UNIVERSIDAD CATÓLICA DE CUENCA



Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Diseño de un Plan de Seguridad de la Información para la Dirección de TIC de EP-EMSEGURIDAD basado en la Norma ISO 27001.

Autor: Ing. Juan David Mejía Donoso

Asesores: Ing. Daniel Andrade Pesántez. Mg

Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2025

Certificación de Asesores

Se certifica que:

El informe de investigación “Diseño de un Plan de Seguridad de la Información para la Dirección de TIC de EP-EMSEGURIDAD basado en la Norma ISO 27001.”, de autoría de la Señor Ingeniera en Electrónica Juan David Mejía Donoso, CC: 1717639973, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Tecnologías de la Información, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2025.

_____

Ing. Diego Cordero Guzmán. PhD
Asesor Científico

_____

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

"Diseño de un Plan de Seguridad de la Información para la Dirección de TIC de EP-EMSEGURIDAD basado en la Norma ISO 27001.", es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Tecnologías de la Información, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2019.

_____

Ing. Juan David Mejía Donoso

CC: 1717639973

Agradecimiento

Agradezco a toda mi familia la cual estuvo continuamente apoyándome en el trascurso de cada módulo hasta culminar mi titulación.

Dedicatoria

Este trabajo dedico a mi hija Amy Anabella Mejía Martínez ya que es mi inspiración y mi fuerza para alcanzar mis metas propuestas.

Resumen

La seguridad de la información es fundamental para garantizar la integridad, disponibilidad y confidencialidad de los activos de datos en las organizaciones. Este estudio busca establecer directrices en seguridad física, informática y electrónica en la EP EMSEGURIDAD, protegiendo la información contra accesos no autorizados, divulgación, interrupción, modificación, robo o mal uso, ya sea intencional o accidental. La investigación adoptó un diseño no experimental, transversal y descriptivo, permitiendo identificar brechas sin manipular variables del entorno. Los hallazgos revelaron deficiencias en la gestión de acceso a sistemas críticos y la implementación de controles de seguridad informática. Se evidencia la ausencia de políticas claras de segmentación de red y autenticación multifactorial, incrementando el riesgo de intrusiones. Además, la falta de programas regulares de capacitación limita la concienciación y el cumplimiento de normativas. En seguridad física, no todos los activos cuentan con medidas adecuadas, como acceso biométrico o vigilancia 24/7. En seguridad electrónica, la ausencia de sistemas automatizados de detección y respuesta a incidentes reduce la capacidad de reacción. Para mitigar estos riesgos, se propuso un PSI estructurado y un programa integral de capacitación, fortaleciendo la postura de seguridad de la EP EMSEGURIDAD ante amenazas emergentes.

Palabras claves: Seguridad, PSI, TIC, ISO 2700, informática.

Abstract

Information security is essential to ensure the integrity, availability and confidentiality of data assets in organizations. This study seeks to establish guidelines in physical, computer and electronic security in the EP EMSECURIDAD, protecting information against unauthorized access, disclosure, interruption, modification, theft or misuse, whether intentional or accidental. The research adopted a non-experimental, transversal and descriptive design, allowing gaps to be identified without manipulating environmental variables. The findings revealed deficiencies in the management of access to critical systems and the implementation of cybersecurity controls. The absence of clear network segmentation and multi-factor authentication policies is evident, increasing the risk of intrusions. Additionally, the lack of regular training programs limits awareness and regulatory compliance. In physical security, not all assets have adequate measures, such as biometric access or 24/7 surveillance. In electronic security, the absence of automated incident detection and response systems reduces the reaction capacity. To mitigate these risks, a structured PSI and a comprehensive training program were proposed, strengthening the security posture of the EP EMSECURIDAD in the face of emerging threats.

Keywords: Security, PSI, ICT, ISO 27001, computing.

Índice de contenidos

Capítulo I. Introducción **1**

1.1 Situación problemática **1**

1.2 Problema científico **3**

1.3 Línea de investigación. **4**

1.4 Objeto de estudio **4**

1.6 Objetivos de la investigación **5**

1.6.1 Objetivo general **5**

1.6.2 Objetivos específicos **5**

1.7.1 Hipótesis **6**

1.8 Justificación - Contribuciones de la investigación **7**

1.9.1 Estado del arte o antecedentes **9**

1.9.2 Modelo de gestión de riesgos en seguridad de la información **11**

1.9.3 Cultura organizacional y concientización en ciberseguridad **12**

1.9.4 Ciberseguridad en el contexto de las organizaciones públicas **12**

1.9.5 Tendencias y nuevas amenazas en seguridad de la información **13**

1.9.6 Conceptos Fundamentales de la Seguridad de la Información **14**

1.9.6.1 Amenazas emergentes **15**

1.9.7 Modelos complementarios: COBIT (Control Objectives for Information and Related Technology) y NIST (National Institute of Standards and Technology) 16

1.9.8 Cultura organizacional y concienciación en seguridad de la información 17

***1.9.8.1 El factor humano como elemento clave* 17**

***1.9.8.2 Rol de la alta dirección en la seguridad* 18**

1.9.9 Evolución de tecnologías y herramientas de seguridad 18

***1.9.9.1 Implementación de soluciones avanzadas* 18**

***1.9.9.2 Enfoque en resiliencia cibernética* 19**

Capítulo II. Diagnóstico situacional 20

2.1 Metodología 20

2.1.1 Enfoque y diseño de la investigación 20

2.1.2 Tipo de investigación 21

2.1.3 Población 21

2.1.4 Técnicas e instrumentos 22

2.1.5 Procesamiento de datos 23

2.1.6 Procesamiento para el desarrollo del Plan de Seguridad de la Información (PSI) 24

2.1.7 Procedimientos éticos 26

2.2 Análisis situacional 27

Capítulo III. Propuesta 41

3.1 Titulo y presentación de la propuesta 41

Conclusiones 72

Recomendaciones 75

Bibliografía 76

Anexos 80

Índice de figuras

Figura 1 Área de trabajo dentro de EP EMSEGURIDAD 27

Figura 2 Años de experiencia en la empresa 28

Figura 3 ¿Conoce las políticas de seguridad de la información actuales en EP EMSEGURIDAD? 29

Figura 4 ¿Cómo calificaría su nivel de conocimiento? 30

Figura 5 ¿Ha recibido capacitación específica sobre seguridad de la información en los últimos 12 meses? 31

Figura 6 ¿Qué aspectos consideran más importantes para garantizar la seguridad de la información en la empresa? 32

Figura 7 ¿Considera que las políticas actuales son suficientes para proteger la información de la empresa? 33

Figura 8 ¿Con qué frecuencia actualizan sus contraseñas de acceso a los sistemas de la empresa? 34

Figura 9 ¿Qué tan seguro considera que es el sistema de correo electrónico institucional frente a ataques externos como phishing? 35

Figura 10 ¿Ha detectado algún incidente de seguridad relacionado con el uso de sistemas o datos en la empresa? 36

Figura 11 ¿Qué tipo de incidente ocurrió? 37

Figura 12 Portada del PSI 41

Índice de tablas

Tabla 1 Línea de investigación 4

Tabla 2 Variables 7

Tabla 3 En su opinión, ¿qué medidas adicionales deben implementarse para fortalecer la seguridad de la información? 37

Tabla 4 ¿Considera importante recibir capacitación periódica sobre seguridad de la información? Explique brevemente: 38

Tabla 5 ¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD? 39

Tabla 6 ¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD? 39

Tabla 7 ¿Tiene alguna sugerencia específica para mejorar las políticas de seguridad actuales? . 40

Tabla 8 Matriz gestión de riesgo 44

Tabla 9 Matriz de priorización de medidas 45

Tabla 10 Medidas de seguridad 47

Tabla 11 Matriz que sintetiza los hallazgos del estudio y las recomendaciones para abordar los riesgos elevados en los sistemas identificados: 49

Tabla 12 Fases del PSI 52

Tabla 13 Gestión de personal 53

Tabla 14 Vulnerabilidades identificadas: 54

Tabla 15 Medidas de seguridad 56

Tabla 16 Herramientas para el monitoreo 57

Tabla 17 Revisión periódica 57

Tabla 18 SNA 58

Tabla 19 Simulaciones de Ataques 58

Tabla 20 Plan de Acción 60

Tabla 21 Comunicación interna 61

Tabla 22 *Análisis Post-Incidente* 61

Tabla 23 Recuperación y continuidad de negocio 62

Tabla 24 Plan de respaldo 63

Tabla 25 Sintetización del PSI 63

Tabla 26 Plan de capacitación del PSI 70

Capítulo I. Introducción

1.1 Situación problemática

En la actualidad, las organizaciones utilizan ampliamente sistemas de información para automatizar, transformar y digitalizar procesos como la planificación, organización y producción, entre otros, que se generan a diario en sus departamentos, (Lema, 2020) sin embargo, la digitalización trae consigo problemas relacionados con la seguridad de la información, por ello; las empresas deben establecer políticas efectivas para proteger los datos que antes se almacenan de manera física, ya que el almacenamiento digital en la nube se ha convertido en una opción más eficiente, escalable y accesible (Chiquito, 2023).

Sin embargo, al trasladar esta información a entornos virtuales, surge la necesidad de implementar medidas de seguridad cibernética que salven la confidencialidad, integridad y disponibilidad de los datos. Al utilizar servicios en la nube, es fundamental adoptar estrategias como la encriptación, el control de acceso y la autenticación multifactorial para prevenir accesos no autorizados o pérdidas de información. La transición hacia el almacenamiento digital no solo mejora la eficiencia operativa, sino que también minimiza los riesgos asociados a la pérdida o el daño de datos almacenados esencialmente, garantizando la continuidad del negocio y el cumplimiento de las normativas de protección de datos (Lema, 2020)

EP-EMSEGURIDAD, como empresa pública, tiene un modelo de negocio centrado en ofrecer servicios esenciales de seguridad y protección a la ciudadanía. Entre los servicios que brinda se incluyen la vigilancia, la protección de bienes y personas, la gestión de emergencias y la implementación de tecnologías para prevenir y responder a situaciones de riesgo. Estos servicios son fundamentales para garantizar la seguridad pública, prevenir delitos y fortalecer la confianza ciudadana en las instituciones gubernamentales.

Sin embargo, La falta de un plan integral de seguridad de la información dentro de EP-EMSEGURIDAD exponen a la organización a riesgos graves. En Ecuador, el 54% de las empresas públicas han reportado intentos de ciberataques, según datos de la Asociación Ecuatoriana de Seguridad Informática (AECI, 2023), con pérdidas económicas que superan los $2 millones por incidente en promedio.

La ausencia de políticas claras, alineadas con estándares internacionales como ISO/IEC 27001, y una evaluación insuficiente de amenazas, dejan a la empresa vulnerable a accesos no autorizados, pérdida de datos y ataques cibernéticos (ISO 27001:2022). Estos riesgos no solo ponen en peligro la integridad de los sistemas de la empresa, sino que también pueden afectar la seguridad de los servicios que se prestan a la ciudadanía, generando impactos negativos en la confianza pública y en la operación eficiente.

La implementación de un sistema de seguridad robusto y la asignación de recursos adecuados son esenciales para proteger la información sensible y garantizar la continuidad operativa de la empresa (Pinda y Moya, 2024). No contar con estas medidas podría generar consecuencias graves, como la exposición de datos personales de los ciudadanos, la interrupción de servicios críticos, la pérdida de confianza por parte del público y, en última instancia, una afectación directa en la seguridad y bienestar de la comunidad. De acuerdo con Chiquito (2023), la falta de políticas claras y la deficiente asignación de recursos impiden la implementación de medidas de seguridad efectivas, lo que aumenta las vulnerabilidades críticas y pone en riesgo el desempeño de la organización.

A esto se suma la ausencia de una cultura de seguridad informática entre los empleados, quienes no están capacitados para identificar o prevenir incidentes, poniendo en riesgo la confidencialidad, integridad y disponibilidad de datos críticos (Ramírez, 2024). Estos problemas generan consecuencias como la pérdida de confianza en los servicios de

seguridad brindados a la ciudadanía y posibles sanciones legales por incumplimiento de normativas.

1.2 Problema científico

La Empresa Pública Metropolitana de Seguridad (EP-EMSEGURIDAD) enfrenta un creciente desafío en la protección de la información sensible gestionada por su departamento de Tecnologías de la Información y Comunicación (TICs). En criterios de Chicaiza (2024) la falta de un plan de seguridad de la información integral expone a la organización a vulnerabilidades como accesos no autorizados, pérdida de datos y ataques cibernéticos. Dada la naturaleza sensible de las operaciones de la empresa, es imprescindible diseñar un plan que contemple estándares internacionales como ISO/IEC 27001 y mejores prácticas para mitigar riesgos.

Este plan debe incluir políticas claras y una evaluación rigurosa de amenazas, es crucial abordar este problema para garantizar la protección de la información crítica y fortalecer la confianza en los servicios de seguridad que la empresa brinda a la ciudadanía. Dada esta situación, se considera este estudio como un esfuerzo para reducir la brecha existente, mediante la propuesta de estrategias viables y alineadas a estándares internacionales, que permitan mitigar riesgos, optimizar los recursos disponibles y construir una base sólida para la gestión segura de la información en la organización (Moya, 2023).

1.3 Línea de investigación.

Tabla 1

Línea de investigación

Tipo de línea	**Líneas de investigación institucionales**	**Sub Línea**	
Investigación	Energía eléctrica y Tecnologías de la Información para la innovación y el desarrollo sostenible	Ciencia de los ordenadores, analítica de datos y algoritmos computacionales	☒
		Sistemas eléctricos de potencia, energía e iluminación	☐
		Modelado, automatización y control	☐

Nota: Adaptado de la Universidad Católica de Cuenca

1.4 Objeto de estudio

El objeto de estudio consiste en diseñar un plan integral de seguridad de la información para el departamento de TICs de EP-EMSEGURIDAD, con el propósito de proteger la confidencialidad, integridad y disponibilidad de los datos críticos. Este plan se alineará con estándares internacionales como ISO/IEC 27001, identificando vulnerabilidades, mitigando riesgos de seguridad informática y fortaleciendo la cultura organizacional en ciberseguridad. Además, se busca garantizar la resiliencia tecnológica de la empresa frente a amenazas internas y externas, asegurando la continuidad operativa y la protección de la información sensible.

1.5 Campo de acción

El plan abarca la identificación y mitigación de riesgos cibernéticos, y asegura el cumplimiento de regulaciones y estándares internacionales como ISO/IEC 27001 y GDPR. Además, se enfoca específicamente en la infraestructura tecnológica y las políticas de seguridad en la Dirección de TIC, promoviendo el uso adecuado de los diferentes sistemas y equipamiento físico. Todo esto está sujeto a un plan presupuestario que permita fortalecer la cultura de seguridad y garantizar un entorno seguro y eficiente de operación.

1.6 Objetivos de la investigación

1.6.1 Objetivo general

Establecer lineamientos y directrices de aspectos de la seguridad física, informática, electrónica en la EP EMSEGURIDAD para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, aplicando políticas para el control de seguridad informática, la cual rige a todos los empleados de EP EMSEGURIDAD con la finalidad de preservar la información y los diferentes recursos informáticos con que cuenta la empresa.

1.6.2 Objetivos específicos

- Analizar las medidas de seguridad que deben implementarse en la EP-EMSEGURIDAD para fortalecer la protección de la información.
- Identificar las amenazas y vulnerabilidades presentes en la EP-EMSEGURIDAD que comprometen la seguridad de la información, con el fin de establecer estrategias que mitiguen los riesgos y garanticen la protección de la información.
- Generar políticas de seguridad para evitar la divulgación y exposición de la información producida.

- Diseñar un programa de capacitación en ciberseguridad para concienciar y formar a los empleados sobre la identificación, prevención y manejo de riesgos cibernéticos en el ámbito de la Dirección de TIC.
- Diseñar un plan de seguridad alineado con la ISO 27001 para garantizar la protección de la información, mitigar vulnerabilidades en la infraestructura tecnológica y establecer políticas de seguridad.

1.7 Problema científico - Preguntas de investigación

Preguntas científicas

¿Cuáles son las principales amenazas y vulnerabilidades que enfrentan las empresas públicas en términos de seguridad de la información?

¿Qué procedimientos deben incluirse en un plan de seguridad de la información para gestionar adecuadamente incidentes de seguridad en empresas públicas?

¿Cómo la capacitación en ciberseguridad puede reducir riesgos en la empresa?

¿Cuál es la percepción de los empleados sobre la eficacia de la implementación de políticas de seguridad en sus actividades diarias?

1.7.1 Hipótesis

¿La implementación de un plan de seguridad de la información basado en ISO 27001 permitirá mitigar los riesgos de ciberseguridad en EP-EMSEGURIDAD y fortalecer la protección de datos críticos?

Variables

Independiente:

Disponibilidad, Amenazas y vulnerabilidades

Dependientes:

Políticas de seguridad informática para EP-EMSEGURIDAD

Tabla 2

Variables

Conceptualización	Unidad de medida	Instrumento
Disponibilidad	- Porcentaje de disponibilidad (%) - Tiempo promedio entre fallos (MTBF) - Tiempo promedio de recuperación (MTTR)	- Encuesta al personal TICs de la EP EMSEGURIDAD - Revisión de la literatura (correo electrónico) sobre ataques a nivel nacional
Políticas de seguridad de la ISO27001	- Evaluación de cumplimiento	- Encuesta al personal TICs de la EP EMSEGURIDAD
Amenazas	- Frecuencia de ocurrencia (incidentes/mes, trimestre, año) - Nivel de riesgo (escala cualitativa o cuantitativa) - Impacto estimado (valor económico o porcentaje de daño)	- Análisis de incidentes de seguridad.
Vulnerabilidades	- Cantidad de vulnerabilidades identificadas - Nivel de criticidad (baja, media, alta, crítica) - Tiempo de exposición (días, horas, meses)	- Auditorías de seguridad - Herramientas de análisis de vulnerabilidades

Nota: Matriz de la operacionalización de variables. Elaboración propia

1.8 Justificación - Contribuciones de la investigación

La protección de la información es un aspecto crucial para cualquier entidad pública o privada, especialmente para aquellas que gestionan datos sensibles como EP-EMSEGURIDAD. La investigación que propone un plan de seguridad de la información para el departamento de TIC tiene un impacto directo en la mejora de las prácticas de seguridad

cibernética, la prevención de incidentes y el cumplimiento normativo. Esta investigación contribuye a la creación de un marco estructurado que permite a la organización identificar, evaluar y mitigar los riesgos asociados con el manejo de la información crítica (Coello, 2024).

Los ciberataques tienen un impacto económico y operativo significativo en las empresas, especialmente en aquellas con infraestructura tecnológica crítica. Según estimaciones internacionales, el costo promedio de un ataque supera los $4 millones, incluyendo pérdidas por interrupciones operativas, recuperación de sistemas y daños reputacionales. En empresas públicas similares, estos eventos pueden provocar retrasos en la prestación de servicios esenciales y costos adicionales por la implementación tardía de medidas correctivas. Además, la falta de un enfoque preventivo puede duplicar estos costos debido a la repetición de vulnerabilidades no resultados. Un plan de seguridad robusto es clave para mitigar estos riesgos y optimizar recursos (Ramírez, 2024).

Además, al alinearse con estándares internacionales como ISO/IEC 27001, se asegura que el plan de seguridad sea robusto, actualizado y acorde a las mejores prácticas globales. Esta integración no solo fortalece la protección de los datos, sino que también aumenta la confianza de la ciudadanía en los servicios proporcionados por la empresa.

La investigación también aporta a la promoción de una cultura organizacional en torno a la seguridad informática, que involucra a todos los niveles de la empresa. A largo plazo, la implementación de este plan contribuirá a una mayor eficiencia operativa, la reducción de riesgos de ciberataques y la mejora continua en la gestión de la seguridad de la información.

Principales resultados a obtener

El estudio tiene como objetivo obtener resultados tangibles que contribuyan significativamente a la mejora de la seguridad de la información en EP-EMSEGURIDAD. Entre los principales resultados esperados, se encuentra el desarrollo de un plan de seguridad

de la información integral que contempla políticas, procedimientos y herramientas para la protección de datos críticos, alineados con estándares internacionales como ISO/IEC 27001. Se espera que la implementación de este plan reduzca los incidentes de seguridad en un X%. Este plan debe ofrecer una estructura clara para la identificación y mitigación de riesgos, mejorando la capacidad de respuesta ante amenazas internas y externas.

Otro resultado clave es la evaluación exhaustiva de las vulnerabilidades y amenazas a las que está expuesta la infraestructura tecnológica de la organización. A partir de esta evaluación, se establecerán medidas preventivas y correctivas, tales como controles de acceso, monitoreo de sistemas y procedimientos de recuperación ante desastres.

Asimismo, se prevé que al menos el 80% del personal complete la capacitación en seguridad, sensibilizándose e instruyéndose sobre buenas prácticas en ciberseguridad, promoviendo una cultura organizacional proactiva en cuanto a la protección de la información. Finalmente, el estudio busca sustentarse y apegarse al cumplimiento de la ISO 27001, mejorando la resiliencia operativa de la empresa frente a incidentes de seguridad, reduciendo así el riesgo de pérdidas de datos y daños a la reputación institucional.

1.9 Fundamentación teórica

1.9.1 Estado del arte o antecedentes

En este contexto, adquiere relevancia el desarrollo de auditorías informáticas (AI), también conocidas como "Auditorías de TI" (ATI). Estas auditorías experimentaron su auge en los años 60, cuando se comenzaron a vincular aspectos de organización, estrategia de TI y negocios en el ámbito empresarial, con el propósito de alcanzar los objetivos establecidos por las organizaciones. Con el transcurso del tiempo, la ATI se ha vuelto más compleja debido al creciente uso de las tecnologías y al aumento de la automatización de procesos en las organizaciones (Imbaquingo et al., 2020).

La norma ISO/IEC 27001 es un estándar internacional diseñado para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque permite a las organizaciones proteger sus activos de información frente a accesos no autorizados, alteraciones y pérdidas, garantizando la confidencialidad, integridad y disponibilidad de los datos (Miranda, 2021). La norma promueve una gestión basada en la identificación y mitigación de riesgos, así como en la mejora continua de los procesos de seguridad. Al seguir los requisitos establecidos, las organizaciones pueden demostrar su compromiso con la protección de la información y su capacidad para gestionar amenazas cibernéticas y riesgos asociados a sus operaciones (ISO 27001: 2022).

Empresas similares a la EP-EMSEGURIDAD han implementado planes basados en la norma ISO/IEC 27001 para fortalecer sus sistemas de seguridad de la información. Por ejemplo, organismos públicos como la Policía Nacional de Colombia han adoptado este estándar para proteger datos críticos relacionados con la seguridad ciudadana (Policía Nacional de Colombia, 2023). Este tipo de organizaciones han logrado reducir significativamente los riesgos asociados a ciberataques y pérdidas de información, asegurando la continuidad operativa y mejorando la confianza en los servicios que brindan Este antecedente refuerza la importancia de implementar un plan basado en la norma ISO/IEC 27001 para abordar los desafíos de seguridad de la información en EP-EMSEGURIDAD.

La norma ISO/IEC 27001 es el estándar internacional que establece los requisitos para implementar, mantener y mejorar el SGSI. La implementación de ISO/IEC 27001 implica un enfoque sistemático basado en la gestión de riesgos, que abarca desde la planificación y evaluación hasta la mejora continua de los procesos de seguridad. A través de este estándar, las organizaciones pueden establecer políticas, objetivos y controles adecuados para salvaguardar sus activos de información frente a amenazas y vulnerabilidades (Carrillo y Asto, 2021).

Al adoptar estas normativas, las organizaciones pueden mejorar su seguridad y reducir los riesgos vinculados a la gestión de la información. Es crucial entender que estas normas no deben considerarse como soluciones aisladas, sino como elementos complementarios que ofrecen un enfoque integral y efectivo para asegurar la protección de la información. Al implementar estos estándares, las empresas pueden evidenciar su compromiso con la seguridad de los datos, aumentar la confianza de los clientes y garantizar el cumplimiento de las normativas vigentes. En resumen, esta normativa juega un papel clave en la creación de un entorno digital seguro y confiable, permitiendo que las organizaciones se desarrollen y afronten los retos de seguridad tanto actuales como futuros (Minaya et al., 2023)

1.9.2 Modelo de gestión de riesgos en seguridad de la información

El análisis de riesgos se puede entender como el proceso de identificar las posibles amenazas y vulnerabilidades que pueden comprometer la seguridad informática, evaluando el impacto potencial de su materialización y determinando las áreas que requieren medidas de protección. Este análisis es fundamental para proteger los activos de información de la organización y garantizar la ejecución exitosa de sus objetivos más críticos (Whitman y Mattord, 2022). Para llevar a cabo un análisis de riesgos efectivo, es necesario que la organización asegure la continuidad de sus operaciones, gestione adecuadamente las amenazas críticas identificadas, promueva la mejora continua de la seguridad de los datos y minimice el impacto sobre las pérdidas financieras, operativas y de tiempo. En estudios previos, se han utilizado diversas metodologías de análisis de riesgos, como el Método de Análisis de Riesgos de la ISO/IEC 27005 , el Análisis de Impacto en el Negocio (BIA) y el Método OCTAVE (Operationally Critical Threat, Asset, and Evaluación de vulnerabilidad), los cuales se aplicaran en este caso para obtener una evaluación precisa y gestionar los riesgos de manera eficiente. (Miranda, 2021)

1.9.3 Cultura organizacional y concientización en ciberseguridad

Uno de los principales factores de riesgo en la seguridad de la información es el factor humano. La falta de concientización y la capacitación insuficiente de los empleados en cuestiones de ciberseguridad pueden conducir a incidentes graves, como accesos no autorizados, filtraciones de datos y ataques de ingeniería social. Según Whitman y Mattord (2022), la formación y concientización del personal son componentes clave en cualquier estrategia de seguridad. Los estudios han demostrado que las organizaciones que invierten en programas de concientización sobre seguridad tienen menos probabilidades de sufrir brechas de seguridad y daños por ciberataques.

Por ejemplo, Chiquito (2023) el estudio analizó cómo los empleados perciben las políticas de seguridad de la información en las organizaciones. Encontraron que la falta de capacitación y la ausencia de una cultura organizacional que promueva la ciberseguridad aumentan la vulnerabilidad de la organización a los ataques. En este contexto, se propondrá la implementación de campañas de concientización mediante mensajes comunicacionales que aporten una cultura de seguridad informática fundamental para proteger los activos de información de las organizaciones.

1.9.4 Ciberseguridad en el contexto de las organizaciones públicas

Las organizaciones gubernamentales y las empresas públicas, como EP-EMSEGURIDAD, enfrentan desafíos adicionales en cuanto a la seguridad de la información debido a la naturaleza sensible de los datos que gestionan. Estas organizaciones son objetivos frecuentes de ciberataques debido a su rol en la infraestructura crítica y la gestión de información sensible de los ciudadanos. Un estudio de Zohar y Ben-Assuli (2016) sobre la seguridad en las entidades gubernamentales subraya la importancia de adoptar un enfoque

integral para la protección de la información, que involucra no solo tecnología, sino también procesos y políticas organizacionales.

La norma ISO/IEC 27001 es un estándar internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Este marco ayuda a proteger la confidencialidad, integridad y disponibilidad de la información mediante la evaluación de riesgos y la implementación de controles. Casos de éxito como el de la Agencia de Innovación Digital de Dinamarca, que logró reducir en un 40% los incidentes de seguridad tras adoptar ISO 27001, demuestran la eficacia de esta norma. Del mismo modo, empresas en América Latina han reportado un incremento en la confianza de sus usuarios al certificar su cumplimiento con este estándar, mejorando tanto su reputación como su resiliencia frente a amenazas.

Ben-Assuli y Chaleco (2022) propone que las organizaciones públicas deben priorizar la evaluación de riesgos y la implementación de controles específicos para proteger la información confidencial. Además, la cooperación con otras entidades gubernamentales y organismos internacionales es crucial para garantizar la efectividad de las medidas de seguridad, dada la naturaleza de las amenazas cibernéticas que enfrentan.

1.9.5 Tendencias y nuevas amenazas en seguridad de la información

Las amenazas en el ámbito de la ciberseguridad están en constante evolución, y las nuevas tecnologías, como la IA, el IoT y el Big Data, presentan riesgos emergentes que las organizaciones deben abordar. Según un informe de la Agencia Europea de Ciberseguridad (ENISA, 2020), las amenazas más recientes incluyen ataques a la cadena de suministro, el uso de técnicas avanzadas de ingeniería social y los ciberataques basados en IA que son más difíciles de detectar y mitigar (Lema, 2020).

ENISA señala que, para enfrentar estas nuevas amenazas, las organizaciones deben adoptar un enfoque más dinámico en su estrategia de seguridad, que contemple no solo los métodos tradicionales de defensa, sino también tecnologías emergentes y un enfoque más colaborativo en la lucha contra los cibercriminales.

1.9.6 Conceptos Fundamentales de la Seguridad de la Información

Los requisitos de seguridad en las organizaciones han experimentado dos transformaciones significativas en las últimas décadas. La primera se originó con la introducción de las computadoras, lo que hizo evidente la necesidad de herramientas automatizadas para proteger los archivos y la información almacenada (Vega y Marrero, 2021). La segunda transformación surgió con la aparición de los sistemas distribuidos y el uso de redes de comunicaciones, que permiten el intercambio de información entre servidores y computadoras o entre computadoras. En este contexto, la seguridad dejó de centrarse únicamente en el ámbito computacional y comenzó a abarcar también los aspectos relacionados con las telecomunicaciones.

La transformación digital, caracterizada por la convergencia de las tecnologías de la información y las comunicaciones, ha tenido un profundo impacto en la seguridad informática. La creciente complejidad de las infraestructuras tecnológicas, con una proliferación de dispositivos interconectados y un flujo constante de datos, ha creado nuevas oportunidades para los ciberdelincuentes.

En este contexto, los principios de seguridad establecidos en la era de las computadoras individuales han tenido que adaptarse para hacer frente a amenazas más sofisticadas y un entorno de mayor riesgo. La protección de la información se ha convertido en una prioridad estratégica para las organizaciones, que deben garantizar la integridad, confidencialidad y disponibilidad de los datos (Lema, 2020). Las amenazas actuales incluyen

ciberataques avanzados, robo de datos y ataques a infraestructuras críticas, lo que exige la implementación de políticas de seguridad más robustas y multifacéticas. Estos cambios obligan a las empresas a evolucionar sus estrategias, integrando tecnologías más complejas y protocolos de protección más estrictos.

Los principios fundamentales de la seguridad de la información, como la confidencialidad , integridad y disponibilidad , siguen siendo esenciales, pero ahora deben ser complementados con nuevas estrategias. La autenticación multifactorial y el control de acceso son vitales para prevenir accesos no autorizados. Además, se han incorporado principios como la auditoría continua y la gestión de riesgos , que permiten identificar vulnerabilidades de manera proactiva. La resiliencia y la recuperación ante desastres también juegan un papel clave, ya que los ataques cibernéticos pueden ser inevitables, pero la capacidad de una organización para recuperarse rápidamente es esencial para minimizar su impacto (Urbini, 2021)

1.9.6.1 Amenazas emergentes

Las amenazas cibernéticas evolucionan constantemente, presentando nuevos desafíos para la seguridad digital. Entre las más preocupantes destacan los ataques de ransomware, que encriptan los datos de las víctimas y exigen un pago para su desbloqueo; el phishing, que busca engañar a usuarios para obtener información confidencial; y los ataques de ingeniería social, que manipulan a las personas para que revelen datos sensibles (Gartner, 2021). Por otra parte, el IoT ha introducido nuevas vulnerabilidades, ya que la proliferación de dispositivos conectados crea una superficie de ataque más amplia. Los cibercriminales también están explotando la IA para automatizar ataques y desarrollar malware más sofisticado, lo que dificulta aún más la detección y la respuesta a las amenazas. Estos ataques no solo buscan el lucro económico, sino también la disrupción de servicios esenciales y el robo de información

confidencial. A diferencia de otros delitos, los ciberataques pueden causar daños a gran escala en poco tiempo, afectando desde sistemas financieros hasta infraestructuras críticas (Gracia, 2024).

En Ecuador, al igual que en otros países, los cibercriminales aprovechan la creciente digitalización para perpetrar sus actividades. Según Ministerio de Telecomunicaciones y Sociedad de la Información (2022), los ataques más frecuentes incluyen el robo de identidad, la suplantación de marcas y el acceso no autorizado a sistemas informáticos. Estas amenazas no solo ponen en riesgo la seguridad de las personas, sino también la reputación y competitividad de las empresas. Es fundamental que tanto el sector público como el privado implementen medidas de seguridad robustas para protegerse de estas amenazas en constante evolución.

1.9.7 Modelos complementarios: COBIT (Control Objectives for Information and Related Technology) y NIST (National Institute of Standards and Technology)

En el estudio, se utilizarán modelos complementarios como COBIT y NIST, que, junto con ISO/IEC 27001, proporcionan una visión integral y detallada de la gestión de la seguridad de la información. COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas) es un modelo que se enfoca en la gobernanza y gestión de las Tecnologías de la Información (TI). Permite a las organizaciones alinear sus políticas y prácticas de seguridad de la información con los objetivos estratégicos y de negocio.

Según ISACA (2019), COBIT proporciona un marco robusto para la gestión de la TI, lo que ayuda a las instituciones públicas a fortalecer sus procesos de gobernanza y asegurar que los controles de seguridad estén integrados en la toma de decisiones a nivel organizacional.

Por otro lado, el marco NIST es ampliamente reconocido por su enfoque práctico y detallado, basado en cinco pilares fundamentales: identificar, proteger, detectar, responder y recuperar (NIST, 2018). Este marco proporciona un enfoque integral que no solo se centra en la prevención de incidentes de seguridad, sino también en la capacidad de recuperación y respuesta ante eventos cibernéticos. Su aplicación en el estudio facilitará una visión global de cómo mejorar la resiliencia organizacional ante amenazas emergentes, asegurando que las prácticas de seguridad sean reactivas y proactivas al mismo tiempo.

La integración de estos modelos con ISO/IEC 27001 en el estudio permitirá una evaluación más completa y estratégica de la seguridad de la información en el entorno público. La combinación de la gestión de riesgos, la optimización de procesos operativos y la gobernanza de TI proporcionará una base sólida para diseñar controles de seguridad efectivos, adaptados a las necesidades específicas de las organizaciones públicas, como EP-EMSEGURIDAD.

Este enfoque multidimensional facilitará la mejora continua de la seguridad cibernética y garantizará que los procesos sean más robustos y alineados con los objetivos organizacionales y las normativas legales vigentes.

1.9.8 Cultura organizacional y concienciación en seguridad de la información

1.9.8.1 El factor humano como elemento clave

El factor humano representa uno de los mayores riesgos en la seguridad de la información. Según un estudio de IBM (2022), el 95% de los incidentes de ciberseguridad tienen origen en errores humanos, como clics en enlaces maliciosos o configuraciones inadecuadas de sistemas. Promover una cultura organizacional orientada a la seguridad es crucial para minimizar este tipo de riesgos. Esto incluye la implementación de programas de capacitación continua, simulacros de ataques cibernéticos y políticas claras de uso de

tecnologías. EP-EMSEGURIDAD podría beneficiarse significativamente al desarrollar campañas internas de concienciación que refuercen prácticas seguras en el manejo de la información.

1.9.8.2 Rol de la alta dirección en la seguridad

La efectividad de cualquier estrategia de ciberseguridad depende del compromiso de la alta dirección. Según Zohar y Ben-Assuli (2016), las organizaciones que cuentan con líderes comprometidos en promover políticas de seguridad y asignar recursos suficientes logran mayores niveles de madurez en ciberseguridad. En el caso de EP-EMSEGURIDAD, esto implicaría designar responsables claros, asignar presupuestos adecuados y establecer métricas para medir la efectividad de las medidas implementadas.

1.9.9 Evolución de tecnologías y herramientas de seguridad

1.9.9.1 Implementación de soluciones avanzadas

El uso de tecnologías como inteligencia artificial (IA) y aprendizaje automático está transformando la forma en que las organizaciones enfrentan las amenazas cibernéticas. Estas herramientas permiten detectar patrones anómalos en tiempo real y responder de manera proactiva a posibles ataques. Por ejemplo, los sistemas de detección de intrusos basados en IA pueden identificar comportamientos sospechosos incluso antes de que ocurra un incidente.

EP-EMSEGURIDAD podría aprovechar diversas tecnologías basadas en IA para fortalecer su infraestructura de seguridad, especialmente en áreas críticas como la protección de redes y la gestión de accesos. Tecnologías como los sistemas de detección y prevención de intrusiones (IDS/IPS), que utilizan IA para identificar patrones anómalos y bloquear amenazas en tiempo real, son fundamentales. Además, el aprendizaje automático (Machine

Learning) puede ayudar a predecir y detectar nuevos tipos de ataques, mejorando la eficacia de las defensas cibernéticas.

La autenticación multifactor (MFA) y la biometría avanzada, impulsadas por IA, también juegan un papel crucial en la mejora de la gestión de accesorios y la protección de sistemas sensibles. Asimismo, la automatización de la respuesta a incidentes con IA puede reducir significativamente los tiempos de intervención, lo que mejora la eficiencia operativa. Según Gartner (2021), las organizaciones que implementan estas tecnologías experimentan una reducción del 40% en los tiempos de respuesta ante incidentes, lo que refuerza aún más la capacidad de EP-EMSEGURIDAD para protegerse contra amenazas emergentes.

1.9.9.2 Enfoque en resiliencia cibernética

La resiliencia cibernética va más allá de la protección preventiva, enfocándose en la capacidad de una organización para recuperarse rápidamente de incidentes de seguridad. Esto incluye estrategias de respaldo y simulaciones periódicas de ataques. Según ENISA (2021), las organizaciones que invierten en resiliencia reducen significativamente el impacto financiero y operativo de los ciberataques. EP-EMSEGURIDAD podría integrar estos principios en su plan de seguridad, asegurando no solo la protección de sus sistemas, sino también la continuidad de sus servicios esenciales.

Capítulo II. Diagnóstico situacional

2.1 Metodología

2.1.1 Enfoque y diseño de la investigación

El análisis de datos se realizó siguiendo un enfoque mixto, combinando métodos cuantitativos y cualitativos para abordar de manera integral la problemática de la seguridad de la información en EP-EMSEGURIDAD. Para el componente cuantitativo, se utilizó un software especializado como SPSS, permitiendo obtener estadísticas descriptivas sobre variables clave como el nivel de cumplimiento de las políticas de seguridad, la frecuencia de incidentes de seguridad y el porcentaje de recursos asignados a ciberseguridad. Este análisis proporcionó una visión objetiva y medible del estado actual de la seguridad.

En cuanto al componente cualitativo, se realizaron entrevistas semiestructuradas y temáticas para evaluar la percepción de los empleados sobre la efectividad de las políticas de seguridad, la calidad de la capacitación en ciberseguridad y las amenazas identificadas. La interpretación de estos datos cualitativos permitió comprender los factores contextuales y subjetivos que influyen en la seguridad de la organización. La integración de ambos enfoques facilitó el desarrollo de propuestas sólidas y alineadas con las necesidades específicas de EP-EMSEGURIDAD, abordando tanto las dimensiones técnicas como humanas de la problemática.

El diseño no experimental se utiliza cuando no se manipulan las variables del entorno, lo que implica que el investigador observa los fenómenos tal como ocurren de manera natural. En este estudio, no se modificaron las políticas de seguridad de EP-EMSEGURIDAD, sino que se recopiló información sobre su estado actual, permitiendo una evaluación objetiva. Este enfoque facilitó la identificación de brechas en las medidas de seguridad sin intervenir directamente en el sistema. De esta forma, se obtuvo una precisa de las áreas de visión que requieren atención. El diseño transversal se caracteriza por la recopilación de datos en un solo

momento o en un corto período de tiempo. Esto fue esencial para realizar un análisis puntual de la seguridad en EP-EMSEGURIDAD.

2.1.2 Tipo de investigación

El tipo de investigación puede clasificarse como exploratoria, descriptiva o explicativa (Gallardo, 2017). Este estudio fue descriptivo, ya que se centró en analizar la situación actual de la seguridad de la información en EP EMSEGURIDAD, detallando políticas, riesgos y vulnerabilidades existentes. Este tipo de investigación permitió identificar las debilidades y amenazas que enfrenta la empresa en materia de seguridad de la información, cumpliendo con el objetivo de generar políticas específicas para proteger los activos digitales y operativos. Además, se empleó para describir los resultados obtenidos en la encuesta y el procesamiento de la información.

2.1.3 Población

La población del estudio estuvo conformada por 5 empleados del Departamento de Dirección de Tecnologías de la Información y Telecomunicaciones de la empresa EP EMSEGURIDAD, quienes tienen responsabilidades relacionadas con la gestión, implementación y uso de sistemas informáticos y de telecomunicaciones. Este grupo incluye tanto técnicos como personal administrativo con acceso y manejo de información sensible.

Para la población de estudio, se recopilaron datos como correos electrónicos: y números de teléfonos para la distribución del link de encuesta mediante WhatsApp de los sujetos de la investigación. Los cuales permitieron obtener una visión detallada de los procedimientos y prácticas actuales relacionados con la seguridad de la información. Esta recopilación de datos facilitó la obtención de información a la población de estudio, sobre la identificación de patrones, fortalezas y debilidades dentro de la organización, proporcionando una base sólida para el desarrollo de propuestas de mejora.

2.1.4 Técnicas e instrumentos

Las técnicas e instrumentos utilizados para el estudio fueron:

- **Encuestas dirigidas al personal TIC de EP-EMSEGURIDAD**

  Instrumento: Formularios de Google

  Técnica: Cuestionario estructurado: Las encuestas se administraron a través de Google Forms, una plataforma digital que permite crear formularios con preguntas prediseñadas. La técnica utilizada fue el cuestionario estructurado, que consistió en formular preguntas cerradas y escalas de evaluación para recopilar datos sobre las prácticas actuales, vulnerabilidades percibidas y el nivel de conocimiento en seguridad de la información por parte del personal TIC. Esta técnica facilitó la obtención de datos cuantitativos y permite un análisis comparativo de las respuestas.

- **Revisión de literatura sobre ataques de correo electrónico**

  Instrumento: Artículos, informes y documentos de ciberseguridad

  Técnica: Revisión documental: La revisión documental se utilizó como técnica para analizar artículos e informes nacionales e internacionales de ciberseguridad. Este proceso permitió comprender las amenazas específicas relacionadas con los ataques de correo electrónico que afectan a la empresa. Los documentos revisados proporcionaron una base teórica que facilitó la identificación de los riesgos relevantes a los que están expuestos EP-EMSEGURIDAD en términos de seguridad informática.

- **Políticas de seguridad basadas en la norma ISO 27001**

  Instrumento: Norma ISO 27001

  Técnica: Análisis normativo: El análisis normativo se utilizó para revisar los estándares internacionales de la norma ISO 27001, que proporciona un marco de referencia para la gestión de la seguridad de la información. Este análisis ayudó a identificar las mejores prácticas y directrices para desarrollar un PSI adecuado para

EP-EMSEGURIDAD, alineado con los estándares internacionales.

2.1.5 Procesamiento de datos

El procesamiento de los datos recopilados en este estudio se estructuró en dos etapas principales, cada una orientada a maximizar la precisión y utilidad de los resultados para diseñar el PSI. En la primera etapa, los datos cuantitativos se analizaron mediante el uso de software estadístico como SPSS, generando estadísticas descriptivas y correlaciones entre variables clave, como el nivel de cumplimiento de políticas de seguridad, la frecuencia de incidentes y la asignación de recursos. Esto permitió identificar patrones y medir de manera objetiva el estado actual de la seguridad de la información.

En la segunda etapa, los datos cualitativos se procesaron mediante un análisis temático, utilizando herramientas para identificar tendencias y categorías emergentes a partir de entrevistas y observaciones. Este análisis se centró en la percepción de los empleados sobre la efectividad de las políticas de seguridad, la calidad de las capacitaciones y las amenazas percibidas. La integración de ambos enfoques permitirá obtener una visión holística de la situación actual y fundamentará el diseño de un PSI adaptado a las necesidades específicas de EP-EMSEGURIDAD.

- **Encuestas**

Las encuestas como técnica de recopilación de información de este estudio estuvieron dirigidas personal del Departamento de Tecnologías de la Información y Telecomunicaciones de EP EMSEGURIDAD fueron diseñadas y administradas a través de la plataforma en línea Google Forms. Esta herramienta permitió recopilar datos de manera eficiente, facilitando la participación de los empleados y asegurando un proceso de recolección organizado y estructurado.

Así mismo, admitió la entrega de los datos procesados con el software SPSS representado en gráficos los valores estadísticos calculando frecuencias, promedios y

distribuciones para comprender la percepción del personal sobre las medidas de seguridad actuales a fin de resumir la información de forma esquematizada y otorgó facilidad para la redacción de los resultados. El procesamiento estadístico no solo identificó las áreas vulnerables en los sistemas y procesos de la empresa, sino que también proporcionó evidencia cuantitativa para priorizar acciones en el diseño del PSI.

- **Plan de Seguridad de la Información (PSI)**

Los resultados obtenidos de las encuestas se integraron con un análisis cualitativo de las políticas de seguridad existentes y un estudio detallado de los ataques documentados a nivel nacional. Se evaluaron las medidas actuales de seguridad en comparación con los estándares establecidos por la norma ISO 27001, identificando brechas que pudieran comprometer la integridad de los datos. Con base en reportes y literatura revisada, se estableció un panorama claro de las amenazas específicas que afectan a empresas similares, como el phishing y el malware, lo que enriqueció la identificación de riesgos.

Los resultados cuantitativos y cualitativos se utilizaron como base para la discusión de los hallazgos y para diseñar políticas, procedimientos y herramientas específicas para la empresa, asegurando que el PSI se alineara tanto con las necesidades internas como con las amenazas externas.

2.1.6 Procesamiento para el desarrollo del Plan de Seguridad de la Información (PSI)

En este apartado se describieron las fases que conllevaron el desarrollo del PSI para el cumplimiento del objetivo de diseñar un plan de seguridad de la información para el departamento de TICs de EP-EMSEGURIDAD, con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos críticos, alineándose con estándares internacionales como ISO/IEC 27001

Fase 1: Evaluación de riesgos y activos: Se identificaron y clasificaron los activos tecnológicos de EP EMSEGURIDAD, asignando prioridades según su importancia operativa.

Se documentaron las vulnerabilidades y dependencias de cada activo.

Fase 2: Análisis de amenazas y vulnerabilidades: Se llevó a cabo un análisis exhaustivo de posibles amenazas como ciberataques, errores humanos y fallos técnicos. Este análisis incluyó escenarios de impacto potencial en los sistemas y servicios esenciales (ver anexo 1).

Fase 3: Desarrollo de políticas y procedimientos de seguridad: Se formularon políticas claras basadas en ISO 27001, que incluyen: a. Gestión y renovación de contraseñas. b. Reglas de acceso restringido a sistemas críticos. c. Estrategias de protección contra malware y d. Políticas de cifrado de datos sensibles (ver anexo 2).

Fase 4: Implementación de medidas de seguridad: La instalación y configuración de herramientas como cortafuegos avanzados y sistemas de detección de intrusos (IDS) fueron el resultado de un análisis riguroso basado en estudios y experiencias previas implementadas en otras instituciones con retos similares. Estas acciones permitieron identificar las mejores prácticas y adaptar las soluciones más efectivas para el contexto organizacional.

Además, se dictaminan procedimientos de respuesta rápida ante incidentes, fundamentados en metodologías comprobadas, que garantizan una reacción eficiente frente a eventos de seguridad. Este proceso incluyó la capacitación del personal, enfatizando la importancia de la seguridad de la información, con el objetivo de fomentar una cultura organizacional alineada con los estándares más altos en protección de datos.

Fase 5: Respuesta ante incidentes: Los protocolos diseñados para manejar eventos como ciberataques o fallos críticos, incluyendo procesos de recuperación de datos y restauración de operaciones, se fundamentaron en marcos de referencia ampliamente reconocidos en la industria. Entre ellos se destaca el *NIST Cybersecurity Framework*, que proporciona un enfoque estructurado basado en los pilares de identificar, proteger, detectar, responder y recuperar, y las recomendaciones de la norma ISO/IEC 27001, enfocada en la

gestión de la seguridad de la información. .

Se tomó como base las mejores prácticas descritas en publicaciones de organismos como ISACA, específicamente el marco COBIT, el cual ofrece lineamientos claros para la gobernanza y gestión de TI. Estas referencias garantizan que los protocolos diseñados no solo sean efectivos, sino que también estén alineados con estándares internacionales, permitiendo una implementación robusta y adaptable a las necesidades específicas de la organización.

Fase 6: Monitoreo y revisión continua: En esta etapa, se dejó planteada la realización de auditorías periódicas, análisis de logs y pruebas de penetración como actividades esenciales para garantizar que las políticas y del PSI evolucionen frente a nuevas amenazas emergentes. Sin embargo, dada la complejidad de su implementación inicial, se priorizó establecer un marco teórico y operativo que sirva de base para futuras ejecuciones de estas actividades.

Este enfoque permite a la organización prepararse de manera progresiva, asegurando los recursos y la capacitación necesaria para realizar estas tareas de manera efectiva en el mediano plazo. Así, se plantea un esquema flexible que puede ser adaptado según las capacidades y prioridades emergentes de la institución, manteniendo el compromiso con la mejora continua de la seguridad de la información.

2.1.7 Procedimientos éticos

Se garantizó el cumplimiento de principios éticos fundamentales, comenzando con la obtención del consentimiento informado por escrito, explicando a los participantes el propósito del estudio, la voluntariedad de su participación, la confidencialidad de sus datos y su derecho a retirarse en cualquier momento. Se protegió la privacidad mediante el uso de códigos o seudónimos, almacenamiento seguro de datos y destrucción posterior a su análisis. Además, se actuó con transparencia, evitando cualquier tipo de manipulación o discriminación, y cumpliendo las normativas legales aplicables, como la LOPD o el GDPR.

Finalmente, los resultados fueron utilizados de forma responsable, exclusivamente para los fines establecidos, asegurando el respeto hacia los participantes y la integridad del estudio.

2.2 Análisis situacional

2.2.1 Resultados de la encuesta

A partir de los datos recopilados en la encuesta se exponen a continuación lis resultados esquematizados y sistematizados:

Figura 1

Área de trabajo dentro de EP EMSEGURIDAD



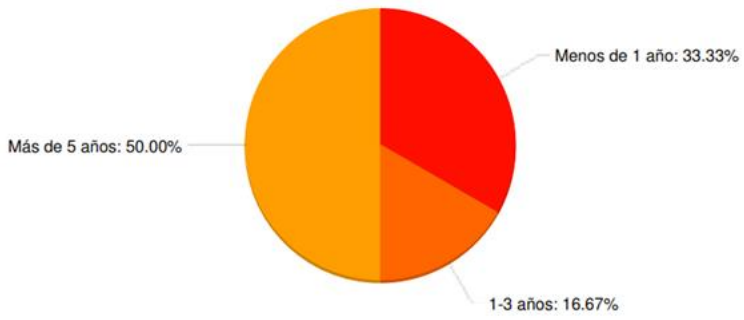
Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la figura 1 se evidencia que el 83.3% de los participantes pertenecen a la Dirección de Tecnologías de la Información y Telecomunicaciones, mientras que un 16.7% proviene de otra área (Jurídico). Esto evidencia una concentración significativa de encuestados en un departamento directamente relacionado con la seguridad de la información. La distribución refleja una visión técnica predominante, pero deja fuera perspectivas valiosas de áreas como Administración. Este enfoque limitado podría afectar la implementación de medidas globales de seguridad. Incorporar más áreas en futuras encuestas podría enriquecer la estrategia,

promoviendo un análisis más inclusivo y efectivo en términos organizacionales. La importancia de un plan de seguridad de la información radica en resguardar datos críticos y asegurar que las operaciones sigan estándares internacionales como ISO/IEC 27001 y GDPR.

Figura 2

Años de experiencia en la empresa

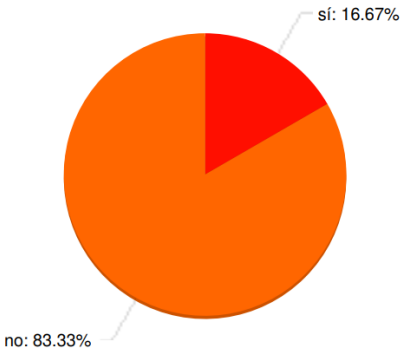


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 2 refleja que el 50% de los encuestados tiene más de 5 años en la empresa, el 33.3% menos de 1 año, y el 16.7% entre 1 y 3 años. Esto indica una mayoría con experiencia prolongada, positiva para evaluar políticas a largo plazo. Sin embargo, el 33.3% con menos de un año sugiere una necesidad de capacitaciones iniciales específicas para integrar a los nuevos empleados en las prácticas de seguridad establecidas. Diseñar programas ajustados a los niveles de experiencia es clave para fomentar una cultura sólida de seguridad en la empresa. Un plan bien estructurado fortalece la gestión de sistemas y equipos físicos, garantizando operaciones eficientes y un entorno seguro**.**

Figura 3

¿Conoce las políticas de seguridad de la información actuales en EP EMSEGURIDAD?

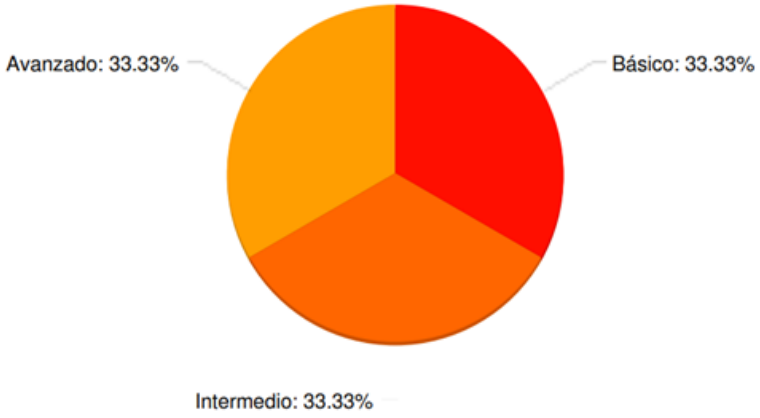


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la figura 3 se observa que el 83.3% de los participantes indicó no conocer las políticas actuales de seguridad de la información, lo cual es alarmante. Este desconocimiento generalizado puede ser un punto crítico de vulnerabilidad. La falta de familiarización implica que los protocolos establecidos no están siendo comunicados de manera efectiva. Mejorar los canales de difusión y garantizar que todos los empleados reciban información clara y accesible es esencial para fortalecer la cultura de seguridad y minimizar riesgos innecesarios. Este desconocimiento subraya la necesidad de un plan integral que fomente el cumplimiento regulatorio y la protección de datos empresariales.

Figura 4

¿Cómo calificaría su nivel de conocimiento?

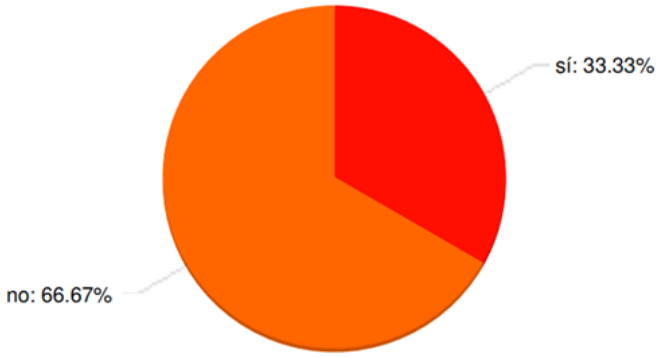


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 4 muestra que los encuestados se dividen equitativamente entre niveles básico, intermedio y avanzado, cada uno con un 33.3%. Esto sugiere una distribución equilibrada de competencias entre el personal, pero también destaca la necesidad de programas formativos adaptados a estos niveles. Implementar capacitaciones diferenciadas por nivel garantizaría un desarrollo uniforme de habilidades en seguridad, promoviendo la eficiencia y reduciendo posibles brechas de conocimiento dentro del equipo. Integrar estas capacitaciones en un plan global fortalecerá tanto la cultura de seguridad como el uso adecuado de recursos tecnológicos.

Figura 5

¿Ha recibido capacitación específica sobre seguridad de la información en los últimos 12 meses?

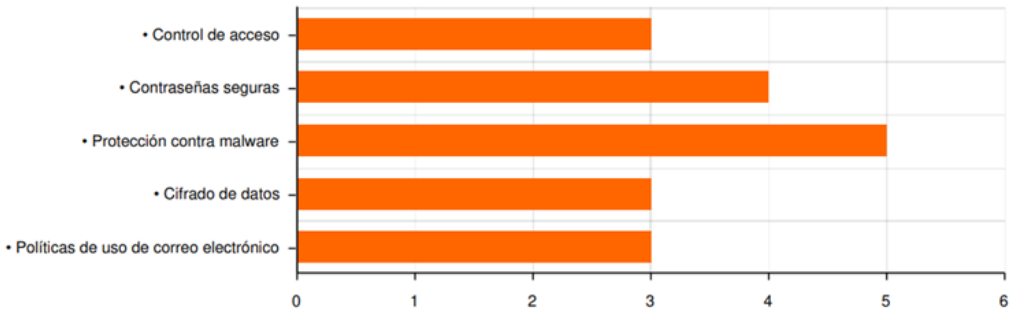


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 5 refleja que el 66.7% de los encuestados no ha recibido capacitación específica en seguridad de la información en los últimos 12 meses. Esta falta de formación reciente representa una oportunidad perdida para actualizar conocimientos y adaptarse a nuevas amenazas. Establecer un plan de capacitación continuo es fundamental para mantener al personal al día frente a los constantes cambios y desafíos en ciberseguridad. Esto no solo aumentaría la preparación técnica, sino también la confianza organizacional. Este enfoque asegura el cumplimiento de estándares internacionales y fortalece la cultura organizacional en seguridad.

Figura 6

¿Qué aspectos consideran más importantes para garantizar la seguridad de la información en la empresa?

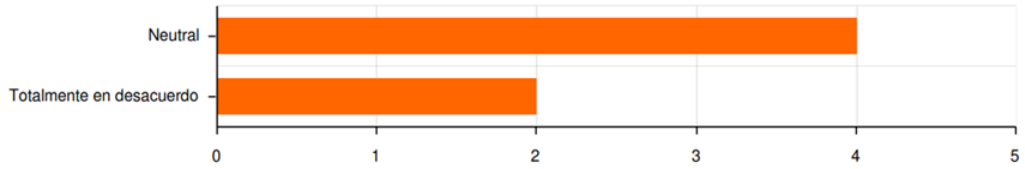


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la figura 6 se evidencia que las prioridades incluyen la protección contra malware (83.3%), contraseñas seguras (66.7%), y el control de acceso (50%). Estas respuestas reflejan una comprensión adecuada de los riesgos principales. Sin embargo, otros aspectos, como la educación del usuario y el uso adecuado del correo electrónico (50%), no deben subestimarse. La empresa podría beneficiarse de un enfoque más holístico que integre tanto medidas técnicas como concienciación para fortalecer la seguridad general. Un plan robusto incluirá estas prioridades y fomentará el cumplimiento de normas internacionales.

Figura 7

¿Considera que las políticas actuales son suficientes para proteger la información de la empresa?

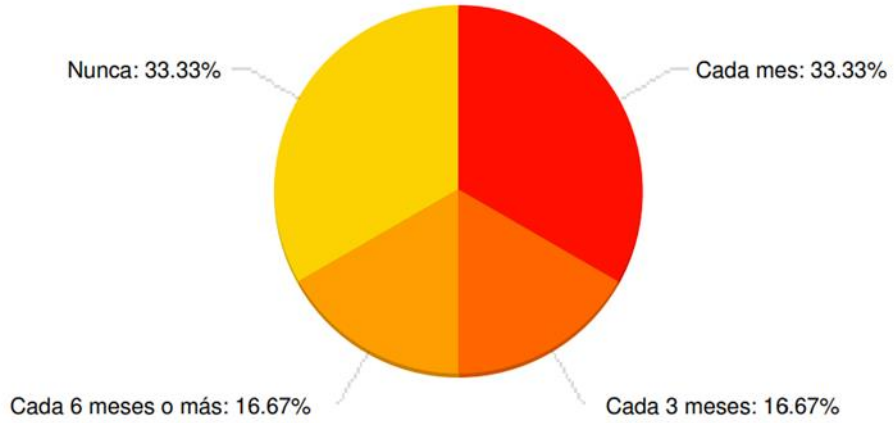


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 6 refleja que el 66.7% de los encuestados se mantiene neutral sobre si las políticas actuales son suficientes, y un 33.3% está totalmente en desacuerdo. Esta percepción indica insatisfacción o falta de confianza en las medidas existentes. Realizar auditorías internas y fomentar la participación del personal en la evaluación y rediseño de políticas podría ser un paso crucial para mejorar tanto la percepción como la efectividad de estas medidas. Esto refuerza la necesidad de un plan que asegure un entorno eficiente y seguro de operación.

Figura 8

¿Con qué frecuencia actualizan sus contraseñas de acceso a los sistemas de la empresa?

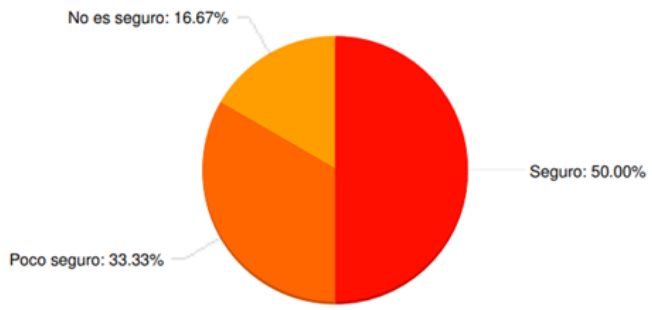


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la figura 8 se evidencia que el 33.3% nunca actualiza sus contraseñas, mientras que solo un 33.3% lo hace mensualmente. Esto expone un riesgo considerable, ya que contraseñas no actualizadas son más vulnerables a ataques. Implementar políticas obligatorias que incluyan recordatorios automáticos y plazos estrictos para la renovación periódica sería crucial para mitigar este riesgo y fortalecer la seguridad. Estas medidas deben formar parte de un plan de seguridad integral que resguarde la información crítica de la empresa.

Figura 9

¿Qué tan seguro considera que es el sistema de correo electrónico institucional frente a ataques externos como phishing?



Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 9 refleja que el 50% considera seguro el sistema de correo, mientras que el 33.3% lo percibe como poco seguro y el 16.7% como inseguro. Estas variaciones reflejan una falta de consenso y confianza. Refuerzos técnicos, como filtros avanzados contra phishing, y campañas de concienciación podrían mejorar tanto la seguridad como la percepción del sistema. Esto es esencial, dado que el correo institucional es un recurso crítico en la comunicación organizacional. Incluir estas medidas en un plan global garantiza un entorno digital más protegido.

Figura 10

¿Ha detectado algún incidente de seguridad relacionado con el uso de sistemas o datos en la empresa?

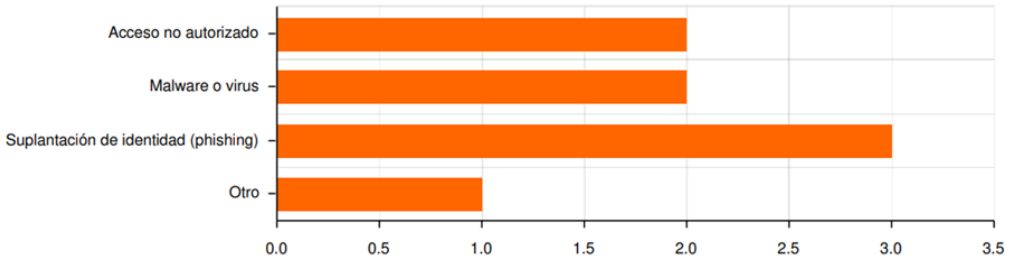


Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La figura 10 muestra que, el 50% de los encuestados ha detectado incidentes de seguridad, siendo la suplantación de identidad (phishing) el más reportado (50%). Este hallazgo subraya la urgencia de implementar programas de concienciación y herramientas específicas para combatir este tipo de amenaza. Adicionalmente, desarrollar un protocolo claro para reportar y gestionar incidentes puede minimizar el impacto de futuros ataques. Estas acciones integradas en un plan global aseguran operaciones más seguras y conformes con regulaciones internacionales

Figura 11

¿Qué tipo de incidente ocurrió?



Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la figura 11 se observa que, las principales propuestas incluyen capacitación continua, auditorías periódicas y cambios en el esquema de seguridad. Estas recomendaciones reflejan un consenso claro sobre las áreas prioritarias. Abordar estas sugerencias mediante un plan estructurado, con indicadores medibles, y promoviendo la participación de los empleados podría mejorar significativamente la seguridad de la información y la confianza en los sistemas actuales. El plan fortalecerá también el uso adecuado de equipos y sistemas, creando un entorno seguro y eficiente.

Tabla 3

En su opinión, ¿qué medidas adicionales deben implementarse para fortalecer la seguridad de la información?

Dato	Resultado
Capacitación realizada	40%
Sin capacitación	60%

Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la tabla 3 el análisis muestra que el 60% de los empleados no ha recibido capacitación, lo que pone en evidencia una brecha crítica en la preparación frente a ciberataques y otras amenazas digitales. Esta falta de entrenamiento no solo incrementa la exposición a riesgos, sino que también afecta la capacidad de respuesta del equipo. Un plan de seguridad debe incluir módulos de capacitación regulares que aborden aspectos técnicos y prácticos, garantizando que todo el personal esté preparado para identificar y mitigar amenazas. Además, este tipo de capacitaciones fomenta una cultura de seguridad proactiva y alineada con estándares internacionales como ISO/IEC 27001, fortaleciendo la resiliencia organizacional ante posibles incidentes.

Tabla 4

¿Considera importante recibir capacitación periódica sobre seguridad de la información? Explique brevemente:

Dato	Resultado
Sistema con riesgo	45%
Sin percepción de riesgo	55%

Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La tabla 4 muestra que el 45% de los encuestados considera que los sistemas presentan riesgos elevados, lo que resalta la necesidad de evaluaciones periódicas de infraestructura digital y auditorías técnicas. Por otro lado, el 55% que no percibe riesgos puede estar subestimando posibles vulnerabilidades. Este dato refleja la importancia de implementar campañas de sensibilización para garantizar que todos los empleados sean conscientes de los riesgos inherentes a los sistemas que utilizan. Integrar estas acciones en un plan estratégico ayuda no solo a identificar fallos críticos, sino también a diseñar soluciones preventivas alineadas con los mejores estándares de seguridad.

Tabla 5

¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD?

Dato	Resultado
Políticas adecuadas	30%
Necesitan actualización	70%

Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

En la tabla 5 se observa que una mayoría del 70% de los encuestados opina que las políticas de seguridad necesitan ser actualizadas, lo cual indica una desconexión entre las normativas actuales y los desafíos operativos. Esto enfatiza la necesidad de una revisión exhaustiva que considere los cambios en el entorno tecnológico y las amenazas emergentes. Además, garantizar que estas actualizaciones estén respaldadas por estándares internacionales como el GDPR e ISO/IEC 27001 es crucial para mantener la relevancia y eficacia de las políticas. Un plan de seguridad robusto debe priorizar estas revisiones como un componente esencial para mitigar riesgos organizacionales.

Tabla 6

¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD?

Dato	Resultado
Respuesta rápida	60%
Retrasos en respuesta	40%

Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La tabla 6 evidencia que, aunque el 60% de los encuestados percibe que las respuestas ante incidentes son rápidas, el 40% restante experimenta demoras, lo cual puede generar un impacto negativo en la contención de incidentes. Estas cifras subrayan la necesidad de implementar protocolos claros y herramientas automatizadas que permitan una reacción inmediata ante amenazas. Además, el fortalecimiento de los equipos de respuesta con capacitación específica y recursos tecnológicos avanzados puede reducir significativamente el tiempo de recuperación. Estas medidas deben ser parte integral del plan general de seguridad.

Tabla 7

¿Tiene alguna sugerencia específica para mejorar las políticas de seguridad actuales?

Dato	Resultado
Conocimiento avanzado	50%
Requieren soporte	50%

Nota: Datos obtenidos de la aplicación de la encuesta a los colaboradores EP EMSEGURIDAD. Elaboración propia. (2024)

La tabla 7 muestra que, el balance entre quienes poseen conocimientos avanzados (50%) y aquellos que requieren soporte (50%) indica una distribución desigual en términos de competencias digitales. Para abordar esta disparidad, es necesario implementar un programa de formación escalonado que se adapte a las necesidades de cada grupo.

Este enfoque garantizará que todos los empleados puedan operar eficientemente los sistemas críticos y contribuir a una gestión segura de la información. Además, este tipo de capacitaciones fomenta un entorno colaborativo donde los empleados con mayor experiencia pueden actuar como mentores, fortaleciendo el equipo en su conjunto.

Capítulo III. Propuesta

3.1 Titulo y presentación de la propuesta

Plan de Seguridad para el Departamento de Dirección de Tecnologías de la Información y Telecomunicaciones de EP-EMSEGURIDAD

Figura 12

Portada del PSI



Plan de Seguridad para el Departamento de Dirección de Tecnologías de la Información y Telecomunicaciones de EP-EMSEGURIDAD

Fecha de Emisión: Enero 2025

Responsable: Juan David Mejía Donoso

Presentación

La Empresa Pública Metropolitana de Seguridad (EP-EMSEGURIDAD) enfrenta importantes retos en la gestión de la seguridad de la información debido a la creciente sofisticación de las amenazas digitales. Este documento detalla un plan integral de seguridad diseñado para salvaguardar los recursos informáticos y los datos sensibles de la organización. Basado en los principios de la norma ISO/IEC 27001, este plan establece políticas, procedimientos y estrategias que garantizan la confidencialidad, integridad y disponibilidad de la información. El objetivo es construir un sistema robusto y resiliente que se anticipe y responda de manera efectiva a las amenazas internas y externa.

Introducción

La seguridad de la información es un pilar fundamental para el correcto funcionamiento de las actividades de EP-EMSEGURIDAD. Este plan busca abordar las vulnerabilidades existentes y establecer un marco estratégico que garantice la protección de los datos críticos. En la actualidad, la ausencia de políticas claras y procedimientos estandarizados aumenta la exposición de la organización a ataques cibernéticos y pérdidas de información.

El documento se estructura en varias secciones que cubren desde la definición de funciones y responsabilidades hasta las acciones específicas para la recuperación ante incidentes. Este enfoque integral está alineado con las mejores prácticas internacionales y los requerimientos legales aplicables.



Funciones y responsabilidades

- **Director del Departamento de TICs:** Responsable de supervisar la implementación del plan de seguridad, garantizar el cumplimiento de las políticas y liderar las estrategias de respuesta a incidentes.
- **Equipo de Seguridad Informática:** Encargado de realizar evaluaciones de riesgos, implementar controles técnicos y monitorear el entorno digital para prevenir intrusiones.
- **Personal Operativo:** Responsable de cumplir con las políticas establecidas y reportar cualquier actividad sospechosa o incidente de seguridad.
- **Auditor de Seguridad:** Realiza auditorías periódicas para evaluar la efectividad de las medidas implementadas y proponer mejoras.



Gestión de riesgo

La gestión de riesgos constituye el eje central del plan de seguridad. Se identifica, analiza y prioriza cada riesgo potencial para establecer medidas de mitigación adecuadas.

Tabla 8

Matriz gestión de riesgo

Nivel de riesgo	Aspecto Evaluado	Medida recomendada
Crítico	Evaluaciones de infraestructura digital	**Programar auditorías trimestrales para verificar el estado de hardware, software y conexiones.**
Crítico	Monitoreo y respuesta a incidentes	**Instalar herramientas avanzadas de monitoreo y definir procesos claros de respuesta rápida ante incidentes.**
Alto	Percepción general de riesgos en sistemas.	**Realizar encuestas y reuniones para identificar áreas específicas de preocupación y priorizar acciones de mejora.**
Alto	Auditorías técnicas de seguridad	**Implementar un calendario de auditorías técnicas con profesionales internos y externos, alineado con normas como ISO/IEC 27001.**
Alto	Capacitación del personal	**Diseñar e implementar programas de formación continua sobre prácticas de ciberseguridad, incluyendo simulacros de ataques.**
Alto	Protección contra amenazas externas	**Integrar soluciones de protección avanzada, como firewalls, IDS/IPS, y realizar campañas de concientización sobre amenazas específicas.**
Medio	**Políticas de seguridad documentadas**	**Revisar, actualizar y comunicar las políticas de seguridad a todo el personal, asegurando que sean claras y accesibles.**

Nota: Matriz para la gestión de riesgo de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 9

Matriz de priorización de medidas

Nivel de riesgo	Aspecto Evaluado	Medida recomendada	Dominio ISO 27001
Crítico	Evaluaciones de infraestructura digital	Programar auditorías trimestrales para verificar el estado de hardware, software y conexiones.	**A.12: Operación de la seguridad de la información**
Crítico	Monitoreo y respuesta a incidentes	Instalar herramientas avanzadas de monitoreo y definir procesos claros de respuesta rápida ante incidentes.	**A.16: Gestión de incidentes de seguridad de la información**
Alto	Percepción general de riesgos en sistemas.	Realizar encuestas y reuniones para identificar áreas específicas de preocupación y priorizar acciones de mejora.	**A.6: Organización de la seguridad de la información**
Alto	Auditorías técnicas de seguridad	Implementar un calendario de auditorías técnicas con profesionales internos y externos, alineado con normas como ISO/IEC 27001.	**A.18: Cumplimiento**
Alto	Capacitación del personal	Diseñar e implementar programas de formación continua sobre prácticas de ciberseguridad, incluyendo simulacros de ataques.	**A.7: Gestión de los recursos humanos**
Alto	**Protección contra amenazas externas**	**Integrar soluciones de protección**	**A.9: Control de acceso y A.10:**

		avanzada, como firewalls, IDS/IPS, y realizar campañas de concientización sobre amenazas específicas.	**Criptografía**
Medio	Políticas de seguridad documentadas	Revisar, actualizar y comunicar las políticas de seguridad a todo el personal, asegurando que sean claras y accesibles.	**A.5: Política de seguridad de la información**

Nota: Matriz de priorización de medidas para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

La gestión efectiva de los recursos digitales incluye la clasificación y protección de datos, así como el control de acceso a los sistemas críticos.

- **Clasificación de datos:** Todos los datos deben ser categorizados según su nivel de sensibilidad (público, interno, confidencial, restringido).
- **Control de acceso:** Se establecerán permisos basados en el principio de privilegio mínimo, garantizando
    - que cada usuario acceda solo a la información necesaria.
- **Protección contra malware:** Se implementará software antivirus y sistemas de detección de intrusiones actualizados.
- **Respaldos periódicos:** Los respaldos se realizarán de forma automática y serán almacenados en ubicaciones seguras

Tabla 10

Medidas de seguridad

Medida de seguridad	Actividad	Descripción	Objetivo	Herramientas/Software Recomendados	Frecuencia
Clasificación de datos	Categorización de datos según nivel de sensibilidad: público, interno, confidencial, restringido.	Asignar niveles de sensibilidad para definir controles adecuados y evitar accesos no autorizados.	Proteger los datos más críticos y priorizar recursos de seguridad donde más se necesiten.	Herramientas de clasificación de datos (Varonis, Spirion).	Inicial, con revisiones anuales.
Control de acceso	Asignación de permisos basados en el principio de privilegio mínimo.	Garantizar que cada usuario tenga acceso únicamente a la información necesaria para sus funciones.	Reducir el riesgo de accesos indebidos y minimizar el impacto en caso de incidentes.	Directorio Activo, Okta, Soluciones IAM.	Permanente, con revisiones trimestrales.
Protección contra malware	Implementación de software antivirus y	Detectar, prevenir y eliminar amenazas	Proteger los sistemas de infecciones	Symantec, McAfee, CrowdStrike y Bitdefender.	Permanente, con actualizacio

	sistemas de detección de intrusiones actualizados.	de malware en tiempo real.	y ataques que comprometen la seguridad de los datos.		nes periódicas.
Respuesta periódica	Realización de respaldos automáticos y almacenamiento en ubicaciones seguras.	Asegurar la recuperación de datos en caso de pérdida, corrupción o ataques como ransomware.	Garantizar la continuidad operativa y minimizar el impacto de incidentes en los sistemas.	Acronis, Veeam, copia de seguridad de AWS, Google Drive.	Automáticos diarios o semanales, con pruebas de restauración trimestrales.

Nota: Matriz de medidas de seguridad para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)



Se establecen procedimientos claros para abordar las diversas etapas del ciclo de vida de la seguridad de la información.

- **Evaluación inicial:** Identificación de activos y valoración de riesgos asociados.

Tabla 11

Matriz que sintetiza los hallazgos del estudio y las recomendaciones para abordar los riesgos elevados en los sistemas identificados:

Aspecto Evaluado	Director de Hallazgo	Nivel de riesgo	Acción recomendada	Responsable	Plaza de Implementación
Percepción general de riesgos en sistemas.	Los encuestados consideran que los sistemas presentan riesgos elevados.	Alto	Realizar encuestas y reuniones para identificar áreas específicas de preocupación y priorizar acciones de mejora.	Departamento de TIC	**Corto plazo (1 mes)**
Evaluaciones de infraestructura digital	Falta de evaluaciones periódicas y detalladas sobre la infraestructura digital.	Crítico	Programar auditorías trimestrales para verificar el estado de hardware, software y conexiones.	Equipo de Seguridad Informática	**Trimestral**
Auditorías técnicas de seguridad	Ausencia de auditorías técnicas regulares para identificar vulnerabilidades críticas.	Alto	Implementar un calendario de auditorías técnicas con profesionales internos y externos, alineado con normas como ISO/IEC 27001.	Auditor de seguridad	**Plazo medio (3 meses)**
Capacitación del personal	Bajo nivel de conocimiento en medidas de ciberseguridad por parte del personal encuestado.	Alto	Diseñar e implementar programas de formación continua sobre prácticas de ciberseguridad, incluyendo simulacros de ataques.	RRHH y Departamento de TICs	**Corto plazo (2 meses)**
Monitoreo y respuesta a incidentes	**Los sistemas carecen de monitoreo constante para detectar actividades sospechosas en**	**Crítico**	**Instalar herramientas avanzadas de monitoreo y definir procesos claros de respuesta rápida**	**Equipo de Seguridad Informática**	**Corto plazo (2 meses)**

Protección contra amenazas externas	Implementación inadecuada de controles frente a ataques como phishing y malware.	Alto	Integrar soluciones de protección avanzada, como firewalls, IDS/IPS, y realizar campañas de concientización sobre amenazas específicas.	Departamento de TIC	Plazo medio (3 meses)
Políticas de seguridad documentadas	Falta de políticas claras y actualizadas sobre la seguridad de la información.	Medio	Revisar, actualizar y comunicar las políticas de seguridad a todo el personal, asegurando que sean claras y accesibles.	Dirección de TICs	Plazo medio (3 meses)

Nota: Matriz de hallazgos y recomendaciones para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

- **Implementación de controles:** Instalación de firewalls, configuración de redes seguras y autenticación de usuarios.
- **Monitoreo constante:** Supervisión en tiempo real de los sistemas y alertas de seguridad.
- **Auditorías regulares:** Revisiones periódicas para asegurar el cumplimiento de las políticas establecidas.

Tabla 12

Fases del PSI

Fase	Actividad	Descripción	Objetivo	Herramientas/Software Recomendados	Frecuencia
Evaluación inicial	Identificación de activos críticos. Valoración de riesgos asociados.	Determinar los sistemas, datos y equipos esenciales para las operaciones. Evaluar amenazas potenciales.	Priorizar acciones de protección según el impacto y probabilidad de riesgos.	RiskWatch, Qualys y Tenable.io.	Una vez al inicio y actualizaciones anuales.
Implementación de controles	Instalación de firewalls y segmentación de red. Configuración de autenticación segura.	Establecer medidas de protección para prevenir accesos no autorizados y mitigar riesgos detectados.	Crear una infraestructura segura y reducir vulnerabilidades.	Cisco Firepower, Palo Alto Networks, Fortinet.	Configuración inicial, con revisión trimestral.
Monitoreo constante	Supervisión en tiempo real de sistemas y alertas de seguridad.	Observe el comportamiento de la red y sistemas para detectar actividades sospechosas rápidamente.	Responder de forma inmediata a incidentes y prevenir daños mayores.	Splunk, Zabbix y SolarWinds.	Permanente.
Auditorias regulares	Revisiones de cumplimiento de políticas y efectividad de los controles.	Evaluar si las medidas implementadas siguen siendo eficaces y cumplen con los estándares.	Mantener un sistema actualizado y alineado con las mejores prácticas.	Nessus, OpenSCAP y Power BI.	Trimestral o según requerimientos normativos.

Nota: Matriz de fase para el PSI implementado a la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 13

Gestión de personal

Programa	Descripción	Frecuencia	Indicador
Capacitación en ciberseguridad	Talleres sobre phishing, contraseñas seguras y buenas prácticas.	Trimestral	Asistencia del 90% del personal.
Evaluaciones periódicas	Pruebas de conocimientos sobre políticas de seguridad.	Semestral	Puntajes promedio >80%.
Concientización	Campañas internas de sensibilización sobre seguridad.	Continuo	Participación
Certificaciones técnicas	Cursos avanzados para el equipo de TIC.	Anual	Incremento del certificado personal.

Nota: Matriz para la gestión de personal de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 14

Vulnerabilidades identificadas:

Vulnerabilidad identificada	Impacto en el diseño del PSI	Medida implementada en el PSI
Ausencia de auditorías técnicas regulares	Sin auditorías periódicas, las vulnerabilidades críticas no se detectan a tiempo, lo que pone en riesgo la seguridad.	**Se incorporó un programa de auditorías técnicas trimestrales, alineadas con las mejores prácticas de seguridad (ISO/IEC 27001).**
Falta de monitoreo constante	La falta de monitoreo en tiempo real dificulta la detección temprana de amenazas y actividades sospechosas.	**Se implementó un sistema de monitoreo avanzado con herramientas IDS/IPS para detectar amenazas en tiempo real.**
Bajo nivel de conocimiento sobre ciberseguridad entre el personal	Los empleados con poca formación en ciberseguridad son más susceptibles a ataques de phishing y errores humanos.	**Se diseñaron programas de capacitación continua en ciberseguridad y simulacros de ataques para mejorar la respuesta del personal.**
Protección inadecuada contra amenazas externas	La falta de protección avanzada facilita la entrada de malware y otros ataques externos.	**Se integraron firewalls, IDS/IPS y sistemas de autenticación multifactorial para fortalecer la defensa perimetral.**
Políticas de seguridad obsoletas o inexistentes	La ausencia de políticas claras puede llevar a decisiones incoherentes en cuanto a seguridad y manejo de incidentes.	**Se revisaron y actualizaron las políticas de seguridad, asegurando que fueran claras y accesibles a todo el personal.**
Deficiencias en la infraestructura digital	Una infraestructura desactualizada o sin auditoría pone en peligro la estabilidad y confiabilidad del sistema.	**Se planificó la actualización y mantenimiento continuo de la infraestructura digital, con evaluaciones trimestrales.**
Falta de una respuesta rápida ante incidentes	**La falta de procesos bien definidos ralentiza la respuesta ante incidentes, aumentando el impacto de los mismos.**	**Se definieron y documentaron procedimientos claros para la respuesta ante incidentes, estableciendo tiempos de reacción específicas.**

Nota: Matriz de vulnerabilidades de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Las vulnerabilidades identificadas llevaron a una mejora en el diseño del PSI mediante la implementación de auditorías periódicas, monitoreo avanzado, capacitación del personal, fortalecimiento de la protección externa, actualización de políticas de seguridad, y mejores procedimientos de respuesta ante incidentes.

Se implementan medidas para prevenir accesos no autorizados y garantizar la seguridad de los sistemas.

- Autenticación robusta: Uso de contraseñas complejas y autenticación multifactorial.
- Segmentación de red: División de redes para minimizar el impacto de posibles intrusiones.
- Sistemas de detección: Implementación de IDS/IPS para identificar y bloquear actividades sospechosas.
- Políticas de acceso remoto: Restricción y monitoreo del acceso a través de conexiones remotas.

Tabla 15

Medidas de seguridad

Medida de seguridad	Descripción	Objetivo	Tecnologías/Software Recomendados	Frecuencia
Autenticación robusta	Uso de contraseñas complejas combinadas con autenticación multifactorial (MFA).	Proteger el acceso a sistemas críticos, dificultando accesos no autorizados.	Autenticador de Google, seguridad Duo, autenticador de Microsoft	Permanente (configuración única).
Segmentación de red	División de la red en subredes aisladas para limitar el movimiento lateral de posibles atacantes.	Minimizar el impacto de posibles intrusiones y mejorar el control de acceso.	VLAN, Cisco Meraki, redes de Palo Alto	Configuración inicial y auditorías trimestrales.
Sistemas de detección (IDS/IPS)	Implementación de sistemas de detección/prevención de intrusos para identificar y bloquear actividades sospechosas.	Detectar ataques en tiempo real y prevenir accesos no autorizados.	Snort, Suricata y Cisco Firepower	Permanente, con actualizaciones periódicas.
Políticas de acceso remoto	Restricción y monitoreo del acceso a sistemas a través de conexiones remotas seguras (VPN, RDP).	Asegurar que solo usuarios autorizados accedan remotamente y evitar ataques externos.	OpenVPN, Fortinet, AnyConnect y Citrix Gateway	Permanente, pagos mensuales.

Nota: Matriz de medidas de seguridad para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Detección de ataques

El plan incluye estrategias para detectar ataques en sus etapas iniciales, minimizando su impacto.

1. **Monitoreo continuo:** Uso de herramientas avanzadas para supervisar el tráfico de red y detectar comportamientos anómalos.

Tabla 16

Herramientas para el monitoreo

Herramienta	Función	Frecuencia	Responsable	Indicador
SIEM	Monitoreo de eventos de seguridad	Continuo	Equipo de seguridad	Alertas tratadas en <24 h.
Antivirus corporativo	Protección contra malware	Continuo	Administrador de Sistemas	Detección de amenazas
Sistema de registros	Análisis y auditoría de logs	Diario	Analista de seguridad	Anomalías identificadas

Nota: Herramientas de monitoreo de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Análisis de registros: Revisión periódica de logs para identificar posibles incidentes.

Tabla 17

Revisión periódica

Etapa	Actividad	Descripción	Software recomendado	Frecuencia
Recopilación de datos	Centralizar los registros en un sistema único.	Recolectar registros de servidores, aplicaciones y dispositivos en un repositorio centralizado.	Splunk, pila ELK (Elasticsearch, Logstash, Kibana), Graylog	Permanente
Análisis automático	Implementar reglas para analizar patrones sospechosos.	Configurar reglas para identificar accesos no autorizados, errores críticos o	Splunk, herramientas SIEM (por ejemplo, IBM	Permanente

		comportamientos inusuales.	QRadar, ArcSight)	
Clasificación	Categorizar los incidentes por nivel de gravedad.	Etiquetar eventos críticos, moderados y leves para priorizar la atención.	ELK Stack, analizador de registros de SolarWinds	Diario
	Realizar auditorías periódicas de registros críticos.			
Manual de revisión	Complementar el análisis automático con revisión humanas para identificar patrones complejos o nuevos riesgos.		Cualquier herramienta SIEM, acceso manual a archivos	Semanal o según necesidad.
Generación de reportes	Crear informes sobre patrones recurrentes o incidentes identificados.	Documentar hallazgos y acciones correctivas tomadas, útiles para auditorías y análisis futuro.	Power BI, Tableau, Kibana	Mensual

Nota: Matriz para la revisión periódica dirigida a la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Alertas tempranas: Configuración de sistemas de notificaciones automáticas ante actividades sospechosas.

Sistemas de Notificaciones Automáticas

Tabla 18

SNA

Etapa	Actividad	Descripción	Software recomendado	Frecuencia
Configuración inicial	Definir eventos que activarán alertas.	Establecer umbrales y reglas específicas (ejemplo: intentos fallidos de inicio de sesión, cambios no autorizados).	Alertas de Zabbix, Nagios y Splunk	Configuración única inicial.

Integración	Conectar el sistema con plataformas de comunicación.	Vincular el sistema con correos, aplicaciones móviles o sistemas de mensajería instantánea como Slack o Teams.	PagerDuty, Opsgenie y Microsoft Teams	Configuración única inicial.
Pruebas de alertas	Eventos similares para verificar el correcto funcionamiento de las alertas.	Validar que los responsables reciban las notificaciones en tiempo real.	Cualquier herramienta SIEM	Mensual.
Automatización	Habilitar alertas automáticas basadas en datos en tiempo real.	Notificar de inmediato a los responsables ante actividades sospechosas o incidentes críticos.	Administrador de alertas Prometheus, Nagios, alertas Splunk	Inmediato.
Monitoreo y ajustes	Revisar y ajustar las reglas de notificación según nuevas amenazas.	Actualizar los parámetros de notificaciones basados en auditorías o cambios en el entorno de seguridad.	ELK Stack, herramientas SIEM	Trimestral.

Nota: Matriz para el SNA de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 19

Simulaciones de Ataques

Etapa	**Descripción**	**Responsable**	**Indicador de Éxito**
Planeación	Diseñar escenarios de ataque realistas.	Equipo de Respuesta	Escenarios aprobados.
Ejecución	Ataques similares (phishing, ransomware, etc.).	Consultor externo	Tiempos de respuesta medidos.
Evaluación	Analizar la efectividad de las respuestas implementadas.	Auditor interno	Informe de brechas cerradas.

Ajustes	Mejorar controles y procedimientos según resultados.	Director de TIC	Reducción de vulnerabilidades.

Nota: Matriz de las etapas de la simulación de ataques para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Respuesta a incidentes

La respuesta a incidentes es fundamental para minimizar el impacto de estos.

Plan de acción: Documento que describe las acciones a tomar en caso de incidentes de seguridad.

Tabla 20

Plan de Acción

Acción	Descripción	Responsable	Plazo	Indicador de Éxito
Desarrollo de políticas de seguridad	Crear y comunicar políticas claras para la protección de la información.	Director de TIC	1 mes	Políticas documentadas y aprobadas.
Implementación de controles técnicos	Instalar herramientas de monitoreo, firewalls y autenticación multifactorial.	Equipo de seguridad	2 meses	Reducción del acceso no autorizado.
Capacitación al personal	Realizar sesiones de formación en ciberseguridad.	Recursos humanos	Continuo	100% del personal capacitado anualmente.
Auditorías internas de seguridad	Evaluar la implementación y efectividad de las medidas de seguridad.	Auditor de seguridad	Trimestral	Informes con cumplimiento >90%.

Nota: Matriz del plan de acción de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 21

Comunicación interna

Nivel	Parte Interesada	Medio de Comunicación	Frecuencia	Contenido
Directiva	Alta Gerencia	Informes mensuales	Mensual	Progreso de seguridad.
Operativo	Personal de TIC	Correos electrónicos	Semanal	Actualización de políticas y riesgos.
General	Toda la organización	Boletines informativos	Trimestral	Campañas de concientización.

Nota: Matriz para la comunicación interna de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 22

Análisis Post-Incidente

Paso	Descripción	Responsable	Herramientas
Identificación	Documentar el incidente y las áreas afectadas.	Equipo de Respuesta	Sistema de tickets.
Análisis de causas	Determinar el origen del problema mediante revisión de registros.	Analista de seguridad	Herramientas de logs.
Evaluación de impacto	Cuantificar daños a datos y sistemas.	Auditor interno	Software de análisis.
Informe final	Redactar un reporte con aprendizajes y recomendaciones.	Director de TIC	Plantillas estándar.

Nota: Matriz para el análisis post – incidente de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Se establecen estrategias para garantizar la continuidad operativa de la organización tras un incidente

Tabla 23

Recuperación y continuidad de negocio

Área	Estrategia	Descripción	Objetivo	Responsables	Frecuencia/Plazo
Análisis de registros	1. Implementar un sistema centralizado de gestión de registros (SIEM). 2. Establecer rutinas de revisión manual y automática. 3. Clasificar y priorizar registros críticos (accesos no autorizados, errores críticos).	Revisar periódicamente los registros generados por sistemas, servidores y aplicaciones para detectar actividades inusuales.	Identificar posibles incidentes y prevenir brechas de seguridad.	Departamento de TI y Seguridad Informática	Diario para críticos, semanal para otros.
Alertas Tempranas	1. Configurar sistemas automáticos de monitoreo y alertas en tiempo real. 2. Definir umbrales para actividades sospechosas (accesos fallidos, cambios no autorizados). 3. Integrar notificaciones a plataformas móviles y correo.	Automatizar el proceso de identificación de actividades sospechosas y notificación al personal de manera inmediata.	Reduzca los tiempos de respuesta ante posibles incidentes y minimice los impactos.	Departamento de TI y Seguridad Informática	Inmediato (notificaciones en tiempo real).

Nota: Matriz para recuperación y continuidad del negocio de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Tabla 24

Plan de respaldo

Componente	Descripción	Frecuencia	Ubicación de Respaldo	Verificación
Respaldos automáticos	Copias diarias de bases de datos y archivos críticos.	Diario	Servidores en la nube	Verificación semanal.
Redundancia de hardware	Uso de espejos para sistemas críticos.	Continuo	Infraestructura local y remota	Pruebas de recuperación trimestrales.
Almacenamiento externo	Copias almacenadas en dispositivos físicos seguros.	Mensual	Ubicación fuera del sitio	Inspección bimestral.

Nota: Matriz del plan de respaldo de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

- Infraestructura redundante: Uso de sistemas alternativos para asegurar la disponibilidad de servicios esenciales.
- Simulacros: Ejercicios regulares para probar la eficacia de los planes de recuperación.
- Evaluación de daños: Análisis detallado del impacto del incidente y medidas para evitar recurrencias.

Tabla 25

Sintetización del PSI

Vulnerabilidad identificada	Impacto en el diseño del PSI	Medida implementada en el PSI	Dominio ISO 27001:2022
Ausencia de auditorías técnicas regulares	Sin auditorías periódicas, las vulnerabilidades críticas no se detectan a tiempo, lo que pone en riesgo la seguridad.	Se incorporó un programa de auditorías técnicas trimestrales, alineadas con las mejores prácticas de seguridad (ISO/IEC 27001).	A.18: Cumplimiento
Falta de monitoreo constante	La falta de monitoreo en tiempo real dificulta la detección temprana de amenazas y actividades sospechosas.	Se implementó un sistema de monitoreo avanzado con herramientas IDS/IPS para detectar amenazas en tiempo real.	A.16: Gestión de incidentes de seguridad de la información
Bajo nivel de conocimiento sobre ciberseguridad entre el personal	Los empleados con poca formación en ciberseguridad son más susceptibles a ataques de phishing y errores humanos.	Se diseñaron programas de capacitación continua en ciberseguridad y simulacros de ataques para mejorar la respuesta del personal.	A.7: Gestión de los recursos humanos
Protección inadecuada contra amenazas externas	La falta de protección avanzada facilita la entrada de malware y otros ataques externos.	Se integraron firewalls, IDS/IPS y sistemas de autenticación multifactorial para fortalecer la defensa perimetral.	A.9: Control de acceso, A.10: Criptografía
Políticas de seguridad obsoletas o inexistentes	La ausencia de políticas claras puede llevar a decisiones incoherentes en cuanto a seguridad y manejo de incidentes.	Se revisaron y actualizaron las políticas de seguridad, asegurando que fueran claras y accesibles a todo el personal.	A.5: Política de seguridad de la información
Deficiencias en la infraestructura digital	Una infraestructura desactualizada o sin auditoría pone en peligro la estabilidad y confiabilidad del sistema.	Se planificó la actualización y mantenimiento continuo de la infraestructura digital, con evaluaciones trimestrales.	A.12: Operación de la seguridad de la información
Falta de una respuesta rápida ante incidentes	La falta de procesos bien definidos ralentiza la respuesta ante incidentes, aumentando el impacto de los mismos.	Se definieron y documentaron procedimientos claros para la respuesta ante incidentes, estableciendo tiempos de reacción específicas.	A.16: Gestión de incidentes de seguridad de la información

Nota: Matriz para la gestión de vulnerabilidades de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

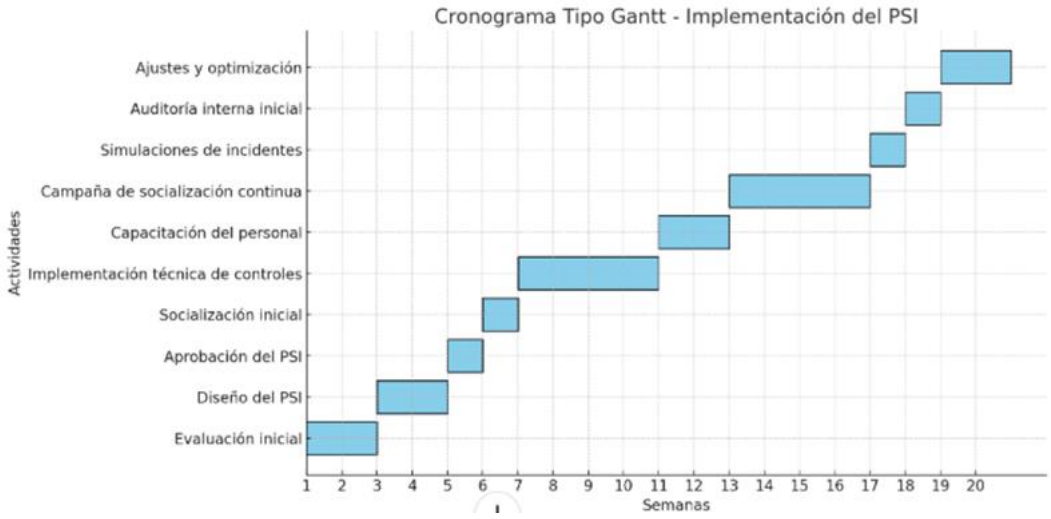
Consideraciones finales

El Plan de Seguridad Informática (PSI) conforme a la ISO 27001:2022, se convierte en un componente estratégico esencial para asegurar la protección de los activos digitales, la continuidad operativa y la integridad de la información dentro de cualquier organización. Las adoptadas, como la clasificación de datos, los controles de acceso basados en el principio de privilegio mínimo, y la protección activa contra amenazas cibernéticas medidas, se integran para mitigar los riesgos asociados a la confidencialidad, disponibilidad y autenticidad de los datos. La evaluación inicial de riesgos y la aplicación de controles adecuados, junto con el monitoreo constante de los sistemas, permiten anticiparse a vulnerabilidades y fortalecer la postura de seguridad.

Este enfoque también promueve una cultura de responsabilidad y cumplimiento normativo dentro de la organización, asegurando que todos los colaboradores estén alineados con los objetivos de seguridad. En conclusión, un PSI bien estructurado y ejecutado, alineado con la ISO 27001:2022, se presenta como una herramienta estratégica que refuerza la resiliencia de la organización frente a los riesgos del entorno digital, minimizando los impactos de incidentes y garantizando un entorno tecnológico seguro. y confiable para el desarrollo de las operaciones.

Figura 13

Cronograma de implementación del PSI



Nota: Cronograma de implementación del PSI para la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

Este plan busca involucrar a todos los niveles de la empresa en la comprensión y aplicación de las políticas y procedimientos del PSI, asegurando que todos los colaboradores actúen de manera responsable y efectiva ante posibles incidentes de seguridad.

Módulos para tratar en el plan

- Introducción al PSI y su importancia: Este módulo cubrirá la relevancia del Plan de Seguridad Informática (PSI), sus objetivos principales y cómo contribuye a la protección de los activos digitales, asegurando la confidencialidad, integridad y disponibilidad de la información.

- Buenas Prácticas de Seguridad: Se enseñarán los conceptos fundamentales de seguridad informática, como la creación de contraseñas seguras, el manejo de accesos y la identificación de amenazas cibernéticas comunes.
- Políticas y Procedimientos de Seguridad Informática: Se socializarán las políticas internas relacionadas con el PSI, las cuales definirán las acciones a seguir en caso de incidentes de seguridad y cómo deben ser manejados los datos sensibles.
- Simulaciones de Incidentes Cibernéticos: En este módulo se realizarán simulaciones prácticas (como ataques de phishing o ciberataques) para evaluar y mejorar la capacidad de respuesta ante incidentes reales.
- Capacitación Técnica Avanzada en Ciberseguridad: Un módulo dirigido al personal técnico de TI, en el que se actualizarán los conocimientos sobre las últimas amenazas y herramientas de protección, así como las normativas internacionales más recientes relacionadas con la seguridad informática.
- Cultura de Seguridad Informática: Campañas de concienciación que refuercen la importancia de una postura proactiva en seguridad informática, asegurando que todos los colaboradores estén alineados con los objetivos de seguridad.

Medición del impacto de la capacitación

Para medir el impacto de la capacitación y socialización del PSI, se tomarán en cuenta los siguientes indicadores:

- Evaluación de Comprensión: Luego de las charlas introductorias, se realizará una evaluación de comprensión con preguntas que verifiquen el nivel de comprensión de los

temas tratados. Se espera que al menos un 80% de los participantes respondan correctamente.

- Reducción de Incidentes: Se monitorizarán los incidentes de seguridad informática antes y después de los talleres prácticos. La capacitación debería generar una reducción significativa de los incidentes causados por errores humanos (con un objetivo de 30% de reducción en 6 meses).

- Cumplimiento en Auditorías Internas: Se medirá el grado de cumplimiento de las políticas y procedimientos del PSI a través de auditorías internas. El indicador de éxito será un nivel de cumplimiento superior al 90% en las auditorías anuales.

- Tiempo de Respuesta ante Incidentes: Durante los ejercicios de simulación, se evaluará el tiempo de respuesta y la efectividad de las acciones tomadas por el personal en escenarios de incidentes cibernéticos. Se espera que más del 80% de los participantes sigan correctamente los protocolos establecidos.

- Certificación de Capacitación: Los cursos avanzados de ciberseguridad para personal técnico serán medidos en función del número de participantes que obtendrán certificación o finalización exitosa. El objetivo es alcanzar un 90% de participación en los cursos de formación.

- Participación y Percepción: La efectividad de las campañas internas se medirá mediante encuestas de percepción y el nivel de participación en las actividades de concienciación. Se buscará que al menos el 85% de los empleados participen y muestren una percepción positiva sobre las acciones realizadas.

A continuación, se presenta el Plan de Capacitación y Socialización del Plan de Seguridad Informática (PSI) diseñado para sensibilizar, capacitar y socializar las medidas y prácticas que garantizan la seguridad de los sistemas de la organización.

Tabla 26

Plan de capacitación del PSI

Objetivo	Actividad	Descripción	Responsables	Objetivo público	Duración/Frecuencia	Indicadores de éxito
Sensibilizar sobre la importancia del PSI.	Charlas introductorias.	Presentar los objetivos y beneficios del PSI, enfocándose en la relevancia de la seguridad informática.	Equipo de TI, Recursos Humanos.	Todo lo personal.	1 sesión inicial (1 hora).	% de asistencia y evaluación de comprensión (>80% de respuestas correctas).
Capacitar en el uso adecuado de sistemas.	Talleres prácticos sobre buenas prácticas de seguridad.	Enseñar el manejo seguro de contraseñas, detección de correos maliciosos y uso de herramientas autorizadas.	Equipo de TI.	Usuarios con acceso a sistemas críticos.	Trimestral (2 horas por sesión).	Reducción de incidentes por errores humanos (>30% en 6 meses).
Socializar políticas y procedimientos del PSI.	Distribución de manuales y guías de usuario.	Entregar documentos claros con las políticas, normas y procedimientos de seguridad informática.	Gestión de Documentación.	Todo lo personal.	Revisión anual.	Nivel de cumplimiento en auditorías internas (>90%).
Respuestas similares ante incidentes.	Ejercicios de simulación (ej. phishing o ciberataques).	Evaluar la reacción del personal ante escenarios simulados para mejorar la respuesta ante incidentes reales.	Equipo de TI, Seguridad.	Áreas críticas de la organización.	Semestral (1 jornada).	Tiempo de respuesta y acciones adecuadas (>80% cumplen los protocolos).

Actualizar conocimientos sobre ciberseguridad.	Cursos avanzados para personal técnico.	Capacitar al personal de TI sobre nuevas amenazas, herramientas y normativas relacionadas con seguridad.	Consultores externos, Equipo de TI.	Personal técnico de TI.	Anual (3 días).	% de participantes certificados o capacitados (>90%).
Fomentar la cultura de seguridad.	Campañas internas de concienciación (carteles, correos informativos, vídeos).	Reforzar conceptos clave mediante mensajes constantes en los canales de comunicación interna.	Recursos Humanos.	Todo lo personal.	Mensual (contenidos cortos).	Nivel de participación y encuestas de percepción positiva (>85%).

Nota: Plan de capacitación de la empresa EP EMSEGURIDAD. Elaboración propia. (2024)

La siguiente tabla detalla las actividades a realizar para el cumplimiento de los objetivos específicos en el marco de la implementación de medidas de seguridad en un centro de datos de una Empresa Pública. El proceso se desarrolla a través de una serie de actividades planificadas y distribuidas a lo largo de varios meses, con el fin de garantizar la protección adecuada de la información y los sistemas de la organización. Cada actividad está asignada a un responsable que se encargará de ejecutar tareas específicas, como la revisión documental, la recopilación y análisis de datos, y la generación de políticas de seguridad. Estas actividades están orientadas a asegurar que el centro de datos cuente con las de seguridad necesarias para mitigar riesgos y fortalecer la infraestructura tecnológica, cumpliendo con las medidas normativas vigentes y las mejores prácticas en el área.

Conclusiones

Se realizó un análisis detallado de las medidas de seguridad que deben implementarse en la EP-EMSEGURIDAD para reforzar la protección de la información. La estrategia propuesta consistió en evaluar exhaustivamente las normativas vigentes y las mejores prácticas en seguridad informática. Se recomienda realizar una evaluación de la infraestructura tecnológica existente, así como de sus capacidades de protección, tales como firewalls, encriptación y autenticación multifactorial, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. Además, se incluyó la revisión de los procesos operativos para identificar áreas vulnerables. La implementación de estas medidas será fundamental para mejorar la seguridad de la información y mitigar posibles brechas en la protección de datos.

En relación con la identificación de las amenazas y vulnerabilidades presentes en la EP-EMSEGURIDAD que comprometen la seguridad de la información, la estrategia propuesta incluyó un diagnóstico completo mediante auditorías de seguridad y el uso de herramientas avanzadas de monitoreo. Se identificaron posibles amenazas externas, como ataques de phishing y malware, así como vulnerabilidades internas que podrían comprometer la protección de los datos. Para mitigar estos riesgos, se propuso la implementación de controles de acceso estrictos, la capacitación continua del personal y la adopción de tecnologías de detección de intrusiones (IDS/IPS). Estas medidas son esenciales para prevenir incidentes de seguridad y proteger la infraestructura tecnológica de la organización.

En cuanto a la generación de políticas de seguridad para evitar la divulgación y exposición no autorizada de la información, se demostró crucial la creación de políticas robustas que aseguren la protección de los datos producidos por la empresa. Se indicará desarrollar políticas claras y actualizadas sobre el manejo de datos, estableciendo controles estrictos sobre el acceso, almacenamiento y transmisión de la información. Asimismo, se recomienda implementar un protocolo de respuesta ante incidentes que permita actuar rápidamente ante cualquier intento de divulgación no autorizada. Estas políticas deben ser comunicadas efectivamente a todo el personal y revisadas periódicamente para adaptarse a los cambios tecnológicos y normativos, garantizando así altos niveles de seguridad y protección de la información.

En lo que, respecto al diseño de un programa de capacitación en ciberseguridad para sensibilizar y formar a los empleados sobre la identificación, prevención y manejo de riesgos cibernéticos dentro de la Dirección de TIC, la estrategia propuesta consistió en crear un programa integral de capacitación. Este programa incluye talleres prácticos, simulaciones de ataques cibernéticos (como phishing) y la entrega de manuales sobre las mejores prácticas de seguridad. Además, se recomienda realizar evaluaciones periódicas del impacto de la capacitación a través de encuestas y análisis de incidentes, lo que permitirá medir la efectividad de las acciones formativas. La capacitación continua será crucial para fortalecer la cultura de seguridad dentro de la organización y reducir los riesgos asociados a errores humanos que puedan comprometer la seguridad de la información.

Finalmente, respecto al diseño de un plan de seguridad alineado con la ISO 27001 para garantizar la protección de la información, mitigar vulnerabilidades en la infraestructura tecnológica y establecer políticas de seguridad, la estrategia propuesta se centró en diseñar un plan alineado con esta norma internacional. Esto implica la implementación de controles y

procedimientos de seguridad que aseguran la integridad de la información. Se recomienda realizar una evaluación inicial de riesgos, establecer medidas preventivas para mitigar vulnerabilidades y garantizar un monitoreo constante de la infraestructura tecnológica. Además, se sugiere la integración de políticas de seguridad claras que aborden desde la gestión de accesos hasta la protección ante incidentes de seguridad, proporcionando así una base sólida para proteger la información y fortalecer la resiliencia de la organización frente a amenazas cibernéticas.

Recomendaciones

- Realizar una auditoría integral de infraestructura tecnológica que incluya pruebas de penetración y análisis de vulnerabilidades. Priorizar la actualización de firewalls, la encriptación de datos sensibles y la implementación obligatoria de autenticación multifactorial para accesos críticos.
- Implementar un sistema de monitoreo de amenazas en tiempo real con herramientas de análisis de tráfico y detección de intrusiones (IDS/IPS). Complementar con programas de capacitación específicos en ciberseguridad para el personal.
- Actualizar y documentar las políticas de seguridad de la información, asegurando que sean revisadas al menos una vez al año. Establecer protocolos específicos para la gestión de accesos y la respuesta ante incidentes de seguridad, con simulaciones periódicas para evaluar su efectividad.
- Establecer un programa de formación continua obligatorio con certificaciones internas en ciberseguridad para los empleados. Incluir simulaciones de ataques y pruebas de respuesta para medir la preparación ante amenazas reales.
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001, con auditorías anuales para garantizar su cumplimiento. Asegurar que la gestión de accesos, protección de datos y respuesta ante incidentes sean parte fundamental del plan.

Bibliografía

AECI. (2023). Estrategia Nacional de Ciberseguridad de Ecuador. https://aeci.org.ec/

Ben Assuli, O. y Chaleco, R. (2022). Visitas de retorno al servicio de urgencias: un análisis utilizando modelos de curvas basados en grupos. Recuperado de https ://www .researchgate .net /publication /361218706_Return_visits_to_the_emergency_department_An_analysis_using_group_based_curve_models

Chicaiza, D. (2024). *Plan de contingencia informática basado en la norma ISO 27001 para el área de TI de la Empresa Pública Municipal Gestión Integral de Desechos Sólidos de Ambato (EPM-GIDSA)* . Recuperado de https ://repositorio .uta .edu .ec /server /api /core /bitstreams /6f117e94 -3668 -4a4b -95f1 -8b47e55c9749 /content

Chiquito, C. (2023). *Implementación de políticas de seguridad en la infraestructura tecnológica del Hospital Básico Jipijapa mediante un aparato Fortinet 80E*. Recuperado de https ://repositorio .unesum .edu .ec /bitstream /53000 /5487 /1 /Chiquito %20Manrique %20Christian %20Dionisio .pdf

Coello, A. (2024). *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano*. Recuperado de https://economicsocialresearch.com/index.php/home/article/view/96

ENISA (Agencia de la Unión Europea para la Ciberseguridad). (2021). *Informe sobre el panorama de amenazas*.

Gallardo, E. (2017). *Metodología de la investigación: Manual autoformativo interactivo*. Recuperado de https://mawil.us/wp-content/uploads/2023/08/metodologia-de-la-investigacion.pdf

Garner. (2021). *Tecnologías emergentes en ciberseguridad*.

Gracia, C (2024). *innova-luz*. Recuperado de https://innova-luz.com/index.php/revista/article/view/5

Herath, T. & Rao, H. (2009). Motivación y disuasión de protección: un marco para el cumplimiento de la política de seguridad en las organizaciones. *Revista europea de sistemas de información, 18* (2), 106–125. https://doi.org/10.1057/ejis.2009.5

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ª ed.). McGraw-Hill.

ISO 27001:2022. (2022). *GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Lema, C. (2020). *Plan de gestión de seguridad de la información*. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7634599

Lema, C. (sf). *Plan de gestión de seguridad de la información* . Recuperado de archivo :///C :/Usuarios /juan .mejia /Descargas /Dialnet -PlanDeGestionDeSeguridadDeLaInformacion -7634599 .pdf

Seguridad de IBM. (2022). *Informe sobre el coste de una vulnerabilidad de datos en 2022*. Recuperado de http ://www .editorialalema .org /index .php /pentaciencias /article /view /700

Organización Internacional de Normalización (ISO). (2013). *ISO/IEC 27001: Sistemas de gestión de seguridad de la información*. ISO.

Jiménez, J. (2021). *ups.edu.ec.* Recuperado de https ://dspace. ups .edu .ec /bitstream /123456789 /20966 /4 /UPS -GT003401 .pdf

Minaya, M., Minaya, R., Intriago, M. & Intriago, A. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5* (4), 584–599. https://doi.org/10.59169/pentaciencias.v5i4.700

Ministerio de Telecomunicaciones y Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. Recuperado de https ://asobanca .org .ec /wp -content /uploads /2022 /08 /ESTRATEGIA -NACIONAL -DE -CIBERSEGURIDAD -DEL -ECUADOR -2022481 .pdf

Moya, C. (2023). *Propuesta de un plan de seguridad informática para la empresa EP-EMAPA-A* . Recuperado de https ://repositorio. puce .edu .ec /server /api /core /bitstreams /f4759b2e -d64b -4b88 -8e3c -cbf6c40b7065 /content

NIST (Instituto Nacional de Normas y Tecnología). (2018). *Marco para mejorar la ciberseguridad de las infraestructuras críticas*.

Pinda, N., & Moya, l. (2024). *Ciberseguridad enfocada en el futuro digital de los estudiantes* . https://dialnet.unirioja.es/descarga/articulo/9541030.pdf

Policía Nacional de Colombia. (2023). *Sistema de Prevención, Convivencia y Seguridad Ciudadana*. Recuperado de https ://www .policía .gov .co /sites /default /files /descargables /5 .%20Sistema %20de %20Prevenci %C3 %B3n %2C %20 %20Convivencia %20y %20Seguridad %20 %20Ciudadana .pdf

Ramírez, L. (2024). *127TECNOLOGÍAS DE DEFENSA FRENTE A INTELIGENCIA DE AMENAZAS Y RESUMENABSTRACTEn la era digital contemporánea, el panorama de la seguridad informática enfrenta constantes desafíos y amenazas en evolución.* https://revistas.itecsur.edu.ec/index.php/inndev/article/view/94/66

Urbini, M (2021). *unlp.edu.ar.* Recuperado de https ://sedici .unlp .edu .ar /bitstream /handle /10915 /147421 /Documento_completo .pdf -PDFA .pdf ?sequence =1 &isAllowed =y

Vega, L. y Marrero, F. (2021). Evolución del control interno hacia una gestión integrada al control de gestión. Recuperado de https ://revistas. uasb .edu .ec /index .php /eg /article /view /2861 /3027

Von Solms, R. y Van Niekerk, J. (2013). De la seguridad de la información a la ciberseguridad. *Computadoras y seguridad, 38,* 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M & Mattord, H (2022). *Principios de seguridad de la información* (7ª ed.). Aprendizaje Cengage.

Zohar, D. & Ben-Assuli, O. (2016). Ciberseguridad para organizaciones gubernamentales: el papel de las políticas de seguridad de la información. *Información gubernamental trimestral, 33* (2), 354–361. https://doi.org/10.1016/j.giq.2016.02.001

Anexos

Anexo 1: Encuesta sobre Seguridad de la Información en EP EMSEGURIDAD

Objetivo de la encuesta:

Identificar las medidas actuales de seguridad de la información, evaluar el nivel de conocimiento del personal sobre estas políticas y recopilar información clave para diseñar un Plan de Seguridad de la Información (PSI) que mejore la protección de los activos de la empresa.

Instrucciones:

Responda las preguntas con sinceridad. La encuesta es anónima y los datos serán utilizados únicamente con fines académicos, atendiendo a los criterios éticos.

Preguntas de Información General

1. Área de trabajo dentro de EP EMSEGURIDAD:
   • Dirección de Tecnologías de la Información y Telecomunicaciones
   • Administración
   • Otros (específicar): _____
2. Años de experiencia en la empresa:
   • Menos de 1 año
   • 1-3 años
   • 3-5 años
   • Más de 5 años

Preguntas con Códigos de Variable

Conocimiento sobre Políticas de Seguridad de la Información

3. [VV] ¿Conoce las políticas de seguridad de la información actuales en EP EMSEGURIDAD?

• Sí

• No

4. [VV] ¿Cómo calificaría su nivel de conocimiento?

• Básico

• Intermedio

• Avanzado

5. [VV] ¿Ha recibido capacitación específica sobre seguridad de la información en los últimos 12 meses?

• Sí

• No

Importancia de los Factores de Seguridad

6. [VV] ¿Qué aspectos consideran más importantes para garantizar la seguridad de la información en la empresa? (Seleccione los tres más relevantes):

• Control de acceso

• Contraseñas seguras

• Protección contra malware

• Cifrado de datos

• Políticas de uso de correo electrónico

• Otros (específicar): _____

Suficiencia y Actualización de las Políticas

7. [VA] ¿Considera que las políticas actuales son suficientes para proteger la información de la empresa?

• Totalmente de acuerdo

• De acuerdo

• Neutral

• En desacuerdo

• Totalmente en desacuerdo

8. [VV] ¿Con qué frecuencia actualizan sus contraseñas de acceso a los sistemas de la empresa?

• Cada mes

• Cada 3 meses

• Cada 6 meses o más

• Nunca

Percepción y Experiencias sobre Seguridad de los Sistemas

9. [VD] ¿Qué tan seguro considera que es el sistema de correo electrónico institucional frente a ataques externos como phishing?

• Muy seguro
• Seguro
• Poco seguro
• No es seguro

10. [VA] ¿Ha detectado algún incidente de seguridad relacionado con el uso de sistemas o datos en la empresa?

• Sí
• No

11. [VA] Si su respuesta anterior fue afirmativa, ¿qué tipo de incidente ocurrió? (puede marcar más de uno):

• Acceso no autorizado
• Pérdida de datos
• Malware o virus
• Suplantación de identidad (phishing)
• Otros (especificar): _____

Propuestas y Sugerencias

12. [VD] En su opinión, ¿qué medidas adicionales deben implementarse para fortalecer la seguridad de la información?

13.[VV] ¿Considera importante recibir capacitación periódica sobre seguridad de la información? Explique brevemente:

14. [VD] ¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD?

15. [VV] ¿Tiene alguna sugerencia específica para mejorar las políticas de seguridad actuales?

Gracias por su participación.

Anexo 2: Matriz de Riesgos 5x5: EP-EMSEGURIDAD

Amenaza/Vulnerabilidad	Impacto (1-5)	Probabilidad (1-5)	Nivel de Riesgo (Impacto x Probabilidad)	Clasificación	Estrategia de mitigación
Accesos no autorizados a la información	5	5	25	Crítico	Implementar controles de acceso basados en roles (RBAC) y autenticación multifactor (MFA).
Pérdida de datos por fallos en los sistemas	5	4	20	Alto	Configurar copias de seguridad automáticas y realizar pruebas periódicas de restauración de datos.
Ataques cibernéticos (phishing, ransomware)	5	5	25	Crítico	Adoptar herramientas de detección de amenazas y capacitar al personal en ciberseguridad.
Falta de políticas claras de seguridad	4	5	20	Alto	Diseñar políticas alineadas a la norma ISO/IEC 27001 y sensibilizar a todo el personal.
Uso no autorizado de dispositivos personales	3	4	12	Moderado	Implementar políticas BYOD (Bring Your Own Device) y sistemas de monitoreo en dispositivos personales.
Ausencia de monitoreo continuo	5	5	25	Crítico	Establecer un SOC (Centro de Operaciones de Seguridad) para monitorear actividad 24/7.
Errores humanos en el manejo de información	4	3	12	Moderado	Implementar programas de capacitación y simulacros regulares para el personal.
Obsolescencia de software o sistemas.	4	4	16	Alto	Realizar actualizaciones periódicas de software y evaluar herramientas de seguridad actuales.

Escalas utilizadas

- Impacto (1-5): 1 = Muy Bajo | 2 = Bajo | 3 = Moderado | 4 = Alto | 5 = Muy Alto
- Probabilidad (1-5): 1 = Muy Improbable | 2 = Improbable | 3 = Posible | 4 = Probable | 5 = Muy probable
- Nivel de Riesgo: Impacto x Probabilidad

  1-5: Bajo

  6-10: Moderado

  11-20: Alto

21-25: Crítico

Clasificación y Prioridad de Riesgos

- Crítico (21-25): Requiere acción inmediata para evitar impacto severo.
- Alto (11-20): Necesita medidas prioritarias para reducir el riesgo.
- Moderado (6-10): Importante, pero puede ser gestionado con medidas estándar.
- Bajo (1-5): Monitoreo ocasional, no se requiere acción inmediata.

Anexo 3: Validación

Validación de instrumento

Validación de la pertinencia de las preguntas de la encuesta sobre seguridad de la información en EP EMSEGURIDAD

Estimado Validador

Con el objetivo de asegurar que las preguntas incluidas en la encuesta sobre seguridad de la información sean pertinentes, claras, y alineadas con los objetivos de la investigación, solicitamos su colaboración para revisar y validar cada una de las preguntas. La validez de las preguntas es fundamental para garantizar la calidad de los datos recolectados, lo que permitirá diseñar un Plan de Seguridad de la Información (PSI) adecuado a las necesidades de EP EMSEGURIDAD.

A continuación, encontrará una matriz que incluye cada una de las preguntas de la encuesta, junto con una serie de criterios para validar su pertinencia. Le agradeceremos proporcionarle sus comentarios y sugerencias.

Datos del validador

- *Nombre y apellido:*

  Roberto Varela

- *Correo electrónico:*

  roberto.varela@emseguridad-q.gob.ec

- *Título:*
  Magíster en Ciberseguridad

- *Cargo actual:*

  Analista de Tecnologías de la Información y Telecomunicaciones

- *Años de experiencia:*
  12 años

Matriz de validación

Pregunta	Pertinencia de la pregunta	SI/NO	Recomendaciones
1. Área de trabajo dentro de EP EMSEGURIDAD • Dirección de Tecnologías de la Información y Telecomunicaciones • Administración • Otros	¿La pregunta es clara y relevante para la encuesta?	[x] Sí [ ] No	
2. Años de experiencia en la empresa	¿La pregunta aporta información	[x] Sí [ ] No	

Menos de 1 año • 1-3 años • 3-5 años • Más de 5 años	significativa sobre el perfil del encuestado?		
3. ¿Conoce las políticas de seguridad de la información actuales en EP EMSEGURIDAD? • Sí • No	¿La pregunta mide efectivamente el conocimiento del encuestado sobre las políticas de seguridad?	[x] Sí [ ] No	
4. ¿Cómo calificaría su nivel de conocimiento? • Básico • Intermedio • Avanzado	¿La pregunta ofrece una escala apropiada para evaluar el nivel de conocimiento del encuestado?	[x] Sí [ ] No	
5. ¿Ha recibido capacitación específica sobre seguridad de la información en los últimos 12 meses? • Sí • No	¿La pregunta es relevante para evaluar la capacitación en seguridad de la información?	[x] Sí [ ] No	
6. ¿Qué aspectos consideran más importantes para garantizar la seguridad de la información en la empresa? • Control de acceso • Contraseñas seguras • Protección contra malware • Cifrado de datos • Políticas de uso de correo electrónico • Otros	¿La pregunta cubre los aspectos claves relacionados con la seguridad de la información?	[x] Sí [ ] No	
7. ¿Considera que las políticas actuales son suficientes para proteger la información de la empresa? • Totalmente de acuerdo • De acuerdo • Neutral • En desacuerdo • Totalmente en desacuerdo	¿La pregunta refleja una evaluación crítica sobre las políticas de seguridad actuales?	[x] Sí [ ] No	
8. ¿Con qué frecuencia actualizan sus contraseñas de acceso a los sistemas de la empresa? • Cada mes • Cada 3 meses • Cada 6 meses o más • Nunca	¿La pregunta es adecuada para evaluar las prácticas de seguridad en cuanto a contraseñas?	[x] Sí [ ] No	
9. ¿Qué tan seguro considera que es el sistema de correo	¿La pregunta es adecuada para	[x] Sí [ ] No	

electrónico institucional frente a ataques externos como phishing? • Muy seguro • Seguro • Poco seguro • No es seguro	evaluar la percepción de la seguridad del sistema de correo electrónico?		
10. ¿Ha detectado algún incidente de seguridad relacionado con el uso de sistemas o datos en la empresa? • Sí • No	¿La pregunta mide adecuadamente los incidentes de seguridad ocurridos?	[x] Sí [ ] No	
11. Si su respuesta anterior fue afirmativa, ¿qué tipo de incidente ocurrió? • Acceso no autorizado • Pérdida de datos • Malware o virus • Suplantación de identidad (phishing) • Otros	¿La pregunta ofrece opciones suficientes para clasificar los incidentes de seguridad?	[x] Sí [ ] No	
12. En su opinión, ¿qué medidas adicionales deben implementarse para fortalecer la seguridad de la información? ( ) Incrementar el uso de herramientas avanzadas de ciberseguridad (como firewalls, IDS, encriptación). ( ) Realizar capacitaciones periódicas para el personal sobre buenas prácticas en seguridad de la información. ( ) Establecer políticas más estrictas de acceso y manejo de datos sensibles. ( ) Implementar auditorías regulares y pruebas de vulnerabilidad. ( ) Fomentar una cultura organizacional orientada a la protección de datos. ( ) Otras:	¿La pregunta invita a una reflexión significativa sobre medidas adicionales para la seguridad?	[x] Sí [ ] No	
13. ¿Considera importante recibir capacitación periódica sobre seguridad de la información? ( ) Software avanzado de detección y prevención de intrusiones (IDS/IPS). ( ) Sí, es fundamental para mantenernos actualizados y proteger los datos.	¿La pregunta es relevante para medir la necesidad de capacitación continua?	[x] Sí [ ] No	

( ) No, consideramos que los conocimientos actuales son suficientes. ( ) No estoy seguro/a, depende de la frecuencia y calidad de las capacitaciones.Explique brevemente:			
14. ¿Qué herramientas o tecnologías creen que podrían mejorar la protección de los datos en EP EMSEGURIDAD? ( ) Software avanzado de detección y prevención de intrusiones (IDS/IPS). ( ) Sistemas de encriptación de datos más robustos. ( ) Implementación de autenticación multifactor (MFA). ( ) Herramientas de monitoreo y auditoría en tiempo real. ( ) Otras:	¿La pregunta cubre posibles soluciones tecnológicas relevantes para la mejora de la seguridad?	[x] Sí [ ] No	
15. ¿Tiene alguna sugerencia específica para mejorar las políticas de seguridad actuales? ( ) Implementar controles más estrictos para acceso a información sensible. ( ) Realizar auditorías internas más frecuentes. ( ) Establecer sanciones más claras por incumplimiento de políticas. ( ) Incluir más capacitaciones para los empleados sobre ciberseguridad. ( ) Otras:	¿La pregunta es abierta y permite una retroalimentación útil sobre las políticas de seguridad?	[x] Sí [ ] No	

Firma del Validador:

Fecha: 2025-01-17

Comentarios adicionales del validador:

FELICITACIONES POR EL TRABAJO REALIZADO