Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN UNA PYME ENFOCADO EN LA PROTECCIÓN DE ACTIVOS CRÍTICOS Y CUMPLIMIENTO DE LA NORMA ISO/IEC 27001

Proyecto de Titulación

Previo a la obtención del Título de:

Magíster en Seguridad Informática

Presentado por:

Ricardo Lenin Caicedo Rodriguez

Hebilly Liliana Trujillo Miranda

Guayaquil-Ecuador

Año: 2025

AGRADECIMIENTO

A mi familia, por ser mi mayor apoyo y fuente inagotable de inspiración. A mi madre, por su amor y enseñanzas; a mis hermanas, por su constante respaldo; y a mis hijas, mi mayor motivación, por darme la fuerza para seguir adelante.

A la universidad y a mis profesores, por su dedicación y guía en este proceso de aprendizaje.

A todos los que de alguna manera contribuyeron a este logro, mi más sincero agradecimiento.

Ing. Ricardo Caicedo

Quiero agradecer profundamente a nuestro Creador, por darme la oportunidad de adquirir nuevos conocimientos y, al mismo tiempo, poder compartirlos.

A mis padres, por su amor incondicional, por su tiempo y esfuerzo que siempre me han brindado para apoyarme en cada paso de este camino.

A mi pequeña hija, mi gran bendición, quien con su presencia me inspira cada día a ser mejor.

A los tutores de este postgrado, que generosamente compartieron con nosotros sus valiosos conocimientos.

Y a todos aquellos que estuvieron a mi lado, motivándome y brindándome su apoyo en todo momento.

LSi. Liliana Trujillo

DEDICATORIA

A mis hijas, por ser mi razón de seguir adelante, mi mayor motivación y el motor de mis sueños.

A mi madre, por su amor incondicional, su esfuerzo y sus enseñanzas, que han sido la base de mi crecimiento.

A mis hermanas, por su apoyo inquebrantable y por estar siempre a mi lado en cada desafío.

Este logro es para ustedes, con todo mi amor y gratitud

Ing. Ricardo Caicedo

Dedico esta tesis a mis padres, que con su ejemplo de esfuerzo y dedicación me enseñaron a nunca rendirme, y a mi querida hija, cuyo amor y comprensión me impulsaron a seguir adelante,
gracias por estar siempre a mi lado, por su confianza y por ser mi mayor fuente de inspiración.

A mi colega y amiga, que no solo has sido una fuente de conocimiento,
sino también un apoyo constante en cada paso de este proyecto.

A todas aquellas personas que, como yo, se sienten motivadas por el deseo de aprender y avanzar en el mundo de las tecnologías en especial en la seguridad de la información.

LSi. Liliana Trujillo

.

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

MSc. Lenin Eduardo Freire Cobo

Tutor

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

MSc. Juan Carlos García Plúa

Revisor

DECLARACIÓN EXPRESA

Nosotros Ricardo Lenin Caicedo Rodriguez y Hebilly Liliana Trujillo Miranda acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique a los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 24 de agosto del 2025.

Firmado electrónicamente por:
RICARDO LENIN
CAICEDO RODRIGUEZ
Validar únicamente con FirmaEC

Ing. Ricardo Lenin Caicedo Rodriguez

Hebilly Liliana
Trujillo Miranda
Time Stamping
Security Data

LSi. Hebilly Liliana Trujillo Miranda

RESUMEN

· El presente documento detalla el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para una Pequeña y Mediana Empresa (PYME) dedicada a la venta de maquinaria, que opera con una infraestructura tecnológica predominantemente "on-premise". El objetivo principal es proteger sus activos críticos y asegurar el cumplimiento con la norma ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador.

El análisis de la postura actual de seguridad (línea base) reveló deficiencias significativas. Se identificó una falta de capacitación formal y concienciación del personal, lo que se traduce en una baja adherencia a las políticas de seguridad existentes. A pesar de la preferencia por la infraestructura local para un control percibido, las prácticas de seguridad para activos críticos como el servidor de bases de datos, el sistema ERP, los datos sensibles y el correo electrónico carecen de políticas formales alineadas con ISO 27001 y de documentación exhaustiva. La gestión de incidentes, aunque presente, opera sin procedimientos formalizados, indicando una postura más reactiva que proactiva.

Se identificaron y evaluaron riesgos asociados a estos activos críticos, destacando la alta probabilidad de ciberataques (malware, ransomware, phishing) y errores humanos, con un impacto potencial alto en las operaciones y la reputación de la empresa.

El SGSI propuesto aborda estas vulnerabilidades mediante un marco estructurado que incluye siete políticas clave: Control de Acceso, Gestión de

Contraseñas, Seguridad del Correo Electrónico, Respaldo y Recuperación, Clasificación y Manejo de la Información, Concienciación y Capacitación, y Gestión de Incidentes de Seguridad. Estas políticas se alinean con ISO/IEC 27001 y LOPDP, y se complementan con controles específicos (preventivos, de detección y de respuesta) diseñados para mitigar los riesgos identificados en cada activo crítico.

La validación empírica del diseño se realizó a través de un caso piloto enfocado en la seguridad del correo electrónico. Este piloto demostró una reducción de más del 80% en la exposición al phishing y la detección temprana de ataques de fuerza bruta, lo que evitó intrusiones mayores. El piloto también confirmó la importancia crítica de la concienciación del usuario y la necesidad de estrategias de respaldo integrales.

En conclusión, el proyecto representa una transformación holística de la postura de seguridad de la PYME, pasando de un estado fragmentado y reactivo a un sistema estructurado, proactivo y en constante evolución. La implementación de este SGSI integral es un imperativo estratégico para la continuidad del negocio, la protección de activos críticos y el mantenimiento de la confianza de clientes y socios en el complejo panorama digital actual.

Se recomienda a la alta dirección formalizar la adopción del SGSI, asignar recursos dedicados, considerar la evolución hacia un modelo de nube híbrida para mejorar la resiliencia, implementar sistemáticamente todas las políticas y controles priorizando los riesgos de alto impacto, establecer programas de capacitación continua, formalizar la gestión de incidentes, y realizar auditorías periódicas para asegurar el cumplimiento continuo con ISO 27001 y LOPDP

ÍNDICE GENERAL

Contenido

ABREVIATURAS Y SÍMBOLOS

AES: Advanced Encryption Standard (páginas 26, 50)

BCP: Plan de Continuidad del Negocio (página 28)

CIA: Confidencialidad, Integridad y Disponibilidad (página 13)

CSF: Marco de Seguridad Cibernética (páginas 14, 16)

DKIM: DomainKeys Identified Mail (páginas 28, 49)

DMARC: Domain-based Message Authentication, Reporting & Conformance (páginas 28, 49)

DRP: Plan de Recuperación ante Desastres (páginas 26, 42, 45)

ERP: Enterprise Resource Planning (páginas ix, xix, 1, 8, 10, 13, 16, 22, 25, 28, 33, 49, 61)

IDS: Sistemas de Detección de Intrusos (páginas 2, 26, 61)

IDS/IPS: Sistemas de Detección y Prevención de Intrusos (páginas 26, 61)

IPS: Sistema de Prevención de Intrusiones (páginas 2, 26, 61)

ISMS: Information Security Management System (páginas 9, 20)

ISO/IEC: Organización Internacional de Normalización / Comisión Electrotécnica Internacional (páginas ix, xix, 1, 4, 7, 8, 9, 10, 20, 27, 28)

LODP: Ley Orgánica de Protección de Datos Personales (páginas ix, 10, 11, 20, 22, 28, 50, 61)

LOPD: Ley Orgánica de Protección de Datos Personales (página 43, 50)

MFA: Autenticación Multifactor (páginas 26, 28, 48, 49, 61)

NIST: Instituto Nacional de Estándares y Tecnología (página 14, 16)

OTRI: Oficina de Transferencia de Resultados de Investigación (página vii)

PDCA: Planificar-Hacer-Verificar-Actuar (página 17, 50)

PYME: Pequeña y Mediana Empresa (páginas ix, xix, 1, 7, 10, 13, 20, 22, 25, 28, 43, 61)

RBAC: Control de Acceso Basado en Roles (páginas 2, 28, 61)

SGSI: Sistema de Gestión de Seguridad de la Información (páginas ix, xix, 1, 4, 7, 8, 9, 10, 20, 27, 28, 43, 60)

SoD: Segregación de Funciones (páginas 2, 26, 61)

SPF: Sender Policy Framework (páginas 28, 49)

TLS: Transport Layer Security (páginas 26, 50)

UPS: Uninterruptible Power Supply (página 28)

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de titulación se centra en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) en una PYME, específicamente enfocado en la protección de activos críticos y el cumplimiento de la norma ISO/IEC 27001. La creciente dependencia de las tecnologías de la información en el ámbito empresarial, junto con el manejo de datos sensibles, ha convertido a la seguridad de la información en un elemento crucial para garantizar la continuidad operativa y la confianza de los clientes. En el contexto de esta PYME, que opta por mantener una infraestructura tecnológica "on-premise", se evidencian riesgos inherentes derivados de la falta de controles robustos que aseguren la integridad, confidencialidad y disponibilidad de la información.

Este estudio surge ante la necesidad de enfrentar incidentes que puedan comprometer la seguridad de los sistemas críticos, tales como el ERP, el servicio de correo electrónico y la administración de bases de datos, los cuales son vitales para las operaciones diarias de la empresa. Además, el diseño propuesto busca establecer un marco preventivo que permita mitigar los riesgos y cumplir con los estándares internacionales de seguridad informática, tal como lo requiere la norma ISO/IEC 27001, aportando así una respuesta integral a las amenazas emergentes en el entorno digital.

La importancia de este proyecto radica en su capacidad para proporcionar a la empresa una estrategia de seguridad estructurada y sostenible, que no solo resguarde sus activos críticos, sino que también contribuya a cumplir con las normativas legales vigentes en materia de protección de datos. A través de un análisis

detallado de la infraestructura y una evaluación de riesgos, se establecerán las bases para un SGSI que, en su fase de diseño, permita sentar las pautas necesarias para una implementación futura que fortalezca la resiliencia de la organización.

CAPITULO 1: GENERALIDADES

1.1 ANTECEDENTES

La creciente preocupación por la seguridad de la información en el sector empresarial, especialmente en las PYMEs que gestionan su infraestructura de manera interna ("on-premise"). En los últimos años, se ha evidenciado un aumento en los incidentes de seguridad y ataques cibernéticos en América Latina, donde muchas empresas han enfrentado brechas que comprometen la integridad y confidencialidad de sus datos. Este escenario, sumado a la necesidad de cumplir con normativas internacionales y locales, como la norma ISO/IEC 27001[1] y la legislación en protección de datos, ha impulsado a las organizaciones a adoptar estrategias de gestión de riesgos que protejan sus activos críticos. Estas tendencias han generado un contexto en el que resulta imperativo diseñar un SGSI robusto que sirva de base para salvaguardar la información y garantizar la continuidad operativa.

1.2 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) en una PYME, con una infraestructura tecnológica "on-premise", para garantizar la protección de la información crítica.

1.3 OBJETIVOS ESPECÍFICOS

- Identificar los sistemas y activos críticos de información en un ambiente local.
- Evaluar los riesgos asociados a sus sistemas críticos, como el correo electrónico, ERP y bases de datos.

- Diseñar controles de seguridad basados en la norma ISO/IEC 27001, garantizando el cumplimiento de los estándares internacionales de seguridad informática.

1.4 DESCRIPCIÓN DEL PROBLEMA

Esta PYME (Pequeña y mediana empresa) dedicada a la venta de maquinaria en el sector industrial y comercial a nivel país, ha optado por mantener su infraestructura tecnológica en sus instalaciones, lo que le permite un control directo sobre sus transacciones y datos. Sin embargo, esta decisión conlleva una serie de riesgos inherentes a la seguridad de la información. [2, pp. 1535–1549]

La vulnerabilidad de los datos se ha convertido en una preocupación crítica para la organización. A medida que la cantidad de información sensible y transacciones aumenta, el riesgo de sufrir ataques cibernéticos y brechas de seguridad se intensifica. Este riesgo es particularmente alarmante, ya que cualquier incidente podría no solo comprometer la integridad de los datos, sino también resultar en la pérdida de confianza de los clientes y, en consecuencia, en una disminución de la base de clientes.

La posibilidad de perder clientes es un factor que no puede ser subestimado. La reputación de la empresa, construida a lo largo de los años, puede verse gravemente afectada por un incidente de seguridad. La pérdida de datos podría llevar a sanciones legales, daños financieros significativos y un aumento en los costos operativos para remediar cualquier falla de seguridad. Además, el tiempo y los recursos necesarios para recuperar la confianza de los clientes podrían ser

desproporcionados en comparación con los esfuerzos que se podrían invertir en una estrategia de seguridad preventiva.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es importante para mitigar riesgos y proteger sus activos de información críticos. Casi un tercio de las organizaciones en Latinoamérica enfrentaron al menos un incidente de seguridad.[3, p. 3]

La dependencia de tecnologías como el correo electrónico y el ERP en una infraestructura "on premise" aumenta la exposición a amenazas cibernéticas y fallos operativos. La norma ISO/IEC subraya la importancia de una gestión efectiva de la seguridad para implementar controles basados en riesgos, previniendo accesos no autorizados y pérdidas de datos[4]. Un SGSI diseñado conforme a este estándar permitirá a la empresa identificar y gestionar amenazas de forma efectiva, fortaleciendo su resiliencia.

Además, el cumplimiento con la Ley Orgánica de Protección de Datos Personales de Ecuador [5] es necesario, ya que exige medidas para proteger los datos de clientes y empleados, garantizando la confidencialidad y evitando sanciones legales, lo que refuerza la confianza de los clientes y socios.

La viabilidad del proyecto se fundamenta en las actividades diarias de la institución, lo que facilita la identificación de áreas de mejora. El enfoque se limitará a la fase de diseño, evitando la implementación inmediata, y se contempla un plazo de tres meses para el estudio y la elaboración de propuestas bien fundamentadas. Se

considerarán las autorizaciones necesarias para garantizar el cumplimiento de normativas internas, y se establecerán medidas para proteger el nombre de la institución. Así, se sientan las bases para un desarrollo exitoso que se alinee con las expectativas institucionales y de los beneficiarios.

CAPÍTULO 2: MARCO TEÓRICO

2.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y BENEFICIOS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

En esta sección se abordan las políticas de seguridad de la información y los beneficios asociados a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Las políticas de seguridad se definen como el conjunto de directrices formales que orientan el manejo seguro de los datos, fundamentadas en los principios de confidencialidad, integridad y disponibilidad, esenciales para salvaguardar los activos críticos de la organización. Estas directrices se elaboran conforme a estándares internacionales, como se establece en la norma ISO/IEC 27001:2016, y se complementan con el marco de la ISO/IEC 27001:2017, lo que permite identificar, evaluar y mitigar riesgos de manera sistemática. La correcta aplicación de un SGSI basado en estas políticas no solo mejora la resiliencia y la eficiencia operativa, sino que también refuerza el cumplimiento normativo y fortalece la confianza de clientes y socios.

2.1.1 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se entienden como un conjunto de directrices establecidas para garantizar la protección de los datos, gestionadas por una persona encargada de asegurar su cumplimiento y correcta implementación frente a cualquier incidente.

Al definir las políticas de seguridad [6] en una organización, es importante considerar los siguientes aspectos:

- El alcance, los recursos, las instalaciones y los procesos de la organización que estarán sujetos a la aplicación de las políticas.
- Las metas y prioridades en cuanto a la protección de la información.
- El apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- La clasificación de los datos y la identificación de los activos que requieren protección.
- La evaluación y gestión de los riesgos asociados.
- Los componentes y personas clave involucradas en la implementación de las medidas de seguridad.
- La asignación de responsabilidades en distintos niveles dentro de la estructura organizacional.
- La definición clara de los comportamientos aceptables y no permitidos para el personal.
- La identificación de las medidas, normativas y procedimientos necesarios para garantizar la seguridad.
- La gestión de las interacciones con terceros, como clientes y proveedores.
- La gestión y respuesta ante incidentes relacionados con la seguridad.
- La existencia de planes de contingencia y estrategias para asegurar la continuidad del negocio.
- El cumplimiento con las leyes y regulaciones aplicables.
- La definición de infracciones a las políticas de seguridad y las sanciones asociadas al incumplimiento.

2.1.2 PRINCIPIOS DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Estos tres principios son esenciales para proteger la información en cualquier organización y formar así la base de una buena gestión de seguridad de la información.

- Confidencialidad: Asegura que solo las personas autorizadas puedan acceder a la información.
- Integridad: Garantiza que los datos sean precisos y no sean alterados sin autorización.
- Disponibilidad: Asegura que la información esté disponible y accesible cuando se necesite.

Ilustración 1. Modelo de Seguridad Informática. La triada CIA [7]

Tanto el software, la base de datos como el correo electrónico, ante la creciente tecnologías presentan amenazas de seguridad, donde no solo los profesionales de TI [8] sino también los que no lo son deben comprender la concienciación sobre seguridad de la información.

2.1.3 BENEFICIOS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Implementar un Sistema de Gestión de Seguridad de la Información [9] (SGSI) proporciona a las empresas una sólida protección frente a diversas amenazas relacionadas con la seguridad de la información.

Dentro del SGSI, la gestión de riesgos juega un papel crucial, ya que implica identificar, evaluar y tomar medidas para mitigar los riesgos hasta un nivel aceptable. Este proceso de evaluación permite detectar riesgos y vulnerabilidades potenciales en relación con la confidencialidad, integridad y disponibilidad de la información.

Además, ayuda a la organización a establecer controles adecuados para gestionar los riesgos en el personal, los procesos y la tecnología, reduciendo de esta manera las posibles pérdidas financieras y el impacto de un desastre o incidente.

Asimismo, mejora la gobernanza de la seguridad de la información y fomenta una mayor conciencia sobre la seguridad en todos los niveles de la organización.

Beneficios	Descripción
Protección contra amenazas	Brindar seguridad frente a diversas amenazas relacionadas con la información.
Gestión de riesgos efectiva	Facilitar la identificación, evaluación y mitigación de riesgos a un nivel aceptable.

Identificación de riesgos y vulnerabilidades	Detectar posibles riesgos y vulnerabilidades en las áreas de confidencialidad, integridad y disponibilidad.
Mejora en el control de riesgos	Ayudar a establecer controles adecuados para gestionar los riesgos en personas, procesos y tecnología.
Reducción de pérdidas financieras	Minimiza el impacto económico durante incidentes o desastres.
Mejor gestión de la gobernanza de seguridad de la información	Fortalece la gestión y supervisión de la seguridad dentro de la organización.
Mayor conciencia sobre seguridad de la información	Incrementa la sensibilización sobre la importancia de la seguridad en todos los niveles de la organización.

Tabla 1 Beneficios de un sistema de Gestión de Seguridad de la Información.

2.2 NORMATIVA ISO/IEC 27001.

La mayoría de las empresas cuentan con información valiosa o confidencial, y no garantizar su adecuada protección puede generar consecuencias graves en términos operativos, financieros y legales.

En algunos casos, incluso podría llevar a la quiebra de la empresa. El desafío principal para muchas organizaciones es cómo proporcionar una protección adecuada. Específicamente, deben preguntarse cómo pueden identificar todos los riesgos a los que están expuestas y gestionarlos de manera proporcional, sostenible y rentable.

La norma ISO 27001, reconocida a nivel internacional, establece un marco robusto para los Sistemas de Gestión de Seguridad de la Información (SGSI), adaptable a cualquier tipo y tamaño de organización.

Las empresas con alto riesgo en cuanto a la seguridad de la información están cada vez más optando por implementar un SGSI conforme a esta norma.

2.2.1 CONTROL PARA ACTIVOS DE LA INFORMACIÓN (ANEXO A)

El Anexo A de la norma ISO 27001 juega un papel crucial en la gestión de la seguridad de la información, ya que ofrece una serie de controles específicos para salvaguardar la información.

Este anexo está compuesto por 14 dominios que abarcan un total de 114 controles, los cuales son fundamentales para construir el marco ISMS (Sistema de Gestión de Seguridad de la Información). Estos controles se utilizan como objetivos de seguridad para proteger la información, especialmente en entornos como los centros de datos.

Dentro de este marco, se identifican cuatro categorías principales que cubren todos los aspectos clave del centro de datos, donde se debe aplicar el control SGSI en cada una de ellas.

- Estas categorías son:

- Recursos Humanos
- Organización
- Políticas
- Procedimientos
- Hardware
- Software.

Los recursos humanos y la organización se centran en las personas, mientras que las políticas y procedimientos abordan los procesos. Por último, el hardware y el software representan los componentes tecnológicos esenciales para la seguridad de la información.

2.3 NORMATIVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LODP).

Vivimos en una época de grandes avances tecnológicos y científicos, donde la "sociedad de la información y la comunicación" nos permite recopilar, almacenar, conectar y compartir todo tipo de datos sobre las personas y las cosas.

Tanto las empresas privadas como las instituciones públicas están interesadas en obtener y usar esta información gracias a las nuevas tecnologías. Con estos datos, se pueden conocer muchos aspectos de la vida de las personas, lo cual puede ser útil para ellas, pero también puede tener efectos negativos si no se maneja de forma adecuada.

En Ecuador, existe una ley específica para proteger los datos personales de los ciudadanos, que es la Ley Orgánica de Protección de Datos Personales (LOPDP) aprobada en 2021 [10]. Esta ley establece un marco legal para garantizar que la información personal de los clientes, proveedores y empleados sea tratada de manera responsable y segura. Su objetivo es proteger los derechos de las personas frente al uso indebido de sus datos, asegurando que las empresas y organizaciones cuiden la privacidad y no utilicen la información personal sin el consentimiento explícito de las personas.

La ley también otorga a los ciudadanos el derecho a acceder, corregir, eliminar y oponerse al tratamiento de sus datos, lo que les permite tener mayor control sobre su información personal. Además, establece sanciones para las entidades que no cumplan con estas normas, buscando así evitar que se produzcan daños o abusos relacionados con la gestión de datos personales.

De esta manera, la legislación en Ecuador busca equilibrar el uso de la tecnología para el progreso, sin descuidar la protección de los derechos y la privacidad de las personas.

2.3.1 OBJETIVOS DE LA LODP

La Ley Orgánica de Protección de Datos Personales de Ecuador busca equilibrar el uso de los datos personales para fines legítimos y el respeto a la privacidad de los ciudadanos, creando un entorno más seguro y transparente en el manejo de la información personal.

Los objetivos principales de la Ley Orgánica de Protección de Datos Personales de Ecuador [5] son los siguientes:

Proteger los derechos fundamentales de las personas: La ley busca salvaguardar la privacidad de los ciudadanos y garantizar que sus datos personales no sean utilizados de manera indebida, sin su consentimiento o sin los controles adecuados.

Regular el tratamiento de datos personales: Establece normas claras sobre cómo las entidades públicas y privadas deben recolectar, almacenar, procesar, y compartir la información personal, asegurando que el uso de estos datos sea transparente y legal.

Garantizar el consentimiento informado: La ley exige que las personas den su consentimiento expreso antes de que sus datos personales sean recogidos o utilizados, asegurando que los individuos comprendan qué datos se están recopilando y para qué fines.

Facilitar el acceso y control sobre los datos: Otorga a los ciudadanos el derecho de acceder, corregir, eliminar o actualizar sus datos personales, lo que les permite tener un control directo sobre su información y proteger su privacidad.

Promover la transparencia y la rendición de cuentas: Las organizaciones que manejen datos personales deben ser transparentes sobre cómo los gestionan y deben responder ante las autoridades si se producen violaciones de la ley.

Fomentar la seguridad en el tratamiento de datos: Establece la obligación de implementar medidas de seguridad adecuadas para proteger los datos personales frente a posibles accesos no autorizados, alteraciones, pérdidas o divulgación indebida.

Garantizar la libre circulación de datos dentro del marco legal: La ley permite que los datos personales puedan ser transferidos entre diferentes sectores y países, siempre y cuando se cumpla con los principios de protección de datos establecidos por la normativa.

Sancionar las infracciones: Establece un sistema de sanciones para aquellos que incumplan las normas, con el fin de asegurar que las organizaciones respeten los derechos de las personas y actúen de manera responsable con la información personal que manejan.

2.3.2 RECOMENDACIONES (PASOS PARA CUMPLIR LA LEY DE PROTECCIÓN DE DATOS)

1. **Asegúrese de tratar los datos personales de manera legal, leal y transparente**: Garantice que el procesamiento de datos siempre sea conforme a la ley, sin engañar ni ocultar información al interesado.

2. **Recoja los datos para fines específicos y legítimos**: Evite recopilar información de manera indiscriminada. Los fines de uso deben ser claros, legítimos y no deben modificarse sin justificación. Si se usan los datos para investigación científica, histórica o estadística, asegúrese de que esta finalidad esté claramente especificada.
3. **Limite la cantidad de datos recogidos**: Recopile solo los datos necesarios para los fines establecidos. No acumule información innecesaria o irrelevante.
4. **Mantenga los datos actualizados y exactos**: Realice esfuerzos para garantizar que los datos personales sean precisos. Si detecta errores, corríjalos o elimínelos lo antes posible.
5. **Conserve los datos solo por el tiempo necesario**: No guarde los datos más tiempo del necesario. Si se requieren para fines específicos (como investigación o archivo público), asegúrese de contar con las medidas necesarias para proteger la privacidad de los interesados.
6. **Proteja los datos personales adecuadamente**: Implemente medidas de seguridad técnicas y organizativas para evitar el acceso no autorizado, pérdida o destrucción accidental de los datos personales.

Se trata de principios fundamentados en el Reglamento General de Protección de Datos. [11]

2.4 PROTECCIÓN DE ACTIVOS CRÍTICOS.

2.4.1 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

La protección de activos críticos es un proceso fundamental para garantizar la continuidad operativa y la resiliencia de una organización frente a amenazas de diversa índole [12]. Esta sección describe la forma de abordar dicha protección, desde

la identificación de activos hasta la implementación y el monitoreo de controles, siguiendo los lineamientos del Marco de Seguridad Cibernética (CSF) del NIST y otras buenas prácticas internacionales.

La importancia de identificación de activos de información permite a las organizaciones reconocer de manera efectiva sus recursos y su relación con los distintos procesos internos. Se consideran activos operativamente relevantes aquellos indispensables para cumplir con los objetivos estratégicos, lo que facilita su categorización y gestión.

2.4.2 CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS CRÍTICOS

Una vez identificados, los activos críticos deben ser clasificados de acuerdo con su relevancia para la organización y el impacto que podría tener su indisponibilidad, alteración o divulgación no autorizada. El Marco de Seguridad Cibernética (CSF) del NIST (2024) recomienda la aplicación de categorías basadas en los requisitos de confidencialidad, integridad y disponibilidad, así como en la criticidad para los procesos de negocio.

- Confidencialidad: Evalúa el nivel de sensibilidad de la información y los daños que produciría su divulgación.

- Integridad: Considera la exactitud y completitud de los datos, así como las repercusiones de su modificación no autorizada.

- Disponibilidad: Determina la necesidad de acceso oportuno a los activos y el costo que representaría su indisponibilidad.

La clasificación debe reflejar los objetivos estratégicos y operativos de la empresa, así como el apetito y la tolerancia al riesgo definidos por la alta gerencia. Esta visión integral permite priorizar la asignación de recursos y la selección de controles de seguridad.

2.4.3 EVALUACIÓN DE RIESGOS Y SELECCIÓN DE CONTROLES

Tras la clasificación, se realiza una evaluación de riesgos para cada activo. Según el CSF del NIST (2024), es recomendable:

1. Identificar y analizar las amenazas internas y externas que puedan afectar la continuidad y seguridad de los activos.

2. Determinar vulnerabilidades existentes en la infraestructura, los procesos y el factor humano.

3. Estimar la probabilidad e impacto de un incidente de seguridad, considerando aspectos financieros, legales y de reputación.

4. Seleccionar los controles basados en el riesgo y priorizar aquellos que ofrezcan un mayor retorno de la inversión en protección.

Entre los controles típicos se incluyen la autenticación multifactor, la segmentación de redes, el cifrado de datos, los sistemas de detección y prevención de intrusiones, así como la implementación de políticas y procedimientos de seguridad. El uso de referencias informativas del NIST —por ejemplo, la vinculación de Subcategorías del CSF con estándares o normativas específicas— facilita la adopción de buenas prácticas reconocidas internacionalmente.

2.4.4 IMPLEMENTACIÓN Y MONITOREO DE LA PROTECCIÓN DE ACTIVOS

Una vez definidos los controles, se procede a su implementación y posterior monitoreo continuo para asegurar su eficacia. El Marco de Seguridad Cibernética (CSF) del NIST propone las siguientes acciones clave:

1. Planificación e Integración: Alinear los controles con los procesos de negocio y la estrategia de riesgos de la organización, garantizando que los responsables de cada área conozcan sus funciones y alcances.

2. Capacitación y Concienciación: Proveer formación regular al personal sobre los procedimientos de seguridad, el uso seguro de la tecnología y la importancia de los activos críticos para la continuidad operativa.

3. Monitoreo de Indicadores: Establecer indicadores de desempeño y riesgo que permitan detectar anomalías o eventos adversos en tiempo real. El registro de incidentes y la correlación de eventos (logs) facilitan la detección temprana de amenazas.

4. Revisión y Mejora Continua: Ajustar los controles según los cambios en el entorno de amenazas, la adopción de nuevas tecnologías o la aparición de brechas de seguridad identificadas en auditorías e incidentes previos.

Este enfoque cíclico de planificar–hacer–verificar–actuar (PDCA) asegura que la organización se mantenga en un proceso de mejora constante, alineado con las mejores prácticas de seguridad y con la gestión de riesgos a nivel empresarial.

2.5 TÉCNICAS DE EVALUACIÓN DE RIESGOS

La evaluación de riesgos es un proceso fundamental en la gestión de la seguridad de la información, ya que permite identificar, analizar y priorizar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los activos críticos de la organización. Este proceso, reconocido en normativas como la ISO/IEC 27001 y desarrollado en detalle en la ISO/IEC 27005, se puede abordar mediante diversas técnicas que permiten una comprensión holística de las amenazas, vulnerabilidades y los impactos potenciales. A continuación, se profundiza en tres enfoques principales utilizados en la evaluación de riesgos.

2.5.1 ENFOQUE CUALITATIVO

El enfoque cualitativo se basa en la identificación y descripción de riesgos utilizando escalas de probabilidad e impacto definidas mediante categorías (por ejemplo, alto, medio y bajo). Este método se apoya en el juicio de expertos, entrevistas, talleres y cuestionarios, permitiendo evaluar de manera subjetiva el riesgo sin requerir datos numéricos precisos. Su principal ventaja es la rapidez en la identificación de riesgos y la facilidad para adaptarlo a contextos específicos, facilitando la comunicación entre las partes interesadas. Esta técnica es útil para organizaciones que no disponen de información cuantitativa detallada, pero que requieren establecer prioridades de mitigación de manera inmediata.

2.5.2 ENFOQUE CUANTITATIVO

El enfoque cuantitativo utiliza datos numéricos y modelos matemáticos para calcular la probabilidad y el impacto de los riesgos, permitiendo una estimación precisa en términos financieros y operativos. Herramientas estadísticas, análisis de

escenarios y simulaciones son comunes en este método. Aunque requiere de información histórica y recursos analíticos, este enfoque facilita la comparación objetiva de riesgos y la asignación de recursos de manera eficiente, lo que resulta fundamental para grandes organizaciones o entornos con alta complejidad tecnológica.

2.5.3 ENFOQUE SEMI-CUANTITATIVO

El enfoque semicuantitativo combina elementos de los métodos cualitativo y cuantitativo asignando valores numéricos a escalas cualitativas predefinidas. Esta técnica permite elaborar una matriz de riesgo en la que se asigna un puntaje global a cada riesgo, integrando la percepción de los expertos con datos cuantificables. De esta forma, se obtiene un equilibrio entre la subjetividad del análisis cualitativo y la precisión del análisis cuantitativo, facilitando la priorización de riesgos y la toma de decisiones en cuanto a la implementación de controles.

En conjunto, estas técnicas permiten a la organización realizar una evaluación de riesgos integral, adaptando el proceso a sus necesidades y recursos, y asegurando la selección de controles que mitiguen eficazmente los riesgos identificados.[13]

CAPÍTULO 3: IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

La identificación de activos críticos es un proceso clave para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo. Este capítulo está orientado a reconocer y clasificar los recursos esenciales que soportan los procesos operativos y estratégicos de la empresa, con énfasis en aquellos con un alto nivel de riesgo, como el sistema ERP, las bases de datos y el correo electrónico.

3.1 LÍNEA BASE

Estableceremos una línea base sobre la situación actual de la seguridad de la información.

3.1.1 DE LA ENCUESTA

La encuesta se diseñó para evaluar al personal en relación con su comprensión de los procesos internos y de seguridad de la información. Consta de 12 preguntas distribuidas en las siguientes secciones:

- Información general (2 preguntas).
- Conocimiento y Uso de Políticas y Procedimientos de Seguridad (3 preguntas).
- Evaluación de Controles y Procedimientos. (4 preguntas).
- Gestión de Riesgos y Cumplimiento de la Norma ISO 27001 (3 preguntas).

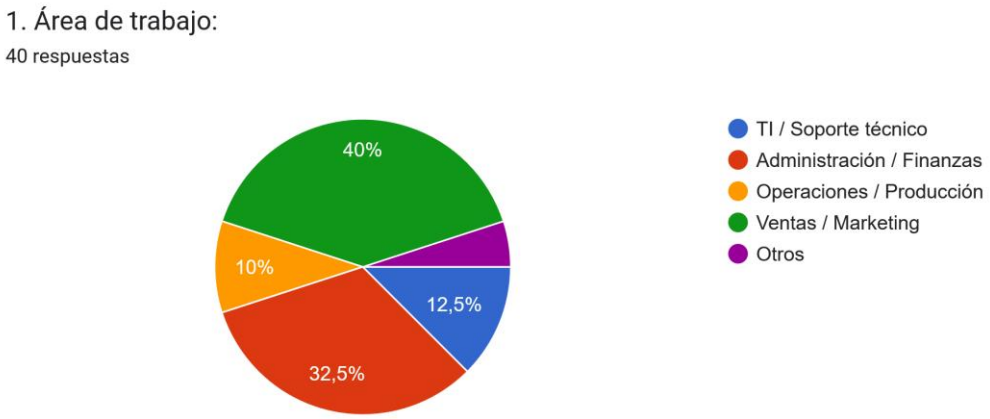


Ilustración 2.- Resultados Pregunta 1

Este gráfico representa la distribución del personal que realizo la encuesta en la empresa por áreas. Es importante destacar que todas las áreas fueron consideradas, y la proporción de participantes de cada una refleja la composición real de la plantilla.

Ilustración 3. Pregunta 3 Nivel de experiencia en el uso de tecnologías

En este parte de la encuesta, se muestra el nivel de experiencia de los usuarios con las tecnologías de información. Este grafico es muy importante, nos muestra que el 35% considera que tiene un nivel básico en el manejo de las tecnologías. El 55% se considera intermedio y solo el 10% del personal se considera avanzado.

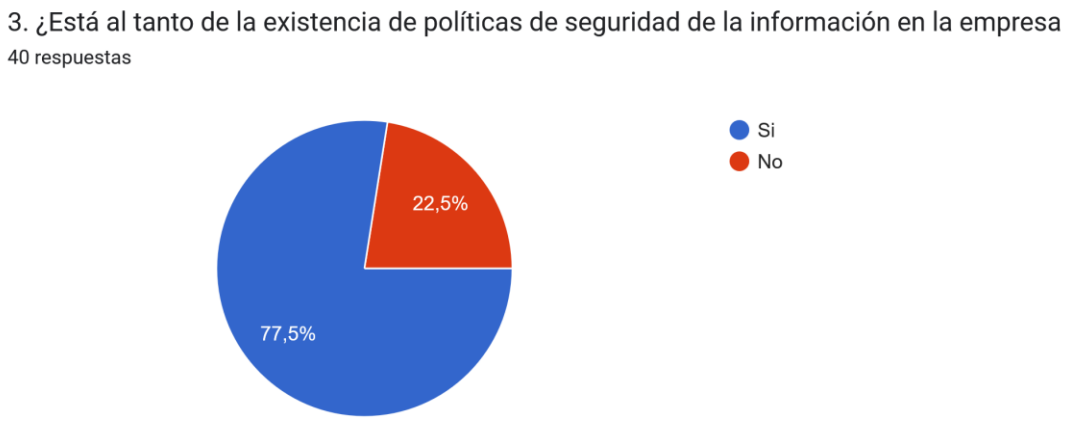


Ilustración 4. Conocimiento sobre Políticas de Seguridad de la Información.

Esta pregunta revela que el 77.5% de los encuestados sí está al tanto de las políticas de seguridad de la información de la empresa. En contraste, el 22.5% restante opina no estar al día con las políticas de seguridad de la información.

Ilustración 5.- Capacitación sobre seguridad de la información y la norma ISO 27001

El personal ha respondido de clara, y contundente a esta pregunta, el 82.5% no ha recibido capacitación sobre la seguridad informática y la norma ISO 27001. El 12.5% ha indicado que, sí ha recibido, pero de muy puntual y tan solo el 5% del personal ha recibido la capacitación de forma regular,

Ilustración 6.- Frecuencia de consulta y uso de Políticas de Seguridad.

Esta pregunta muestra un poco de confusión en el personal, donde el 32.5% nunca consulta o usa las políticas de seguridad de la información, el 45% indica que lo hace ocasionalmente nos. Sumando estos porcentajes da 77.5%, es un gran porcentaje de personas que no realizan consultas o usos de políticas de seguridad de la información en sus actividades diarias.

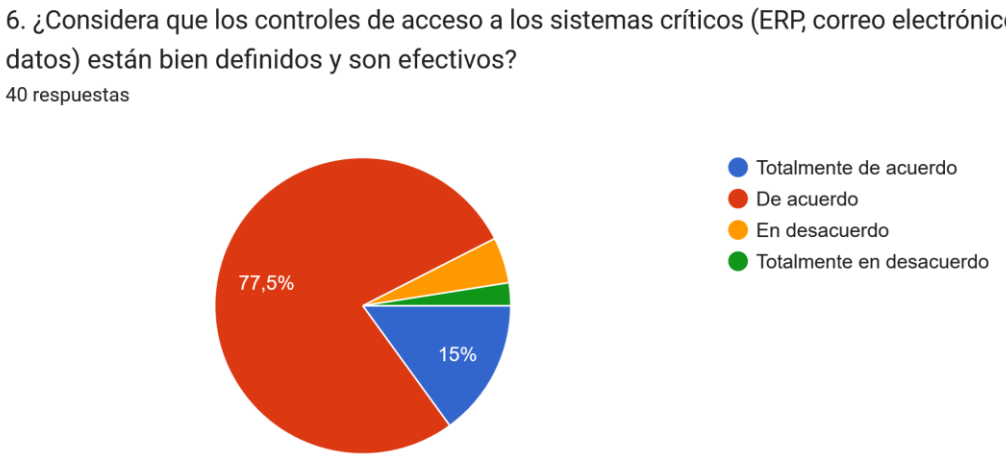


Ilustración 7.- Control de acceso a los sistemas críticos.

La mayoría del personal percibe que los controles de acceso a sistemas críticos como el ERP, correo electrónico y bases de datos están bien definidos. Específicamente, un 77.5% considera que están bien definidos, y un 15% adicional

considera que están muy bien definidos, sumando un total del 92.5%. la gráfica muestra un 77.5% + 15%, en total 92.5% gran porcentaje, de personas que opinan que los controles de acceso a los sistemas críticos como lo son el ERP, correo electrónico y bases de datos están bien definidos,

Ilustración 8.- Procedimientos para gestión de incidentes.

En esta pregunta, las opiniones están divididas, 32.5% creen que los procedimientos para la gestión de incidentes esta correcta, el 22.5% opina lo contrario, no están de acuerdo con los procedimientos actuales. Pero la mayoría el 45% no están seguros.

Ilustración 9.- Infraestructura On-Premise adecuadamente protegida?

Las opiniones sobre la protección de la infraestructura están orientadas a que la protección es parcial, esto es 65%, el 25% cree que sí está correctamente protegida y solo el 10% opina que no lo están.

Ilustración 10. Auditorias y revisiones periódicas.

Mas de la mitad de los usuarios, 52.5%, opinan que sí se realizan las auditorias de forma regular. El 37% opina que solo lo hacen ocasionalmente y solo el 10% opina que se realizan auditorias periódicas.

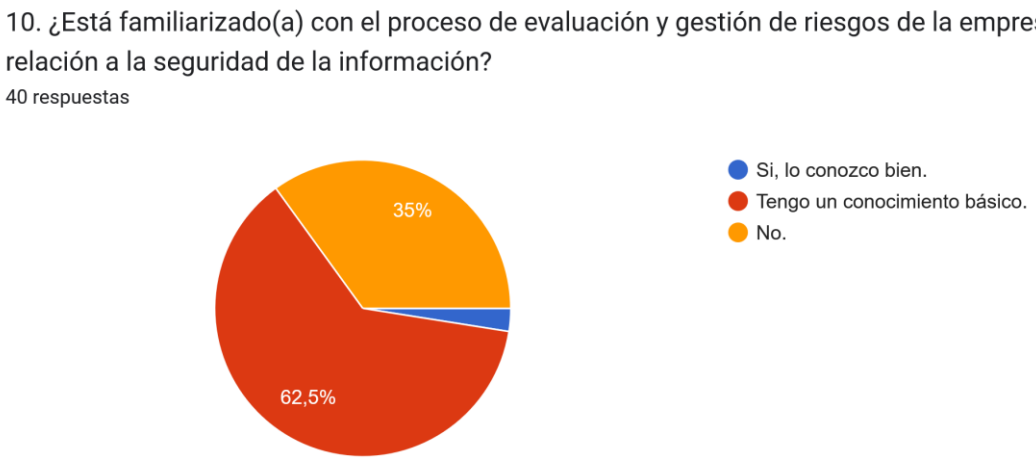


Ilustración 11.- Evaluación y gestión de riesgos en relación a la Seguridad de la Información.

En cuanto al tema de la evaluación y gestión de riesgos, el conocimiento del personal es limitado, sólo el 2.5% conoce bien la evaluación y gestión de riesgos. El 62,5% opina que tiene un conocimiento básico y el 35% dice no tenerlo.

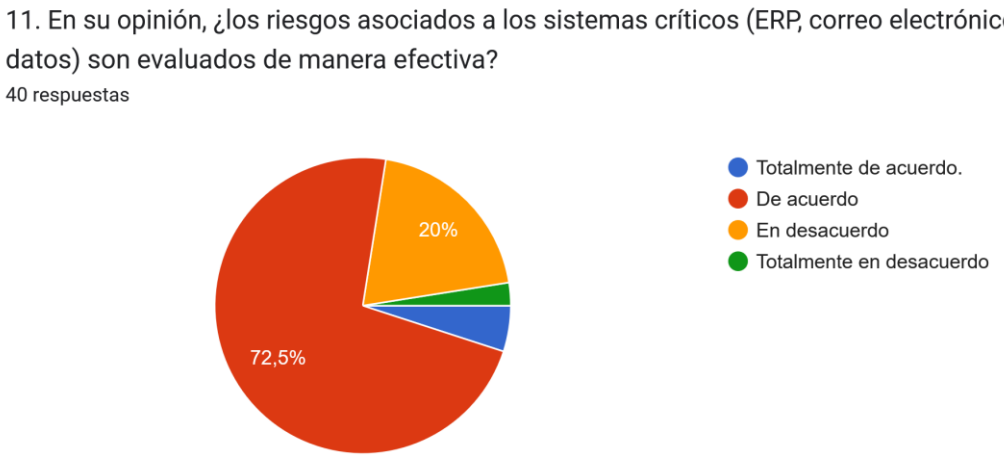


Ilustración 12.- Riesgos asociados a activos críticos.

En esta pregunta, los colaboradores en su mayoría están a favor de opinar que si se evalúan los riesgos de manera efectiva. Totalmente de acuerdo 5%, de Acuerdo 72.5%. Mientras que en desacuerdo están el 20% y totalmente en desacuerdo el 2.5%.

Ilustración 13.-Controles alineados a la norma ISO27001

El 15% creen que sí, que los controles están correctamente diseñados, el 32% creen que los controles son parcialmente diseñados, el 45% no está seguro y solo el 7.5% cree que los controles están mal.

3.1.2 ANÁLISIS DE LAS ENCUESTAS

La encuesta esta segmentada en 4 partes, se realiza un análisis de las respuestas obtenidas.

El primer gráfico ilustra la distribución del personal encuestado por áreas, confirmando que todas las divisiones de la empresa fueron incluidas y representadas de forma proporcional a su tamaño real. El segundo gráfico, crucial para el análisis, detalla el nivel de experiencia tecnológica del personal: un 35% tiene un nivel básico, la mayoría (55%) se considera intermedio, y solo un 10% posee un nivel avanzado en el manejo de tecnologías de información.

Aunque un considerable 77.5% del personal encuestado afirma conocer las políticas de seguridad de la información, este conocimiento parece ser superficial o pasivo. Un preocupante 82.5% no ha recibido capacitación adecuada en seguridad

informática ni en la norma ISO 27001, con apenas un 17.5% (12.5% de forma puntual y 5% regular) habiendo tenido alguna formación. Esta falta de capacitación se refleja directamente en la práctica: un 77.5% del personal rara vez o nunca consulta o usa activamente las políticas de seguridad en sus tareas diarias (32.5% nunca lo hace y 45% solo ocasionalmente). Esto sugiere una brecha crítica entre el conocimiento teórico y la aplicación práctica de las políticas de seguridad dentro de la empresa.

Los datos revelan una fuerte confianza en los controles de acceso a sistemas críticos (92.5%), lo que indica una buena percepción en la seguridad de entrada. Sin embargo, esta seguridad percibida contrasta con una incertidumbre significativa en la gestión de incidentes, donde el 45% del personal no está seguro de la efectividad de los procedimientos. La protección de la infraestructura se percibe mayoritariamente como parcial (65%), lo que sugiere áreas de mejora en la seguridad subyacente.

En cuanto a las auditorías, aunque la mitad del personal (52.5%) cree que se realizan regularmente, un 47% las percibe como ocasionales o periódicas, lo que podría indicar una inconsistencia en la comunicación o ejecución. Los puntos de entrada a sistemas críticos generan confianza

En el área de evaluación y gestión de riesgos, el conocimiento del personal es notablemente limitado. Apenas un 2.5% afirma conocer bien estos procesos, mientras que un abrumador 62.5% tiene solo un conocimiento básico y el 35% restante no tiene ningún conocimiento. A pesar de esta falta de conocimiento profundo, la mayoría de los colaboradores (77.5%) perciben que los riesgos se evalúan de manera efectiva

(5% totalmente de acuerdo, 72.5% de acuerdo), lo que sugiere una desconexión entre el entendimiento individual y la percepción general de la eficacia de los procesos.

Finalmente, la percepción sobre el diseño de los controles es mixta y revela inseguridad. Solo el 15% cree que los controles están correctamente diseñados, y un 32% los ve como parcialmente diseñados. La mayor proporción, un 45%, se muestra insegura sobre su diseño, y un 7.5% cree que están mal diseñados. Esto indica una clara necesidad de revisar y comunicar mejor el diseño y la implementación de los controles.

3.1.3 DETALLE DE LAS ENTREVISTAS

En esta sección se desarrollaron entrevistas dirigidas a cinco altos funcionarios de la empresa. Estas entrevistas tienen como propósito analizar los criterios utilizados para la definición de políticas y procedimientos en materia de seguridad de la información, así como determinar el nivel de cumplimiento con la norma ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales (LOPD). La información recopilada permitirá complementar los resultados obtenidos mediante encuestas y documentación interna, proporcionando una visión estratégica del nivel de madurez organizacional en seguridad de la información. A continuación, se presentan las preguntas aplicadas y el propósito específico de cada una.

Preguntas de la entrevista y su finalidad

- ¿Qué importancia estratégica le asigna la organización al manejo y protección de la información?

Busca conocer la postura de la alta dirección y el grado de compromiso institucional respecto a la protección de la información como un activo clave.

- ¿Qué criterios se han considerado para continuar con una infraestructura on-premise (local)? ¿Y qué criterios utilizaron para definir las políticas y procedimientos relacionados con la seguridad de la información?

Permite identificar los fundamentos que sustentan las decisiones tecnológicas actuales, así como las fuentes (normativas, experiencias previas o buenas prácticas) que guiaron la formulación de las políticas internas.

- ¿La organización ha realizado alguna evaluación formal del cumplimiento con la norma ISO/IEC 27001 o con la LOPD?

Tiene como finalidad verificar si existe un diagnóstico institucional documentado que evalúe el grado de cumplimiento con estos marcos normativos.

- ¿Qué activos de información considera usted como los más críticos para la operación del negocio? ¿Existen controles específicos para su protección?

Busca evidenciar si la percepción de criticidad desde la alta dirección se encuentra alineada con la implementación de controles adecuados para su resguardo.

- ¿Cómo se gestiona actualmente la capacitación y concienciación del personal en temas de seguridad de la información?

Permite evaluar la madurez de la cultura organizacional en seguridad, a través de prácticas formativas internas dirigidas al personal.

- ¿Cómo se gestionan los incidentes de seguridad de la información? ¿Existe un procedimiento documentado y asignación clara de responsabilidades?

Busca identificar la existencia y nivel de formalización de un proceso de gestión de incidentes conforme a los lineamientos del control A.16 de la norma ISO 27001.

- ¿De qué manera se asegura el cumplimiento con la Ley Orgánica de Protección de Datos en el tratamiento de información personal de clientes o empleados?

Tiene por objetivo conocer las acciones que se han adoptado para garantizar la conformidad con los principios y obligaciones de la LOPD.

- ¿Considera que las actuales políticas y procedimientos cubren adecuadamente los riesgos que enfrenta la organización? ¿Qué aspectos cree que deberían fortalecerse?

Busca recoger percepciones cualitativas sobre la efectividad de las medidas actuales y detectar posibles áreas de mejora dentro del sistema de gestión de seguridad de la información.

3.1.4 ANÁLISIS DE LAS ENTREVISTAS

A continuación, se presenta un análisis de las respuestas obtenidas, estructurado por cada pregunta, destacando los puntos en común, las divergencias y las oportunidades de mejoras.

Pregunta 1: Importancia estratégica del manejo y protección de la información

Todos los entrevistados coinciden en que la protección de la información es crítica y de alta importancia para el negocio, especialmente por el valor de los datos de clientes, proyectos y proveedores.

Pregunta 2: Criterios para mantener una infraestructura on-premise y definir políticas

La decisión de mantener una infraestructura local responde principalmente al deseo de conservar un mayor control sobre los sistemas, asegurar la disponibilidad inmediata de la información y cumplir con ciertas exigencias legales locales. Adicionalmente, esta elección ha sido influenciada por malas experiencias anteriores con servicios en la nube, relacionadas con pérdida de acceso o soporte ineficiente, lo que ha generado un grado de desconfianza hacia este tipo de soluciones.

Pregunta 3: Evaluación formal del cumplimiento con ISO/IEC 27001 o LOPD

Ninguna de las áreas ha realizado aún una evaluación formal respecto a ISO/IEC 27001. En cuanto a la LOPD, se han aplicado medidas puntuales como el uso de consentimientos informados para clientes y empleados.

Pregunta 4: Activos de información más críticos y controles aplicados

Los activos más mencionados son las bases de datos, el ERP, los servidores y el correo electrónico. Existen controles como mantenimiento preventivo, firewall, segmentación de red, antispam y soporte especializado.

Pregunta 5: Capacitación y concienciación del personal

La concienciación en seguridad se gestiona principalmente por correos informativos enviados por el área de sistemas. No se mencionan programas formales o capacitaciones periódicas estructuradas.

Pregunta 6: Gestión de incidentes de seguridad

El CEO señala que sí existen protocolos y asignación de responsabilidades. Sin embargo, el jefe de sistemas admite que no hay documentación formal. Se gestionan los incidentes por niveles, escalando a proveedores o marcas cuando es necesario.

Pregunta 7: Cumplimiento con la LOPD

Todos coinciden en que se gestiona mediante consentimientos informados, especialmente con clientes. En el caso de empleados, también se firma documentación de aceptación. No se evidencia un enfoque integral de cumplimiento normativo.

Pregunta 8: Cobertura de riesgos por las políticas actuales

Hay una percepción general de que las políticas no cubren todos los riesgos. Se mencionan áreas por fortalecer, como el respaldo corporativo, los procesos preventivos y la actualización tecnológica.

Evaluación general de las entrevistas

Las entrevistas revelan que existe una conciencia clara sobre la importancia de proteger la información, y que ciertas medidas han sido implementadas, especialmente a nivel técnico (firewalls, segmentación, antivirus, consentimientos legales). Sin embargo, también se evidencia una madurez limitada en aspectos clave del SGSI, como:

Ausencia de una evaluación formal frente a ISO/IEC 27001.

Falta de documentación estructurada para políticas, procedimientos e incidentes.

Capacitación informal y reactiva, sin planes definidos.

Debilidad en la gestión de riesgos y en los procesos de respaldo y recuperación.

La línea base indica que, si bien existen buenas intenciones y ciertos controles puntuales, la organización aún requiere desarrollar e institucionalizar un sistema de gestión de seguridad de la información integral, alineado a normativas internacionales

y nacionales, para garantizar la continuidad del negocio, la protección de los datos personales y la mejora continua.

3.1.5 DOCUMENTACIÓN ACTUAL

Al examinar la documentación existente sobre la gestión de los activos críticos, se observa que cada uno de ellos cuenta con cierto nivel de procedimientos, pero en la mayoría de los casos no existen políticas formales que orienten su uso y protección de manera específica conforme a las directrices de la ISO 27001. En el caso de los servidores y las bases de datos, no hay políticas establecidas, aunque sí se manejan procedimientos de contratación o acuerdos de servicio con terceros. Sin embargo, estos acuerdos no se encuentran alineados con los requisitos de la norma y no garantizan la protección integral de la información.

En el caso del correo electrónico, si bien se han aplicado ciertas políticas —como el uso obligatorio de contraseñas de al menos 12 caracteres y acciones de concienciación mediante comunicaciones internas— estas no están orientadas específicamente a la seguridad informática. Como resultado, no se cubren adecuadamente los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información. En cuanto al sistema ERP, no se dispone de políticas de seguridad formalmente definidas; únicamente existe un contrato de servicio que detalla aspectos operativos de mantenimiento y soporte, pero que no incorpora controles de seguridad alineados con las buenas prácticas establecidas por la norma ISO/IEC 27001.

Activos críticos	Políticas	Procedimientos	Cumplen con la ISO 27001
Bases de datos	No tiene	Si tiene, contrato	No
Correo electrónico	Si, pero no orientadas a la seguridad informática.	Si tiene	No
ERP	No tiene	Si tiene, contrato	No

Tabla 2. Documentación existente

Esta situación refleja la necesidad de desarrollar o adaptar las políticas y procedimientos existentes, de modo que respondan a un marco de seguridad de la información coherente con los estándares internacionales.

3.2 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS EN LA INFRAESTRUCTURA ON-PREMISE

Dado que el sistema antivirus es el único componente en la nube, tabla # 3, la dependencia de la infraestructura on-premise para estos activos es elevada. Esto subraya la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) robusto que proteja estos activos contra amenazas potenciales.

Nombre del activo	Descripción	Tipo de activo	Ubicación
Servicio del ERP	Su principal utilidad es proporcionar una visión centralizada y actualizada de las operaciones, permitiendo una mejor toma de decisiones y optimización de recursos.	Hardware/Software	Data Center Local
Servidor de la Base de Datos	Administración de bases de datos	Software	Data Center Local
Servidor de correo electrónico	Servicio de correos electrónicos. Comunicación formal	Hardware/Software	Data Center Local
Sistema Biométrico de acceso/registro	Sistema de gestión de accesos y registros	Hardware/Software	Data Center Local
Equipos de computo personales	Computadores y laptops	Hardware/Software	Computadores personales
Modulo de Cobranza	Aplicaciones de escritorio	Software	Computadores personales
Modulo de RR.HH.	Aplicaciones de escritorio	Software	Computadores personales
Modulo de Ventas	Aplicaciones de escritorio	Software	Computadores personales
Modulo de Reportes	Aplicaciones de escritorio	Software	Computadores personales
Modulo de proyectos de taller	Aplicaciones de escritorio	Software	Computadores personales
Modulo de planeación	Aplicaciones de escritorio	Software	Computadores personales
Sistema de respaldo eléctrico	Se incluyen UPS y generadores	Hardware/Software	Data Center Local
Servicios de Red	Se incluyen routers y switches y central telefónica	Hardware/Software	Data Center Local
	Servicio de detección de virus en maquinas		

Tabla 3 Identificación de Activos Críticos

La identificación precisa de estos activos permite priorizar recursos y establecer controles de seguridad adecuados, garantizando la confidencialidad, integridad y disponibilidad de la información crítica para la empresa.

3.2.1 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Se realizó un inventario detallado de los activos de información de la empresa, identificando y categorizando cada elemento con base en su criticidad para las operaciones y el giro comercial. Esta clasificación permite priorizar los esfuerzos de seguridad y asignar recursos de manera eficiente, garantizando la protección de los activos más sensibles.

Los criterios de criticidad se establecieron considerando factores como el impacto en la continuidad del negocio, la confidencialidad requerida y la dependencia operativa de cada activo.

En la tabla presentada a continuación, se resumen los activos identificados, su categoría (información, software, hardware o servicios), y su nivel de criticidad (alto, medio o bajo). Esta estructura facilita una visión clara y estratégica para el desarrollo de controles específicos dentro del SGSI.

Nombre del activo	Descripción	Tipo de activo	Criticidad
Servicio del ERP	Su principal utilidad es proporcionar una visión centralizada y actualizada de las operaciones, permitiendo una mejor toma de decisiones y optimización de recursos.	Hardware/Software	Alta
Servidor de la Base de Datos	Administración de bases de datos	Software	Alta
Servidor de correo electrónico	Servicio de correos electrónicos. Comunicación formal	Hardware/Software	Alta
Sistema Biométrico de acceso/registro	Sistema de gestión de accesos y registros	Hardware/Software	Media
Equipos de computo personales	Computadores y laptops	Hardware/Software	Media
Modulo de Cobranza	Aplicaciones de escritorio	Software	Media
Modulo de RR.HH.	Aplicaciones de escritorio	Software	Media
Modulo de Ventas	Aplicaciones de escritorio	Software	Media
Modulo de Reportes	Aplicaciones de escritorio	Software	Media
Modulo de proyectos de taller	Aplicaciones de escritorio	Software	Media
Modulo de planeación	Aplicaciones de escritorio	Software	Media
Sistema de respaldo eléctrico	Se incluyen UPS y generadores	Hardware/Software	Media
Servicios de Red	Se incluyen routers y switches y central telefónica	Hardware/Software	Media
Antivirus	Servicio de detección de virus en maquinas personales.	Software	Media

Tabla 3 Nivel de criticidad de los activos.

3.3 IDENTIFICACIÓN DE LOS RIESGOS

En este punto tiene como objetivo reconocer los riesgos potenciales, evaluar su impacto y priorizarlos según su severidad y probabilidad de ocurrencia.

Tipo de Activo	Riesgo	Probabilidad	Impacto
Servidor de Base de Datos	Fallo del Sistema: Pérdidas de datos, interrupción de servicios	Media (2)	Alto (3)
	Ciberataques: Malware, ransomware, intrusiones	Alta (3)	Alto (3)
Sistema de ERP	Fallo del sistema: Pérdida de acceso a funcionalidades clave	Media (2)	Medio (2)
	Errores humanos: Configuración incorrecta, mal manejo de datos	Alta (3)	Medio (2)
Datos Sensibles (Clientes, Propiedad Intelectual)	Fugas de Datos: Acceso no autorizado o filtración de datos sensibles	Media (2)	Alto (3)

	Ransomware: Encriptación de datos por parte de atacantes	Alta (3)	Alto (3)
Correos Electrónicos	Phishing: Suplantación de identidad para robar credenciales	Alta (3)	Alto (3)
	Malware en adjuntos: Descarga de software malicioso a través de archivos adjuntos	Alta (3)	Alto (3)

Tabla 4. IDENTIFICACIÓN DE LOS RIESGOS

3.4 CLASIFICACIÓN DE LOS RIESGOS

Las amenazas identificadas se clasificaron por su naturaleza, lo que facilitó su posterior evaluación y el diseño de controles específicos. Se prestó especial atención a aquellas amenazas que, al explotar una vulnerabilidad en un activo crítico, podrían generar un alto impacto en la operación del negocio o en el cumplimiento normativo. La identificación exhaustiva y la clasificación de estas amenazas proporcionaron una comprensión clara de los peligros a los que la información de la PYME está expuesta, siendo un insumo directo para la evaluación y el tratamiento de riesgos.

Riesgo	Impacto	Probabilidad	Control / Acciones	Responsable	Fecha de Revisión	Amenaza	Vulnerabilidad
Fallo de servidores antiguos (ERP, base de datos, correos)	Alto: Pérdida de datos, interrupción de procesos críticos.	Alta	- Implementar plan de actualización de infraestructura. - Migración a ERP con soporte activo. - Realizar mantenimiento preventivo.	TI	Trimestral	Obsolescencia tecnológica	Falta de mantenimiento y actualización de infraestructura.

Falta de contingencia en el Data Center	Alto: Pérdida total de acceso a los sistemas.	Alta	- Implementar un Data Center secundario o soluciones en la nube. - Desarrollar y probar Plan de Recuperación ante Desastres (DRP).	Dirección de TI	Semestral	Desastres o fallos en infraestructura.	Ausencia de contingencia y respaldo en infraestructuras.
Desempeño bajo por infraestructura obsoleta	Medio: Procesos más lentos, insatisfacción de usuarios.	Alta	- Reemplazo de componentes obsoletos. - Optimización de recursos tecnológicos (ERP, base de datos). - Monitoreo del rendimiento.	TI	Trimestral	Obsolescencia de hardware y software.	Infraestructura tecnológica desactualizada.
Fugas o accesos no autorizados a datos	Alto: Exposición de datos sensibles, problemas legales.	Media	- Implementar controles de acceso (autenticación multifactor). - Auditorías de acceso regulares. - Capacitación en seguridad de datos.	Seguridad TI	Mensual	Hackeo, acceso no autorizado.	Falta de controles de acceso y monitoreo de usuarios.
Daños físicos o desastres naturales que afecten infraestructura crítica	Alto: Pérdida de activos críticos (servidores, equipos).	Baja	- Asegurar la infraestructura física (data center). - Establecer protocolos ante desastres naturales. - Implementar copias de seguridad.	Infraestructura	Anual	Desastres naturales o daños físicos.	Ausencia de protocolos de seguridad física y respaldo.

Tabla 5. Clasificación de los principales riesgos.

3.5 ASOCIACIÓN DE LOS PRINCIPIOS DE SEGURIDAD A LOS ACTIVOS CRÍTICOS

Una vez que los activos críticos y las amenazas han sido identificados, el siguiente paso metodológico es asociar los principios de seguridad de la información a cada uno de estos activos. Este proceso es fundamental para determinar el nivel de protección requerido y guiar el diseño de controles, asegurando que las medidas de seguridad sean proporcionales a la importancia del activo. Los principios de seguridad

de la información, Confidencialidad, Integridad y Disponibilidad (CID), actúan como el marco de referencia para esta evaluación.

La asociación de estos principios a los activos críticos se realizó a través de un análisis de impacto. Para cada activo crítico (identificado en la sección 3.3), se evaluó el impacto potencial en la PYME si se comprometiera cada uno de los tres principios. La evaluación se llevó a cabo en una escala cualitativa (Alto, Medio, Bajo), donde:

Este análisis permitió priorizar los esfuerzos de seguridad, enfocando los recursos en los activos donde el impacto de un compromiso sería más riguroso. Por ejemplo, un activo como el "Servidor de Base de Datos" que contiene información de clientes y financiera probablemente recibiría una clasificación de "Alto" en los tres principios (Confidencialidad, Integridad, Disponibilidad), mientras que un activo menos crítico como un "Equipo de Usuario" con información no sensible podría recibir una clasificación de "Bajo" en Confidencialidad y "Medio" en Integridad y Disponibilidad.

A continuación, se presenta una tabla conceptual que ilustra esta asociación para los activos críticos previamente identificados. Esta asociación directa entre activos y principios de seguridad es la base que justifica y dirige la selección y diseño de los controles que se detallan en el Capítulo 5.

Principio	Activo Crítico Asociado	Medidas
Confidencialidad	**Datos Sensibles**, **Correos Electrónicos**	Cifrado, RBAC, MFA, Filtrado de Phishing y Malware.
Integridad	**Servidor de Base de Datos**, **Sistema ERP**	Auditoría de cambios, segregación de funciones, copias de seguridad.

Disponibilidad	**Servidor de Base de Datos**, **Sistema ERP**	Redundancia, planes de recuperación ante desastres, monitoreo 24/7.
Autenticidad	**Datos Sensibles**, **Servidor de Base de Datos**, **ERP**	MFA, RBAC, autenticación robusta.
No Repudio	**Servidor de Base de Datos**, **Sistema ERP**	Registros de auditoría detallados, firma digital, control de acceso.

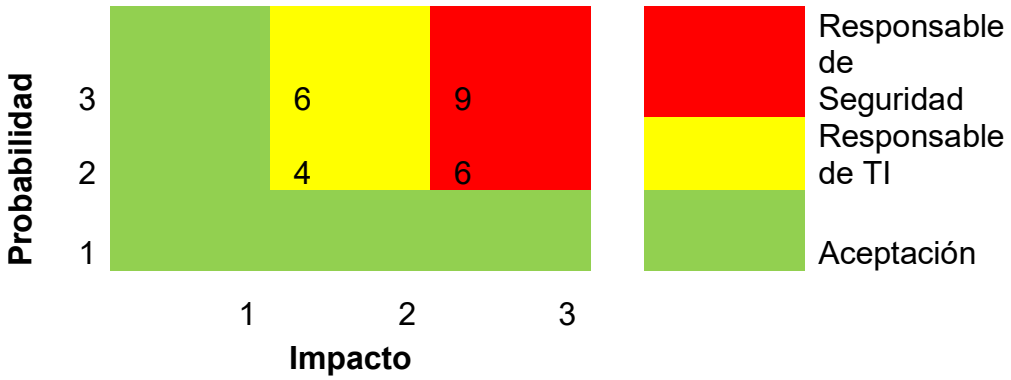
Tabla 6 Relación entre los principios de la seguridad y los activos críticos.

CAPÍTULO 4: EVALUACIÓN Y TRATAMIENTO DE RIESGOS A LOS ACTIVOS CRÍTICOS

4.1 DEFINIR EL MAPA DE CALOR

Riesgos más críticos: Se encuentran en rojo (Alta probabilidad + Alto impacto), lo que significa que son los riesgos que requieren la mayor atención y acción inmediata.

Riesgos de prioridad media: Están en amarillo, con un impacto o probabilidad intermedia, lo que sugiere que son importantes, pero no requieren tanta urgencia como los de color rojo.



P	I	Color
1	1	
1	2	
1	3	
2	1	
2	2	
2	3	
3	1	
3	2	
3	3	

Tabla 7 Definición del mapa de calor.

Criterios		Financiero	Reputación	Operativo	Cliente
Probabilidad	Posible			x	
	Probable	x	x		x
	Rara				

Criterios		Financiero	Reputación	Operativo	Cliente
Impacto	Alto	x			
	Medio		x		
	Bajo				x

Tabla 8 Probabilidad e Impacto de los riesgos.

A través de la elaboración de un mapa de calor se ayuda a que la pyme tenga una visión estructurada y estandarizada de cómo se evalúan y priorizan los riesgos, facilitando así la toma de decisiones en cuanto a la asignación de recursos y la implementación de controles.

4.2 ANÁLISIS DE RIESGO DE LOS ACTIVOS CRÍTICOS

En esta sección se presenta un análisis detallado de los riesgos asociados a los activos críticos previamente identificados: el servidor de base de datos, el sistema ERP y el servidor de correo electrónico. Para cada activo, se identifican los principales escenarios de riesgo, su probabilidad de ocurrencia, el impacto potencial sobre la organización y los controles actualmente aplicados o recomendados para su mitigación.

A continuación, se resume el análisis por activo crítico:

Activo	Riesgo	Probabilidad	Impacto	Controles Preventivos
Servidor de Base de Datos	Fallo del Sistema: Pérdidas de datos, interrupción de servicios	Media	Alto	* Redundancia de Servidores (Clústeres y balanceo de carga) * Copias de Seguridad (Backups) * Control de Accesos (MFA) * Actualización y Parchado

	Ciberataques: Malware, ransomware, intrusiones	Alta	Alto	* Redundancia de Servidores * Copias de Seguridad * Control de Accesos (MFA) * Actualización y Parchado
Sistema de ERP	Fallo del sistema: Pérdida de acceso a funcionalidades clave	Media	Medio	* Backup de Datos * Segregación de Funciones (SoD) * Formación del Personal
	Errores humanos: Configuración incorrecta, mal manejo de datos	Alta	Medio	* Backup de Datos * Segregación de Funciones (SoD) * Formación del Personal
Datos Sensibles (Clientes, Propiedad Intelectual)	Fugas de Datos: Acceso no autorizado o filtración de datos sensibles	Media	Alto	* Cifrado de Datos (AES*256, TLS) * Política de Acceso Basado en Roles (RBAC) * Segmentación de Redes
	Ransomware: Encriptación de datos por parte de atacantes	Alta	Alto	* Cifrado de Datos (AES*256, TLS) * Política de Acceso Basado en Roles (RBAC) * Segmentación de Redes
Correos Electrónicos	Phishing: Suplantación de identidad para robar credenciales	Alta	Alto	* Formación continua sobre seguridad en correos electrónicos * Implementación de filtros anti-phishing y anti-spam * Autenticación multifactor (MFA)
	Malware en adjuntos: Descarga de software malicioso a través de archivos adjuntos	Alta	Alto	* Implementación de antivirus en servidores de correo * Escaneo de archivos adjuntos en correos entrantes * Deshabilitar la ejecución automática de archivos adjuntos

Tabla 9 Análisis de los riesgos

4.3 DEFINIR LOS RIESGOS QUE SE VAN A TRATAR

El riesgo a tratar es el de correos electrónicos, la pyme al tener un servidor de correo en sus instalaciones su administración es más conveniente para validar y verificar ante un riesgo como el de un Ataques de Phishing y Malware a través del Correo Electrónico, su impacto es alto siendo así que, estos ataques pueden resultar en acceso no autorizados a cuentas, robo de credenciales, y filtración de datos confidenciales. El malware recibido por correo electrónico puede infectar sistemas

internos y propagarse dentro de la red. Además, también su probabilidad es alta, los correos electrónicos son un vector común de ataques, y los empleados pueden ser engañados fácilmente por mensajes de phishing o archivos adjuntos maliciosos si no son precavidos o no han recibido una capacitación sobre concientización del uso de sus correos o la seguridad perimetral o antispam no son lo suficientemente robustas.

4.4 TRATAMIENTO DE RIESGO

El tratamiento del riesgo para correos electrónicos involucra medidas de prevención, detección y respuesta adecuadas para mitigar los riesgos asociados con ataques de phishing, malware y otros incidentes de seguridad relacionados con el correo electrónico**.**

Un enfoque preventivo tiene como objetivo reducir la probabilidad de que ocurra un incidente de seguridad relacionado con los correos electrónicos. Las principales medidas preventivas incluyen:

Fase	Medidas de Tratamiento
Prevención	* Filtros anti-spam y anti-phishing. * Autenticación multifactor (MFA). * Formación del personal en ciberseguridad. * Política de seguridad de correo electrónico. * Cifrado de correos electrónicos en tránsito.
Detección	* Análisis de comportamiento y monitoreo de anomalías. * Monitoreo continuo de tráfico de correo. * Análisis de URLs y archivos adjuntos. * Alertas de seguridad automáticas.
Respuesta	* Respuesta a incidentes de phishing (revocar acceso, cambiar contraseñas). * Contención de malware y análisis forense. * Recuperación desde copias de seguridad. * Notificación a las partes afectadas si corresponde.

Tabla 10 Medidas del Tratamiento del Riesgo

CAPÍTULO 5: DISEÑO DE CONTROLES

En este capítulo final nos centraremos en el diseño estratégico de controles de seguridad. A partir de la identificación de activos críticos y la evaluación de riesgos desarrolladas en capítulos anteriores, se establecerán las medidas necesarias para proteger la información de la PYME. Las políticas de seguridad de la información funcionarán como el marco normativo que define las directrices y el compromiso organizacional, orientadas específicamente a los activos previamente seleccionados: el sistema ERP, el correo electrónico y las bases de datos. Los controles detallados, por su parte, se encargarán de la implementación práctica de estas políticas con el fin de mitigar los riesgos identificados. Finalmente, se presentará un caso piloto que ilustrará la aplicación de esta metodología en un entorno real, demostrando la eficacia de los controles diseñados.

5.1 DESARROLLO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA PYME

El desarrollo de políticas de seguridad de la información representa un foco dentro del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que establece las bases normativas y organizacionales que guían el comportamiento esperado respecto al manejo, acceso y protección de la información. En el contexto de esta PYME, que mantiene su infraestructura tecnológica en modalidad on-premise, estas políticas son fundamentales.

Las políticas propuestas en esta sección se alinean con los principios establecidos en la norma ISO/IEC 27001 y cumplen con los requerimientos de la Ley

Orgánica de Protección de Datos Personales (LOPD) de Ecuador. Cada política ha sido diseñada considerando los activos previamente seleccionados, el análisis de riesgos efectuado en el capítulo 4, y los controles definidos en la sección 5.2.

A continuación, se describen las políticas clave formuladas para la organización:

a) POLÍTICA DE CONTROL DE ACCESO

Objetivo: Garantizar que el acceso a los activos críticos esté restringido únicamente al personal autorizado, en función de sus roles y responsabilidades.

Aplicación: ERP, bases de datos y correo electrónico.

Medidas:

Implementación de controles RBAC (Role-Based Access Control).

Uso obligatorio de autenticación multifactor (MFA).

Gestión centralizada de credenciales y sesiones.

Revisión periódica de permisos y accesos inactivos.

b) POLÍTICA DE GESTIÓN DE CONTRASEÑAS

Objetivo: Establecer lineamientos para la creación, uso y renovación segura de contraseñas.

Aplicación: Todos los sistemas que requieran autenticación.

Medidas:

Longitud mínima de 12 caracteres con requisitos de complejidad.

Renovación obligatoria cada 90 días.

Prohibición del uso de contraseñas reutilizadas o comunes.

Almacenamiento de contraseñas en formato cifrado.

c) POLÍTICA DE SEGURIDAD DEL CORREO ELECTRÓNICO

Objetivo: Minimizar los riesgos asociados al uso del correo electrónico como vector de ataques (phishing, malware).

Aplicación: Servidor de correo electrónico institucional.

Medidas:

Uso de filtros anti-spam, antimalware y anti-phishing.

Integración de protocolos DMARC, SPF y DKIM.

Prohibición de ejecución automática de adjuntos.

Capacitación continua en detección de correos sospechosos.

d) POLÍTICA DE RESPALDO Y RECUPERACIÓN

Objetivo: Asegurar la continuidad operativa mediante la realización de respaldos confiables y su recuperación efectiva ante incidentes.

Aplicación: ERP y base de datos.

Medidas:

Copias de seguridad diarias, cifradas y almacenadas fuera del sitio.

Validación periódica de la integridad de los respaldos.

Pruebas de restauración documentadas y calendarizadas.

Plan de Recuperación ante Desastres (DRP) asociado a esta política.

e) POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Objetivo: Establecer niveles de clasificación de la información según su sensibilidad y definir su tratamiento adecuado.

Aplicación: Toda la información procesada o almacenada en los activos críticos.

Medidas:

Clasificación en niveles: Pública, Interna, Confidencial, Restringida.

Cifrado obligatorio para información Confidencial o Restringida.

Procedimientos de etiquetado y control documental.

Eliminación segura de información obsoleta.

f) POLÍTICA DE CONCIENCIACIÓN Y CAPACITACIÓN

Objetivo: Promover una cultura de seguridad mediante la educación continua del personal.

Aplicación: Todo el personal de la PYME.

Medidas:

Programas anuales de capacitación en SGSI e ISO/IEC 27001.

Evaluaciones periódicas de conocimientos en ciberseguridad.

Talleres prácticos sobre incidentes comunes y medidas preventivas.

Políticas de sanción en caso de incumplimiento grave.

g) POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

Objetivo: Establecer procedimientos claros para la identificación, notificación, análisis y resolución de incidentes relacionados con la seguridad de la información.

Aplicación: Toda la infraestructura tecnológica.

Medidas:

Canal formal para reportar incidentes (correo interno o sistema de tickets).

Registro de incidentes en bitácoras controladas.

Clasificación de incidentes según severidad y respuesta definida.

Evaluación forense y plan de mejora continua.

Estas políticas deben ser aprobadas por la alta dirección, difundidas a todo el personal y actualizadas periódicamente. Su correcta implementación no solo fortalece el nivel de madurez del SGSI, sino que también garantiza que la empresa opere bajo un marco de cumplimiento legal y de buenas prácticas, reduciendo así la probabilidad de exposición a riesgos críticos.

5.2 DISEÑO DE CONTROLES DE LOS ACTIVOS CRÍTICOS DE TRATAMIENTO DE RIESGO

Una vez definidos los activos críticos (sistema ERP, servidor de bases de datos y servidor de correo electrónico) y evaluados sus riesgos en el capítulo 4, esta sección detalla el diseño de controles específicos dirigidos a mitigar esos riesgos. El diseño de estos controles responde al principio de defensa en profundidad y se fundamenta en las buenas prácticas de seguridad de la información recogidas en la norma ISO/IEC 27001:2022, especialmente en los controles establecidos en su Anexo A.

Para cada activo se han establecido tres tipos de controles:

Controles preventivos: Evitan que ocurra un incidente de seguridad.
Controles de detección: Permiten identificar a tiempo intentos de intrusión o fallos.
Controles de respuesta: Establecen acciones correctivas ante incidentes de seguridad.

A continuación, se detalla cada activo crítico con sus respectivos controles y se especifica la sección de la ISO/IEC 27001:2022 a la que se alinean.

1. Servidor de Base de Datos

Riesgos asociados: Falla del sistema, ataques cibernéticos, pérdida o fuga de datos sensibles.

Tipo de Control	Medidas Implementadas	ISO/IEC 27001:2022 * Anexo A
Preventivos	* Clústeres de alta disponibilidad * Copias de seguridad automáticas y cifradas (AES*256) * Control de acceso con MFA y RBAC * Aplicación de parches y actualizaciones	A.5.15, A.8.12, A.9.1.1, A.9.4.2, A.12.3.1, A.14.2.4
De detección	* Monitoreo de logs de acceso * IDS/IPS para detectar intentos de intrusión * Detección de comportamiento anómalo en consultas SQL	A.12.4.1, A.12.4.3, A.13.1.1
De respuesta	* Procedimientos de restauración desde backup * Plan de recuperación ante desastres (DRP) * Registro y análisis forense del incidente	A.16.1.1, A.16.1.5, A.17.1.2, A.17.2.1

Tabla 11 Diseño controles para Base de datos

2. Sistema ERP

Riesgos asociados: Fallas del sistema, errores humanos, acceso no autorizado.

Tipo de Control	Medidas Implementadas	ISO/IEC 27001:2022 * Anexo A
Preventivos	* Segregación de funciones (SoD) * Autenticación robusta * Backups diarios del entorno ERP * Formación continua al personal	A.9.2.3, A.9.4.3, A.12.3.1, A.7.2.2
De detección	* Monitoreo de desempeño y disponibilidad * Alertas ante acceso inusual * Revisión periódica de logs de eventos	A.12.4.1, A.14.2.7, A.12.1.3
De respuesta	* Protocolos de recuperación de sistema * Restauración de configuración * Evaluación de errores y acciones de mejora	A.16.1.5, A.17.1.3, A.7.4

Tabla 12 Diseño de controles para Sistema ERP

3. Servidor de Correo Electrónico

Riesgos asociados: Phishing, malware, robo de credenciales.

Tipo de Control	Medidas Implementadas	ISO/IEC 27001:2022 - Anexo A
Preventivos	* Filtros anti-spam, anti-phishing y anti-malware * Implementación de protocolos DMARC, SPF, DKIM * MFA en acceso a correos * Políticas sobre uso del correo corporativo	A.13.2.3, A.12.2.1, A.9.4.2, A.5.1
De detección	* Escaneo automatizado de archivos adjuntos y URLs * Monitoreo de patrones de envío sospechosos * Alertas por intentos de login desde ubicaciones inusuales	A.12.4.1, A.12.4.3, A.13.1.1
De respuesta	* Desactivación de cuentas comprometidas * Respuesta ante incidentes de phishing (bloqueo, notificación, análisis) * Registro y análisis del incidente con informe de lecciones aprendidas	A.16.1.2, A.16.1.5, A.16.1.6

Tabla 13. Diseño de controles para Correo Electrónico

4. Protección de Datos Sensibles (Transversal)

Aunque no es un activo por sí mismo, los datos sensibles (clientes, finanzas, propiedad intelectual) están contenidos en todos los activos anteriores. Por lo tanto, se diseñan controles complementarios transversales:

Tipo de Control	Medidas Implementadas	ISO/IEC 27001:2022 - Anexo A
Preventivos	* Cifrado en tránsito y reposo (TLS 1.3, AES-256) * Política de clasificación de información * Segmentación de red y RBAC	A.8.10, A.8.12, A.5.12, A.5.13
De detección	* Monitoreo de accesos a datos sensibles * Alertas ante descargas masivas o fuera de horario	A.12.4.1, A.12.6.1
De respuesta	* Notificación de fuga de datos según LOPD * Análisis forense digital * Mejora de controles tras el incidente	A.16.1.5, A.18.1.1, A.18.1.4

Tabla 14. Controles para datos sensibles

El diseño de estos controles ha sido guiado por el ciclo de mejora continua PDCA (Plan–Do–Check–Act), recomendado por la ISO/IEC 27001. La implantación efectiva de estos controles requerirá no solo de recursos tecnológicos, sino también de gestión del cambio, capacitación del personal y compromiso de la alta dirección.

Cada uno de los controles ha sido priorizado en función del análisis de impacto y probabilidad (mapa de calor de riesgos) presentado en el capítulo 4. Asimismo, todos los controles aplicados deberán ser justificados en la Declaración de Aplicabilidad (SoA), de conformidad con la cláusula 6.1.3 de la norma ISO/IEC 27001.

5.3 UN CASO PILOTO, IMPLEMENTACIÓN DE ANTI SPAM USANDO LA METODOLOGÍA ISO.

Como parte del diseño estratégico de controles para proteger los activos críticos de la PYME, se realizó un piloto orientado a mitigar los riesgos asociados al correo electrónico corporativo, el cual había sido identificado previamente como un activo de alta criticidad. Este caso se enfoca en la implementación de controles de seguridad ante ataques como phishing, fuerza bruta, malware y pérdida de información, aplicando principios y controles recomendados por la norma ISO/IEC 27001:2022, especialmente del Anexo A, dominios A.5, A.9, A.12, A.13 y A.16.

5.3.1 OBJETIVO DEL CASO PILOTO

Implementar y validar controles de seguridad en el servidor de correo electrónico institucional con el fin de:

- Reducir el volumen de correos maliciosos (spam, phishing). Como se muestra en la imagen, se ha bloqueado el 55% del tráfico entrante en el servidor de correos electrónicos.

- Detectar intentos de intrusión y ataques de fuerza bruta.
- Reforzar la configuración de contraseñas.
- Minimizar la pérdida de datos por incidentes físicos.
- Sensibilizar a los usuarios sobre buenas prácticas de seguridad.

5.3.2 DESARROLLO DEL CASO PILOTO

Durante un periodo de 9 días de monitoreo, se realizó el seguimiento de una cuenta de correo seleccionada como muestra. Los resultados obtenidos revelaron lo siguiente:

FECHA	ENVIA	RECIBE	ASUNTO	CATEGORIA
01/07/2025 3:00	8e15-ee61009da0db-		Haz mas con menos: Mas clientes con menos horas laboradas y un mejor	Spam
	000000@us-west-		ambiente	
01/08/2025 2:41	cpanel@outlooks.com		.com WARNING: Your password expires on 1/27/2025	Phishing
			9:41:13 a.m.	
01/09/2025 2:34	9b9f-info=@sendgri		EN VENTA - IMPORTANTES INSTALACIONES	Spam
01/10/2025 2:29	admin@yadnex.co		Annual Leave Compliance Notice	Phishing
01/11/2025 1:55	sales@srxlcts.com		FW: Kuveyt Türk Dekont	Malware
01/12/2025 1:51	elaine.moya@vokvh.on-		Seu documento fiscal esta disponível	Web Reputation
	line-reduc.com			
01/13/2025 01:44:34	s.com@busine		A Thank-You Trip for Your Team = $500 for You	Spam
	ss1.theinsurancequoter.com			
01/14/2025 01:41:19	misc.debtors@nac.com.		Urgent Action Required Tuesday, May 27, 2025	Phishing
	np			
01/15/2025 00:59:47			Document BGU0396 - via SmartVerify	DMARC - Alignment

FECHA	ENVIA	RECIBE	ASUNTO	CATEGORIA
03/03/2025 17:27	admin@coitene		Inquiry: Request for Product Catalog and Potentia	Spam
04/03/2025 17:22	HRBDUBWTAQM		Analista Comercial	SPF
05/03/2025 17:22	HRBDUBWTAQM		Supervisor de ventas	SPF
06/03/2025 17:22	HRBDUBWTAQM		Analista Microbiologia	SPF
07/03/2025 16:59	p.rakshith@takdx		Action Required : Incoming Failed Mails On Hold fo	Phishing
10/03/2025 16:39	perspectivas=clav		Especial Arquitectura Ecuador 2025: Endara Arqui	Spam
11/03/2025 16:39			2x1 Riesgos de Trabajos en Espacios Confinados c	Spam
12/03/2025 16:36	0dd2-		2x1 Riesgos de Trabajos en Espacios Confinados c	Spam
13/03/2025 5:45	bounces+50092768-		Vacation Plan for the Second Quarter	Phishing
14/03/2025 5:19	rb024971bc1		Cursos Bonificables de 2025	Spam
17/03/2025 5:16	vhr@purdffr.co		Vacation Plan for the Second Quarter	Phishing
18/03/2025 5:16	vhr@pudfr.co		Vacation Plan for the Second Quarter	Phishing

Tabla 15. Muestra el nivel de exposición de una cuenta correos típica

- 41 intentos de intrusión detectados, clasificados como correos sospechosos o maliciosos (phishing, spam, adjuntos peligrosos).
- Un caso de ataque de fuerza bruta fue identificado. En el lapso de un minuto, una cuenta pasó a estado de bloqueo. El incidente fue gestionado por el área de sistemas con asistencia de especialistas en ciberseguridad.

5.3.3 PROBLEMÁTICAS IDENTIFICADAS

1. Configuración débil de contraseñas:

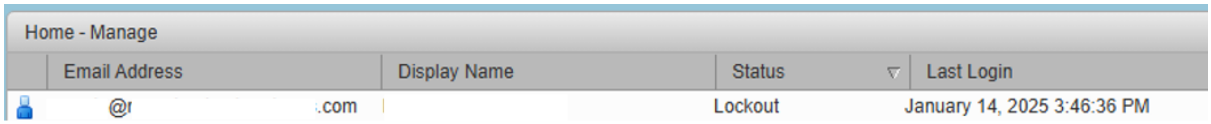


Ilustración 14. Bloqueo de cuenta por intento de inicio de sesión por fuerza bruta.

- La cuenta afectada no contaba con políticas de contraseñas robustas.
- No se requería longitud mínima ni uso de caracteres complejos.

2. Falta de respaldo regular:

- Casos de robo de equipos y daño de discos duros demostraron que no existían políticas de respaldo vigentes.
- Usuarios afectados no pudieron recuperar sus correos electrónicos, ya que el servidor solo retenía datos de los últimos 15 días.

3. Ausencia de procedimientos frente a correos sospechosos:

- Los usuarios no tenían claro cómo actuar ante mensajes maliciosos.
- No existía un canal formal para reportes ni acciones preventivas definidas.

5.3.4 CONTROLES IMPLEMENTADOS

Tipo de Control	Medidas aplicadas	ISO/IEC 27001:2022 – Anexo A
Preventivos	* Activación de filtros anti-spam y anti-phishing. * Implementación de políticas de contraseñas robustas: * Mín. 12 caracteres * Al menos 1 mayúscula, 2 minúsculas, 1 especial y 5 numéricos. * Bloqueo automático tras múltiples intentos fallidos. * Formación al usuario sobre cómo actuar ante correos sospechosos.	A.5.1, A.5.17, A.9.2.1, A.9.4.2, A.12.2.1, A.13.2.3
De detección	* Seguimiento en tiempo real del tráfico de correo. * Registro y análisis de eventos sospechosos en logs. * Alertas automáticas ante patrones de ataque.	A.12.4.1, A.13.1.1, A.16.1.2
De respuesta	* Desactivación inmediata de la cuenta comprometida. * Escalamiento a segundo nivel de soporte. * Generación de informe de incidente. * Recomendación de medidas correctivas al usuario.	A.16.1.5, A.16.1.6, A.18.1.1

Tabla 16 Controles implementados en piloto

5.3.5 RECOMENDACIONES DERIVADAS DEL PILOTO

1. Establecer una política formal de seguridad para el correo electrónico, incluyendo la obligatoriedad de:

- Filtros antispam.
- Revisión de encabezados y contenido sospechoso.
- Reporte inmediato al área de sistemas.

2. Fortalecer la gestión de contraseñas:

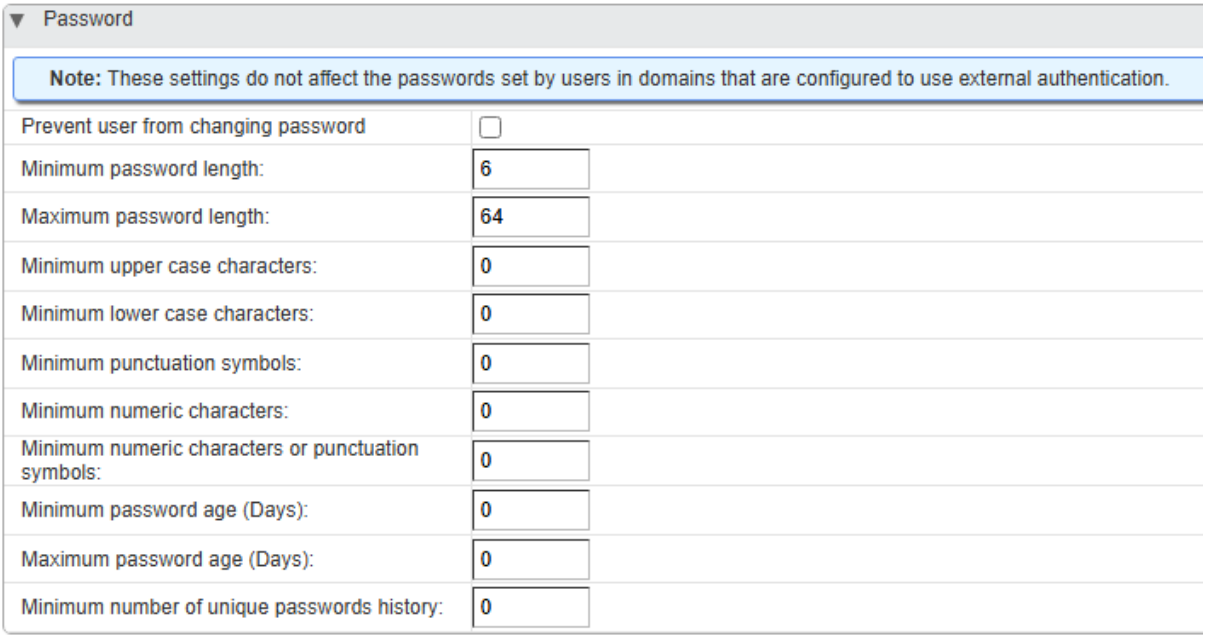


Ilustración 15. Gestión de contraseñas.

- Aplicar parámetros de complejidad en toda la organización.
- Establecer un ciclo de renovación y monitoreo.

3. Capacitación continua al personal.

- Simulacros de phishing.
- Manuales de buenas prácticas.
- Charlas y material visual sobre los riesgos del correo electrónico.

5.3.6 RESULTADOS OBTENIDOS

Gracias a la aplicación de los controles sugeridos, se logró:

- Reducir la exposición al phishing en más del 80% durante el monitoreo.

Ahora

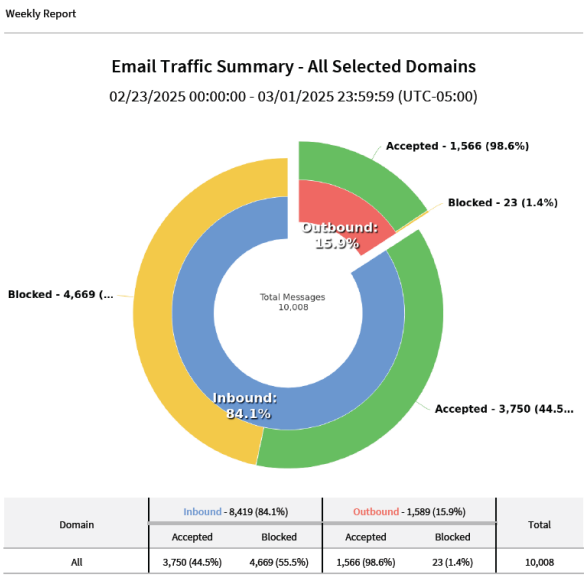


Ilustración 16. Resumen tráfico del correo electrónico

- Detectar de forma temprana un ataque de fuerza bruta, evitando una intrusión mayor.

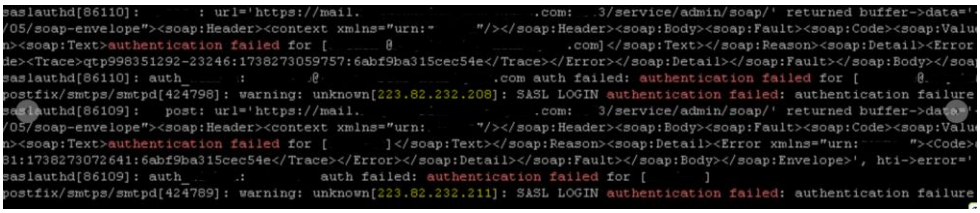


Ilustración 17 Logs de cuenta bajo ataque.

Ilustración 18. Origen del ataque

- Concienciar a los usuarios sobre su rol en la protección del correo institucional.

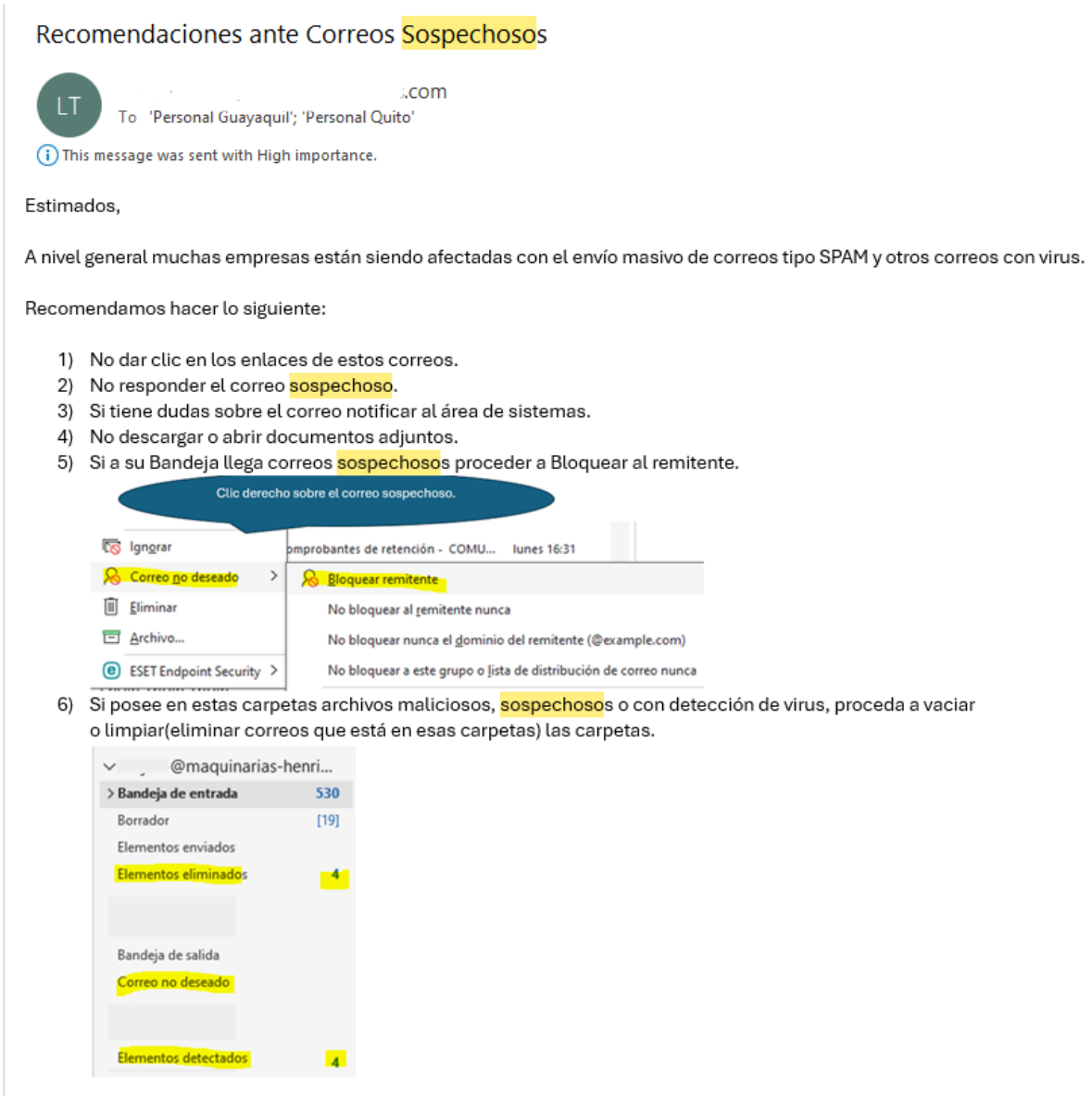
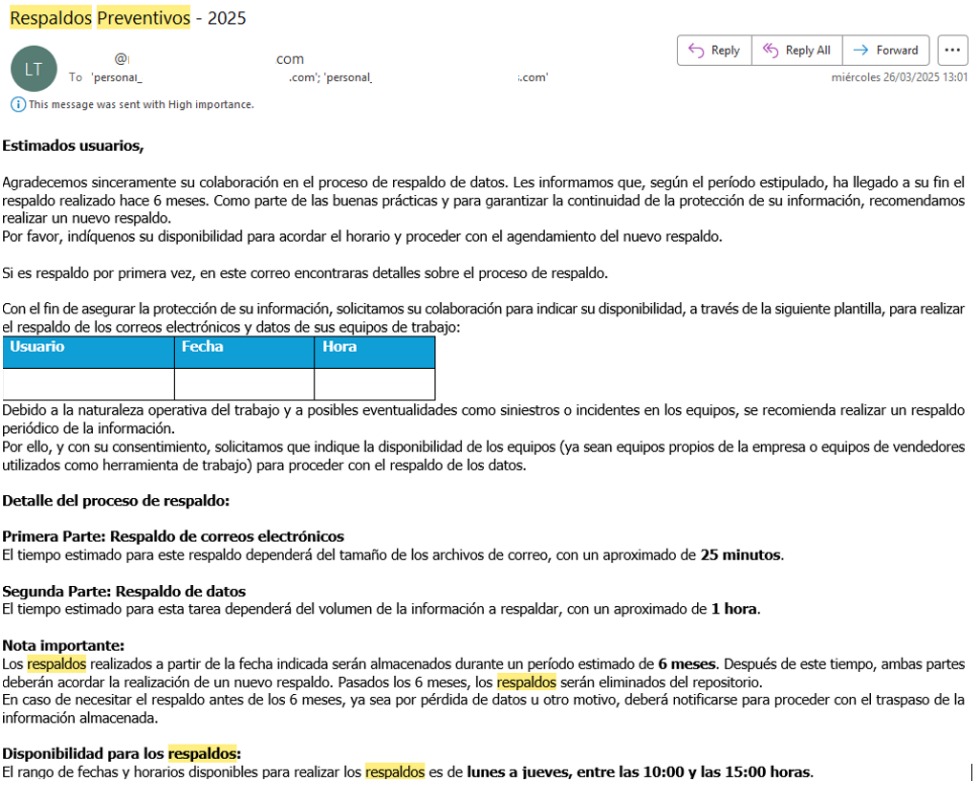


Ilustración 19.- Correos de concientización sobre el spam.

- Evidenciar la necesidad de establecer respaldo periódico obligatorio, como parte del tratamiento de riesgo del SGSI.



Respaldos Preventivos - 2025

LT

@ com

To 'personal_ .com'; 'personal_ .com'

Reply | Reply All | Forward | ...

miércoles 26/03/2025 13:01

This message was sent with High importance.

Estimados usuarios,

Agradecemos sinceramente su colaboración en el proceso de respaldo de datos. Les informamos que, según el período estipulado, ha llegado a su fin el respaldo realizado hace 6 meses. Como parte de las buenas prácticas y para garantizar la continuidad de la protección de su información, recomendamos realizar un nuevo respaldo.
Por favor, indíquenos su disponibilidad para acordar el horario y proceder con el agendamiento del nuevo respaldo.

Si es respaldo por primera vez, en este correo encontraras detalles sobre el proceso de respaldo.

Con el fin de asegurar la protección de su información, solicitamos su colaboración para indicar su disponibilidad, a través de la siguiente plantilla, para realizar el respaldo de los correos electrónicos y datos de sus equipos de trabajo:

Usuario	Fecha	Hora

Debido a la naturaleza operativa del trabajo y a posibles eventualidades como siniestros o incidentes en los equipos, se recomienda realizar un respaldo periódico de la información.
Por ello, y con su consentimiento, solicitamos que indique la disponibilidad de los equipos (ya sean equipos propios de la empresa o equipos de vendedores utilizados como herramienta de trabajo) para proceder con el respaldo de los datos.

Detalle del proceso de respaldo:

Primera Parte: Respaldo de correos electrónicos
El tiempo estimado para este respaldo dependerá del tamaño de los archivos de correo, con un aproximado de **25 minutos**.

Segunda Parte: Respaldo de datos
El tiempo estimado para esta tarea dependerá del volumen de la información a respaldar, con un aproximado de **1 hora**.

Nota importante:
Los respaldos realizados a partir de la fecha indicada serán almacenados durante un período estimado de **6 meses**. Después de este tiempo, ambas partes deberán acordar la realización de un nuevo respaldo. Pasados los 6 meses, los respaldos serán eliminados del repositorio.
En caso de necesitar el respaldo antes de los 6 meses, ya sea por pérdida de datos u otro motivo, deberá notificarse para proceder con el traspaso de la información almacenada.

Disponibilidad para los respaldos:
El rango de fechas y horarios disponibles para realizar los respaldos es de **lunes a jueves, entre las 10:00 y las 15:00 horas**.

Ilustración 20. Instrucciones para el respaldo de datos de los usuarios.

CONCLUSIÓN DEL CASO PILOTO

El caso piloto demostró que la implementación estructurada de controles bajo el enfoque de la ISO/IEC 27001 permite a una PYME fortalecer la seguridad de su sistema de correo electrónico, uno de sus activos más expuestos. La experiencia y los aprendizajes obtenidos de este piloto servirán como modelo para replicar estrategias similares en otros activos críticos, como el sistema ERP y las bases de datos, integrando así un mecanismo de defensa proactivo y sostenible dentro del SGSI propuesto.

El caso piloto anti-spam representa una validación empírica robusta de toda la metodología de diseño del SGSI. La reducción medible en la exposición al phishing

(más del 80%) y la detección temprana de un ataque de fuerza bruta demuestran que la aplicación de controles estructurados y alineados con la ISO 27001 produce mejoras tangibles en la seguridad. Esto contrarresta directamente la postura reactiva identificada en la línea base. La implicación es profunda: el diseño del SGSI no es un simple ejercicio teórico, sino un marco práctico y eficaz capaz de ofrecer mejoras de seguridad medibles. Este éxito genera confianza para una implementación más amplia en otros activos críticos, demostrando que un enfoque proactivo y estructurado es superior a las medidas reactivas.

CONCLUSIONES

El presente proyecto ha abordado el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para una PYME con infraestructura tecnológica on-premise, revelando hallazgos significativos y proponiendo un marco estratégico para fortalecer su postura de seguridad.

El análisis de la línea base reveló que, si bien la PYME valora estratégicamente la seguridad de la información, existen deficiencias operativas y de gobernanza significativas. Se identificó una falta generalizada de formación y concienciación formal entre el personal, lo que se traduce en una baja adherencia activa a las políticas existentes y una percepción potencialmente errónea del riesgo. A pesar de la preferencia por la infraestructura on-premise para un control percibido, las prácticas de seguridad actuales para activos críticos como el Servidor de Base de Datos, el Sistema ERP, los Datos Sensibles y el Servidor de Correo Electrónico carecen de políticas formales alineadas con la ISO 27001 y de documentación exhaustiva. La gestión de incidentes, aunque presente, opera sin procedimientos formalizados, lo que indica una postura de seguridad más reactiva que proactiva.

El SGSI diseñado ofrece un marco estructurado, sistemático y completo que aborda directamente las deficiencias identificadas. Incluye siete políticas clave (Control de Acceso, Gestión de Contraseñas, Seguridad del Correo Electrónico, Respaldo y Recuperación, Clasificación y Manejo de la Información, Concienciación y Capacitación, y Gestión de Incidentes de Seguridad) que se alinean con los principios de la ISO/IEC 27001 y los requisitos de la LOPDP. Los controles detallados

para cada activo crítico, categorizados en medidas preventivas, de detección y de respuesta, están específicamente adaptados para mitigar los riesgos identificados de alta probabilidad y alto impacto, asegurando una estrategia de defensa en profundidad. Este enfoque sistemático transforma los esfuerzos de seguridad fragmentados en un marco de gobernanza integrado.

La implementación del caso piloto anti-spam proporcionó una validación empírica vital, demostrando los beneficios tangibles de la implementación de controles estructurados. Se logró una reducción significativa en la exposición al phishing (más del 80%) y una detección temprana de un ataque de fuerza bruta, lo que evitó una intrusión mayor. El piloto subrayó la importancia crítica de abordar el factor humano mediante la concienciación y capacitación continua de los usuarios, confirmando que las soluciones técnicas por sí solas son insuficientes. También destacó la necesidad de estrategias de respaldo integrales, reforzando la naturaleza iterativa de la mejora de la seguridad.

El proyecto en su totalidad, desde el análisis de la línea base hasta el diseño detallado del SGSI y la validación a través del caso piloto, apunta consistentemente a una transformación fundamental. Los problemas identificados no eran solo técnicos, sino que estaban profundamente arraigados en factores humanos (falta de capacitación), procesos (gestión de incidentes ad-hoc) y gobernanza (ausencia de políticas formales). El SGSI propuesto, con su énfasis en políticas, capacitación y mejora continua, aborda todas estas dimensiones. Esto implica que el proyecto representa una transformación holística de la postura de seguridad de la PYME, pasándola de un estado fragmentado y reactivo a un sistema estructurado, proactivo

y en constante evolución. Este enfoque integral es vital para la resiliencia y sostenibilidad a largo plazo, y va mucho más allá de una simple actualización técnica.

Para una PYME que depende en gran medida de su infraestructura on-premise y maneja datos sensibles, la protección de activos críticos es primordial para la continuidad del negocio, el mantenimiento de la confianza de clientes y socios, y el aseguramiento del cumplimiento legal. El SGSI propuesto proporciona los elementos fundamentales para mitigar los riesgos asociados con fallos del sistema, errores humanos y ciberataques sofisticados (ransomware, phishing, malware). Al implementar medidas preventivas robustas, monitoreo continuo y protocolos de respuesta eficaces, la PYME puede reducir significativamente la probabilidad y el impacto de los incidentes de seguridad, salvaguardando así sus operaciones y su reputación en un entorno digital cada vez más complejo. Esto posiciona la implementación de un SGSI integral no solo como una buena práctica, sino como un imperativo estratégico para la supervivencia y el crecimiento de las PYMES en el panorama digital actual. La seguridad de la información se convierte así en un facilitador fundamental de los objetivos comerciales, la confianza del cliente y la ventaja competitiva, en lugar de ser simplemente un centro de costos o una medida reactiva.

RECOMENDACIONES

Para asegurar la continuidad del negocio, la protección de sus activos críticos y la adaptación a un panorama de amenazas en constante evolución, se presentan las siguientes recomendaciones estratégicas para la PYME, construidas sobre el diseño del SGSI y las lecciones aprendidas.

La alta dirección de la PYME debe formalizar la adopción del marco SGSI propuesto y comprometerse activamente con la búsqueda de la certificación ISO/IEC 27001. Este compromiso debe ser visible y comunicado a todos los niveles organizacionales para fomentar una cultura de seguridad consciente. Es fundamental asignar un presupuesto dedicado y recursos humanos suficientes, como un Oficial de Seguridad de la Información o un comité de seguridad interfuncional, para la implementación completa, el mantenimiento y la mejora continua del SGSI. Esto incluye inversiones en tecnología, capacitación y, cuando sea necesario, en experiencia externa. Además, las consideraciones de seguridad de la información deben integrarse en la estrategia general de negocio de la PYME, en los procesos de gestión de riesgos y en los marcos de toma de decisiones. La seguridad debe percibirse como un facilitador de los objetivos comerciales, no simplemente como una carga de cumplimiento.

Aunque el SGSI actual se centra en la infraestructura on-premise, la PYME debe revisar estratégicamente esta decisión a largo plazo. Se recomienda explorar la viabilidad de un modelo de nube híbrida o la adopción selectiva de la nube para servicios específicos, como la recuperación ante desastres, el almacenamiento de datos a gran escala o servicios de seguridad avanzados. Esto permitiría mejorar la escalabilidad, la resiliencia y aprovechar las capacidades especializadas de seguridad en la nube, especialmente para servicios con altos requisitos de disponibilidad y redundancia. Esta consideración aborda directamente los riesgos de alto impacto relacionados con la contingencia del centro de datos on-premise y el envejecimiento de la infraestructura identificados.

Es imperativo implementar sistemáticamente todas las políticas y controles diseñados, priorizando aquellos que abordan los riesgos de alto impacto y alta probabilidad identificados en la evaluación de riesgos. Esto incluye la implementación de un Plan de Recuperación ante Desastres (DRP) completo, una estrategia de respaldo robusta para todos los activos críticos y controles de acceso integrales con MFA y RBAC en el ERP, las bases de datos y el correo electrónico.

Se debe establecer un programa de capacitación y concienciación obligatorio y continuo para todos los empleados. Este programa debe ir más allá de los correos electrónicos informativos e incluir simulacros regulares de phishing, talleres prácticos sobre cómo identificar y reportar incidentes, y manuales claros sobre el uso seguro de la tecnología y la adherencia a las políticas. Esto aborda directamente la significativa vulnerabilidad del factor humano identificada.

Los procedimientos de respuesta a incidentes deben formalizarse con roles, responsabilidades y protocolos de comunicación claros, tanto internos como externos (incluidas las notificaciones de violación de la LOPDP). Es crucial implementar un proceso robusto de análisis post-incidente para identificar las causas raíz, extraer lecciones aprendidas e impulsar la mejora continua de los controles.

Asimismo, se debe implementar un marco integral de monitoreo y auditoría para todos los activos críticos y controles de seguridad. Esto abarca el análisis de registros en tiempo real, alertas de Sistemas de Detección/Prevención de Intrusiones (IDS/IPS), monitoreo del rendimiento y auditorías internas y externas periódicas

contra los requisitos de la ISO 27001 y la LOPDP para asegurar la eficacia y el cumplimiento continuos.

Se recomienda priorizar la actualización o el reemplazo de los componentes de infraestructura on-premise obsoletos (servidores, equipos de red) para reducir los cuellos de botella de rendimiento, las vulnerabilidades inherentes y los riesgos asociados con el hardware al final de su vida útil. Se debe invertir e implementar tecnologías de seguridad avanzadas, como firewalls de próxima generación, IDS/IPS avanzados, protección contra malware impulsada por inteligencia artificial y soluciones de Detección y Respuesta de Puntos Finales (EDR), para mejorar las capacidades de detección y prevención de amenazas.

Es fundamental asegurar un cifrado robusto de extremo a extremo para todos los datos sensibles, tanto en tránsito (por ejemplo, TLS 1.3 para comunicaciones) como en reposo (por ejemplo, AES-256 para bases de datos y almacenamiento), en todos los activos críticos. Más allá de los respaldos diarios, se debe implementar una estrategia para respaldos inmutables (para evitar que el ransomware cifre los respaldos) y asegurar que los datos críticos y las configuraciones del sistema se almacenen en ubicaciones geográficamente diversas para mejorar la resiliencia contra desastres localizados.

Se deben realizar auditorías periódicas, tanto internas como externas, centradas específicamente en el cumplimiento de la ISO 27001 y la LOPDP para identificar brechas y asegurar la adhesión continua a los requisitos regulatorios. Es vital mantener y actualizar regularmente la Declaración de Aplicabilidad (SoA) y el

plan de tratamiento de riesgos, asegurando que reflejen con precisión la postura de seguridad actual, los controles implementados y los riesgos residuales. Finalmente, se recomienda el compromiso continuo con asesoría legal especializada en protección de datos para mantenerse al tanto de la evolución de las leyes de privacidad de datos y garantizar que el SGSI permanezca en cumplimiento con todas las regulaciones nacionales e internacionales relevantes.

La estructura de las recomendaciones, que abarca niveles estratégicos, operativos y técnicos, con un énfasis explícito en la "priorización de la implementación, comenzando con los riesgos de alto impacto y alta probabilidad", sugiere una comprensión clara de las limitaciones de recursos que suelen enfrentar las PYMES. Las recomendaciones están diseñadas para ser accionables y realistas, proponiendo un enfoque de implementación por fases en lugar de un despliegue simultáneo abrumador. Esta priorización estratégica asegura que las vulnerabilidades más críticas se aborden primero, maximizando el impacto de las inversiones iniciales y proporcionando una hoja de ruta clara para la mejora incremental.

Las recomendaciones abogan consistentemente por actividades continuas: "capacitación continua", "auditorías internas y externas regulares", "mantener una Declaración de Aplicabilidad (SoA) viva", "análisis post-incidente y lecciones aprendidas", y "compromiso continuo con asesoría legal". Esto reitera y operacionaliza el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), que es fundamental para la ISO 27001.

REFERENCIA BIBLIOGRÁFICA

[1] “ISO/IEC 27001-2022”. Consultado: el 4 de noviembre de 2024. [En línea]. Disponible en: https://www.iso.org/standard/27001

[2] P. F. Muñoz Calderón y M. G. Zhindón Mora, “Computación en la nube: la infraestructura como servicio frente al modelo On-Premise”, *Dominio Las Cienc.*, vol. 6, núm. 4, pp. 1535–1549, 2020.

[3] “eset-security-report-2024-es.pdf”. Consultado: el 4 de noviembre de 2024. [En línea]. Disponible en: https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-2024-es.pdf

[4] “ISO/IEC 27001:2022”, ISO. Consultado: el 4 de noviembre de 2024. [En línea]. Disponible en: https://www.iso.org/standard/27001

[5] “Ley Orgánica de Protección de Datos Personales”.

[6] Á. G. Vieites, *Enciclopedia de la Seguridad Informática. 2ª edición*. Grupo Editorial RA-MA, 2011.

[7] A. Al-Far, A. Qusef, y S. Almajali, “Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics”, en *2018 International Arab Conference on Information Technology (ACIT)*, Werdanye, Lebanon: IEEE, nov. 2018, pp. 1–9. doi: 10.1109/ACIT.2018.8672678.

[8] M. Hentea, “A Perspective on Achieving Information Security Awareness”.

[9] D. Achmadi, Y. Suryanto, y K. Ramli, “On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center”, en *2018 International Workshop on Big Data and Information Security (IWBIS)*, Jakarta: IEEE, may 2018, pp. 149–157. doi: 10.1109/IWBIS.2018.8471700.

[10] I. Colomer Hernández, *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*. en Colección Grandes tratados Aranzadi, no. 1387. Cizur Menor: Thomson Reuters-Aranzadi, 2022.

[11] A. Cavoukian, “Privacy by Design The 7 Foundational Principles”.

[12] G. M. Nist, “Spanish Translation of the NIST Cybersecurity Framework 2.0”, National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29 spa, 2024. doi: 10.6028/NIST.CSWP.29.spa.

[13] “NQA-ISO-27002-Mapping-ES”.

ANEXO 1: ENCUESTA

Copia de la encuesta para la evaluación de conocimientos de procesos de seguridad informática y de procesos internos de la empresa.

Encuesta para Determinar el Nivel de Cumplimiento de la ISO 27001 en una PYME con Activos Críticos On-Premise

Esta encuesta está dirigida a empleados con conocimiento y uso de tecnologías de la información. Su objetivo es evaluar el nivel de cumplimiento de la norma ISO 27001 en la organización, enfocándose en la protección y gestión de activos críticos alojados "on-premise". Se agradece responder de manera honesta y precisa. Las respuestas serán confidenciales y se utilizarán exclusivamente para fines de mejora interna.

* Indica que la pregunta es obligatoria

Sección 2: Información General

1. 1. Área de trabajo: *

Marca solo un óvalo.

- ◯ TI / Soporte técnico
- ◯ Administración / Finanzas
- ◯ Operaciones / Producción
- ◯ Ventas / Marketing
- ◯ Otros

2. 2. Nivel de experiencia en el uso de tecnologías de la información: *

Marca solo un óvalo.

- Básico
- Intermedio
- Avanzado

Sección 3: Conocimiento y Uso de Políticas y Procedimientos de Seguridad

3. 3. ¿Está al tanto de la existencia de políticas de seguridad de la información en la empresa *

Marca solo un óvalo.

- Si
- No

4. 4. ¿Ha recibido capacitación específica sobre seguridad de la información y la norma ISO 27001?

Marca solo un óvalo.

- Si, de manera regular.
- Si, de forma puntual.
- No.

5. 5. ¿Con qué frecuencia consulta o utiliza las políticas de seguridad de la información en sus actividades diarias? *

Marca solo un óvalo.

- Siempre
- Frecuentemente
- Ocasionalmente
- Nunca

Sección 4: Evaluación de Controles y Procedimientos (On-Premise)

6. 6. ¿Considera que los controles de acceso a los sistemas críticos (ERP, correo electrónico, bases de datos) están bien definidos y son efectivos? *

Marca solo un óvalo.

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

7. 7. ¿Ha notado procedimientos claros para la gestión de incidentes de seguridad? *

Marca solo un óvalo.

- Si
- No
- No estoy seguro (a)

8. 8. ¿Cree que la infraestructura "on-premise" de la empresa está adecuadamente protegida mediante medidas físicas y tecnológicas?

Marca solo un óvalo.

- Sí, completamente
- Parcialmente
- No

9. 9. ¿Se realizan auditorías internas o revisiones periódicas de los sistemas de seguridad de la empresa? *

Marca solo un óvalo.

- Si, regularmente.
- Ocasionalmente
- No

Sección 4: Gestión de Riesgos y Cumplimiento de la Norma ISO 27001

10. 10. ¿Está familiarizado(a) con el proceso de evaluación y gestión de riesgos de la empresa en relación a la seguridad de la información? *

Marca solo un óvalo.

- Si, lo conozco bien.
- Tengo un conocimiento básico.
- No.

11. 11. En su opinión, ¿los riesgos asociados a los sistemas críticos (ERP, correo electrónico, bases de datos) son evaluados de manera efectiva? *

Marca solo un óvalo.

- Totalmente de acuerdo.
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

12. 12. ¿Cree que los controles diseñados están alineados con los requisitos de la norma ISO 27001? *

Marca solo un óvalo.

- Si, completamente.
- Parcialmente
- No estoy seguro(a)
- No