

Endpoint security = Estrategia de ciberseguridad para proteger dispositivos

Firewall = Sistema de seguridad que protege una red privada de redes externas

Fortinet = Plataforma unificada de empresa líder en ciberseguridad

Hive = Un tipo de ransomware de cifrado sofisticado

Inforfish = Software para control perteneciente a la industria pesquera

Ingeniería social = Modalidad de manipulación psicológica empelada para obtener datos confidenciales

Kaspersky = Empresa global de ciberseguridad

LockBit = Tipo de ataque que cifra archivos en ordenadores

Malvertising = Tipo de ciberataque que utiliza publicidad en línea infectada para distribuir programa malicioso

Malware = Cualquier programa o código diseñado para dañar sistemas, robar datos e interrumpir operaciones

NAS = dDspositivo de almacenamiento centralizado conectado a una red

NIST = Instituto Nacional de Estándares y Tecnología de Estados Unidos

MFA = Autenticación Multifactor, método de seguridad que pide varias credenciales

Phishing = Estafa cibernética mediante correos, llamadas o mensajes que usa la identidad de bancos, empresas entre otros.

PoE (Power over Ethernet) = Tecnología que permite enviar datos y energía eléctrica simultáneamente a través de un único cable Ethernet

Qbiz = Software de gestión empresarial utilizado para digitalizar y optimizar procesos

Ransomware = Tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta

Software = conjunto de instrucciones, programas y datos que le dicen a un dispositivo electrónico qué hacer y cómo hacerlo

Troyano AIDS = Software malicioso que se "disfraza" para ocultar sus verdaderas intenciones