UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales

SORIANO HERRERA ROGER HITLER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

VELASQUEZ PORRAS DIANA MARIBEL
INGENIERA EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2024

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales

SORIANO HERRERA ROGER HITLER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

VELASQUEZ PORRAS DIANA MARIBEL
INGENIERA EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2024

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTAS TECNOLÓGICAS

Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales

SORIANO HERRERA ROGER HITLER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

VELASQUEZ PORRAS DIANA MARIBEL
INGENIERA EN TECNOLOGIAS DE LA INFORMACION

LOJA MORA NANCY MAGALY

MACHALA
2024

Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales

por Nancy Magaly Loja Mora

Fecha de entrega: 25-jul-2024 09:26a.m. (UTC-0500)

Identificador de la entrega: 2422282033

Nombre del archivo: Grupo09_Soriano-Roger-y-Velásquez-Diana-Proyecto_Integración_Curricular_1_2_.docx (13.33M)

Total de palabras: 29767

Total de caracteres: 177370

Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales

INFORME DE ORIGINALIDAD

9%	5%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	openaccess.uoc.edu Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%
3	Submitted to Universidad Técnica de Machala Trabajo del estudiante	1%
4	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	1%
5	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	1%
6	bibdigital.epn.edu.ec Fuente de Internet	<1%
7	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
8	repositorio.espe.edu.ec Fuente de Internet	<1%

9	www.gobiernoelectronico.gob.ec Fuente de Internet	<1 %
10	dspace.udla.edu.ec Fuente de Internet	<1 %
11	nanopdf.com Fuente de Internet	<1 %
12	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1 %
13	documentop.com Fuente de Internet	<1 %
14	www.barrancabermeja.gov.co Fuente de Internet	<1 %
15	repositorio.uta.edu.ec Fuente de Internet	<1 %
16	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1 %
17	Submitted to Escuela Superior Politécnica del Litoral Trabajo del estudiante	<1 %
18	Elka Panduro-Alvarado, José Elías Sandoval-Ríos. "Gestión de riesgos para la seguridad de edificaciones públicas", Revista Minerva, 2022 Publicación	<1 %

19	Diana Lizeth Carvajal Portilla, Arturo Cardona Londoño, Francisco Javier Valencia Duque. "Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana", Entre ciencia e ingeniería, 2019 Publicación	<1 %
20	fipcaec.com Fuente de Internet	<1 %
21	repositorio.unbosque.edu.co Fuente de Internet	<1 %
22	Brenda Marina Martínez Herrera, Ileana Elizabeth Martínez Michel. "Diagnóstico de la gestión actual de manejo de riesgos con el uso de las tecnologías de información para asegurar una correcta presentación de la prima de riesgo de trabajo", Interconectando Saberes, 2023 Publicación	<1 %
23	Roberto Lopez-Chila, Joe Llerena-Izquierdo, Nicolas Sumba-Nacipucha. "Using ExamView to Create Questionnaires for Online Evaluation in VLEs", 2021 Second International Conference on Information Systems and Software Technologies (ICI2ST), 2021 Publicación	<1 %
24	dspace.unl.edu.ec Fuente de Internet	

		<1 %
25	repositorio.pucese.edu.ec Fuente de Internet	<1 %
26	Rainer Schmidt, Axel Kieninger. "DYNSEA — A dynamic service-oriented Enterprise Architecture based on S-D-logic", 2009 13th Enterprise Distributed Object Computing Conference Workshops, 2009 Publicación	<1 %
27	es.slideshare.net Fuente de Internet	<1 %
28	repositorio.ucv.edu.pe Fuente de Internet	<1 %
29	revistas.ulasalle.edu.pe Fuente de Internet	<1 %
30	repositorio.utn.edu.ec Fuente de Internet	<1 %
31	Submitted to UNIV DE LAS AMERICAS Trabajo del estudiante	<1 %
32	William Oñate, Ricardo Sanz. "Analysis of architectures implemented for IIoT", Heliyon, 2023 Publicación	<1 %

33	Segundo Moisés Toapanta Toapanta, Rodrigo Humberto Del Pozo Durango, Luis Enrique Mafla Gallegos, Eriannys Zharayth Gómez Díaz et al. "Prototype to Mitigate the Risks, Vulnerabilities and Threats of Information to Ensure Data Integrity", Advances in Science, Technology and Engineering Systems Journal, 2022 Publicación	<1 %
34	repository.unad.edu.co Fuente de Internet	<1 %
35	Caren B. Goldberg, David A. Waldman. "Modeling employee absenteeism: testing alternative measures and mediated effects based on job satisfaction", Journal of Organizational Behavior, 2000 Publicación	<1 %
36	docplayer.es Fuente de Internet	<1 %
37	pt.scribd.com Fuente de Internet	<1 %
38	Wilson Anthony Lazo Tapia, Carlos Enrique Alvarez Montalvan, Fiorella Katiuska Lazo Tapia. "Mobile APP Development for Recording Car Incidents in Public Transport Companies Promoting SmartCity Models",	<1 %

2021 6th International Conference on Cloud Computing and Internet of Things, 2021
Publicación

39	Submitted to Universidad Tecnica De Ambato-Direccion de Investigacion y Desarrollo , DIDE Trabajo del estudiante	<1 %
40	Submitted to ulacit Trabajo del estudiante	<1 %
41	Miguel Leonardo Catagua Briones, María Fernanda Pinargote Macías, Marcelo Eduardo Mendoza Vinces. "Control interno y modelo COSO en la gestión administrativa y financiera empresarial", PODIUM, 2023 Publicación	<1 %
42	Jimy Oblitas, Jhon Jorge. "Differences in Student Satisfaction in Online Learning and Remote Teaching Courses during the COVID-19 Adaptation Stage", 2021 IEEE World Conference on Engineering Education (EDUNINE), 2021 Publicación	<1 %
43	Submitted to Universidad EAFIT Trabajo del estudiante	<1 %
44	Submitted to Universidad San Marcos Trabajo del estudiante	<1 %
45	Submitted to consultoriadeserviciosformativos	<1 %

Trabajo del estudiante

46	orisasite.files.wordpress.com Fuente de Internet	<1 %
47	www.lamesa-cundinamarca.gov.co Fuente de Internet	<1 %
48	Submitted to Instituto Tecnologico de Costa Rica Trabajo del estudiante	<1 %
49	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Trabajo del estudiante	<1 %
50	Submitted to Universidad Autónoma Metropolitana-Xochimilco Trabajo del estudiante	<1 %
51	Submitted to Universidad Continental Trabajo del estudiante	<1 %
52	Submitted to Universidad Privada del Norte Trabajo del estudiante	<1 %
53	Victor Gonzalo Rodriguez-Ahuanari, Miguel Angel Vega-Ramirez, Hugo Eladio Chumpitaz-Caycho, Ericka Nelly Espinoza-Gamboa et al. "Intelligent system for data protection in higher education institutions: A systematic review", 2022 IEEE International Conference on Smart Internet of Things (SmartIoT), 2022 Publicación	<1 %

54	repositorio.unasam.edu.pe Fuente de Internet	<1 %
55	repositorio.uprit.edu.pe Fuente de Internet	<1 %
56	www.estrategia.gobiernoenlinea.gov.co Fuente de Internet	<1 %
57	www.rberny.com Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

Los que suscriben, SORIANO HERRERA ROGER HITLER y VELASQUEZ PORRAS DIANA MARIBEL, en calidad de autores del siguiente trabajo escrito titulado Gestión de riesgos de seguridad de la información en una empresa pública: Propuestas de mejoras y adopción de normas nacionales, otorgan a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tienen potestad para otorgar los derechos contenidos en esta licencia.

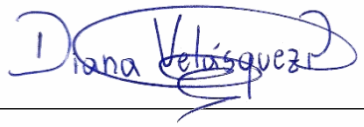
Los autores declaran que el contenido que se publicará es de carácter académico y se enmarca en las disposiciones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

Los autores como garantes de la autoría de la obra y en relación a la misma, declaran que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asumen la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

SORIANO HERRERA ROGER HITLER
0706467115



VELASQUEZ PORRAS DIANA MARIBEL
0202634978

DEDICATORIA

Dedico este trabajo principalmente a mis padres, quienes me han apoyado y ayudado a lo largo de toda esta etapa universitaria con sus consejos y valores brindados desde que era un niño. A mis hermanos, que de igual manera han mostrado su apoyo constante para que finalmente cumpla mis objetivos.

Soriano Herrera Roger Hitler

Dedico el presente trabajo de titulación a mis padres, quienes han sido un pilar fundamental en mi proceso de formación académica. Su amor incondicional, constante apoyo, sabios consejos y los innumerables sacrificios que han hecho por mí me han acompañado a lo largo de esta etapa crucial de mi vida. A mi tía, cuya generosidad y aliento han sido una fuente constante de inspiración y motivación, le agradezco de corazón por creer en mí y por su inquebrantable apoyo en los momentos más difíciles. A todos ustedes, padres y tía, les dedico este logro, pues sin su apoyo, amor y sacrificio, no habría sido posible.

Velásquez Porras Diana Maribel

AGRADECIMIENTO

Quiero agradecer a mis padres por su gran esfuerzo para ayudarme a alcanzar mis metas y objetivos. Su sacrificio me ha ayudado a mejorar como persona. A mis hermanos, que siempre han estado ahí cuando los he necesitado, a mi tía y a mis amigos.

Agradezco enormemente a la ingeniera Nancy Loja, mi tutora de tesis, quien nos ha brindado su conocimiento, ayuda, consejos y orientaciones para llevar a cabo este trabajo de manera exitosa.

Soriano Herrera Roger Hitler

Agradezco principalmente a mis padres por su constante apoyo y confianza, que me ha permitido continuar con mi formación profesional y superar cada desafío en este camino académico. Sus palabras de aliento y fe en mis capacidades han sido cruciales para alcanzar este logro. A mi tía, cuyo continuo ánimo ha sido una fuente de inspiración y motivación, les expreso mi más sincero agradecimiento.

A la Ing. Nancy Loja, mi tutora del trabajo de titulación, le agradezco por su guía, paciencia y conocimientos compartidos. Asimismo, extiendo mi gratitud a los docentes de la Universidad Técnica de Machala que me han orientado y apoyado durante mi formación académica, cuyo compromiso y enseñanzas han sido vitales para mi crecimiento profesional.

Velásquez Porras Diana Maribel

RESUMEN

La gestión de riesgos de seguridad de la información en una empresa pública es esencial para proteger datos sensibles y asegurar la integridad, disponibilidad y confidencialidad de la información. Sin embargo, la falta de estructuras basadas en normas nacionales puede exponer a la empresa a vulnerabilidades y riesgos significativos, comprometiendo la confianza del público y la eficacia operativa, en contraste, la implementación de normas nacionales, como la Norma Técnica Ecuatoriana ISO/IEC 27005:2012 y la Guía para la gestión de riesgos de seguridad de la información del MINTEL, resulta fundamental para mitigar las vulnerabilidades y riesgos. Este proyecto tuvo como objetivo proponer mejoras mediante la adopción de estas normas. La metodología incluyó una investigación exhaustiva del estado del arte sobre la gestión de riesgos de seguridad de la información, con un enfoque en estándares nacionales para la propuesta de mejores prácticas. Se documentaron las vulnerabilidades en la infraestructura tecnológica y se diseñó un prototipo de propuesta de mejoras con estrategias específicas para la mitigación de riesgos, basadas en los controles de la ISO/IEC 27001. Los procesos clave considerados para la gestión de riesgos incluyeron el análisis del riesgo, tratamiento del riesgo, aceptación, comunicación y monitorización de los riesgos. El plan de evaluación se enfocó en validar la viabilidad de la propuesta mediante encuestas a expertos. Los resultados respaldaron la hipótesis demostrando que el uso de normas nacionales permitió desarrollar un plan de mejoras viable para la seguridad de la información en la empresa pública, fomentando prácticas seguras en la institución al ofrecer un análisis detallado y recomendaciones concretas para la gestión de riesgos de seguridad de la información.

Palabras Clave

Gestión de riesgos, seguridad de la información, empresa pública, normativa ecuatoriana, ISO/IEC 27001, ISO/IEC 27005.

ABSTRACT

Information security risk management in a public company is essential to protect sensitive data and ensure the integrity, availability and confidentiality of information. However, the lack of structures based on national standards can expose the company to significant vulnerabilities and risks, compromising public trust and operational efficiency, in contrast, the implementation of national standards, such as the Ecuadorian Technical Standard ISO/IEC 27005:2012 and the Guide for information security risk management of MINTEL, is essential to mitigate vulnerabilities and risks. The objective of this project was to propose improvements through the adoption of these standards. The methodology included an exhaustive investigation of the state of the art on information security risk management, with a focus on national standards for the proposal of best practices. Vulnerabilities in the technological infrastructure were documented and a prototype improvement proposal was designed with specific risk mitigation strategies based on ISO/IEC 27001 controls. The key processes considered for risk management included risk analysis, risk treatment, risk acceptance, risk communication and risk monitoring. The evaluation plan focused on validating the feasibility of the proposal through expert surveys. The results supported the hypothesis by demonstrating that the use of national standards made it possible to develop a viable improvement plan for information security in the public company, promoting secure practices in the institution by providing a detailed analysis and concrete recommendations for information security risk management.

Keywords

Risk management, information security, public company, Ecuadorian regulations, ISO/IEC 27001, ISO/IEC 27005

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

A

Activos críticos. - Son los elementos de información, sistemas o recursos que son considerados esenciales para el funcionamiento y la operatividad de una organización, cuya pérdida o compromiso puede tener un impacto significativo en la seguridad y la continuidad del negocio.

Análisis de satisfacción. - Es la evaluación del grado en que los usuarios o clientes están satisfechos con un producto o servicio, realizada mediante encuestas y otras herramientas para identificar áreas de mejora.

E

Escaneo de vulnerabilidades. - Proceso mediante el cual se realizan evaluaciones automáticas o manuales de sistemas, redes o aplicaciones con el fin de identificar y clasificar las vulnerabilidades de seguridad susceptibles de ser aprovechadas por amenazas externas o internas.

G

Gestión de riesgos. - Proceso sistemático para identificar, evaluar y reducir los riesgos potenciales que puedan impactar en la organización, sus activos, operaciones o reputación, con el fin de minimizar la probabilidad de pérdidas o impactos negativos.

M

Mitigación de riesgos. - Acciones o estrategias implementadas para reducir la probabilidad de ocurrencia de eventos adversos o minimizar su impacto en caso de que ocurran, con el objetivo de proteger los activos y la integridad de la institución.

P

Plan de gestión de riesgos. - Registro donde se describe las políticas, procedimientos y estrategias establecidas para identificar, evaluar, tratar y monitorear los riesgos en una organización, con el fin de garantizar la seguridad y la continuidad del negocio.

V

Viable. - Se refiere a la capacidad de un proyecto, plan o idea para ser realizado con éxito, considerando que es factible y que los recursos y condiciones necesarios están disponibles.

Vulnerabilidades. - Debilidades o deficiencias en los sistemas, aplicaciones, infraestructuras o procedimientos de una entidad que podrían ser aprovechadas por amenazas o atacantes para comprometer la seguridad, la disponibilidad o la integridad de la información y los activos.

INTRODUCCIÓN

La eficaz gestión de los riesgos de seguridad de la información es crucial para empresas públicas, donde la falta de un marco integral basado en normas ISO expone a riesgos financieros y legales. En este proyecto se enfrenta la carencia de una evaluación detallada de riesgos y la ausencia de una estrategia de seguridad planificada, lo que compromete la confidencialidad, disponibilidad e integridad de los datos.

La presencia del riesgo se define por la incertidumbre acerca de la posibilidad de que ocurra un imprevisto y, en caso de que suceda, las consecuencias que podría tener [1].

En la actualidad, la carencia de controles de seguridad en equipos y sistemas de información y comunicaciones conlleva múltiples riesgos para organizaciones de todos los tamaños. Estos incluyen amenazas como el espionaje industrial, el robo de información, interrupciones en los servicios y fallos críticos en la infraestructura y sistemas centrales [2].

Ante esta problemática, se propone el desarrollo de una propuesta de mejoras, respaldada por normas nacionales, para abordar de manera específica las vulnerabilidades identificadas. La implementación de un plan de gestión de riesgos busca fortalecer la seguridad de la información en entidades públicas, así como establecer estándares que promuevan prácticas seguras en el ámbito público y privado, protegiendo así datos sensibles y previniendo potenciales incidentes de seguridad [3].

Para esto se realizan las actividades relacionadas con la gestión de riesgos de la seguridad de la información , que incluyen: establecimiento de contexto, evaluación de riesgos, gestión de riesgos, aceptación de riesgos, comunicación de riesgos, seguimiento y revisión de riesgos [4] [5].

A continuación, se presenta la declaración y formulación del problema, el objeto de estudio y campo de acción, los objetivos, hipótesis y variables o preguntas de investigación y justificación.

i. Declaración y formulación del Problema

En la actualidad, la administración de riesgos de seguridad de la información en las organizaciones se ve confrontada por desafíos significativos. La ausencia de un enfoque integral respaldado por estándares ISO revela las debilidades en la infraestructura de tecnologías de la información de la empresa, poniendo en riesgo la privacidad, integridad y accesibilidad de información crítica. En el ámbito particular de la institución pública, se evidencia una carencia de enfoque en el análisis de debilidades, lo cual no solo expone a la empresa a riesgos financieros y legales, sino que también limita su capacidad para adaptarse proactivamente a las amenazas emergentes (Figura 1). En este sentido, se destaca la importancia fundamental de implementar un plan de gestión de riesgos que aborde específicamente las vulnerabilidades identificadas. Este problema se agrava aún más debido a la falta de una evaluación detallada de riesgos y a la carencia de una estrategia de seguridad planificada. Por tanto, se destaca la relevancia que el plan de gestión de riesgos aborde de manera específica las vulnerabilidades identificadas, este proyecto se concibe como un documento con propuestas de mejoras de los riesgos identificados.

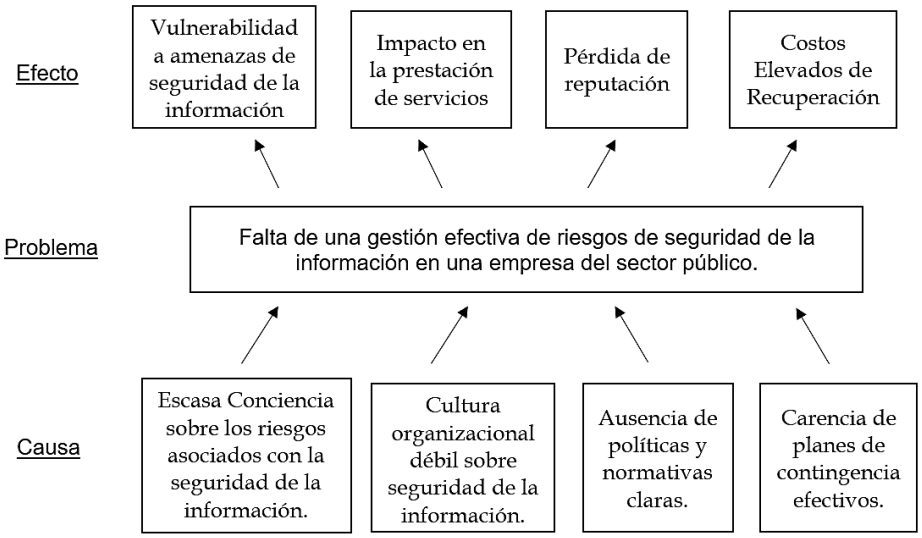


Figura 1: Árbol de causas, problema y efectos

A continuación, se formuló el problema de investigación de este trabajo: Necesidad de proponer mejoras significativas en la gestión de riesgos de seguridad de la información en una empresa pública, mediante el cumplimiento de normativas nacionales.

Y se determinó los siguientes problemas específicos:

- ¿Cómo se pueden identificar y definir de manera exhaustiva los activos críticos para la seguridad de la información que deben ser evaluados en el proceso de gestión de riesgos?

- ¿Cuáles son las herramientas y metodologías más adecuadas para realizar un escaneo completo de vulnerabilidades en los activos identificados?

- ¿Cómo se puede realizar una valoración precisa del nivel de riesgo asociado a las vulnerabilidades identificadas en los activos, considerando tanto impactos como probabilidades?

- ¿Cuáles son los enfoques estratégicos para diseñar planes de mitigación efectivos que aborden las vulnerabilidades y reduzcan el riesgo a niveles aceptables en los activos críticos para la seguridad de la información?

ii. Objeto de estudio y Campo de acción

Objeto de estudio

Gestión de riesgos de seguridad de la información en una empresa pública.

Campo de acción

Aplicación de normativas nacionales para mejorar la seguridad de la información en la empresa.

iii. Objetivos

Objetivo General

Elaborar un plan de gestión de riesgos en una empresa pública, basado en normas nacionales, para la propuesta de mejoras de seguridad de la información.

Objetivos específicos

- Desarrollar el estado del arte sobre la gestión de riesgos de seguridad de la información en empresas, enfocado en normas nacionales y mejores prácticas.

- Identificar las vulnerabilidades existentes en la infraestructura tecnológica de la empresa.

- Diseñar un prototipo de la propuesta de mejoras que incluya estrategias para la gestión de riesgos de seguridad de la información.

- Validar el plan de mejoras a través de la revisión por parte de expertos.

iv. Hipótesis y variables o Preguntas de investigación

Se formuló la siguiente hipótesis para este trabajo: Si se gestionan los riesgos usando normas nacionales, se podrá proponer un plan de mejoras viable para la seguridad de la información de una empresa pública.

La correcta definición y evaluación de las variables en el proyecto son fundamentales para comprender la efectividad del plan para gestionar los riesgos de seguridad de la información y su adopción de normas nacionales. Estas variables, detalladas en la Tabla 1, permiten una medición precisa de la implementación de normas ISO y la calidad del plan propuesto.

Tabla 1: Tabla de variables y Dimensionamiento

Variable	Definición	Categorías	Indicadores	Ítems
Variable Independiente: Gestión de riesgos usando normas nacionales	El grado de adopción de las normas nacionales en la gestión de riesgos de seguridad de la información, incluyendo procesos para identificar, evaluar y gestionar riesgos.	-Implementación de normas nacionales basadas en normas ISO. -Grado de adopción de normas. -Plan de Gestión -Documentación de procesos normativos.	- Relevancia de los principios de la ISO 27005 en la propuesta. -Reconocimiento de los beneficios de la adopción de normas nacionales. -Medidas de mitigación y estrategias de respuesta.	-Incorporación de los principios clave de normas nacionales en la propuesta -Documentación y seguimiento de procesos normativos. -Coherencia entre los controles propuestos con las mejores prácticas sugeridas por la norma.
Variable Dependiente: Propuesta de mejoras	Conjunto de acciones y recomendaciones específicas diseñadas para	-Grado de efectividad de las propuestas.	-Efectividad de las propuestas en la mitigación de riesgos	-Identificación y descripción de medidas de gestión y estrategias de respuesta en la

Variable	Definición	Categorías	Indicadores	Ítems
	mejorar la gestión de riesgos de seguridad de la información	-Alineación con estándares y normativas. -Integración con procesos existentes de la empresa.	identificados. -Aceptación y apoyo del plan. -Coherencia con los requisitos de las normas nacionales.	propuesta. -Claridad y pertinencia de los documentos relacionados con procesos normativos en la propuesta.

v. Justificación

El manejo eficiente de riesgos de seguridad de la información es crucial en el actual entorno digital, y esta investigación busca aportar mediante la adopción de normas nacionales, basadas en la ISO 27005. Este enfoque teórico busca proponer mejoras en base a estas normativas en una empresa del sector público. La creciente sofisticación de amenazas cibernéticas y la necesidad de cumplir con normativas nacionales motivan la investigación, que se propone como una solución para administrar los riesgos de seguridad de la información.

En el ámbito de una entidad gubernamental, esta investigación se enfocará en desarrollar un plan para administrar riesgos fundamentado en la adopción de normas nacionales. El objetivo es proporcionar un marco estandarizado que permita la identificación, evaluación y creación de un plan de mitigación de riesgos de seguridad de la información.

La relevancia social de la investigación se evidencia en su contribución a la confianza ciudadana y al cumplimiento normativo. Además, al establecer prácticas de gestión de riesgos, la investigación puede servir como modelo para otras entidades gubernamentales que enfrentan desafíos similares. La factibilidad de llevar a cabo esta investigación se respalda en el acceso a recursos y la colaboración activa de la entidad pública, para abordar los retos emergentes acerca de la seguridad de la información a nivel gubernamental.

vi. Organización del documento

Este documento está estructurado en tres capítulos que describen cada actividad realizada durante el trabajo de titulación:

En el **Capítulo I**, se exploran los antecedentes de la investigación, históricos, teóricos y contextuales relevantes para el tema del trabajo, proporcionando un marco sólido para la comprensión del problema abordado, detallando los puntos clave que fundamentan la investigación.

El **Capítulo II** se enfoca en el desarrollo del prototipo, abordando su definición, metodologías empleadas y las herramientas utilizadas en su creación. Aquí se documenta el proceso de diseño y construcción del prototipo, proporcionando una visión detallada de su estructura y funcionamiento.

En el **Capítulo III**, se realiza una evaluación del prototipo a través de un plan específico. Se analizan los resultados obtenidos durante la ejecución del prototipo y se elaboran las conclusiones y recomendaciones. Este capítulo cierra el ciclo de desarrollo del prototipo, brindando una visión integral de su desempeño y su impacto en relación con los objetivos planteados.

CAPÍTULO I. MARCO TEÓRICO

En esta sección, se adentrará en las fundamentos conceptuales y teóricos que respaldan el producto de este trabajo. Se detallan los antecedentes de la investigación, los antecedentes históricos, teóricos y contextuales.

1.1. Antecedentes de la Investigación

La adecuada definición y evaluación de las variables en el proyecto son fundamentales para comprender la eficacia de la propuesta de gestión de riesgos de seguridad de la información y su adopción de normas nacionales. Estas variables, detalladas en la Tabla 2, permiten una medición precisa de la implementación de normas ISO y la calidad del plan propuesto.

Tabla 2: Preguntas de Investigación

Pregunta de investigación	Descripción y motivación
RQ1. ¿Cuáles son los principales riesgos de seguridad de la información que enfrentan las empresas del sector público en Ecuador?	El propósito de esta pregunta es identificar los riesgos de seguridad de la información a los que se enfrentan las empresas públicas en Ecuador. Conocer estos riesgos es fundamental para poder desarrollar estrategias efectivas para prevenirlos y mitigarlos.
RQ1.1. ¿Cómo se pueden aplicar las normas ecuatorianas de seguridad de la información para mejorar la gestión de riesgos en las empresas públicas?	El objetivo de esta pregunta es identificar cómo se pueden aplicar las normas ecuatorianas de seguridad de la información para mejorar la gestión de riesgos en las empresas públicas. Comprender las mejores prácticas y estrategias para aplicar estas normas es fundamental para garantizar la seguridad de la información en las empresas públicas.
RQ1.2. ¿Cuáles son las mejores prácticas para la gestión de riesgos de seguridad de la información en las empresas públicas?	El propósito de esta pregunta es identificar las mejores prácticas para la gestión de riesgos de seguridad de la información en las empresas públicas. Al conocer que mejores prácticas usar podemos hacer un rápido monitoreo para la gestión de riesgos.

Pregunta de investigación	Descripción y motivación
RQ1.3. ¿Cuáles son las técnicas más efectivas para el análisis de riesgos de seguridad de la información en las empresas públicas?	Esta pregunta tiene como objetivo identificar las técnicas (procedimientos sistemáticos, métodos, fórmulas, rutinas mediante las cuales se realiza una tarea) más efectivas para el análisis de riesgos de seguridad de la información en las empresas públicas.
RQ1.4. ¿Cómo se pueden mejorar los procesos de gestión de riesgos de seguridad de la información en las empresas públicas utilizando tecnologías de la información?	El objetivo de esta pregunta es investigar cómo las tecnologías de la información, como sistemas avanzados de gestión de identidad y acceso, pueden ser implementadas para mejorar estos procesos. Se busca reducir la exposición a amenazas derivadas de prácticas inseguras de gestión de contraseñas y, al mismo tiempo, optimizar la eficiencia de la gestión de acceso a recursos críticos para la empresa pública.
RQ2 ¿Cuáles son los principales desafíos que enfrentan las empresas públicas en Ecuador en la gestión de riesgos de seguridad de la información?	Esta pregunta tiene como propósito identificar y comprender los desafíos específicos que las empresas públicas en Ecuador enfrentan en la gestión de riesgos de seguridad de la información. Se busca analizar las barreras y limitaciones que pueden obstaculizar la implementación efectiva de medidas de seguridad, permitiendo así desarrollar estrategias adaptadas para mejorar la resiliencia de estas instituciones ante amenazas cibernéticas.

Palabras claves y Cadenas de búsqueda

Para llevar a cabo la búsqueda de información, se utilizó la siguiente cadena de términos de búsqueda, considerando múltiples bases de datos que albergan publicaciones científicas.

Cadena de búsqueda:

(“Gestión de riesgos” OR “riesgos de seguridad” OR “riesgos de seguridad de la información”)

AND

(“Tecnologías de la información” OR “tecnología de la información” OR “seguridad de la información” OR “informática”)

AND

(“Empresa” OR “empresa pública” OR “empresas públicas”)

AND

(“Normas ecuatorianas” OR “normativa ecuatoriana” OR “regulaciones ecuatorianas” OR “leyes ecuatorianas”)

Cadena de búsqueda en inglés:

("Risk management" OR "security risks" OR "information security risks")

AND

("Information technology" OR "information security" OR "informatics")

AND

("Public" OR "public enterprise")

AND

("Ecuadorian standards" OR "Ecuadorian regulations" OR "Ecuadorian laws")

Criterios de inclusión y exclusión

En la Tabla 3 se proporcionan directrices específicas para la selección de recursos pertinentes, asegurando la relevancia y calidad de la información recopilada. Los criterios, establecidos son esenciales para garantizar la coherencia y pertinencia de la revisión bibliográfica en el contexto del proyecto.

Tabla 3: Criterios de inclusión y exclusión

#	Criterio de inclusión
1	Estudio de fuentes primarios.
2	Investigaciones que se centran en los objetivos de gestionar los riesgos de seguridad de la información y proponen mejoras mediante el uso de estándares ecuatorianos.
3	Estudio publicado en desde el 2018 hasta la actualidad.
4	Estudios que establecen vínculos entre la gestión de riesgos de seguridad de la información y las organizaciones gubernamentales.
5	Estudios que exploran la relación entre la gestión de riesgos de seguridad de la información y la tecnología de la información.
#	**Criterio de exclusión**
1	Estudio de fuentes secundarias.
2	Documentos, artículos científicos (≤ 3 páginas).
3	Investigaciones duplicadas (se ha incluido solamente una copia de cada estudio).
4	Artículos escritos en idiomas distintos al español e inglés.
5	Investigaciones evidentemente no pertinentes para la investigación, considerando las preguntas de investigación.
6	Literatura gris.
7	Repetición de trabajo por parte del mismo autor.
8	Publicaciones cuyo contenido no estaba accesible, ya sea a través de motores de búsqueda o al intentar contactar a los autores.
9	Estudios cuyo enfoque no sea la gestión de riesgos de seguridad de la información y propuestas de mejoras utilizando normas ecuatorianas en empresas públicas. (Ejemplo: análisis específicos de sistemas, desarrollo ágil, líneas de productos de software, estándares no relacionados con la seguridad de la información, entre otros).

Proceso y resultados de la búsqueda

- Se identificaron las palabras clave y los términos principales bajo investigación: gestión de riesgos, seguridad de la información, empresas públicas, normativas ecuatorianas.

- Se realizó una búsqueda en bases de datos digitales seleccionadas y consultadas como Science Direct, SpringerLink, ACM Digital Library, IEEE Xplore, Scopus y Compendex.

- Se diseñó una cadena de búsqueda utilizando los términos clave y se llevaron a cabo investigaciones preliminares con el fin de ajustar de forma repetitiva la cadena de búsqueda.

- Exclusión de términos clave que no resultaron en la obtención de nuevos artículos durante las indagaciones automatizadas. Se definieron criterios de inclusión y exclusión para seleccionar los estudios relevantes. Se incluyeron 25 artículos de revista como mínimo de los últimos 5 años (2018 - actualidad), y otros trabajos relevantes.

- Se realizó una revisión de la literatura científica y se recopilaron los resultados en un informe.

- Se crearon diagramas para visualizar los resultados de la búsqueda, incluyendo el proceso de selección de papers, cantidad de trabajos por año, y cantidad de trabajos por tópicos de IoT.

- Se incorporaron las referencias de los trabajos que tratan las preguntas de investigación o las palabras clave de búsqueda.

- Se consultó la Biblioteca Digital de la Administración (B.D.A) para obtener información adicional.

Fuentes confiables:

- IEEE Xplore

- Science Direct

- SpringerLink

- ACM Digital Library

- Scopus

- Compendex

- Biblioteca Digital de la Administración (B.D.A)

Resultados de búsqueda:

Tabla de resumen: Esta tabla resume los resultados de la búsqueda, incluyendo el número total de estudios encontrados, el número de estudios seleccionados para su revisión, y el número de estudios incluidos en el informe final. En la Figura 2 se muestra un ejemplo de tabla:

Vendor City	Vendor Name	Product Class			
		03		09	
		Suma de Unit Cost	Suma de Quantity On Hand	Suma de Unit Cost	Suma de Quantity On Hand
Ann Arbor	Arizona Industries	0	0	2,88	40
Austin	DIDA Limited	0	0	-6,8	408
Austin	Global Trade Hardware	1,22	587	0	0
Austin	Liberty Trading	0	0	0,63	112
Austin	Miller Lights	0,73	1.478	0	0
Baton Rouge	Harris Projects	0	0	9	47
Bay Minette	Larson Supplies	0	0	3	212
Bellevue	MGMT Mfg.	0	0	21,4	43
Boise	O'Conner And Daughters	12,5	248	0	0
Charleston	US Mfg. Corp	0	0	173,8	147
Charlotte	Lilydale Hardware	4,98	624	0	0
Chicago	Meridian Industries	4,12	536	0	0
Des Moines	NOVATECH Wholesale	11,53	700	0	0
Des Moines	Steel Case Manufacturing	0	0	8,08	200
Englewood	Adams & Meddick	0	0	0,43	300
Farmington Hills	Carr International	0	0	4,82	714
Gibsland	Herbie's Hardware	41,23	600	0	0

Figura 2: Tabla de resumen acerca de los costos unitarios y las cantidades de diferentes proveedores en su lista de proveedores

Fuente: Tabla de Resumen [6]

También se pueden usar gráficos estadísticos, clasificaciones por año, por cantidad de trabajos, entre otros.

1.2. Antecedentes históricos

La administración de riesgos de seguridad de la información en una entidad pública constituye un proceso crucial para salvaguardar la eficiencia y eficacia de los proyectos y procesos relacionados con la tecnología. En el ámbito gubernamental, los riesgos de TI pueden tener un impacto significativo en áreas clave como el suministro de servicios públicos, la seguridad de la información gubernamental, la transparencia y la efectividad operativa. La ejecución de una política de gestión de riesgos TI adaptada a las normativas y estándares gubernamentales vigentes, como la NTE INEN-ISO/IEC 27001:2014 o la NTE INEN-ISO/IEC 31000:2018, es esencial. Este enfoque tiene como objetivo atenuar eventos adversos potenciales que podrían

impactar la calidad, seguridad y continuidad de los servicios públicos, aportando de esta manera a mejorar el desempeño y la seguridad de los sistemas de información. Además, busca reducir pérdidas, costos y demoras asociados al riesgo [7].

Para la administración de riesgos se pueden utilizar diversas metodologías, por ejemplo, en [8], propone una metodología sustentada por COBIT 5, que es una guía de buenas prácticas para la gestión de TI. La metodología se divide en cuatro fases: reconocer los riesgos, examinar los riesgos, valorar los riesgos y abordar los riesgos.

La gestión de riesgos de seguridad de la información se posiciona como un componente crucial para el éxito de las instituciones, particularmente en el contexto de empresas públicas, donde las T.I desempeñan un papel esencial en la eficiencia operativa y la prestación de servicios gubernamentales. Aunque los proyectos de TI en entidades gubernamentales comparten desafíos similares, como el riesgo de alcance, calidad, costo y plazo, también enfrentan consideraciones únicas asociadas con la naturaleza del sector público. Es imperativo establecer políticas y metodologías de gestión de riesgos que se ajusten a las normativas gubernamentales vigentes, como la (NTE) INEN-ISO/IEC 27001:2014 o la (NTE) INEN-ISO/IEC 31000:2018. La propuesta metodológica presentada en [7], basada en estándares internacionales del Project Management Institute (PMI) y el Microsoft Solutions Framework (MSF), junto con las lecciones aprendidas de profesionales en el sector peruano, ofrece valiosas perspectivas aplicables a empresas públicas. La gestión de riesgos de proyectos de TI en el ámbito gubernamental aún enfrenta desafíos, incluida la limitación de recursos, la necesidad de una mayor utilización de herramientas cuantitativas y la importancia de sensibilizar a los ejecutivos senior. Recomendaciones clave para mejorar la gestión de riesgos incluyen la capacitación, la investigación, la difusión y la aplicación de mejores prácticas, aspectos que podrían ser particularmente beneficiosos para una empresa pública que busque fortalecer su enfoque en la gestión de riesgos de proyectos de TI. Estas recomendaciones pueden adaptarse a las normativas ecuatorianas pertinentes [7].

Esto resulta beneficioso para mejorar la implementación de principios y directrices mediante la incorporación de normas adicionales que integren los lineamientos de la norma internacional ISO 31000, adaptándose de manera coherente al contexto y los objetivos específicos de la organización. Asimismo, es esencial considerar la adhesión a las normas ecuatorianas pertinentes en el ámbito de TI, como la NTE INEN-ISO/IEC 27001, la cual define las especificaciones de un sistema de gestión de la seguridad de la información, y la NTE INEN-

ISO/IEC 20000-1, que detalla los requerimientos en un sistema de gestión de la calidad de los servicios de TI. La aplicación de estas normativas no solo proporciona un sólido marco de referencia, sino que también ofrece criterios de evaluación y buenas prácticas esenciales para prevenir, mitigar y controlar de manera efectiva las vulnerabilidades asociadas a la seguridad de la información en el ámbito de una empresa pública [9].

En el ámbito del manejo de riesgos laborales para una institución de gran envergadura que hace utiliza Tecnologías de la Información y Comunicación (TIC), la atención está centrada en tres dimensiones cruciales: estructura organizacional, gestión administrativa y tecnología de información. La finalidad principal es abordar la importancia de modernizar procesos mediante la implementación de TIC para garantizar el cumplimiento de las obligaciones fiscales como empleador, destacando particularmente la determinación del año de la prima de riesgo de trabajo (PRT). Esta propuesta aboga por una investigación cuantitativa de naturaleza exploratoria, descriptiva y experimental. La metodología abarca el análisis bibliográfico y documental, así como la aplicación de encuestas y entrevistas dirigidas a empleados y directivos de la organización. El proceso metodológico se estructura en identificar los riesgos laborales, evaluar los riesgos, implementar de medidas preventivas y correctivas, y monitorear de manera continua, junto con revisiones periódicas para asegurar la eficacia de las estrategias implementadas. Este estudio busca proporcionar una perspectiva integral sobre la administración de riesgos laborales en el ámbito de una organización, destacando la necesidad de integrar las TIC como herramienta clave para la modernización y el cumplimiento efectivo de las obligaciones fiscales [10].

Los importantes recursos institucionales y los departamentos de TI no están exentos de riesgos. Las nuevas tendencias empresariales y las nuevas empresas exigen la implementación de las tecnologías de la información (TI), que se definen como el medio que permite optimizar los recursos informáticos y de procesamiento, los recursos de información y publicidad y la conectividad a nivel global. Todos estos elementos cada vez se ven más en las empresas públicas. Se están realizando numerosos esfuerzos para establecer medios que promuevan estrategias para una administración eficaz de TI, incluyendo formas de garantizar su relevancia, reducir los riesgos asociados y satisfacer especificaciones de control más estrictas [11].

En Ecuador, el uso de marcos o modelos de TI estandarizados, modelados y reconocidos internacionalmente no es muy frecuente entre las empresas públicas. Algunas entidades, basándose en experiencias internas y en las opiniones de los responsables de los departamentos

informáticos, han adoptado esta práctica, lo cual incrementa considerablemente la probabilidad de fracaso debido a la carencia de datos y registros adecuados. Un reducido grupo de instituciones, principalmente aquellas de mayor tamaño y pertenecientes al sector privado, asumen esta actividad con la debida responsabilidad [12].

Otros investigadores, como Viteri et al. [12], han llevado a cabo estudios en el ámbito de las Tecnologías de la Información (TI), evaluando niveles de desarrollo y procesos para identificar factores que podrían contribuir a una administración más eficiente. A su vez, Oviedo et al. [13] ha examinado la seguridad cibernética de una unidad de TI y propuesto el uso de aplicaciones informáticas con el fin de mejorar la seguridad de los datos de instituciones estatales. A pesar de estos escenarios explorados, se ha prestado atención a la administración de TI; sin embargo, no se ha tenido en cuenta el tiempo, los recursos financieros y personal necesarios en la mejora efectiva de las entidades de TI del país.

En investigaciones previas, como la realizada por Ping et al. [14], en 2018, se identificaron seis aspectos fundamentales: disponibilidad, seguridad, confiabilidad, visibilidad, capacidad de respuesta y empatía. Además, sugirieron la evaluación de la calidad de los servicios en la nube utilizando el estándar ISO/IEC 25010, aplicando métricas definidas en la norma ISO. No obstante, en lugar de incorporar todas las características propuestas en el estándar, se centraron en aquellas que consideraron esenciales.

En 2020, se desarrolló una propuesta de gestión de riesgos para la Agencia Nacional de Infraestructura con el fin de evaluar los riesgos asociados a los recursos, considerando el grado de desarrollo de la seguridad existente. Su objetivo principal radica en promover la conformidad del personal de la Agencia Nacional de Infraestructura (ANI) con las normas y procedimientos pertinentes al ámbito de seguridad de los datos y recursos [15].

El objetivo principal de la Estrategia de Tratamiento de Riesgos para la Seguridad de la Información 2023 era evaluar y debatir las posibles medidas que pueden adoptarse para reducir las amenazas actuales. En esta estrategia se tienen en cuenta las normas de aceptación de riesgos establecidas por la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD). Concebido como parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de la UNGRD, busca establecer regulaciones y acciones efectivas y transversales. Para garantizar la disponibilidad, integridad y confidencialidad de la información de la entidad, estas acciones deben estar bien documentadas, sistematizadas y estructuradas. La estrategia

proporciona un marco crucial para la adopción de decisiones y la administración eficaz de la seguridad de la información en la UNGRD, al esbozar normas precisas para el estudio y valoración de las amenazas a la seguridad de la información [16].

1.3. Antecedentes Teóricos

Los temas y subtemas que se abordarán en esta sección se detallan en la Figura 3.

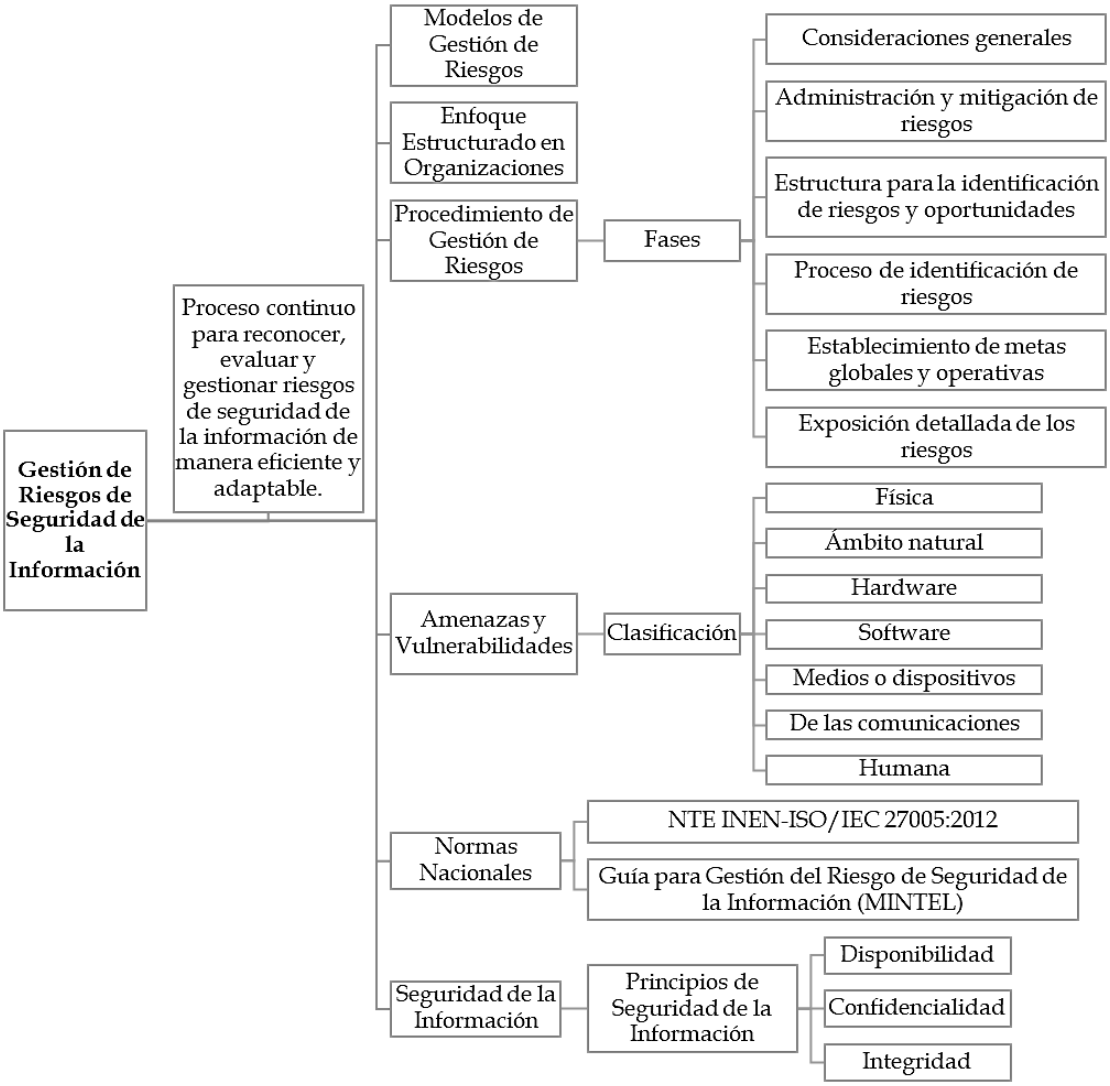


Figura 3: Gestión de riesgos de seguridad de la información

1.3.1 Gestión de la seguridad de información

El énfasis en la importancia de la información se extiende al sector público, donde su gestión adecuada no solo es crucial para los procesos internos, sino también para definir estrategias organizativas. Esto incluye una atención particular a la protección de la información en este ámbito [17].

La Seguridad de la Información abarca diversos aspectos. Por ejemplo, el control informático y de sistemas puede garantizarla, pero puede pasar por alto el factor humano que podría acceder al sistema. De igual manera, si solo se enfoca en el factor humano, se podría descuidar el aspecto legal. Es fundamental considerar todos estos aspectos de manera integral para garantizar una seguridad efectiva de la información [18].

La seguridad en los procesos logísticos se ha vuelto esencial para las empresas, siendo un factor determinante para su eficacia y rentabilidad operativa. Desde la cadena de suministro hasta la satisfacción del cliente, la seguridad es un aspecto crucial que antes se subestimaba. Sin embargo, se ha demostrado que evaluar los riesgos en estos procesos es vital para mantener la competitividad empresarial [19].

El objetivo principal de la gestión de la seguridad de la información, que se establece como una operación continua, es asegurarse de que los riesgos para la seguridad de la información se identifican, evalúan, gestionan y tratan de una manera que sea eficiente, repetible, ordenada, organizada, documentada y sensible a las variaciones en los riesgos, el ambiente y las tecnologías. Este enfoque implica la involucración activa de todos los integrantes dentro de la organización [20].

Independiente de la naturaleza o el sector de mercado al que pertenezcan, las organizaciones y sus sistemas de información se enfrentan cada vez más a una variedad de amenazas. Estas amenazas tienen la capacidad de poner en peligro los activos de información vitales aprovechando los puntos débiles ya presentes y dejándolos expuestos al fraude, el vandalismo, el sabotaje y el espionaje. La información y los sistemas y procedimientos que la emplean se han convertido en recursos vitales para las empresas en la era moderna. La Integridad, confidencialidad y accesibilidad de los datos sensibles es crucial para garantizar la competitividad, rendimiento, cumplimiento legal e imagen empresarial necesarios para alcanzar los objetivos dentro de la organización y garantizar beneficios económicos [21].

Las vulnerabilidades son defectos o debilidades de seguridad presentes en el diseño de un software, plataforma o programa informático. A veces, estos fallos no son detectados por el programador o administrador del sistema, pero pueden ser identificados y aprovechados por atacantes o cibercriminales. Esto les permite llevar a cabo acciones perjudiciales como la eliminación de datos o la introducción de malware. [22].

También tenemos los activos que comprenden la información en su forma más elemental, así como los dispositivos o repositorios que almacenan esta información. Por ejemplo, las bases de datos, los servidores y los centros de datos se consideran activos de información, ya que contienen y gestionan la información vital para una empresa o persona [23].

La introducción de tecnologías avanzadas presenta desafíos que deben ser enfrentados de manera adecuada, y la adopción de planes de gestión basados en normativas reconocidas se revela como una estrategia efectiva para fortalecer la seguridad [24].

La gran parte de los incidentes de robo o pérdida de información en América Latina impacta principalmente al sector empresarial. Según [25], señala que estos eventos suelen derivarse de la falta de medidas de protección adecuadas. Esta carencia conduce a consecuencias significativas, incluyendo pérdidas de productividad, afectación de la credibilidad, disminución de la competencia empresarial y daños económicos que amenazan la sostenibilidad misma de la entidad [26].

1.3.2 Enfoques para la gestión de riesgos

Actualmente, se emplean diversos esquemas para llevar a cabo un procedimiento ordenado y metódico que se aplica al tomar decisiones que optimizan la eficacia y eficiencia de las organizaciones. Estos esquemas facilitan la identificación y preparación para posibles eventualidades, consistiendo en implementar medidas proactivas para evitar y minimizar la exposición a los gastos u otros impactos de los eventos que puedan suceder, en vez de responder después de que el evento ha sucedido y enfrentar los gastos asociados a la recuperación de la situación [27].

La gestión de riesgos para la seguridad sostenible implica la implementación de diversas tácticas destinadas a potenciar el desempeño empresarial, identificar posibles riesgos y amenazas mediante políticas variadas con el fin de prevenirlos, al mismo tiempo que se considera el bienestar tanto de los empleados como de los usuarios [28].

La demanda de las organizaciones de gestionar los riesgos de manera sistemática ha dado origen a la gestión de riesgos y las normativas relacionadas. Muchas amenazas no se evalúan ni controlan adecuadamente, por lo que es esencial implementar un sistema de gestión de riesgos. Se requiere una estrategia para manejar de manera más efectiva tanto los riesgos como las

oportunidades, equilibrando la perspectiva del riesgo y minimizando los peligros mientras se controlan las incertidumbres [29].

La evolución de la gestión de riesgos se enfoca en minimizar pérdidas financieras y garantizar objetivos estratégicos, además de prevenir la pérdida de vidas humanas. Las organizaciones están adquiriendo una "conciencia del riesgo" debido a experiencias pasadas y la presión externa que enfrentan [30].

1.3.3 Enfoque sistemático de la gestión de riesgos en las organizaciones

La gestión de riesgos es un proceso de organización y supervisión de los elementos de una organización que están vinculados al riesgo. Se caracteriza por la evaluación de las ventajas, desventajas, inquietudes y situaciones que pueden afectar todas las operaciones de una empresa. Al establecer este sistema, se previene la mal versión de los recursos y se facilita el logro de metas de crecimiento y rentabilidad.

Dos estándares prominentes en el manejo de riesgos son ISO 31000 y COSO 2013. ISO 31000 se centra en guiar a las instituciones en la administración del riesgo considerando la diversidad de los riesgos. COSO 2013, emitido por el Committee of Sponsoring Organizations of the Treadway Commission, se actualizó para adaptarse a los cambios empresariales. La adopción de estos estándares facilita la comparación internacional y promueve una gestión eficiente del riesgo y buen gobierno corporativo [31].

Los desafíos actuales que enfrentan las organizaciones en un entorno competitivo e incierto han llevado a la necesidad de adoptar nuevos enfoques de gestión para fomentar la innovación en sus prácticas diarias. Esto implica la redefinición formal de estrategias para promover la innovación dentro de las organizaciones [32].

Es una obligación constitucional para las instituciones públicas proteger la información de los ciudadanos, ya sea de funcionarios que contribuyen al objetivo de la entidad o de los usuarios que confían sus datos personales para acceder a servicios gubernamentales. Existe el riesgo de difusión o uso indebido de esta información, lo que subraya la importancia de su protección [33].

En el contexto de esta investigación, se destaca el afán de comprender el riesgo financiero, que implica la variación entre el rendimiento previsto y el rendimiento efectivo o cambios en la cartera de inversión. Este tipo de riesgo se desglosa en riesgo financiero, financiamiento,

funcional, legítimo y de solidez financiera. La comprensión de estos riesgos financieros resulta fundamental para sostener un balance entre los riesgos y la ganancia, asegurando la solidez financiera de la empresa y atrayendo potenciales inversores [31].

1.3.4 Fases del procedimiento elaborado para la gestión de riesgos, integrado al sistema de gestión de la calidad

- **Consideraciones generales**

  Para instaurar un control interno eficaz, resulta esencial que la organización lleve a cabo un ejercicio estratégico destinado a identificar los elementos del entorno externo e interno, así como sus tendencias.

- **Administración y mitigación de riesgos**

  Esto se basa en la identificación y evaluación de los riesgos críticos para la consecución de los objetivos. Después de clasificar los riesgos en internos y externos, por procesos, actividades y operaciones, y evaluar las vulnerabilidades principales, se establecen las metas de gestión y regulación y se formula el programa de prevención de riesgos para definir cómo gestionarlos. Para lograr una gestión de riesgos efectiva, las organizaciones deben aplicar los principios de gestión de riesgos en todos sus niveles. Es crucial identificar todos los riesgos dentro de los procesos; todos los trabajadores están involucrados en el proceso, por lo tanto, deben expresar sus opiniones e identificar aquellas significativos, utilizando técnicas específicas cualitativas y cuantitativas. Para esto, es necesario contar con información, datos y antecedentes, evaluando la frecuencia de eventos a lo largo de los años. El análisis se presenta a la dirección de la organización por cada proceso y se abordan los riesgos significativos. Los riesgos se incorporan al plan de prevención de gestión de calidad, incluyendo aquellos que puedan ser aprovechados como oportunidades. Se establecen indicadores para medir los riesgos.

- **Estructura para la identificación de riesgos y oportunidades**

  Es crucial colaborar con un grupo de individuos que posean una comprensión de la naturaleza de los cambios significativos, como posibles avances tecnológicos, y que cuenten con la capacidad imaginativa para proyectarse en el futuro. Además, resulta beneficioso tener acceso a documentación y datos relacionados con cambios ya

ocurridos, así como identificar riesgos, peligros y vulnerabilidades clave. Este enfoque simplificará el proceso de diagnóstico y permitirá la identificación de objetivos de control concretos en cada uno de los procesos.

- **Proceso de identificación de riesgos**

  Se busca la participación activa de los trabajadores, incluyendo la obtención de sus opiniones sobre los riesgos a los que se enfrentan. Esto implica reconocer condiciones potenciales de daño y analizar factores internos y externos que puedan obstaculizar los objetivos. Se considerarán aspectos históricos relevantes en este análisis.

- **Establecimiento de metas globales y operativas**

  - **Establecimiento de los objetivos generales de la entidad y de las estrategias clave que han sido definidas.**

    Para asegurar un control eficaz, es imperativo que una entidad establezca objetivos concretos. Las metas de la entidad, respaldadas por los correspondientes planes estratégicos, son expresiones amplias que describen los objetivos generales.

  - **Establecimiento de los objetivos específicos u operativos para cada proceso y subproceso crítico.**

    Los objetivos se definen tanto para las actividades fundamentales en la secuencia de entrega de productos y servicios, como para las funciones de respaldo, las cuales tienen una importancia crucial en la realización de esos objetivos.

- **Exposición detallada de los riesgos**

  Con el fin de realizar una evaluación eficiente de los riesgos, se llevan a cabo entrevistas, discusiones en grupo y sesiones de lluvia de ideas en colaboración con los trabajadores [9].

1.3.5 Amenazas y Vulnerabilidades

En teoría, estos conceptos son similares, es decir, se refieren a lo mismo; ambos pertenecen al campo de la seguridad informática.

Las vulnerabilidades en el ámbito informático representan las potenciales debilidades que una organización podría enfrentar ante amenazas que puedan comprometer el estado íntegro de la información. Cualquier incidente, independientemente de su origen, tiene el potencial de alterar la integridad de datos y provocar deterioro en los sistemas informáticos. En la Tabla 4 se detalla la clasificación de las vulnerabilidades informáticas.

Tabla 4: Clasificación de las vulnerabilidades informáticas

CLASIFICACIÓN DE LAS VULNERABILIDADES INFORMÁTICAS	
Vulnerabilidad física	Ejemplo: infraestructura de la organización.
Vulnerabilidad en el ámbito natural	Relacionado a fenómenos naturales.
Vulnerabilidad relacionada al hardware	Fallas de computadoras.
Vulnerabilidad relacionada al software	Accesos ilícitos a sistemas informáticos, sin conocimiento del usuario.
Vulnerabilidad de medios o dispositivos	Soportes físicos utilizados para grabar información.
Vulnerabilidad de las comunicaciones	Recorrido de la información, hacia donde va a llegar.
Vulnerabilidad humana	Daños por parte de las personas a los equipos de cómputo o a la información.

Fuente: Gestión del riesgo del área informática del Centro de Educación Continua de la Universidad Técnica de Machala [34]

1.3.6 Norma Técnica Ecuatoriana - Instituto Ecuatoriano de Normalización ISO/IEC 27005:2012

La aplicación de la Norma Técnica Ecuatoriana del Instituto Ecuatoriano de Normalización ISO/IEC 27005 (2012) es extensible a diversas organizaciones que aspiran a administrar los riesgos que pueden poner en riesgo la integridad de los datos. Según esta norma, su objetivo central es presentar un sistema para gestionar los riesgos de seguridad de la información, con especial atención en la tecnología de la información. Considerando este contexto, se subraya

que la organización tiene la responsabilidad de definir su enfoque específico para la gestión de riesgos, proporcionando así flexibilidad y adaptabilidad a diferentes contextos y necesidades [4].

El detalle de la estructura de la norma ISO / IEC 27005: 2012 se muestra en la Tabla 5, ofreciendo una visión organizada de los elementos clave que guiarán la propuesta de mejora en el manejo de riesgos de seguridad de la información en la entidad pública.

Tabla 5: Estructura de la Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012

NTE INEN-ISO/IEC 27005:2012
1. Alcance
2. Referencias Normativas
3. Términos y definiciones
4. Estructura de esta norma
5. Información general
6. Visión general del proceso de gestión del riesgo de la seguridad de la información
7. Establecimiento del contexto **7.1** Consideraciones generales **7.2** Criterios básicos **7.3** El alcance y los límites **7.4** Organización para la gestión del riesgo de la seguridad de la información
8. Valoración del riesgo de la seguridad de la información **8.1** Descripción general de la valoración del riesgo en la seguridad de la información **8.2** Análisis del riesgo **8.2.1** Identificación del riesgo 8.2.2 Estimación del riesgo **8.3** Evaluación del riesgo
9. Tratamiento del riesgo de la seguridad de la información **9.1** Descripción general del tratamiento del riesgo **9.2** Reducción del riesgo **9.3** Retención del riesgo **9.4** Evitación del riesgo **9.5** Transferencia del riesgo

NTE INEN-ISO/IEC 27005:2012
10. Aceptación del riesgo de la seguridad de la información
11. Comunicación de los riesgos de la seguridad de la información
12. Monitoreo y revisión del riesgo de la seguridad de la información **12.1** Monitoreo y revisión de los factores de riesgo **12.2** Monitoreo, revisión y mejora de la gestión del riesgo
13. Anexo A (Informativo) Definición del alcance y los límites del proceso de gestión del riesgo de la seguridad de la información
14. Anexo B (Informativo) Identificación y valoración de los activos y valoración del impacto
15. Anexo C (Informativo) Ejemplos de amenazas comunes
16. Anexo D (Informativo) Vulnerabilidades y métodos para la valoración de la vulnerabilidad
17. Anexo E (Informativo) Enfoques para la valoración de riesgos en la seguridad de la información
18. Anexo F (Informativo) Restricciones para la reducción de riesgos

Fuente: [4]

1.3.7 Normas INEN - Guía para la gestión de riesgos de seguridad de la información (MINTEL)

La digitalización de procesos impulsa un cambio significativo en la manera en que las organizaciones a nivel global gestionan la información, convirtiéndose en el actor central de este proceso transformador. Este fenómeno ha propiciado la formación de nuevas alianzas y la reducción de brechas entre naciones, donde el internet se ha convertido en un elemento clava para facilitar la comunicación en este nuevo paradigma [5].

Adoptar una visión metodológica de la administración de riesgos es necesario para garantizar la seguridad de la información (Tabla 6). Este método se centra en la identificación de los requisitos particulares de la institución con respecto a las condiciones de seguridad de la información, con el propósito de establecer un sistema de gestión de la seguridad de la

información (SGSI) eficaz. Esto permite abordar un tratamiento exhaustivo de los posibles peligros que puedan surgir, protegiendo datos sensibles que son cruciales para el funcionamiento de la entidad [5].

Tabla 6: Proceso para la norma INEN - gestión del riesgo de seguridad de la información

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	**1** Consideraciones Generales - Levantamiento de información inicial **2** Establecer criterios básicos para la Gestión del Riesgo **3** Definir alcance y límites de la Gestión del Riesgo **4** Establecer una organización para la operación del SGRSI
Valoración del Riesgo	**5** Identificar Activos de Información **6** Identificar las amenazas y las vulnerabilidades **7** Identificar los controles existentes **8** Identificar consecuencias **9** Valorar las consecuencias **10** Valorar los incidentes **11** Determinar el nivel de estimación del riesgo **12** Evaluar el riesgo
Tratamiento del Riesgo	**13** Seleccionar controles
Aceptación del Riesgo	**14** Aceptar el riesgo
Comunicación del Riesgo	**15** Comunicar el riesgo
Monitoreo y Revisión del Riesgo	**16** Monitorear y revisar los riesgos

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5]

1.3.8 Norma Técnica Ecuatoriana - Instituto Ecuatoriano de Normalización ISO/IEC 27001:2011

Esta norma ofrece una visión clara sobre los requisitos fundamentales para establecer, implementar y mejorar de manera continua un sistema sólido que proteja la integridad, confidencialidad y disponibilidad de la información en una organización [20].

Esta norma utiliza el modelo "Planificar-hacer-verificar-actuar" (conocido como PDCA) para estructurar todos los procesos del Sistema de Gestión de Seguridad de la Información (SGSI) [20].

El proceso PDCA lo podemos observar en la figura 4.

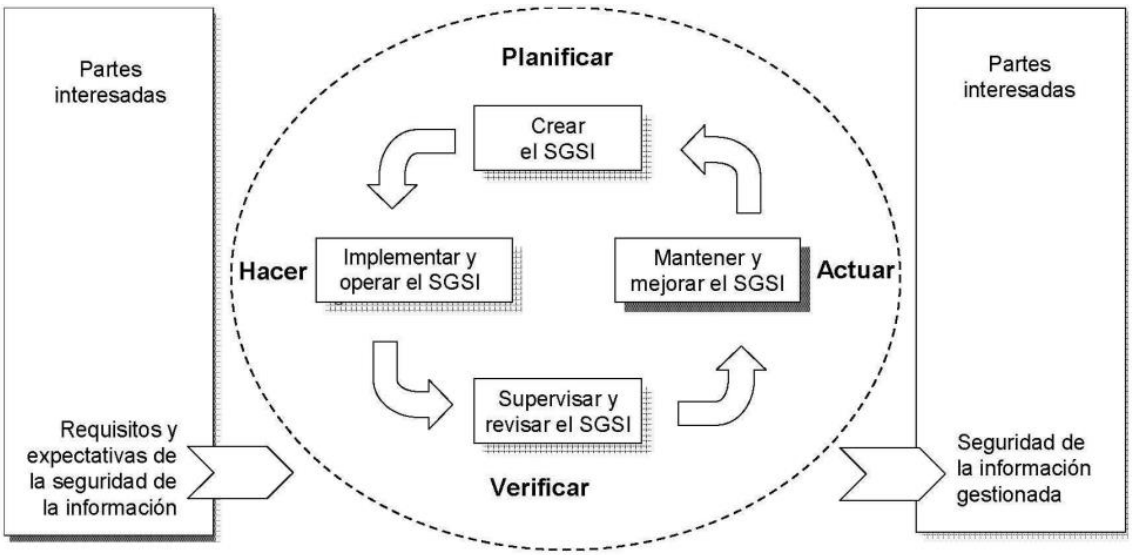


Figura 4: Modelo PDCA aplicado a los procesos del SGSI

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27001:2011 [20]

1.3.9 Seguridad de la Información

La seguridad de la información se ocupa de proteger, valorar y gestionar los activos de información y sus vulnerabilidades, teniendo en cuenta las repercusiones que pueden tener en una empresa. Esta idea va más allá de la seguridad básica de las TIC para incluir todos los recursos relacionados a la información valiosos para la entidad. En consecuencia, la seguridad de la información se concibe como una práctica integral que engloba una serie de estrategias, medidas preventivas y correctivas implementadas en las instituciones con el fin de preservar los datos críticos y asegurar que se encuentren disponibles, completos y seguros. [4].

La seguridad de la información implica la ejecución tanto de estrategias preventivas como reactivas por parte de individuos, entidades y sistemas técnicos. Esto se lleva a cabo con el propósito de preservar la integridad, privacidad y autenticidad de los datos [4].

El veloz avance tecnológico ha simplificado el acceso, procesamiento y utilización de la información, generando una mayor incidencia de problemas en la seguridad de la información que amenazan los recursos más cruciales en cualquier organización: la información [4] [35]. Ante este escenario, las organizaciones establecen normas y modelos de protección destinados a resguardar la accesibilidad, seguridad y exactitud de los datos. Basados en técnicas de

seguridad, estos esfuerzos tienen como objetivo asegurar el apropiado funcionamiento y circulación de datos e información entre usuarios.

Para garantizar una seguridad efectiva de los datos o la información, es fundamental que las entidades identifiquen las amenazas a las que se encuentran susceptibles. Esto es especialmente crucial para las empresas involucradas en la gestión económica y comercial, ya que suelen enfrentar pérdidas significativas debido a fallos y ataques dirigidos a sus servidores [36].

Las empresas que proporcionan productos y servicios tecnológicos se encuentran sometidas a una presión continua de mantener la calidad del servicio y suministrar las herramientas estables que necesitan los consumidores [37].

1.3.10 Principios de seguridad de la información

La pérdida de acceso, privacidad o integridad de la información puede ser el resultado de la ocurrencia de varios incidentes contra los recursos de TI. Frecuentemente, este escenario lleva consigo consecuencias significativas para las empresas, a veces resultando en daños irreparables.

- **Disponibilidad**

  El propósito fundamental de este principio es garantizar que tanto los datos como los sistemas que los respaldan se encuentren accesibles al instante que son requeridos, siempre para el personal autorizado que deba emplearlos.

- **Confidencialidad**

  El objetivo primordial de este principio es garantizar que únicamente el personal autorizado pueda acceder a la información específica. Los datos, tanto internos como externos de una entidad, no necesariamente está destinada a accesible para cualquier persona, sino que se encuentra dirigida a un grupo específico de personas o, en algunos casos, a una única persona. En consecuencia, es esencial asegurar que aquellos individuos no autorizados no puedan acceder a datos importantes.

- **Integridad**

  Busca asegurar que la información no se vea alterada o modificada por individuos no autorizados o de manera inapropiada, teniendo como objetivo principal preservar su

integridad. Además, se extiende a los sistemas, con la intención de tener certeza de la precisión y fiabilidad de estos.

1.4. Antecedentes Contextuales

En los modelos contemporáneos de gestión empresarial, la información es vista como el recurso más valioso. Esta puede presentarse en múltiples formas: impresa, almacenada digitalmente, transmitida a través de varios canales como el correo electrónico, representada en videos o discutida en conversaciones. En el contexto financiero actual, dicha información está constantemente sujeta a amenazas de diversas fuentes, ya sean internas o externas, accidentales o intencionadas. Con la creciente adopción de tecnologías emergentes para el almacenamiento, transmisión y recuperación de información, se han abierto más vías que permiten una mayor diversidad y cantidad de amenazas. Por lo tanto, es esencial aplicar un plan de seguridad de la información en todas las organizaciones. El objetivo de este plan es asegurar la confidencialidad, integridad y disponibilidad de la información crítica para la organización y sus clientes.

Como ejemplo, las empresas de menor tamaño, que poseen una estructura limitada y sistemas informáticos de gestión que no implican el almacenamiento o procesamiento de datos sensibles, y que no están sujetas a estrictas normativas regulatorias, por lo general, enfrentarán riesgos de menor magnitud. Estas empresas deben considerar aspectos distintos en comparación con grandes corporativos o grupos empresariales del sector financiero. La dimensión del problema, tanto en su complejidad como en la capacidad de gestión de la solución, también difiere. En consecuencia, sus estrategias y decisiones se ajustarán a estas variaciones estructurales.

Por el contrario, las organizaciones de mayor tamaño, como aquellas en los sectores financiero, de salud, telecomunicaciones, gubernamentales, entre otros, necesitan abordar la seguridad de la información de manera rigurosa y planificada, implementando planes específicos con un enfoque en la continuidad del negocio y la mejora continua. Además de considerar parámetros y dimensiones diferentes en su evaluación costo-beneficio, estas organizaciones enfrentan motivaciones legales, regulaciones y contratos que demandan privacidad de datos sensibles, junto con la consideración crítica de la estrategia del negocio [38].

En la actualidad, las organizaciones, independientemente de su clasificación, cuentan con diversos activos que incluyen infraestructura o instalaciones físicas, mobiliario, equipos informáticos, plataformas de comunicación, equipos de red, activos financieros líquidos y

vehículos, entre otros. Sin embargo, a pesar de la diversidad de activos, el elemento más fundamental, que a veces no recibe la atención necesaria por parte del gobierno corporativo y la gestión de las organizaciones, es la información. Además, en la actualidad se reconoce que algunos de los desafíos más importantes que enfrentan estas entidades están relacionados con asuntos como el tráfico, espionaje y sustracción de información [39].

La falta de eficacia en la gestión de los riesgos cibernéticos en las organizaciones a menudo resulta en consecuencias económicas significativas. Por lo tanto, es fundamental adoptar un enfoque sistemático y constante, priorizando las acciones preventivas sobre las correctivas. Este método tiene como objetivo evaluar la susceptibilidad a los riesgos cibernéticos y tomar medidas para mitigarlos. La evaluación de vulnerabilidades implica identificar, medir y dar prioridad a las deficiencias de seguridad en un sistema informático, lo que resulta fundamental para protegerse contra las posibles amenazas cibernéticas [40].

Los modelos de evaluación de sistemas de seguridad brindan perspectivas sobre la madurez de una organización en términos de sus políticas, prácticas, herramientas y métodos relacionados con la seguridad. Para una entidad enfocada en su seguridad informática, es esencial disponer de estándares y herramientas adecuadas para evaluar su conformidad con dichos estándares [3].

La gestión de riesgos se considera un elemento fundamental para garantizar de manera efectiva el cumplimiento de los objetivos institucionales. A nivel global, el Committee of Sponsoring Organizations of the Treadway Commission (COSO) ha encabezado investigaciones significativas sobre este tema, ofreciendo marcos y directrices generales a lo largo de varios años. Su enfoque se ha centrado en mejorar el desempeño empresarial, lo que ha resultado en una evolución constante en las ideas y enfoques relacionados con la gestión de riesgos [41].

En Ecuador, se ha avanzado significativamente hacia la implementación de controles internos con el objetivo de facilitar el logro de metas en las organizaciones. La Constitución de la República del Ecuador de 2008 estableció que la Contraloría General del Estado (CGE) es la entidad técnica responsable de supervisar el uso de los recursos del estado. Además, tiene la responsabilidad de liderar la estructura de gestión administrativa, que engloba análisis interno y externo y supervisión interna tanto en organismos gubernamentales como en aquellos privadas que manejan recursos públicos [42].

Las modificaciones a la legislación ecuatoriana, junto con las reformas realizadas en la Ley Orgánica de la CGE y los progresos en las prácticas de gestión pública moderna, fueron el

motor para actualizar los reglamentos de gestión interna en Ecuador. En respuesta a las reformas en el marco regulatorio del control interno, la CGE determinó que cada entidad estatal debía desarrollar normativas, políticas y manuales específicos adaptados a sus necesidades de gestión. Estos documentos debían abordar directrices generales y otras específicas relacionadas con la gestión financiera gubernamental, la gestión de recursos humanos, tecnologías de la información y la gestión de proyectos. Además, se promovió la implementación del marco COSO, que propone cinco componentes integrados y conectados al proceso de gestión, con el objetivo de ayudar a las entidades a alcanzar sus metas [41].

La gestión de riesgos y su evolución desde el control interno en Ecuador

En Ecuador, la evolución del control interno ha seguido diversos planteamientos conceptuales y legales, siendo la Contraloría General del Estado (CGE) la entidad encargada de emitir normativas al respecto. En 1977, la Ley Orgánica de Hacienda fue reemplazada por la Ley Orgánica de Administración Financiera y Control, que adoptó un enfoque sistemático de los componentes de la administración financiera. La CGE formuló las Normas Técnicas de Control Interno, actualizadas en 1994 [41].

A partir de los años 90, influencias internacionales, como el informe COSO, impactaron el desarrollo del control interno en Ecuador. En el 2002, la CGE emitió nuevas Normas Técnicas alineadas con el informe COSO, introduciendo la evaluación de riesgos como componente clave del control interno. Estos cambios se centraron principalmente en los riesgos asociados a la información financiera [41].

Posteriormente, ante cambios legislativos, la CGE actualizó las normas de control interno, considerando la nueva Constitución de la República del Ecuador, reformas a la Ley Orgánica de la CGE y avances en la administración pública moderna. La evaluación del riesgo se consolidó como componente esencial, con la máxima autoridad responsable de establecer mecanismos para reconocer, examinar y abordar riesgos. Normativas específicas como Análisis del riesgo, Plan de mitigación de riesgos, Evaluación del riesgo y Respuesta al riesgo fueron incluidas [41].

Fundamentos del sistema de gestión de la seguridad 27005

La norma ISO 27005 se aplica en una variedad de contextos organizativos para manejar los riesgos que podrían comprometer la seguridad de la información en su entorno. No prescribe

una estrategia específica, ya que la elección dependerá de varios aspectos, dependiendo del alcance efectivo del SGSI o del sector empresarial al que pertenezca la institución. Los interesados tienen la flexibilidad de elegir libremente el enfoque que más se ajuste a sus requisitos, pudiendo optar, como muestra, por una revisión general del riesgo seguido por un análisis minucioso de las áreas de mayor riesgo. [43].

1.4.1 Ámbito de aplicación

Este proyecto de se enfoca en la administración de riesgos de seguridad de la información en una empresa pública, con el propósito de proponer mejoras y promover la adopción de normas nacionales pertinentes. La empresa objeto de estudio podría enfrentar desafíos significativos en la seguridad de la información por no contar con un enfoque integral respaldado por estándares ISO, lo que compromete la privacidad, integridad y accesibilidad de los datos.

La importancia de este proyecto radica en la necesidad de optimizar los componentes críticos de protección de la información, así como en la detección y reducción de vulnerabilidades en la infraestructura tecnológica empresarial. La ausencia de una evaluación exhaustiva de riesgos y de una estrategia de seguridad planificada agrava aún más esta problemática, lo que puede exponer a la empresa a riesgos financieros, legales y operativos.

Mediante el uso de normas nacionales de seguridad de la información en la propuesta de mejores prácticas, se busca fortalecer la seguridad de la información de la empresa pública. Se espera que este proyecto contribuya a promover prácticas seguras y a mitigar los riesgos asociados con la gestión de la información sensible. La adopción de normas nacionales también puede mejorar la capacidad de la empresa para adaptarse proactivamente a las amenazas emergentes y salvaguardar la seguridad de los datos críticos.

1.4.2 Establecimiento de requerimientos

El desarrollo de la propuesta de mejoras y la adopción de normas nacionales para la gestión de riesgos de seguridad de la información en la empresa pública requiere:

- **Establecimiento claro del contexto de gestión del riesgo:** Definir el contexto en el que se llevará a cabo la gestión del riesgo de seguridad de la información, incluyendo consideraciones generales, criterios básicos, alcance y límites.

- **Asignación de responsabilidades organizacionales:** Designar roles y responsabilidades dentro de la organización para la gestión de riesgos.

- **Identificación de activos críticos:** Identificar los activos de seguridad de la información y sistemas críticos para la empresa pública.

- **Análisis de amenazas potenciales:** Analizar y documentar las posibles amenazas que puedan afectar a los activos de seguridad de la información.

- **Establecimiento de criterios de evaluación de riesgos:** Consiste en establecer los criterios que se utilizarán para analizar y clasificar los riesgos asociados a la seguridad de la información.

- **Establecimiento de medidas para tratar los riesgos identificados:** Incluyendo la reducción del riesgo, la retención, la evitación o la transferencia del mismo, según sea apropiado.

- **Establecer un mecanismo de recepción y comunicación de la gestión de riesgos de seguridad de la información con las partes interesadas:** Informar a la empresa los resultados, asegurando que posea la información disponible para tomar decisiones

- **Elaboración de propuesta de mejoras:** En base a la gestión de riesgos de seguridad de la información identificados en la empresa [4] [5].

CAPÍTULO II. DESARROLLO DEL PROTOTIPO

En el presente capítulo, se abordará el desarrollo de la propuesta. Se relacionará la definición del proyecto junto con la metodología a utilizar, además se abarcará tanto el enfoque, alcance y diseño de investigación. Añadiendo a esto, también se tratará las unidades de análisis (población y muestra), así como los métodos y herramientas de recopilación y procesamiento de los datos.

2.1 Definición del prototipo

La elaboración del proyecto aborda la gestión de riesgos de seguridad de la información en una empresa pública, cuya finalidad es proponer mejoras a la seguridad de la información. La investigación se apoya en un análisis exhaustivo de la literatura, estudios de caso y evaluación de normas nacionales basadas en la NTE INEN-ISO/IEC 27005 y Normas INEN - Guía para la gestión de riesgos de seguridad de la información, pertenecientes al estado ecuatoriano.

Los principales procesos de mejoras a realizar incluyen: definición del contexto, evaluación de riesgos, gestión de riesgos, aceptación de riesgos y comunicación de riesgos (Figura 5). Todo esto permite a la empresa tener mayor seguridad de la información de su infraestructura tecnológica.

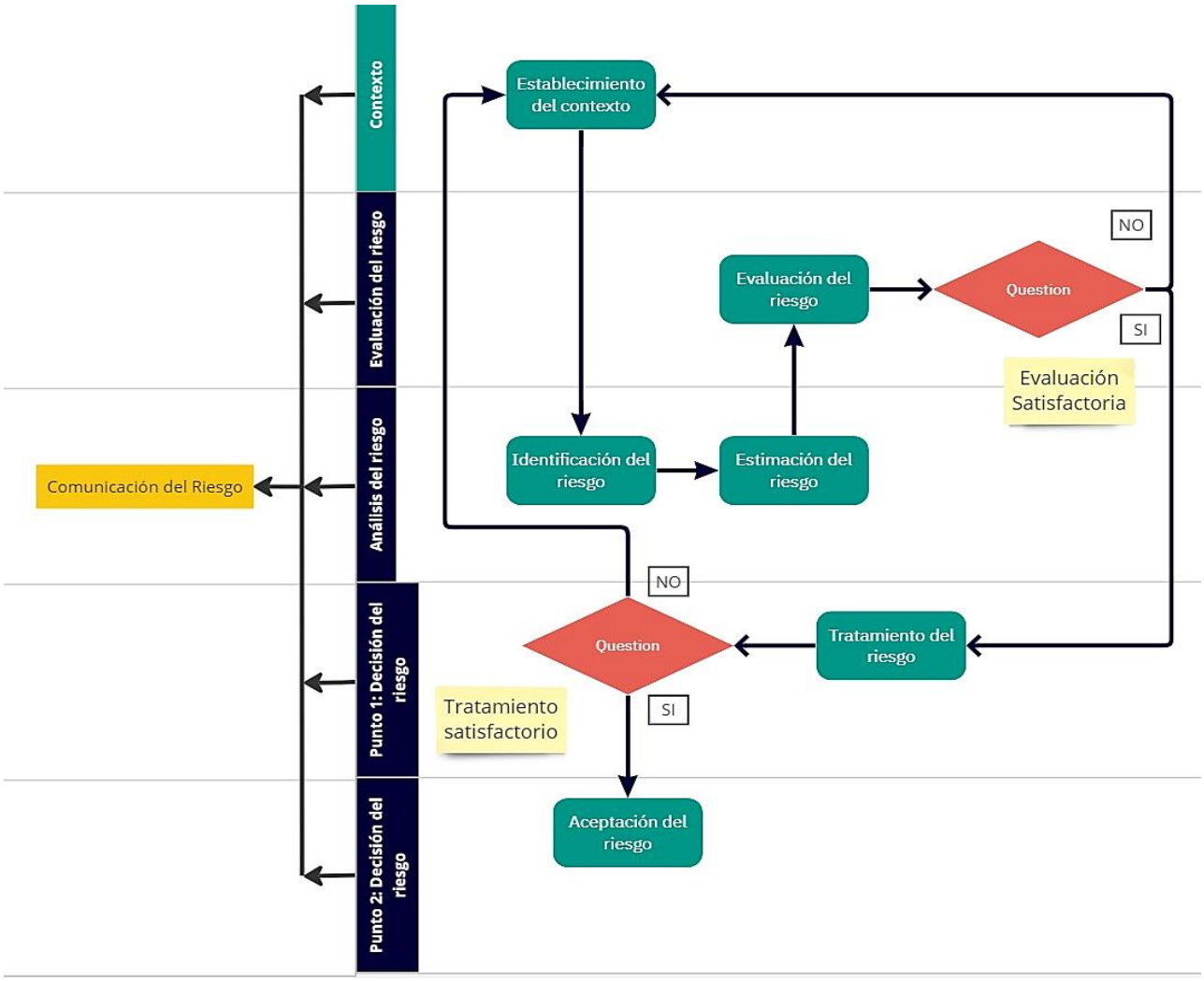


Figura 5: Definición del prototipo

Elaborado a partir de: [5]

2.2 Metodología de desarrollo del prototipo

2.2.1 Enfoque, alcance y diseño de investigación

Para este proyecto se utilizará la NTE INEN-ISO/IEC 27005 que ofrece pautas para administrar el riesgo de seguridad de la información en una entidad, respaldando específicamente los criterios de un SGSI [44].

Se usará un enfoque cuantitativo; analizando los estándares de la Norma, dando como resultado una aplicación correcta de estas mismas, determinando las vulnerabilidades en la seguridad de la empresa.

El alcance será descriptivo y explicativo. En la dimensión descriptiva, se llevará a cabo un análisis detallado de la situación actual de la empresa en términos de gestión de riesgos de

seguridad de la información, identificando sus vulnerabilidades y procesos actuales. En la dimensión explicativa, se buscará comprender las relaciones entre la adopción de normas nacionales y la optimización de la gestión de riesgos.

La investigación seguirá un diseño no experimental transversal, recopilar datos en un punto en el tiempo. Dado que el proyecto se enfoca en la documentación de propuestas de mejora, un diseño transversal permite capturar una instantánea de la situación actual en la empresa pública en relación con la gestión de riesgos de seguridad de la información. El diseño proporcionará una visión integral y detallada sin la necesidad de intervenciones en el entorno de la empresa.

2.2.2 Unidades de análisis

Población (universo)

La infraestructura tecnológica de la empresa pública, todos los procesos relacionados con la seguridad de la información en la institución, y todo el personal involucrado en la gestión de riesgos y seguridad de la información.

Muestra

No aplica, se analizarán todos los activos de la empresa entre estos se incluye: sistemas informáticos, página web, equipos clave y segmentos de red LAN. Se incluirán representantes dentro del personal involucrado como administradores de sistemas, personal de TI.

2.2.3 Técnicas e instrumentos de recopilación de datos

- **Análisis de Documentos**

  Descripción: Revisar la documentación existente.

  Instrumentos: Listas de verificación y matrices de análisis.

- **Entrevistas**

  Descripción: Entrevistar a los principales interesados, como líderes de la empresa, gerentes de TI, y personal de seguridad, puede proporcionar información valiosa sobre su conocimiento en la seguridad de la empresa.

Instrumentos: Cuestionarios estructurados o semiestructurados.

- **Encuestas**

  Descripción: Recopilar opiniones y percepciones sobre la seguridad de la información a través de encuestas.

  Instrumentos: Encuestas estructuradas.

- **Análisis de Vulnerabilidades**

  Descripción: Utilizar herramientas automatizadas y manuales para evaluar la seguridad de sistemas y redes e identificar posibles vulnerabilidades.

  Instrumentos: Escáneres de vulnerabilidades, evaluaciones de seguridad.

2.2.4 Técnicas de procesamiento de datos para la obtención de resultados

Análisis Descriptivo: Este análisis ayudará a entender la distribución de los datos.

Análisis Inferencial: Este análisis permitirá hacer inferencias sobre la población a partir de la muestra de datos.

Análisis de Regresión: Este análisis ayudará a entender la relación entre diferentes variables en los datos.

Identificación de áreas críticas: Identificar áreas críticas donde los riesgos son más significativos. Esto ayuda a asignar recursos de mitigación de manera más eficiente.

2.2.5 Metodología o métodos específicos

Metodología: NTE INEN-ISO/IEC 27005

Valoración del riesgo de la seguridad de la información:

- **Análisis del riesgo**

  Se encarga de estudiar las diversas causas que generan vulnerabilidad en la seguridad en la empresa.

- **Identificación de riesgo**

  Identificar las posibles fuentes de pérdidas potenciales y analizar las razones subyacentes de dichas pérdidas.

- **Estimación del riesgo**

  Estimación cualitativa: Se puede realizar mediante escalas: bajo, medio y alto.

  Estimación cuantitativa: Se puede usar una escala numérica.

- **Evaluación del riesgo**

  Los contextos internos y externos de la seguridad de la información para la gestión de riesgos deben ajustarse con los estándares para el proceso de evaluar de riesgos y la toma de decisiones. Estos criterios deben considerar los objetivos organizativos y las perspectivas de las partes interesadas. La cantidad de riesgo aceptable es el principal factor que influye en las decisiones tomadas durante la evaluación de riesgos. Sin embargo, las consecuencias, la probabilidad y la confianza deben tenerse en cuenta a la hora de identificar y analizar los riesgos. Cuando se combinan muchos peligros que se consideran bajos o moderados, los riesgos agregados pueden aumentar drásticamente, haciendo necesaria una gestión adecuada [44].

Proceso de tratamiento de riesgo

Se tiene 4 opciones disponibles:

- **Reducción del riesgo**

  Disminuir el nivel de riesgo requiere establecer medidas de control para que el riesgo residual sea reevaluado y considerado aceptable.

- **Retención del riesgo**

  Decidir mantener el riesgo sin tomar acciones adicionales debe estar respaldado por la evaluación correspondiente del riesgo.

- **Evitación del riesgo**

  Es recomendable abstenerse de llevar a cabo la actividad o acción que origina un riesgo específico.

- **Transferencia del riesgo**

  Es aconsejable trasladar el riesgo a otra entidad capaz de gestionarlo de manera más efectiva, según lo determinado al valorar el riesgo.

Proceso de aceptación de riesgo

Decidir asumir riesgos y responsabilidades de tal elección debe llevarse a cabo y documentarse de manera formal.

Proceso de comunicación de riesgo

La información relativa al riesgo debería ser compartida entre la persona encargada de tomar decisiones decisión y las demás partes involucradas.

Proceso de monitoreo y revisión de riesgo

Mantener una comprensión completa de la perspectiva general del riesgo implica monitorear y revisar constantemente los riesgos y componentes, que incluyen la valía de los activos, las consecuencias, los peligros, los puntos débiles y la probabilidad de suceso. Este seguimiento tiene como objetivo detectar cualquier cambio temprano en la situación de la organización.

Metodología: Normas INEN - Guía para la gestión de riesgos de seguridad de la información

En particular, durante las etapas de evaluación y tratamiento de riesgos, el método de gestión de riesgos para la seguridad de la información puede evolucionar repetidamente. La profundidad y la cantidad de información en la evaluación de riesgos pueden mejorarse gradualmente con la repetición en cada ciclo. Utilizando un método iterativo, es posible analizar con precisión los riesgos que tienen un impacto importante y, al mismo tiempo, reducir el tiempo y el esfuerzo necesarios para establecer controles [5].

Establecimiento del contexto

Establecer las normas esenciales para llevar a cabo con éxito la gestión de riesgos en el ámbito de la seguridad de la información involucra la determinación del contexto en esta gestión. Definir con de forma precisa parámetros y alcance de la gestión de riesgos es un requisito fundamental. Además, es crucial establecer una estructura organizativa adecuada encargada de dirigir y supervisar esta gestión de riesgos. Este paso inicial sienta las bases necesarias para implementar un enfoque integral y efectivo en el tratamiento del riesgo asociado a la seguridad de la información [5].

Valoración del riesgo

La evaluación del riesgo comprende las tareas de:

- Análisis de riesgo
    - Identificación de riesgo
    - Estimación de riesgo
- Evaluación de riesgo [5]

Tratamiento

En la Figura 6 se muestran las opciones para el tratamiento de riesgos.

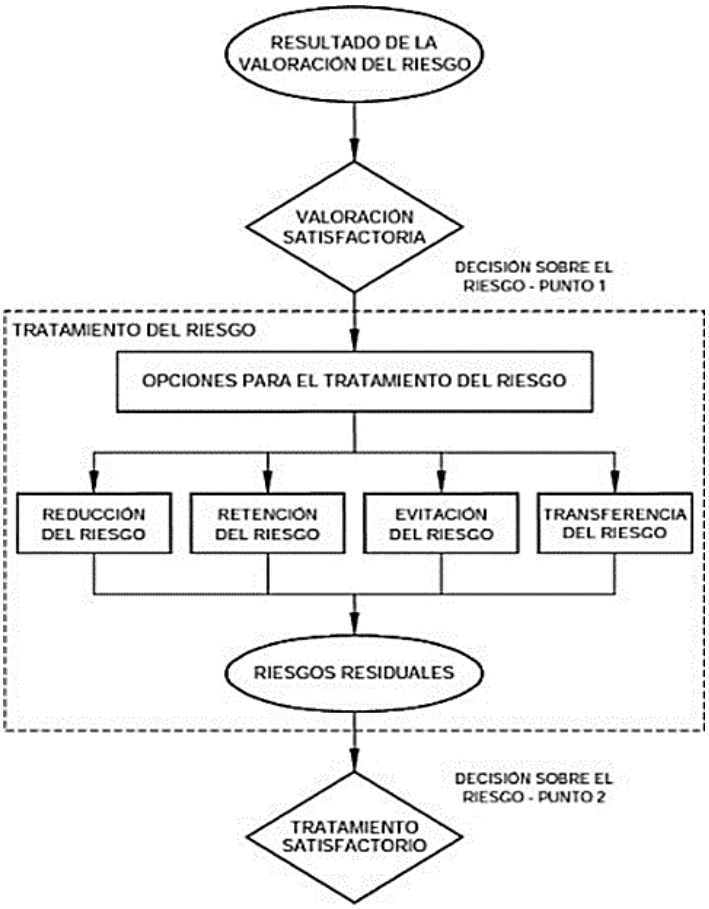


Figura 6: Actividades para tratar los riesgos

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012 [44] [4]

Aceptación

Es crucial adoptar decisiones conscientes acerca de la aceptación de riesgos y las responsabilidades correlativas, documentando de manera formal este procedimiento a través de registros pertinentes. Esta elección se efectúa cuando los gastos para aplicar medidas de resguardo superan el valor del recurso informativo que se busca resguardar o cuando la magnitud del riesgo se percibe como reducida. En ambas situaciones, la institución asume los posibles perjuicios derivados de la materialización del riesgo. En determinadas instancias, el riesgo restante podría no cumplir los estándares de aprobación debido a circunstancias específicas que podrían no estar contempladas en los criterios estándar. Por ejemplo, la aceptación de riesgos podría ser necesaria si los beneficios asociados son significativos o si reducir el riesgo resulta prohibitivamente costoso. Para enfrentar estas decisiones, es esencial que la organización defina su propio criterio para evaluar y aceptar los niveles de riesgo, ajustándolas a sus circunstancias y metas específicas [5].

Comunicación o transmisión del riesgo

La comunicación o transmisión del riesgo se orienta a lograr consenso en la gestión de riesgos mediante el intercambio y compartición de información relativa a su existencia, naturaleza, probabilidad, gravedad, tratamiento y aceptabilidad. Esta actividad, que abarca aspectos en el proceso de tomar decisiones e implementación dentro de la gestión del riesgo, destaca la importancia de una comunicación efectiva entre las partes involucradas. Asegurar un entendimiento claro entre aquellos encargados de la implementación y aquellos con intereses establecidos es esencial para fundamentar las decisiones y justificar las acciones necesarias. La comunicación en este contexto se establece como un proceso bidireccional para maximizar su eficacia [5].

Monitoreo y revisión del riesgo

Es fundamental que las organizaciones aseguren un monitoreo continuo de varios aspectos clave en la gestión del riesgo, entre ellos:

- Inclusión de nuevos activos.
- Adaptaciones dependiendo de los requisitos del negocio en el valor de los activos.
- Identificación y evaluación de nuevas amenazas tanto internas como externas, que puedan no haber sido previamente valoradas.
- Evaluación de la probabilidad de que las amenazas puedan afectar las nuevas vulnerabilidades.
- Revisión de la exposición de las vulnerabilidades.
- El aumento en las repercusiones o efectos de los riesgos, vulnerabilidades y amenazas combinados, generando un nivel de riesgo que se considera inaceptable.
- El incremento en las repercusiones o resultados de los riesgos, vulnerabilidades y amenazas combinados, resulta en una magnitud del riesgo que se considera inadmisible.
- Supervisión de percances. [5].

2.2.6 Herramientas y/o Materiales

La información detallada sobre las herramientas y materiales a emplear se presenta en la Tabla 7.

Tabla 7: Herramientas y/o Materiales

Categoría	Herramientas y/o Materiales
Hardware	• Laptop • Smartphone • Impresora
Software	• Paquete de Office
Metodologías	• NORMA TÉCNICA ECUATORIANA INEN-ISO/IEC 27005:2012 • Guía para la gestión de riesgos de seguridad de la información perteneciente el ministerio de telecomunicaciones y de sociedad de información en Ecuador. (MINTEL)

2.3 Desarrollo del prototipo

2.3.1 Establecimiento del contexto

2.3.1.1 Establecer criterios básicos para la gestión del riesgo

En esta sección, se emplea la metodología sugerida para administrar los riesgos de seguridad de la información en una entidad pública de Ecuador, de la provincia de El Oro. El propósito fundamental radica en confirmar la validez de cada etapa delineada en el capítulo previo del proyecto. Por razones vinculadas a la política de confidencialidad de la institución colaboradora, se abstiene de revelar el nombre de la empresa, de igual manera, se omiten nombres de los encargados que participan en la ejecución del proyecto.

El levantamiento de información inicial constituye una fase crítica de la estrategia de gestión de riesgos de seguridad de la información. Su adecuada ejecución sienta las bases para el reconocimiento, análisis y manejo efectivo de los riesgos vinculados a la información sensible en la entidad. En el contexto de este proyecto, se enfatiza la importancia de recopilar datos

relevantes que permitan comprender el entorno operativo, la información de los recursos, las amenazas presentes y las debilidades posibles [45].

La recopilación de información se llevará a cabo mediante diversas técnicas, que pueden incluir entrevistas con personal clave, revisión de documentación, evaluación del entorno tecnológico y de los procedimientos organizacionales relacionados con la seguridad de la información. Es crucial garantizar la privacidad y la integridad de la información recabados durante este proceso [5].

2.3.1.2 Definir alcance y límites de la gestión del riesgo

En el contexto del proyecto, se establece el alcance de la gestión de riesgos de seguridad de la información. Dicho alcance se define en concordancia con la naturaleza y las necesidades específicas de la entidad pública bajo estudio [46].

2.3.1.3 Estudio de la organización

Visión: La empresa pública, con un enfoque de responsabilidad social, busca liderar el desarrollo de la provincia de manera eficiente.

Misión: Fomentar el desarrollo socioeconómico de la provincia mediante servicios de calidad, participación ciudadana, transparencia, liderazgo y cooperación, contribuyendo así a mejorar el bienestar de sus residentes y preservar los recursos naturales.

Objetivos:

- Impulsar el fortalecimiento institucional y mejorar las capacidades administrativas, financieras y operativas.
- Liderar las actividades de participación de la ciudadanía y escrutinio ciudadano.
- Contribuir con la prestación de servicios eficientes para mejorar la calidad de vida de los habitantes.

Análisis del departamento de informática

El departamento de Informática está dividido en áreas: desarrollo de aplicaciones, redes y comunicaciones, soporte y mantenimiento, servicios en línea. Cada área cuenta con un

responsable o jefe, y un ayudante, siendo todos ellos responsabilidad del director del departamento de Informática.

Alcance de la gestión de riesgo de seguridad de la información

El alcance de la de gestión de riesgo de seguridad de la información se define como el análisis de los procedimientos esenciales que pueden interrumpir la ejecución de los servicios públicos proporcionados [47]. Esto incluye:

- El equipo del departamento de informática.
- La documentación que está incluida en los procesos esenciales.
- La estructura tecnológica que respalda los procedimientos esenciales.
- La información producida por medio de la estructura tecnológica [44]

Limitaciones del alcance

Se consideran las restricciones del alcance en función de las leyes y regulaciones pertinentes, como la "Ley Orgánica De Transparencia Y Acceso A La Información Pública" y la constitución ecuatoriana. Estas restricciones garantizan la accesibilidad a la información de dominio público y protegen la información privada, sin comprometer la integridad ni la confidencialidad de los datos recolectados durante el proceso de gestión de riesgos de seguridad de la información [47].

Comité de seguridad de la información

	Roles asignados	**Responsabilidades**
Comité de evaluación	Jefe unidad de TIC	Ayudar en la identificación y evaluación de riesgos relacionados con la infraestructura de TI.
	Responsable de TIC	Aportar conocimientos técnicos sobre sistemas y tecnologías relevantes.
	Directora talento humano	Contribuir con perspectivas sobre riesgos relacionados con el factor humano en la organización.

	Roles asignados	Responsabilidades
Comité de desarrollo	Soriano Herrera Roger Hitler - Desarrollador del proyecto	Participar en la elaboración de medidas de tratamiento de riesgos.
	Velásquez Porras Diana Maribel -Desarrollador del proyecto	Participar en la elaboración de medidas de tratamiento de riesgos.

2.3.2 Valoración del riesgo de la seguridad de la información

Para llevar a cabo la valoración de los activos, resulta fundamental primero la identificación de los recursos. En líneas generales, es posible distinguir dos categorías de activos:

Activos primarios:

- **Actividades y procesos del negocio:** Procesos críticos de negocio, su importancia y su contribución a los objetivos de la empresa.

- **Información:** Información sensible y crítica para la empresa, como datos de clientes, información financiera y políticas internas. Determinar la ubicación de los datos, tanto en sistemas informáticos como en documentos físicos [4] [5].

Activos de soporte:

- **Hardware:** Servidores, computadoras, dispositivos de red y otros equipos de TI que soportan las operaciones. Evaluar la importancia de cada dispositivo en función de su función y su impacto en la disponibilidad de los servicios.

- **Software:** Sistemas de software críticos para las operaciones. Evaluar la vulnerabilidad, mantenimiento y seguridad de la configuración.

- **Redes:** Infraestructura de red utilizada para la comunicación interna y externa. Evaluar la seguridad de la red en función de la configuración, el monitoreo.

- **Personal:** Personal clave que tiene acceso a información sensible y sistemas críticos. Evaluar el riesgo de actividades maliciosas o negligentes por parte del personal.

- **Ubicación:** Ubicaciones físicas de los activos de y sistemas de TI, incluidas las oficinas corporativas, los centros de datos y las sucursales. Evaluar el riesgo de amenazas físicas, como robos, incendios o desastres naturales.

- **Estructura de la organización:** Estructura organizativa, incluyendo las funciones y obligaciones del personal, además de los procesos de toma de decisiones. Evaluar el riesgo de conflictos de intereses, fraudes internos y otros riesgos relacionados con la estructura organizativa [4] [5].

2.4 Ejecución del prototipo

2.4.1 Análisis del Riesgo

Durante el estudio del riesgo, se evalúan meticulosamente posibles amenazas y vulnerabilidades que podrían afectar la integridad, confidencialidad y accesibilidad de los activos de información. Este procedimiento supone reconocer posibles escenarios de riesgo, la estimación de su probabilidad de ocurrencia y el impacto correspondiente en caso de materialización [5].

2.4.1.1 Identificación del riesgo

- **Identificación de los activos**

  En la Tabla 8 podemos observar los diversos tipos de activos:

Tabla 8: Identificación de tipo de activo

TIPO DE ACTIVO	DETALLE
Base de Datos	Conjunto de información relacionada que se encuentra agrupada o estructurada en medio electrónico.
Hardware	Dispositivo de la infraestructura tecnológica que soporta información de la Corporación. Incluye el dispositivo físico y el sistema operativo nativo del mismo, como es el caso de equipos de cómputo de usuario final, servidores y otros equipos físicos.
Información Electrónica	Cualquier tipo de información contenida en medios electrónicos. Por ejemplo: Archivos en formatos Excel, Word o Outlook (ppt)
Información Física	Cualquier tipo de información contenida en un medio impreso o cualquier información archivada físicamente.
Medio de almacenamiento	Medio de información que se puede conectar a un computador o a una red computadores para el almacenamiento de datos.
Persona	Cualquier individuo que realice funciones para la Corporación y haga uso de la información de la compañía, ya sea personal interno o contratista.
Red	Dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información.
Servicio	Servicio interno de la Corporación que para su funcionamiento requiera el uso de componentes de hardware, software e infraestructura de comunicaciones de red.
Sitio	Instalaciones de procesamiento o almacenamiento de información. Ejemplo: Centro de datos principal y de respaldo, archivo documental, entre otros.
Software	Cualquier aplicativo, adquirido o desarrollado, que haga uso de la información para realizar operaciones o transacciones.

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012 [4]

Para determinar la valoración del impacto se presentan las siguientes referencias basadas en la Guía para la gestión de riesgos de seguridad de la información (MINTEL).

Se muestra calificación del impacto en términos de confiabilidad (Tabla 9), integridad (Tabla 10) y disponibilidad (Tabla 11).

Tabla 9: Valoración del impacto en términos de confiabilidad

Nivel de Confidencialidad		
NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN
ALTO	3	La divulgación no autorizada de la información tiene un efecto crítico para la institución
MEDIO	2	La divulgación no autorizada de la información tiene un efecto limitado para la institución
BAJO	1	La divulgación de la información no tiene ningún efecto para la institución

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

Tabla 10: Valoración del impacto en términos de integridad

Nivel de Integridad		
NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN
ALTO	3	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
MEDIO	2	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
BAJO	1	La destrucción o modificación de la información tiene un efecto leve para la institución

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

Tabla 11: Valoración del impacto en términos de disponibilidad.

Nivel de Disponibilidad		
NIVEL	EQUIVALENCIA CUANTITATIVA	DESCRIPCIÓN
ALTO	3	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
MEDIO	2	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
BAJO	1	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

Para determinar la evaluación del impacto de un activo se usa la siguiente fórmula:

$$VA = \frac{C + I + D}{3}$$

Seguidamente, se presenta la identificación de los activos y su calificación (Tabla 12).

Tabla 12: Identificación de activos y valoración.

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-001	Servidores	Equipos de hardware dedicados a proporcionar servicios y recursos en red.	**Hardware**	3	3	3	3,00
RSI-002	Computadores de escritorio	Computadoras de uso general utilizadas por los usuarios de la organización.	**Hardware**	2	2	2	2,00
RSI-003	Portátiles	Computadoras portátiles utilizadas por el personal de la organización.	**Hardware**	2	2	2	2,00
RSI-004	Dispositivos móviles	Dispositivos móviles como teléfonos inteligentes y tabletas.	**Hardware**	2	1	1	1,33
RSI-005	Impresoras	Dispositivos de hardware utilizados para imprimir documentos.	**Hardware**	2	1	1	1,33

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-006	Equipos multifuncional	Equipos que combinan diversas funciones como impresión, escaneo y copiado.	**Hardware**	2	1	2	1,67
RSI-007	Routers	Dispositivos de red utilizados para dirigir el tráfico entre redes.	**Hardware**	3	3	3	3,00
RSI-008	Teléfonos	Dispositivos telefónicos utilizados para comunicaciones internas y externas.	**Hardware**	2	1	1	1,33
RSI-009	Modems	Dispositivos para la conexión a redes de comunicación.	**Hardware**	3	2	2	2,33
RSI-010	Memoria USB	Dispositivos de almacenamiento portátiles basados en USB.	**Medio de almacenamiento**	2	2	2	2,00

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-011	Discos Portables	Discos de almacenamiento portátiles utilizados para respaldo y transporte.	**Medio de almacenamiento**	2	2	2	2,00
RSI-012	Cámaras de Seguridad	Dispositivos de videovigilancia para la seguridad de las instalaciones.	**Hardware**	3	2	3	2,67
RSI-013	Televisores	Equipos de visualización de contenido multimedia.	**Hardware**	1	1	1	1,00
RSI-014	Sistemas Operativos	Software que administra recursos de hardware y proporciona servicios.	**Software**	3	3	3	3,00
RSI-015	Antivirus	Software diseñado para detectar y eliminar software malicioso.	**Software**	3	3	3	3,00

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-016	Servidores Aplicaciones/ Contenedores	Software de servidor para alojar aplicaciones y servicios.	**Software**	3	3	3	3,00
RSI-017	Página WEB	Servicio de alojamiento y acceso a páginas web.	**Servicio**	3	3	3	3,00
RSI-018	Navegadores	Software para acceder y navegar por internet.	**Software**	1	1	2	1,33
RSI-019	Office	Suite de aplicaciones de productividad de Microsoft.	**Software**	2	1	3	2,00
RSI-020	Motor de Base de Datos	Software que proporciona acceso y gestión de bases de datos.	**Software**	3	3	3	3,00
RSI-021	Licencias	Permisos legales para el uso de software.	**Software**	2	3	2	2,33

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-022	Base de Datos	Repositorio centralizado de datos estructurados.	**Base de Datos**	3	3	3	3,00
RSI-023	Archivos de Datos	Documentos y archivos electrónicos con datos organizados.	**Información Electrónica**	3	3	2	2,67
RSI-024	Manuales de Usuario	Documentación para usuarios sobre cómo utilizar sistemas y servicios.	**Información Electrónica**	1	2	2	2,00
RSI-025	Documentación del sistema	Información sobre la arquitectura y funcionamiento de sistemas.	**Información Electrónica**	3	3	3	3,00
RSI-026	Solicitudes	Formularios o solicitudes electrónicas para procesos internos.	**Información Electrónica**	3	1	2	1,33
RSI-027	Formatos	Plantillas y formatos electrónicos para documentos.	**Información Electrónica**	3	1	2	1,33

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-028	Documentos internos	Documentos electrónicos utilizados internamente en la organización.	**Información Electrónica**	3	3	3	3,00
RSI-029	Material Físico (Impreso)	Documentos impresos y materiales físicos utilizados en la organización.	**Información Física**	1	2	2	2,00
RSI-030	Información en carpetas compartidas en red	Datos almacenados y compartidos a través de redes internas.	**Información Electrónica**	2	3	3	3,00
RSI-031	Información Disco	Datos almacenados en discos físicos.	**Información Electrónica**	3	3	3	3,00
RSI-032	Información memorias USB	Datos almacenados en dispositivos de memoria USB.	**Información Electrónica**	2	2	2	2,33
RSI-033	Datos de identificación	Información personal o de identificación de individuos.	**Información Electrónica**	3	3	3	3,00

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-034	Información Financiera	Datos financieros de la organización.	**Información Electrónica**	3	3	3	3,00
RSI-035	Información de Recursos Humanos	Datos relacionados con el personal y recursos humanos de la organización.	**Información Electrónica**	2	3	3	3,00
RSI-036	Información Urbanística	Datos sobre planificación y uso del territorio.	**Información Electrónica**	3	2	3	2,33
RSI-037	Capacitaciones	Servicio de formación y capacitación.	**Servicio**	1	1	2	1,33
RSI-038	Telefonía	Servicio de comunicación telefónica.	**Servicio**	1	3	3	2,67
RSI-039	Internet	Servicio de acceso a la red mundial	**Servicio**	3	3	3	2,33

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-040	Red Inalámbrica	Red de comunicación inalámbrica utilizada para conectividad de dispositivos.	**Red**	2	2	3	2,00
RSI-041	Almacenamiento de información	Medio físico o virtual para almacenar y gestionar datos.	**Medio de almacenamiento**	3	2	3	2,67
RSI-042	Electricidad	Suministro de energía eléctrica para operaciones de la organización.	**Servicio**	3	3	3	2,33
RSI-043	Instalaciones de la Organización	Edificaciones y áreas físicas de la organización.	**Sitio**	3	2	3	2,00
RSI-044	Centro de datos principal	Centro principal para alojar servidores y equipos de red.	**Sitio**	3	3	3	3,00
RSI-045	Archivo documental	Almacenamiento físico de documentos y registros importantes.	**Sitio**	3	2	2	2,33

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-046	Red eléctrica	Infraestructura de distribución de energía eléctrica.	**Red**	3	3	3	2,67
RSI-047	Red de datos	Infraestructura de red para transmitir datos entre dispositivos.	**Red**	2	3	3	3,00
RSI-048	Personal Interno	Personal empleado directamente por la organización.	**Persona**	1	3	3	3,00
RSI-049	Directores de área	Personal encargado de supervisar y dirigir áreas específicas.	**Persona**	2	3	3	3,00
RSI-050	Personal Administrativo	Personal que realiza tareas administrativas y de oficina.	**Persona**	1	3	3	3,00
RSI-051	Administrador de Página Web	Persona encargada de gestionar y mantener la página web de la organización.	**Persona**	1	3	3	3,00

				EVALUACIÓN DEL IMPACTO			
				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	EVALUACIÓN DEL ACTIVO
IDENTIFICADOR ACTIVO	NOMBRE	DESCRIPCIÓN	TIPO	CUANTITATIVO	CUANTITATIVO	CUANTITATIVO	
RSI-052	Proveedores	Entidades externas que suministran bienes o servicios a la organización.	**Persona**	3	2	2	2,00

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

- **Identificación de las amenazas**

En la tabla 13 se identifican amenazas de los activos, estas amenazas pueden ser deliberadas (D), accidentales (A) o ambientales (E), y podrían desencadenar, por ejemplo, deterioro o privación de servicios esenciales. Para cada tipo de amenaza. La designación D se asigna a las acciones planificadas dirigidas a los activos, mientras que la letra A se emplea para acciones humanas que podrían afectar los activos de forma accidental. Por otro lado, la letra E se reserva para incidentes no vinculados con acciones humanas. Los conjuntos de amenazas no siguen un orden de prioridad específico [5].

Tabla 13: Clasificación de las amenazas

Origen de las Amenazas	
Clasificación	**Descripción**
A	**Accidentales:** Clasifica las acciones humanas que pueden dañar accidentalmente los activos de información
D	**Deliberadas:** Clasifica todas las acciones deliberadas que tienen como objetivo los activos de la información
E	**Ambientales:** Clasifica todos los incidentes que no se basa en acciones humanas

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012 [4]

A continuación, se muestra la identificación de las amenazas y sus orígenes (Tabla 14).

Tabla 14: Amenazas y su origen

Tipo	Amenazas	Origen
Acciones no autorizadas	Acceso lógico no autorizado a la base de datos / Fuga, robo o pérdida de información	D, A
	Alteración, Eliminación, Pérdida o Robo de los dispositivos	D
	Problemas de detección de actividades no autorizadas	D
	Acceso lógico no autorizado	D
	Alteración de la información	D, A
	Divulgación de información	D
	Acceso no autorizado / Fuga, robo o pérdida de información / Condiciones inadecuadas	D
	Acceso lógico no autorizado a los servicios de red / Manipulación de la configuración	D
	Acceso no autorizado	D
Compromiso de la información	Alteración de la información	D, A
	Divulgación de información	D
	Cambios no autorizados de la configuración	D
	Fallas en el servicio	D, A
	Fallas en el software	D, A
	Ocurrencia o reincidencia de incidentes	D, A, E
Fallas técnicas	Errores de mantenimiento / actualización de programas (software)	D, A, E
	Fallas en el dispositivo	D, A, E
	Condiciones inadecuadas de temperatura o humedad	A, E
	Falla o degradación de los servicios	D, A, E

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012 [4]

- **Identificación de vulnerabilidades**

  Es fundamental detectar las vulnerabilidades que las amenazas pueden aprovechar para causar daños a los activos de una organización [5].

  En la tabla 15 se muestran las vulnerabilidades que pueden ser explotadas por las amenazas.

Tabla 15: Amenazas – Vulnerabilidades

TIPO	AMENAZA	VULNERABILIDAD
Base de Datos	Acceso lógico no autorizado a la base de datos / Fuga, robo o pérdida de información	Falta de controles de acceso lógico
Hardware	Alteración, Eliminación, Pérdida o Robo de los dispositivos	Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos
Hardware	Errores de mantenimiento / actualización de programas (software)	Falta de actualización de versiones o parches
Hardware	Fallas en el dispositivo	Manipulación de los equipos
Hardware	Problemas de detección de actividades no autorizadas	Falta de generación y monitoreo de registros de auditoría
Información Electrónica	Acceso lógico no autorizado	Debilidad en las contraseñas / Falta de controles de acceso lógico
Información Electrónica	Alteración de la información	Falta de políticas / normas / procedimientos / estándares
Información Electrónica	Divulgación de información	Falta de políticas / normas / procedimientos / estándares
Información Electrónica	Fuga, robo o pérdida de información	Falta de clasificación y condiciones de manejo de la información
Información Física	Acceso no autorizado / Fuga, robo o perdida de información / Condiciones inadecuadas	Falta de controles en el manejo de información
Persona	Alteración de la información	Concentración de funciones
Persona	Ataque Informático	Falta de entrenamiento en seguridad de la información
Persona	Divulgación de información	Falta de políticas / normas / procedimientos / estándares
Persona	Incumplimiento en la disponibilidad del personal	Ausencia del personal
Red	Acceso lógico no autorizado a los servicios	Falta de controles en los servicios

TIPO	AMENAZA	VULNERABILIDAD
	de red / Manipulación de la configuración	
Red	Falla o degradación de los servicios	Falta de controles sobre la gestión del cambio
Servicio	Acceso lógico no autorizado / Divulgación de información	Configuración débil y/o por defecto / Falta de monitoreo de privilegios
Servicio	Cambios no autorizados de la configuración	Falta de controles sobre la gestión del cambio
Servicio	Errores de mantenimiento	Falta de monitoreo del servicio
Servicio	Fallas en el servicio	Falta de gestión de vulnerabilidades
Sitio	Acceso no autorizado	Falta de controles de acceso físico
Sitio	Condiciones inadecuadas de temperatura o humedad	Falta de monitoreo de las condiciones ambientales
Software	Acceso lógico no autorizado	Falta de monitoreo de privilegios
Software	Cambios no autorizados de la configuración del sistema	Falta de controles sobre la gestión del cambio
Software	Fallas en el servicio	Falta de gestión de vulnerabilidades
Software	Fallas en el software	Falta de gestión de vulnerabilidades
Software	Ocurrencia o reincidencia de incidentes	Falta de gestión de incidentes de seguridad

Fuente: Norma Técnica Ecuatoriana (NTE) INEN-ISO/IEC 27005:2012 [4]

- **Identificación de la existencia de controles.**

La identificación de los controles existentes y planificados es esencial para evitar redundancias y gastos innecesarios, como la duplicación de controles. Durante este proceso, se recomienda verificar la efectividad de los controles existentes, lo cual puede agilizarse mediante la referencia a informes de auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) ya disponibles. Si un control no está funcionando correctamente, podría generar vulnerabilidades [4] [5].

Se puede observar (Tabla 20) los controles detectados, su tipo, nivel de efectividad y nivel de riesgo con el control implementado en cada uno de los activos.

2.4.1.2 Estimación o Análisis del riesgo

Se busca emplear enfoques cualitativos y cuantitativos con el fin de realizar una evaluación de los riesgos detectados, considerando los activos, las amenazas y las políticas pertinentes [5].

La probabilidad de ocurrencia se determinará en base a lo establecido en la Tabla 16.

Tabla 16: Criterio de probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA		
CRITERIO	**VALOR**	**PERIODICIDAD**
IMPROBABLE	1	No ha sucedido
MEDIANAMENTE PROBABLE	2	Ha ocurrido o podría ocurrir en un periodo a largo plazo (1 año)
MUY PROBABLE	3	Ha ocurrido o podría ocurrir en un periodo a corto plazo

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

El valor del grado de eficacia de los controles se determinará en base a lo establecido en la Tabla 17.

Tabla 17: Criterio para el nivel de efectividad controles

NIVEL DE EFECTIVIDAD CONTROLES	
Valor	**Descripción**
MUY ALTA	Mitiga totalmente el riesgo (Controles Implementados)
ALTA	Mitiga parcialmente el riesgo (Controles definidos y documentados)
MUY BAJA	No se mitiga el riesgo (Controles no definidos o en estado inicial)

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

La probabilidad de los riesgos inherentes (Tabla 18) y actual (Tabla 19) se terminarán de acuerdo a lo siguiente:

Tabla 18: Mapa de Calor - Riesgo Inherente

PROBABILIDAD	3 – Muy probable			
	2 – Medianamente probable			
	1 – Muy improbable			
		1 – Bajo	2 - Medio	3 – Alto
		IMPACTO		

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

Tabla 19: Mapa de Calor - Riesgo Actual

PROBABILIDAD	3 – Muy probable			
	2 – Medianamente probable			
	1 – Muy improbable			
		1 – Bajo	2 - Medio	3 – Alto
		IMPACTO		

Fuente: Guía para la gestión de riesgos de seguridad de la información (MINTEL) [5].

2.4.2 Evaluación del Riesgo

En la Tabla 20 se muestra el desarrollo de la evaluación del riesgo:

Tabla 20: Matriz de riesgos de activos

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 001	Servidores	**Hardware**	**Fallas en el dispositivo**	**Manipulación de los equipos**	Fallas en el dispositivo debido a manipulación de los equipos sobre el activo servidores	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Políticas de control de acceso / Aseguramiento de oficinas, salas e instalaciones	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar políticas de control de acceso y aseguramiento de oficinas, salas e instalaciones para disminuir la manipulación de equipos y evitar fallas en los dispositivos.
RSI - 002	Computadores de escritorio	**Hardware**	**Problemas de detección de actividades no autorizadas**	**Falta de generación y monitoreo de registros de auditoría**	Problemas de detección de actividades no autorizadas debido a falta de generación y monitoreo de registros de auditoría sobre el activo computadores de escritorio	2	Medio	2	Medio	2	Medio	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Concienciación, educación y formación en seguridad de la información	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Realizar concienciación, educación y formación en seguridad de la información para mitigar problemas de detección de actividades no autorizadas.
RSI - 003	Portátiles	**Hardware**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo portátiles	2	Medio	2	Medio	2	Medio	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Protección contra malware	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Implementar protección contra malware para mitigar el riesgo de alteración, eliminación, pérdida o robo de dispositivos debido a la falta de políticas de seguridad para su ubicación.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 004	Dispositivos móviles	**Hardware**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo dispositivos móviles	2	Medio	1	Bajo	1	Bajo	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Protección contra malware	Muy baja	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 005	Impresoras	**Hardware**	**Fallas en el dispositivo**	**Manipulación de los equipos**	Fallas en el dispositivo debido a manipulación de los equipos sobre el activo impresoras	2	Medio	1	Bajo	1	Bajo	1	3	Muy probable	3	**Medio**	**Medio**	Correctivo	Mantenimiento del equipo	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Realizar mantenimiento del equipo para reducir el riesgo de fallas debido a la manipulación de los equipos.
RSI - 006	Equipos multifuncional	**Hardware**	**Fallas en el dispositivo**	**Manipulación de los equipos**	Fallas en el dispositivo debido a manipulación de los equipos sobre el activo equipos multifuncional	2	Medio	1	Bajo	2	Medio	1	3	Muy probable	3	**Medio**	**Medio**	Correctivo	Mantenimiento del equipo	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Realizar mantenimiento del equipo para reducir el riesgo de fallas debido a la manipulación de los equipos.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 007	Routers	**Hardware**	**Fallas en el dispositivo**	**Manipulación de los equipos**	Fallas en el dispositivo debido a manipulación de los equipos sobre el activo routers	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Seguridad de redes / Gestión de configuraciones	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de redes y gestión de configuraciones para mitigar el riesgo de fallas debido a la manipulación de los equipos.
RSI - 008	Teléfonos	**Hardware**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo teléfonos	2	Medio	1	Bajo	1	Bajo	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Control de acceso	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 009	Modems	**Hardware**	**Fallas en el dispositivo**	**Manipulación de los equipos**	Fallas en el dispositivo debido a manipulación de los equipos sobre el activo modems	3	Alto	2	Medio	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Seguridad de redes / Gestión de configuraciones	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de redes y gestión de configuraciones para reducir el riesgo de fallas en los dispositivos.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI-010	Memoria USB	**Medio de almacenamiento**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo memoria USB	2	Medio	2	Medio	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Copia de seguridad de la información	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Realizar copias de seguridad de la información para mitigar el riesgo de alteración, eliminación, pérdida o robo de dispositivos debido a la falta de políticas de seguridad para su ubicación.
RSI-011	Discos Portables	**Medio de almacenamiento**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo discos portables	2	Medio	2	Medio	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Copia de seguridad de la información	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Realizar copias de seguridad de la información para mitigar el riesgo de alteración, eliminación, pérdida o robo de dispositivos debido a la falta de políticas de seguridad para su ubicación.
RSI-012	Cámaras de Seguridad	**Hardware**	**Errores de mantenimiento / actualización de programas**	**Falta de actualización de versiones o parches**	Errores de mantenimiento / actualización de programas (software) debido a falta de actualización de versiones o parches sobre el activo cámaras de seguridad	3	Alto	2	Medio	3	Alto	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Políticas de seguridad de la información	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Implementar políticas de seguridad de la información para mitigar errores de mantenimiento o actualización de programas.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
			(software)																						
RSI - 013	Televisores	**Hardware**	**Alteración, Eliminación, Pérdida o Robo de los dispositivos**	**Falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos**	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a falta de políticas / normas / procedimientos / estándares / consideraciones de seguridad para la ubicación de los equipos sobre el activo televisores	1	Bajo	1	Bajo	1	Bajo	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Aseguramiento de oficinas, salas e instalaciones	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 014	Sistemas Operativos	**Software**	**Acceso lógico no autorizado**	**Falta de monitoreo de privilegios**	Acceso lógico no autorizado debido a falta de monitoreo de privilegios sobre el activo sistemas operativos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Instalación de software en sistemas operativos	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y la instalación de software para mitigar el riesgo de acceso lógico no autorizado.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 015	Antivirus	**Softwa re**	**Fallas en el softwar e**	**Falta de gestión de vulnerabil idades**	Fallas en el software debido a falta de gestión de vulnerabilidades sobre el activo antivirus	3	Alto	3	Alto	3	Alto	3	2	Media namen te proba ble	6	**Alto**	**Alto**	Pre vent ivo	Protección contra malware	Alta	**Medio**	**Medi o**	**No**	**Reducir**	Implementar protección contra malware para reducir el riesgo de fallas en el software debido a la falta de gestión de vulnerabilidades.
RSI - 016	Servid ores Aplica ciones / Conte nedor es	**Softwa re**	**Cambio s no autoriz ados de la configu ración del sistema**	**Falta de controles sobre la gestión del cambio**	Cambios no autorizados de la configuración del sistema debido a falta de controles sobre la gestión del cambio sobre el activo servidores aplicaciones/ contenedores	3	Alto	3	Alto	3	Alto	3	1	Muy impro bable	3	**Medi o**	**Medi o**	Pre vent ivo	Control de acceso	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 017	Págin a WEB	**Servic io**	**Fallas en el servicio**	**Falta de gestión de vulnerabil idades**	Fallas en el servicio debido a falta de gestión de vulnerabilidades sobre el activo página web	3	Alto	3	Alto	3	Alto	3	2	Media namen te proba ble	6	**Alto**	**Alto**	Pre vent ivo	Codificaci ón segura	Alta	**Medio**	**Medi o**	**No**	**Reducir**	Implementar codificación segura para reducir el riesgo de fallas en el servicio debido a la falta de gestión de vulnerabilidades.
RSI - 018	Naveg adores	**Softwa re**	**Fallas en el softwar e**	**Falta de gestión de vulnerabil idades**	Fallas en el software debido a falta de gestión de vulnerabilidades sobre el activo navegadores	1	Bajo	1	Bajo	2	Medio	1	1	Muy impro bable	1	**Bajo**	**Bajo**	Pre vent ivo	Prevenció n de fugas de datos	Muy baja	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 019	Office	**Software**	**Ocurrencia o reincidencia de incidentes**	**Falta de gestión de incidentes de seguridad**	Ocurrencia o reincidencia de incidentes debido a falta de gestión de incidentes de seguridad sobre el activo office	2	Medio	1	Bajo	3	Alto	2	1	Muy improbable	2	**Bajo**	**Bajo**	Preventivo	Prevención de fugas de datos	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 020	Motor de Base de Datos	**Software**	**Cambios no autorizados de la configuración del sistema**	**Falta de controles sobre la gestión del cambio**	Cambios no autorizados de la configuración del sistema debido a falta de controles sobre la gestión del cambio sobre el activo motor de base de datos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Implementar control de acceso para reducir el riesgo de cambios no autorizados de la configuración del sistema.
RSI - 021	Licencias	**Software**	**Fallas en el software**	**Falta de gestión de vulnerabilidades**	Fallas en el software debido a falta de gestión de vulnerabilidades sobre el activo licencias	2	Medio	3	Alto	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Políticas de seguridad de la información	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 022	Base de Datos	**Base de Datos**	**Acceso lógico no autorizado a la base de datos / Fuga, robo o pérdida**	**Falta de controles de acceso lógico**	Acceso lógico no autorizado a la base de datos / Fuga, robo o pérdida de información debido a falta de controles de acceso lógico sobre el activo base de datos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Copia de seguridad de la información	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y copias de seguridad de la información para mitigar el riesgo de acceso lógico no autorizado y fuga, robo o pérdida de información.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
			de información																						
RSI - 023	Archivos de Datos	**Información Electrónica**	**Acceso lógico no autorizado**	**Debilidad en las contraseñas / Falta de controles de acceso lógico**	Acceso lógico no autorizado debido a debilidad en las contraseñas / falta de controles de acceso lógico sobre el activo archivos de datos	3	Alto	3	Alto	2	Medio	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Copia de seguridad de la información	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y copias de seguridad de la información para mitigar el riesgo de acceso lógico no autorizado y fuga, robo o pérdida de información.
RSI - 024	Manuales de Usuario	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo manuales de usuario	2	Medio	2	Medio	2	Medio	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Políticas de seguridad de la información / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar políticas de seguridad de la información y derechos de acceso para mitigar el riesgo de divulgación de información.
RSI - 025	Documentación del sistema	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo documentación del sistema	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Políticas de seguridad de la información / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar políticas de seguridad de la información y derechos de acceso para mitigar el riesgo de divulgación de información.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 026	Solicitudes	**Información Electrónica**	**Alteración de la información**	**Falta de políticas / normas / procedimientos / estándares**	Alteración de la información debido a falta de políticas / normas / procedimientos / estándares sobre el activo solicitudes	1	Bajo	1	Bajo	2	Medio	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Políticas de seguridad de la información / Monitoreo de seguridad física	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 027	Formatos	**Información Electrónica**	**Alteración de la información**	**Falta de políticas / normas / procedimientos / estándares**	Alteración de la información debido a falta de políticas / normas / procedimientos / estándares sobre el activo formatos	1	Bajo	1	Bajo	2	Medio	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Políticas de seguridad de la información /Monitoreo de seguridad física	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 028	Documentos internos	**Información Electrónica**	**Fuga, robo o pérdida de información**	**Falta de clasificación y condiciones de manejo de la información**	Fuga, robo o pérdida de información debido a falta de clasificación y condiciones de manejo de la información sobre el activo documentos internos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Políticas de seguridad de la información / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar políticas de seguridad de la información, derechos de acceso y clasificación de la información para mitigar el riesgo de fuga, robo o pérdida de información.
RSI - 029	Material Físico (Impreso)	**Información Física**	**Acceso no autorizado / Fuga, robo o perdida de**	**Falta de controles en el manejo de información**	Acceso no autorizado / Fuga, robo o perdida de información / Condiciones inadecuadas debido a falta de controles en el manejo de información	2	Medio	2	Medio	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Protección contra amenazas físicas y ambientales / Monitoreo de	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Implementar protección contra amenazas físicas y ambientales, y monitoreo de seguridad física para mitigar el riesgo de acceso no autorizado, fuga, robo

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
			información / Condiciones inadecuadas		sobre el activo material físico (impreso)														seguridad física						o pérdida de información.
RSI - 030	Información en carpetas compartidas en red	**Información Electrónica**	**Acceso lógico no autorizado**	**Debilidad en las contraseñas / Falta de controles de acceso lógico**	Acceso lógico no autorizado debido a debilidad en las contraseñas / falta de controles de acceso lógico sobre el activo información en carpetas compartidas en red	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso para mitigar el riesgo de acceso lógico no autorizado a los servicios de red.
RSI - 031	Información Disco	**Información Electrónica**	**Fuga, robo o pérdida de información**	**Falta de clasificación y condiciones de manejo de la información**	Fuga, robo o pérdida de información debido a falta de clasificación y condiciones de manejo de la información sobre el activo información disco	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso para mitigar el riesgo de fuga, robo o pérdida de información.
RSI - 032	Información memorias USB	**Información Electrónica**	**Fuga, robo o pérdida de información**	**Falta de clasificación y condiciones de manejo de la información**	Fuga, robo o pérdida de información debido a falta de clasificación y condiciones de manejo de la información sobre el activo información memorias USB	3	Alto	2	Medio	2	Medio	2	1	Muy improbable	2	**Bajo**	**Bajo**	Preventivo	Control de acceso	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 033	Datos de identificación	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo datos de identificación	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y derechos de acceso para mitigar el riesgo de divulgación de información.
RSI - 034	Información Financiera	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo información financiera	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y derechos de acceso para mitigar el riesgo de divulgación de información.
RSI - 035	Información de Recursos Humanos	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo información de recursos humanos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso / Derechos de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso y derechos de acceso para mitigar el riesgo de divulgación de información.
RSI - 036	Información Urbanística	**Información Electrónica**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo información urbanística	2	Medio	2	Medio	3	Alto	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Control de acceso / Derechos de acceso	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 037	Capacitaciones	**Servicio**	**Fallas en el servicio**	**Falta de gestión de vulnerabilidades**	Fallas en el servicio debido a falta de gestión de vulnerabilidades sobre el activo capacitaciones	1	Bajo	1	Bajo	2	Medio	1	1	Muy improbable	1	**Bajo**	**Bajo**	Preventivo	Concienciación, educación y formación en seguridad de la información	Muy baja	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 038	Telefonía	**Servicio**	**Fallas en el servicio**	**Falta de gestión de vulnerabilidades**	Fallas en el servicio debido a falta de gestión de vulnerabilidades sobre el activo telefonía	2	Medio	3	Alto	3	Alto	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Seguridad de redes	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A
RSI - 039	Internet	**Servicio**	**Fallas en el servicio**	**Falta de gestión de vulnerabilidades**	Fallas en el servicio debido a falta de gestión de vulnerabilidades sobre el activo internet	1	Bajo	3	Alto	3	Alto	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Seguridad de redes	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de redes para mitigar el riesgo de fallas en el servicio.
RSI - 040	Red Inalámbrica	**Red**	**Cambios no autorizados de la configuración**	**Falta de controles sobre la gestión del cambio**	Cambios no autorizados de la configuración debido a falta de controles sobre la gestión del cambio sobre el activo red inalámbrica	1	Bajo	2	Medio	3	Alto	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Seguridad de los servicios de red	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de los servicios de red para mitigar el riesgo de cambios no autorizados de la configuración.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 041	Almacenamiento de información	**Medio de almacenamiento**	**Acceso lógico no autorizado / Divulgación de información**	**Configuración débil y/o por defecto / Falta de monitoreo de privilegios**	Acceso lógico no autorizado / Divulgación de información debido a configuración débil y/o por defecto / falta de monitoreo de privilegios sobre el activo almacenamiento de información	3	Alto	2	Medio	3	Alto	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Control de acceso	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso para mitigar el riesgo de acceso lógico no autorizado y divulgación de información.
RSI - 042	Electricidad	**Servicio**	**Errores de mantenimiento**	**Falta de monitoreo del servicio**	Errores de mantenimiento debido a falta de monitoreo del servicio sobre el activo electricidad	1	Bajo	3	Alto	3	Alto	2	2	Medianamente probable	4	**Medio**	**Medio**	Correctivo	Mantenimiento del equipo	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Realizar mantenimiento del equipo para mitigar el riesgo de errores debido a falta de monitoreo del servicio.
RSI - 043	Instalaciones de la Organización	**Sitio**	**Acceso no autorizado**	**Falta de controles de acceso físico**	Acceso no autorizado debido a falta de controles de acceso físico sobre el activo instalaciones de la organización	1	Bajo	2	Medio	3	Alto	2	3	Muy probable	6	**Alto**	**Alto**	Preventivo	Entrada física	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Implementar controles de acceso físico para mitigar el riesgo de acceso no autorizado.
RSI - 044	Centro de datos principal	**Sitio**	**Condiciones inadecuadas de temperatura o humedad**	**Falta de monitoreo de las condiciones ambientales**	Condiciones inadecuadas de temperatura o humedad debido a falta de monitoreo de las condiciones ambientales sobre el activo centro de datos principal	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Protección contra amenazas físicas y ambientales	Muy baja	**Alto**	**Alto**	**No**	**Reducir**	Implementar protección contra amenazas físicas y ambientales para mitigar el riesgo de condiciones inadecuadas de temperatura o humedad.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 045	Archivo documental	**Sitio**	**Condiciones inadecuadas de temperatura o humedad**	**Falta de monitoreo de las condiciones ambientales**	Condiciones inadecuadas de temperatura o humedad debido a falta de monitoreo de las condiciones ambientales sobre el activo archivo documental	3	Alto	2	Medio	2	Medio	2	2	Medianamente probable	4	**Medio**	**Medio**	Preventivo	Protección contra amenazas físicas y ambientales	Muy baja	**Medio**	**Medio**	**No**	**Reducir**	Implementar protección contra amenazas físicas y ambientales para mitigar el riesgo de condiciones inadecuadas de temperatura o humedad.
RSI - 046	Red eléctrica	**Red**	**Falla o degradación de los servicios**	**Falta de controles sobre la gestión del cambio**	Falla o degradación de los servicios debido a falta de controles sobre la gestión del cambio sobre el activo red eléctrica	2	Medio	3	Alto	3	Alto	2	3	Muy probable	6	**Alto**	**Alto**	Correctivo	Mantenimiento del equipo	Alta	**Medio**	**Medio**	**No**	**Reducir**	Realizar mantenimiento del equipo para mitigar el riesgo de falla o degradación de los servicios.
RSI - 047	Red de datos	**Red**	**Acceso lógico no autorizado a los servicios de red / Manipulación de la configuración**	**Falta de controles en los servicios**	Acceso lógico no autorizado a los servicios de red / Manipulación de la configuración debido a falta de controles en los servicios sobre el activo red de datos	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Seguridad de los servicios de red	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de los servicios de red para mitigar el riesgo de acceso lógico no autorizado y manipulación de la configuración.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 048	Personal Interno	**Persona**	**Alteración de la información / Falta de personal**	**Concentración de funciones**	Alteración de la información / Falta de personal debido a concentración de funciones sobre el activo personal interno	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Control de acceso	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar control de acceso para mitigar el riesgo de alteración de la información debido a la concentración de funciones.
RSI - 049	Directores de área	**Persona**	**Incumplimiento en la disponibilidad del personal**	**Ausencia del personal**	Incumplimiento en la disponibilidad del personal debido a ausencia del personal sobre el activo directores de área	3	Alto	3	Alto	3	Alto	3	3	Muy probable	9	**Alto**	**Alto**	Preventivo	Roles y responsabilidades de seguridad de la información	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar roles y responsabilidades de seguridad de la información para mitigar el riesgo de incumplimiento en la disponibilidad del personal.
RSI - 050	Personal Administrativo	**Persona**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo personal administrativo	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Roles y responsabilidades de seguridad de la información / Registro	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar roles y responsabilidades de seguridad de la información y registro para mitigar el riesgo de divulgación de información.
RSI - 051	Administrador de Página Web	**Persona**	**Ataque Informático**	**Falta de entrenamiento en seguridad de la información**	Ataque Informático debido a falta de entrenamiento en seguridad de la información sobre el activo administrador de página web	3	Alto	3	Alto	3	Alto	3	2	Medianamente probable	6	**Alto**	**Alto**	Preventivo	Seguridad de la información en relaciones con proveedores	Alta	**Medio**	**Medio**	**No**	**Reducir**	Implementar seguridad de la información en relaciones con proveedores para mitigar el riesgo de ataques informáticos debido a la falta de entrenamiento.

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE EVALUACIÓN DE RIESGOS											RIESGO ACTUAL				RIESGOS RESIDUAL TRATAMIENTO			
						Valoración del Impacto																		
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo	Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	Probabilidad		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado	Nivel Riesgo Residual	Aceptable (SI /NO)	Método de Tratamiento de Riesgos	Plan de Tratamiento
RSI - 052	Proveedores	**Persona**	**Divulgación de información**	**Falta de políticas / normas / procedimientos / estándares**	Divulgación de información debido a falta de políticas / normas / procedimientos / estándares sobre el activo proveedores	2	Medio	2	Medio	2	Medio	2	1	Muy improbable	2	**Bajo**	**Bajo**	Preventivo	Abordar la seguridad de la información dentro de acuerdos con proveedores	Alta	**Bajo**	**Bajo**	**Si**	**Aceptar**	N/A

Fuente: [4] [5]

2.5 Tratamiento del Riesgo

Se desarrollan estrategias y medidas para reducir, transferir, prevenir o aceptar los riesgos identificados [5].

Los controles propuestos, se basan la norma ISO/IEC 27001. El estándar ISO 27001 describe los objetivos de control y controles de seguridad de la información, para dar a las organizaciones las mejores prácticas para un SGSI.

Propuesta de mejoras:

- **RSI-001 Servidores**

Riesgo Identificado: Fallas en el dispositivo debido a manipulación no autorizada.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.1 Emplazamiento y protección de equipos

Ubicación Segura: Asegurar que los servidores estén ubicados en salas de servidores dedicadas, con acceso restringido solo a personal autorizado. Estas áreas deben contar con medidas físicas de seguridad para prevenir el acceso no autorizado.

Monitoreo: Instalar sistemas de videovigilancia (CCTV) para monitorear continuamente las áreas donde se encuentran los servidores. Los registros de video deben ser almacenados y revisados periódicamente.

Mantenimiento Regular: Establecer un programa de mantenimiento preventivo para los servidores, que incluya inspecciones regulares de hardware y software, actualización de sistemas y verificación de la integridad física de los equipos. Documentar todas las actividades de mantenimiento y cualquier problema detectado.

A.9.1.1 Perímetro de seguridad física

Barreras Físicas: Implementar barreras físicas como puertas de seguridad o cerraduras electrónicas en las áreas de servidores. Estas barreras deben estar diseñadas para resistir intentos de intrusión y proporcionar una primera línea de defensa.

Control de Acceso: Utilizar sistemas de control de acceso avanzados, como tarjetas de proximidad, autenticación biométrica o códigos PIN. Configurar estos sistemas para registrar los accesos y generar alertas en caso de intentos de acceso no autorizados.

Personal de Seguridad: Asignar personal de seguridad capacitado para patrullar las áreas críticas y monitorear las cámaras de seguridad. Este personal debe estar entrenado para responder rápidamente a cualquier incidente de seguridad.

A.10.4.1 Controles contra el código malicioso

Antivirus y Antimalware: Instalar software antivirus y antimalware y configurarlos para realizar escaneos automáticos regulares. Asegurarse de que las definiciones de virus se actualicen automáticamente.

Actualizaciones de Software: Implementar políticas de actualización de software que aseguren que todos los sistemas operativos y aplicaciones se mantengan actualizados con los últimos parches de seguridad. Utilizar herramientas automatizadas para gestionar y aplicar estas actualizaciones.

Escaneo Regular: Programar escaneos de seguridad regulares utilizando herramientas de detección de vulnerabilidades para identificar y mitigar posibles amenazas. Documentar los resultados de estos escaneos y tomar medidas correctivas inmediatas para cualquier vulnerabilidad encontrada.

A.12.6.1 Gestión de vulnerabilidades técnicas

Parcheo Regular: Establecer un calendario de parcheo que incluya todas las actualizaciones de seguridad críticas y no críticas. Priorizar la instalación de parches que aborden vulnerabilidades de alto riesgo y realizar pruebas antes de su implementación en el entorno de producción.

Evaluación de Vulnerabilidades: Realizar evaluaciones de vulnerabilidades y pruebas de penetración periódicas para identificar debilidades en la infraestructura de servidores. Utilizar los resultados para mejorar las políticas y procedimientos de seguridad.

Reportes de Vulnerabilidad: Implementar un sistema para que los empleados puedan reportar vulnerabilidades de manera segura. Asegurando que todas las vulnerabilidades reportadas sean abordadas y documentar todo el proceso de resolución.

- **RSI-002 Computadores de escritorio**

Riesgo Identificado: Acceso no autorizado a la información.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.11.5.2 Identificación y autenticación de usuario

Contraseñas Fuertes: Establecer políticas que requieran contraseñas fuertes, compuestas por al menos 12 caracteres, incluyendo letras mayúsculas, minúsculas, números y símbolos. Forzar el cambio de contraseñas cada 90 días.

Autenticación de Dos Factores: Implementar autenticación de dos factores (2FA) para acceder a sistemas críticos, asegurando una capa adicional de seguridad. Proporcionar tokens físicos o aplicaciones móviles para la generación de códigos de acceso temporales.

Registro de Acceso: Configurar sistemas para registrar todos los intentos de acceso, exitosos o fallidos, y almacenar estos registros en un lugar seguro. Revisar estos logs regularmente para detectar y responder a posibles intentos de acceso no autorizados.

A.11.3.1 Uso de contraseñas

Educación y Concienciación: Realizar sesiones de capacitación periódicas para concienciar a los empleados sobre la importancia de mantener sus contraseñas seguras y no compartirlas con nadie. Proporcionar ejemplos de buenas prácticas y técnicas para crear contraseñas seguras.

Política de Contraseñas: Desarrollar y comunicar una política de uso de contraseñas que especifique los requisitos mínimos de complejidad, la frecuencia de cambio de contraseña y las consecuencias de no cumplir con la política. Asegurar que todos los empleados firmen un documento de conformidad.

Herramientas de Gestión: Utilizar herramientas de gestión de contraseñas que permitan a los usuarios almacenar sus contraseñas de manera segura y generar contraseñas complejas

automáticamente. Asegurarse de que estas herramientas cumplan con los estándares de seguridad de la organización.

A.10.5.1 Copias de seguridad de la información

Backup Regular: Configurar sistemas de backup automatizados para realizar copias de seguridad diarias de todos los datos críticos. Asegurarse de que estas copias de seguridad se almacenen en ubicaciones seguras y separadas de los sistemas originales.

Almacenamiento Seguro: Utilizar medios de almacenamiento cifrados y almacenarlos en ubicaciones físicamente seguras, como centros de datos con acceso restringido.

Pruebas de Restauración: Realizar pruebas de restauración periódicas para asegurar que las copias de seguridad puedan ser recuperadas de manera rápida y efectiva. Documentar los procedimientos de recuperación y entrenar al personal en su ejecución.

A.9.2.3 Seguridad del cableado

Canalización y Protección: Utilizar canalizaciones de alta calidad para proteger el cableado de red y eléctrico de daños físicos y manipulaciones. Estas canalizaciones deben estar hechas de materiales resistentes y cumplir las normativas de seguridad.

Inspecciones Regulares: Realizar inspecciones regulares del cableado para detectar signos de desgaste, daño o manipulación. Documentar los resultados de estas inspecciones y tomar medidas correctivas cuando se detecten problemas.

Documentación: Mantener una documentación detallada y actualizada de toda la infraestructura de cableado, incluyendo diagramas de red, rutas de cableado y puntos de terminación. Esta documentación debe estar disponible para el personal autorizado y ser revisada periódicamente.

- **RSI-003 Portátiles**

Riesgo Identificado: Pérdida o robo de dispositivos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.11.7.1 Equipos portátiles y comunicaciones móviles

Rastreo de Dispositivos: Instalar software de rastreo y localización en todos los portátiles para poder localizarlos en caso de pérdida o robo. Este software debe permitir el borrado remoto de datos para proteger la información sensible.

Política de Uso: Desarrollar una política de uso de equipos portátiles que incluya directrices sobre el manejo seguro, la protección contra el acceso no autorizado y la obligación de reportar inmediatamente cualquier pérdida o robo del dispositivo.

A.9.2.5 Seguridad de los equipos fuera de las instalaciones

Acceso Seguro: Configurar el inicio de sesión seguro y la autenticación de dos factores en todos los portátiles. Implementar políticas de bloqueo automático de pantalla tras un período de inactividad y exigir la autenticación para reanudar el uso.

Seguridad en Viajes: Capacitar a los empleados sobre las mejores prácticas de seguridad durante los viajes, como mantener los portátiles en su posesión en todo momento, no dejar dispositivos desatendidos y usar conexiones seguras para acceder a redes públicas.

A.10.4.1 Controles contra el código malicioso

Software Antivirus: Instalar software antivirus y antimalware en todos los portátiles, asegurándose de que se actualicen automáticamente y realicen escaneos periódicos. Configurar el software para que realice escaneos de archivos descargados y dispositivos conectados.

Política de Descargas: Establecer una política que restrinja la descarga e instalación de software desde fuentes no verificadas. Permitir solo la instalación de aplicaciones aprobadas por el departamento de TI y utilizar listas blancas de software.

Actualizaciones de Sistema: Configurar los portátiles para recibir y aplicar actualizaciones automáticas del sistema operativo y de las aplicaciones. Establecer procedimientos para verificar que todas las actualizaciones se instalen correctamente y en tiempo.

A.9.2.6 Reutilización o retirada segura de equipos

Borrado Seguro: Implementar procedimientos de borrado seguro de datos para todos los portátiles antes de su reutilización o disposición.

Destrucción Física: En casos donde los dispositivos no sean funcionales, considerar la destrucción física del disco duro para garantizar que los datos no puedan ser recuperados. Contratar servicios certificados si es necesario.

Registro de Retiro: Mantener un registro detallado de la retirada y disposición segura de los dispositivos. Este registro debe incluir la identificación del dispositivo, la fecha de retirada, el método y la firma de la persona responsable del proceso.

- **RSI-005 Impresoras**

Riesgo Identificado: Acceso no autorizado.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.1 Emplazamiento y protección de equipos

Ubicación Controlada: Colocar impresoras en áreas con acceso restringido, como oficinas cerradas o salas de impresión dedicadas. Asegurarse de que solo el personal autorizado pueda acceder.

Monitoreo de Impresión: Utilizar software de monitoreo de impresión para registrar todas las actividades de impresión.

A.10.4.1 Controles contra el código malicioso

Actualización de Firmware: Mantener el firmware de las impresoras actualizado para proteger contra vulnerabilidades conocidas. Configurar las impresoras para recibir actualizaciones automáticas del fabricante y verificar que estas se apliquen correctamente.

Seguridad de Red: Configurar las impresoras en una red segmentada y protegida. Utilizar firewalls y controles de acceso para limitar la comunicación con las impresoras a dispositivos autorizados.

Escaneos de Seguridad: Realizar escaneos de seguridad regulares para detectar y mitigar posibles amenazas.

A.11.7.1 Equipos portátiles y comunicaciones móviles

Protección de Transferencias: Utilizar protocolos de comunicación seguros (como HTTPS o IPsec) para la transferencia de documentos desde y hacia las impresoras. Configurar las impresoras para aceptar solo conexiones seguras y autenticadas.

Eliminación Segura de Documentos: Asegurarse de que las impresoras eliminen de manera segura cualquier documento almacenado temporalmente después de la impresión. Configurar políticas para el borrado automático y seguro de todos los datos después de cada sesión de impresión.

A.12.6.1 Gestión de vulnerabilidades técnicas

Evaluaciones de Seguridad: Realizar evaluaciones de seguridad periódicas en las impresoras para identificar y abordar posibles vulnerabilidades. Utilizar las evaluaciones para mejorar las políticas y procedimientos de seguridad de las impresoras.

Parcheo Regular: Establecer un calendario de parcheo que incluya todas las actualizaciones de seguridad críticas para las impresoras. Priorizar la instalación de parches que aborden vulnerabilidades de alto riesgo y verificar su correcta aplicación.

- **RSI-006 Equipos multifuncionales**

Riesgo Identificado: Acceso no autorizado a documentos y datos almacenados.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.1 Emplazamiento y protección de equipos

Ubicación Segura: Colocar los equipos multifuncionales en áreas con acceso controlado. Implementar controles de acceso físico para limitar el uso a personal autorizado.

Monitoreo de Actividades: Utilizar software de monitoreo para registrar todas las actividades realizadas en los equipos multifuncionales, revisando estos registros periódicamente para detectar usos indebidos.

A.10.4.1 Controles contra el código malicioso

Actualización de Firmware: Mantener el firmware de los equipos actualizado para proteger contra vulnerabilidades conocidas. Configurar actualizaciones automáticas y verificar su correcta aplicación.

Seguridad de Red: Configurar los equipos en una red segmentada y protegida. Utilizar firewalls y controles de acceso para limitar las comunicaciones a dispositivos autorizados.

Escaneos de Seguridad: Realizar escaneos de seguridad regulares en los equipos multifuncionales para detectar y mitigar amenazas.

A.11.7.1 Equipos portátiles y comunicaciones móviles

Protección de Transferencias: Utilizar protocolos de comunicación seguros (como HTTPS o IPsec) para la transferencia de documentos. Configurar los equipos para aceptar solo conexiones seguras y autenticadas.

Eliminación Segura de Documentos: Configurar los equipos para eliminar de manera segura cualquier documento almacenado temporalmente después de su uso. Implementar políticas para el borrado automático de datos después de cada sesión.

A.12.6.1 Control de las vulnerabilidades técnicas

Evaluaciones de Seguridad: Realizar evaluaciones de seguridad periódicas en los equipos para identificar vulnerabilidades. Usar las evaluaciones para mejorar las políticas de seguridad.

Parcheo Regular: Establecer un calendario de parcheo que incluya todas las actualizaciones de seguridad críticas.

Monitoreo Continuo: Implementar sistemas de monitoreo continuo en los equipos multifuncionales para detectar y alertar sobre actividades sospechosas.

- **RSI-007 Routers**

Riesgo Identificado: Acceso no autorizado a la red y compromisos de seguridad.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.11.4.1 Política de uso de los servicios en red

Configuración Segura: Configurar los routers con políticas de seguridad robustas, deshabilitando servicios innecesarios y cambiando las contraseñas predeterminadas por contraseñas fuertes.

Autenticación de Usuario: Implementar autenticación para acceder a la configuración del router. Utilizar certificados digitales o contraseñas complejas para asegurar el acceso.

Monitoreo de Acceso: Registrar todas las actividades de acceso a los routers y revisar regularmente estos registros para detectar intentos de acceso no autorizados.

A.10.6.1 Controles de red

Segmentación de Red: Segmentar la red en diferentes zonas de seguridad para limitar el acceso a recursos críticos. Utilizar VLANs y firewalls para gestionar y controlar el tráfico de red.

Filtrado de Tráfico: Implementar políticas de filtrado de tráfico entrante y saliente. Bloquear puertos y protocolos no necesarios para reducir la superficie de ataque.

Detección y Prevención de Intrusiones: Implementar sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear y analizar el tráfico de red, alertando sobre actividades sospechosas.

A.10.4.1 Controles contra el código malicioso

Actualización de Firmware: Mantener el firmware de los routers actualizado con las últimas correcciones de seguridad. Configurar actualizaciones automáticas y verificar su correcta aplicación.

Escaneos de Seguridad: Realizar escaneos de seguridad periódicos en los routers para detectar y mitigar vulnerabilidades. Usar herramientas específicas para identificar y corregir debilidades.

Protección contra Malware: Utilizar software de seguridad para proteger los routers contra el malware. Configurar el router para bloquear conexiones sospechosas y escanear archivos descargados.

A.10.10.1 Registro de auditorias

Registro Detallado: Configurar los routers para mantener registros detallados de todas las actividades. Almacenar registros de conexión, cambios de configuración y accesos administrativos.

Revisión Periódica: Revisar regularmente los registros de auditoría para identificar y abordar cualquier actividad sospechosa. Implementar alertas para detectar y responder a incidentes de seguridad.

Protección de Registros: Asegurar que los registros de auditoría sean almacenados de manera segura y no puedan ser alterados. Utilizar encriptación y accesos controlados para proteger los registros.

- **RSI-009 Modems**

Riesgo Identificado: Acceso no autorizado a la red y compromisos de seguridad.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.11.4.1 Política de uso de los servicios en red

Configuración Segura: Configurar los modems con políticas de seguridad robustas, deshabilitando servicios innecesarios y cambiando contraseñas predeterminadas por contraseñas fuertes y únicas.

Autenticación de Usuario: Implementar autenticación para acceder a la configuración del modem. Utilizar contraseñas complejas.

Monitoreo de Acceso: Registrar todas las actividades de acceso al modem y revisar regularmente estos registros para detectar intentos de acceso no autorizados.

A.10.6.1 Controles de red

Segmentación de Red: Segmentar la red en diferentes zonas de seguridad para limitar el acceso a recursos críticos. Utilizar VLANs y firewalls para gestionar y controlar el tráfico de red.

Filtrado de Tráfico: Implementar políticas de filtrado de tráfico entrante y saliente. Bloquear puertos y protocolos no necesarios para reducir la superficie de ataque.

Detección y Prevención de Intrusiones: Implementar sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear y analizar el tráfico de red en tiempo real, alertando sobre actividades sospechosas.

A.10.4.1 Controles contra el código malicioso

Actualización de Firmware: Mantener el firmware de los modems actualizado con las últimas correcciones de seguridad. Configurar actualizaciones automáticas y verificar su correcta aplicación.

Escaneos de Seguridad: Realizar escaneos de seguridad periódicos en los modems para detectar y mitigar vulnerabilidades. Usar herramientas específicas para identificar y corregir debilidades.

Protección contra Malware: Utilizar software de seguridad para proteger los modems contra el malware. Configurar el modem para bloquear conexiones sospechosas y escanear archivos descargados.

A.10.10.1 Registro de auditorias

Registro Detallado: Configurar los modems para mantener registros detallados de todas las actividades. Almacenar registros de conexión, cambios de configuración y accesos administrativos.

Revisión Periódica: Revisar regularmente los registros de auditoría para identificar y abordar cualquier actividad sospechosa. Implementar alertas automáticas para detectar y responder a incidentes de seguridad.

Protección de Registros: Asegurar que los registros de auditoría sean almacenados de manera segura y no puedan ser alterados.

- **RSI-010 Memoria USB**

Riesgo Identificado: Pérdida de datos y compromisos de seguridad por dispositivos portátiles.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.7.1 Gestión de soportes extraíbles

Control de Acceso: Restringir el uso de memorias USB solo a usuarios autorizados. Implementar políticas para aprobar y registrar el uso de dispositivos USB.

Políticas de Uso: Desarrollar y comunicar políticas claras sobre el uso de memorias USB. Incluir directrices sobre la protección de datos y la prevención de malware.

A.10.4.1 Controles contra el código malicioso

Escaneo Automático: Configurar los sistemas para escanear automáticamente las memorias USB al conectarlas. Utilizar software antivirus actualizado para detectar y eliminar malware.

Actualización de Seguridad: Mantener el software de seguridad y los sistemas operativos actualizados para proteger contra amenazas conocidas.

Educación de Usuarios: Capacitar a los usuarios sobre los riesgos de utilizar memorias USB desconocidas y las mejores prácticas para mantener la seguridad de los datos.

A.9.2.6 Reutilización o retirada segura de equipos

Borrado Seguro: Implementar procedimientos para el borrado seguro de datos en memorias USB antes de su reutilización o eliminación. Utilizar herramientas de borrado que cumplan con estándares de seguridad.

Inventario y Auditoría: Mantener un inventario de todas las memorias USB utilizadas en la organización y realizar auditorías periódicas para asegurar el cumplimiento de las políticas de seguridad.

Disposición Segura: Establecer procedimientos para la disposición segura de memorias USB, para prevenir el robo de datos.

A.10.8.1 Políticas y procedimientos de intercambio de información

Políticas Claras: Desarrollar políticas claras para el intercambio de información utilizando memorias USB. Incluir directrices sobre qué tipo de información se puede transferir y cómo debe ser protegida.

- **RSI-011 Discos Portables**

Riesgo Identificado: Pérdida de datos y compromisos de seguridad por dispositivos portátiles.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.7.1 Gestión de soportes extraíbles

Control de Acceso: Restringir el uso de discos portables solo a usuarios autorizados. Implementar políticas para aprobar y registrar el uso de estos dispositivos.

Políticas de Uso: Desarrollar y comunicar políticas claras sobre el uso de discos portables. Incluir directrices sobre la protección de datos y la prevención de malware.

A.10.4.1 Controles contra el código malicioso

Escaneo Automático: Configurar los sistemas para escanear automáticamente los discos portables al conectarlos. Utilizar software antivirus actualizado para detectar y eliminar malware.

Actualización de Seguridad: Mantener el software de seguridad y los sistemas operativos actualizados para proteger contra amenazas conocidas. Configurar actualizaciones automáticas.

Educación de Usuarios: Capacitar a los usuarios sobre los riesgos de utilizar discos portables desconocidos y las mejores prácticas para mantener la seguridad de los datos.

A.9.2.6 Reutilización o retirada segura de equipos

Borrado Seguro: Implementar procedimientos para el borrado seguro de datos en discos portables antes de su reutilización o eliminación. Utilizar herramientas de borrado que cumplan con estándares de seguridad.

Inventario y Auditoría: Mantener un inventario de todos los discos portables utilizados en la organización y realizar auditorías periódicas para asegurar el cumplimiento de las políticas de seguridad.

Disposición Segura: Establecer procedimientos para la disposición segura de discos portables, incluyendo la destrucción física si es necesario, para prevenir la recuperación de datos.

A.10.8.1 Políticas y procedimientos de intercambio de información

Políticas Claras: Desarrollar políticas claras para el intercambio de información utilizando discos portables. Incluir directrices sobre qué tipo de información se puede transferir y cómo debe ser protegida.

Controles de Encriptación: Asegurar que toda la información sensible transferida a través de discos portables esté encriptada. Utilizar soluciones de encriptación aprobadas por la organización.

Supervisión y Monitoreo: Implementar sistemas para supervisar y monitorear el uso de discos portables. Revisar regularmente los registros de uso para detectar y abordar cualquier actividad sospechosa.

- **RSI-012 Cámaras de Seguridad**

Riesgo Identificado: Compromiso de la seguridad física y privacidad por acceso no autorizado a las cámaras.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.1.1 Perímetro de seguridad física

Instalación Segura: Colocar las cámaras en ubicaciones que minimicen la manipulación física. Utilizar carcasas a prueba de vandalismo y fijaciones seguras.

Monitoreo Constante: Implementar un sistema de monitoreo constante de las cámaras para detectar y responder rápidamente a cualquier intento de acceso no autorizado.

Mantenimiento Regular: Realizar inspecciones y mantenimientos periódicos para asegurar que las cámaras y sus carcasas estén en buenas condiciones y funcionando correctamente.

A.10.10.1 Registro de auditorias

Registro de Accesos: Configurar las cámaras para registrar todos los accesos y modificaciones de configuración. Almacenar estos registros de forma segura.

Revisión Periódica: Revisar regularmente los registros de auditoría para identificar patrones inusuales de acceso o actividad que podrían indicar un compromiso.

A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración

Protección de Puertos: Asegurar que los puertos de configuración de las cámaras estén protegidos mediante contraseñas fuertes y autenticación multifactor.

Deshabilitar Accesos No Necesarios: Deshabilitar todos los puertos y protocolos no necesarios para el funcionamiento de las cámaras para reducir la superficie de ataque.

Actualización de Firmware: Mantener el firmware de las cámaras actualizado para proteger contra vulnerabilidades conocidas.

A.12.3.1 Política de uso de los controles criptográficos

Gestión de Claves: Implementar una política robusta de gestión de claves para asegurar que las claves de encriptación estén protegidas y sean rotadas regularmente.

Auditoría de Encriptación: Realizar auditorías periódicas para verificar que las políticas de encriptación y gestión de claves se estén aplicando correctamente.

- **RSI-014 Sistemas Operativos**

Riesgo Identificado: Vulnerabilidades de seguridad y ataques debido a sistemas operativos desactualizados o mal configurados.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.12.6.1 Control de las vulnerabilidades técnicas

Parcheo Regular: Implementar parches periódicamente para mantener los sistemas operativos actualizados con las últimas correcciones de seguridad.

Escaneo de Vulnerabilidades: Realizar escaneos regulares de vulnerabilidades para identificar y mitigar problemas de seguridad en los sistemas operativos.

Pruebas de Penetración: Realizar pruebas de penetración periódicas para evaluar la resistencia de los sistemas operativos frente a ataques.

A.10.1.1 Documentación de los procedimientos de operación

Procedimientos Documentados: Desarrollar y mantener documentación detallada de los procedimientos de instalación, configuración y mantenimiento de los sistemas operativos.

Estándares de Configuración: Implementar y aplicar estándares de configuración seguros basados en mejores prácticas y guías de referencia de seguridad.

Revisión y Actualización: Revisar y actualizar regularmente los procedimientos para reflejar cambios en el entorno tecnológico y en las amenazas.

A.11.5.2 Identificación y autenticación de usuario

Autenticación Segura: Implementar métodos de autenticación robustos para todos los accesos a sistemas operativos, incluyendo autenticación multifactor donde sea posible.

Gestión de Credenciales: Asegurar que las credenciales de acceso sean gestionadas de forma segura, con políticas de cambio regular de contraseñas y uso de contraseñas complejas.

A.10.10.4 Registros de administración y operación

Registro de Eventos: Configurar los sistemas operativos para registrar eventos críticos, incluyendo accesos, cambios de configuración y errores.

Protección de Registros: Asegurar que los registros estén protegidos contra accesos no autorizados y manipulaciones, utilizando encriptación y controles de acceso.

Análisis Regular: Revisar y analizar los registros de forma regular para detectar y responder a posibles incidentes de seguridad.

- **RSI-015 Antivirus**

Riesgo Identificado: Infecciones de malware y pérdida de datos debido a la falta de protección antivirus adecuada.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.4.1 Controles contra el código malicioso

Instalación de Antivirus: Asegurar que todos los dispositivos y sistemas cuenten con software antivirus instalado y configurado correctamente.

Escaneos Programados: Programar escaneos de seguridad regulares en todos los dispositivos para detectar y eliminar malware.

A.11.2.3 Gestión de contraseñas de usuario

Protección de Antivirus: Configurar el software antivirus para requerir contraseñas robustas para acceder a la configuración y realizar cambios administrativos.

Restricción de Accesos: Limitar los accesos administrativos al software antivirus solo a personal autorizado y capacitado.

A.10.10.1 Registro de auditorias

Registro de Actividades: Configurar el software antivirus para mantener registros detallados de todas las actividades, detecciones y acciones tomadas.

Monitoreo de Registros: Implementar un sistema para monitorear y revisar los registros de actividades del antivirus de forma regular.

Alertas de Seguridad: Configurar alertas para notificar al personal de seguridad sobre detecciones y actividades sospechosas.

A.8.2.2 Concienciación, formación y capacitación en seguridad de la información

Capacitación Continua: Proveer capacitación continua a todos los empleados sobre la importancia del software antivirus y las mejores prácticas de seguridad.

Simulaciones de Amenazas: Realizar simulaciones de amenazas y ataques para evaluar la preparación del personal y la efectividad del software antivirus.

Actualización de Conocimientos: Mantener al personal informado sobre las últimas amenazas y tendencias en malware para mejorar la respuesta y prevención.

- **RSI-017 Página WEB**

Riesgo Identificado: Exposición a ataques cibernéticos, como inyecciones.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.4.1 Controles contra el código malicioso

WAF (Web Application Firewall): Implementar un WAF para filtrar y monitorear el tráfico HTTP y detectar actividades maliciosas.

Escaneo de Seguridad: Utilizar herramientas de escaneo de seguridad web para identificar y mitigar vulnerabilidades como XSS y SQL injection.

Actualización de Software: Mantener todas las aplicaciones web y sus dependencias actualizadas con los últimos parches de seguridad.

A.12.1.1 Análisis y especificación de los requisitos de seguridad

Desarrollo Seguro: Integrar prácticas de desarrollo seguro desde el inicio del ciclo de vida de desarrollo de software (SDLC).

Revisiones de Código: Realizar revisiones de código estático y dinámico para identificar y corregir vulnerabilidades de seguridad.

Pruebas de Penetración: Ejecutar pruebas de penetración periódicas para evaluar la seguridad de la página web frente a ataques.

A.11.5.2 Identificación y autenticación de usuario

Autenticación Segura: Implementar autenticación robusta para el acceso administrativo a la página web.

Gestión de Sesiones: Utilizar mecanismos seguros para la gestión de sesiones de usuarios, incluyendo la caducidad y revocación de sesiones.

Protección de Contraseñas: Almacenar contraseñas de manera segura utilizando algoritmos de hashing y salting.

A.10.10.1 Registro de auditorias

Protección de Registros: Asegurar que los registros estén protegidos contra accesos no autorizados y manipulaciones.

Revisión de Registros: Revisar los registros de auditoría regularmente para identificar y responder a actividades sospechosas.

- **RSI-020 Motor de Base de Datos**

Riesgo Identificado: Falla o vulnerabilidad en el motor de base de datos que comprometa la integridad y disponibilidad de los datos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.12.6.1 Gestión de vulnerabilidades técnicas

Implementar un programa de gestión de parches que asegure que todas las actualizaciones y parches de seguridad del motor de base de datos se apliquen de manera oportuna. Realizar pruebas en un entorno de prueba antes de aplicarlos en producción.

Realizar auditorías regulares de seguridad en el motor de base de datos para identificar y mitigar vulnerabilidades. Utilizar herramientas de escaneo de vulnerabilidades.

Configurar el motor de base de datos para minimizar la superficie de ataque, deshabilitando servicios y funcionalidades no utilizados, y aplicando principios de mínimos privilegios.

A.10.5.1 Copias de seguridad de la información

Establecer políticas de copias de seguridad regulares y asegurarse de que las copias de seguridad se almacenen en ubicaciones seguras y redundantes. Realizar pruebas periódicas de restauración para garantizar la integridad de las copias.

Automatizar el proceso de copias de seguridad y establecer alertas para fallos en las copias de seguridad. Documentar y revisar los procedimientos regularmente.

Cifrar las copias de seguridad para proteger la información durante el almacenamiento y transporte, asegurando que solo personal autorizado tenga acceso a ellas.

A.9.2.4 Mantenimiento de los equipos

Programar y documentar el mantenimiento preventivo regular del hardware que soporta el motor de base de datos, incluyendo limpieza, actualizaciones de firmware y comprobaciones de integridad.

Establecer un contrato de mantenimiento con proveedores especializados para asegurar una respuesta rápida en caso de fallos críticos.

Monitorizar continuamente el rendimiento del hardware y el software para detectar signos de posibles fallos antes de que ocurran, utilizando herramientas de monitoreo y alertas.

A.12.5.1 Procedimientos de control de cambios

Implementar un proceso formal de gestión de cambios que incluya la revisión y aprobación de cambios en el motor de base de datos, asegurando que todos los cambios sean probados antes de su implementación.

Mantener un registro detallado de todos los cambios realizados en el sistema, incluyendo la fecha, descripción del cambio, y la persona responsable.

Realizar revisiones periódicas del historial de cambios para identificar patrones o problemas recurrentes y mejorar los procedimientos de gestión de cambios.

- **RSI-022 Base de Datos**

Riesgo Identificado: Pérdida, corrupción o acceso no autorizado a la base de datos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.5.1 Copias de seguridad de la información

Implementar una estrategia de copias de seguridad completas y diferenciales, asegurando que las copias se realicen regularmente y se almacenen en ubicaciones seguras y redundantes.

Realizar pruebas de restauración de copias de seguridad para garantizar que los datos pueden ser recuperados correctamente y en el menor tiempo posible.

Documentar y revisar los procedimientos de copias de seguridad regularmente para mejorar su efectividad y adaptarlos a nuevos riesgos.

A.11.6.1 Restricción del acceso a la información

Implementar controles de acceso basados en roles (RBAC) para limitar el acceso a la base de datos únicamente al personal autorizado, asignando los privilegios mínimos necesarios.

Monitorear y auditar los accesos a la base de datos para detectar y responder a actividades sospechosas o no autorizadas.

A.12.3.1 Política de uso de los controles criptográficos

Cifrar los datos sensibles almacenados en la base de datos utilizando algoritmos de cifrado robustos y actualizados.

Asegurar que las claves de cifrado se gestionen adecuadamente, almacenándolas de manera segura y restringiendo su acceso solo a personal autorizado.

Implementar cifrado para los datos en tránsito entre la base de datos y las aplicaciones, utilizando protocolos seguros como TLS.

A.12.4.3 Control de acceso al código fuente de los programas

Restringir el acceso al código fuente de las aplicaciones que interactúan con la base de datos, asegurando que solo el personal autorizado pueda modificarlo.

Realizar revisiones de código y pruebas de seguridad antes de desplegar cambios en las aplicaciones que acceden a la base de datos.

Mantener un control de versiones del código fuente y documentar todos los cambios realizados para facilitar auditorías y recuperación en caso de fallos.

- **RSI-023 Archivos de Datos**

Riesgo Identificado: Pérdida, corrupción o acceso no autorizado a archivos de datos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.5.1 Copias de seguridad de la información

Implementar una estrategia de copias de seguridad para archivos de datos que incluya copias regulares y almacenadas en ubicaciones seguras.

Probar periódicamente las copias de seguridad para garantizar que los archivos pueden ser recuperados en caso de pérdida o corrupción.

Documentar y revisar los procedimientos de copias de seguridad, actualizándolos según sea necesario para adaptarse a cambios en los sistemas o nuevas amenazas.

A.9.2.6 Reutilización o retirada segura de equipos

Implementar procedimientos para la eliminación segura de archivos de datos de los equipos antes de su retiro o reutilización, utilizando métodos de borrado seguro.

Asegurar que los discos duros y otros dispositivos de almacenamiento se destruyan físicamente si no pueden ser reutilizados de manera segura.

Mantener un registro de todos los equipos retirados y el método de eliminación utilizado para asegurar la trazabilidad.

A.11.6.1 Restricción del acceso a la información

Implementar políticas de control de acceso para los archivos de datos, asegurando que solo el personal autorizado pueda acceder a ellos.

Monitorear y auditar los accesos a los archivos de datos para detectar y responder a actividades no autorizadas.

A.12.3.1 Política de uso de los controles criptográficos

Cifrar los archivos de datos sensibles tanto en reposo como en tránsito para protegerlos contra accesos no autorizados.

Implementar políticas claras sobre el uso y gestión de cifrado, capacitando a los empleados sobre su importancia y correcto uso.

- **RSI-024 Manuales de Usuario**

Riesgo Identificado: Acceso no autorizado y manipulación de los manuales de usuario.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.7.2.2 Etiquetado y manejo de la información

Implementar un sistema de clasificación y etiquetado de los manuales de usuario según su nivel de sensibilidad. Establecer procedimientos para el manejo adecuado de cada tipo de documento.

Capacitar al personal sobre la importancia del etiquetado y el manejo seguro de los manuales de usuario. Realizar talleres de sensibilización periódicos.

Realizar auditorías internas para asegurar el cumplimiento de las políticas de etiquetado y manejo de la información. Documentar los hallazgos y tomar acciones correctivas cuando sea necesario.

A.9.2.3 Seguridad del cableado

Asegurar que los manuales de usuario en formato digital estén almacenados en ubicaciones seguras y con acceso restringido. Implementar controles de acceso basados en roles.

Implementar medidas físicas y lógicas para proteger el cableado y las conexiones de red que soportan el acceso a los manuales de usuario. Utilizar racks cerrados y sistemas de monitoreo.

Realizar pruebas de penetración periódicas para identificar vulnerabilidades en la seguridad del cableado y tomar medidas correctivas para mitigar los riesgos.

A.10.5.1 Copias de seguridad de la información

Establecer un programa de copias de seguridad regular para los manuales de usuario en formato digital. Asegurar que las copias de seguridad estén almacenadas en ubicaciones seguras y separadas físicamente.

Verificar periódicamente la integridad de las copias de seguridad mediante pruebas de restauración. Documentar los resultados y ajustar los procedimientos según sea necesario.

Implementar políticas de retención y destrucción segura de copias de seguridad antiguas para evitar el almacenamiento innecesario y la exposición de datos sensibles.

A.11.2.1 Registro de usuario

Establecer un sistema de registro de usuarios que acceden a los manuales de usuario. Registrar y monitorear todos los accesos para identificar actividades sospechosas o no autorizadas.

Revisar periódicamente los registros de acceso y realizar análisis de comportamiento para detectar posibles incidentes de seguridad. Tomar medidas proactivas para prevenir brechas de seguridad.

Implementar políticas de gestión de identidades y acceso, incluyendo la revisión y actualización periódica de los permisos de usuario para garantizar que solo el personal autorizado tenga acceso a los manuales de usuario.

- **RSI-025 Documentación del sistema**

Riesgo Identificado: Divulgación de información.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.7.2.2 Etiquetado y manejo de la información

Implementar un sistema de clasificación de documentos: Establecer categorías de sensibilidad (confidencial, interno, público) y etiquetar cada documento en consecuencia. Esta acción asegura que el personal maneje la información de acuerdo con su nivel de sensibilidad.

Establecer procedimientos de manejo seguro: Desarrollar guías específicas sobre cómo almacenar, transportar y eliminar documentos según su clasificación. Esto reducirá el riesgo de acceso no autorizado o pérdida de información.

Capacitar al personal: Realizar sesiones de formación para todos los empleados sobre la importancia de la clasificación y manejo seguro de la información. Asegurar que entienden y aplican las políticas de etiquetado.

A.10.8.1 Políticas y procedimientos de intercambio de información

Desarrollar políticas claras de intercambio: Documentar políticas que especifiquen qué tipo de información puede ser compartida y bajo qué condiciones. Estas políticas deben ser revisadas y actualizadas regularmente.

Auditorías de cumplimiento: Realizar auditorías periódicas para asegurar que las políticas de intercambio de información se están siguiendo correctamente. Esto incluye revisar registros de intercambio y entrevistas con el personal.

Capacitación continua: Proveer capacitación regular sobre las políticas de intercambio de información, enfocándose en escenarios específicos y mejores prácticas para mantener la seguridad durante el intercambio de información.

A.11.3.1 Uso de contraseñas

Políticas de contraseñas fuertes: Implementar requisitos para la longitud, complejidad y renovación periódica de contraseñas. Esto puede incluir la combinación de letras, números y caracteres especiales.

Monitoreo y auditorías de contraseñas: Realizar revisiones periódicas de la efectividad de las políticas de contraseñas y auditorías de seguridad para identificar y corregir vulnerabilidades.

A.8.2.2 Concienciación, formación y capacitación en seguridad de la información

Programa de capacitación continuo: Desarrollar un programa de formación en seguridad de la información que incluya módulos específicos sobre la protección de la documentación del sistema y actualizarlo periódicamente.

Evaluación de la eficacia: Implementar mecanismos para evaluar la eficacia de las formaciones, como encuestas post capacitación y pruebas de conocimiento.

Simulacros y ejercicios prácticos: Realizar simulacros de incidentes de seguridad y ejercicios prácticos para reforzar la formación teórica y asegurar que el personal esté preparado para manejar situaciones reales.

- **RSI-028 Documentos internos**

Riesgo Identificado: Fuga, robo o pérdida de información.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.7.2.2 Etiquetado y manejo de la información

Clasificación de documentos: Establecer un sistema para clasificar documentos internos según su nivel de sensibilidad (confidencial, interno, público) y etiquetarlos en consecuencia.

Políticas de manejo: Desarrollar políticas claras sobre el manejo y almacenamiento de documentos clasificados, incluyendo procedimientos para la protección y destrucción segura.

Capacitación sobre clasificación: Realizar capacitaciones regulares para el personal sobre la importancia de la clasificación y manejo adecuado de la información.

A.8.2.2 Concienciación, formación y capacitación en seguridad de la información

Programa de concienciación: Establecer un programa continuo de concienciación sobre seguridad de la información, enfocándose en la protección de documentos internos.

Evaluación de conocimiento: Realizar pruebas periódicas para evaluar el conocimiento del personal sobre las políticas y procedimientos de seguridad de la información.

Simulacros de incidentes: Organizar simulacros de incidentes de seguridad para asegurar que el personal esté preparado para manejar situaciones reales de manera eficaz.

A.10.1.1 Documentación de los procedimientos de operación

Procedimientos documentados: Crear y mantener documentación detallada de los procedimientos operativos para la gestión de documentos internos.

Actualización regular: Revisar y actualizar los procedimientos documentados regularmente para asegurarse de que reflejan las mejores prácticas y los cambios en el entorno.

Distribución controlada: Asegurar que solo el personal autorizado tenga acceso a los procedimientos documentados y que estos se almacenen en un sistema seguro.

A.13.2.3 Recopilación de evidencias

Procedimientos de recolección: Establecer y documentar procedimientos claros para la recolección de evidencias en caso de incidentes de seguridad relacionados con documentos internos.

Capacitación en manejo de evidencias: Proveer formación sobre la recolección, manejo y preservación adecuada de evidencias, asegurando su integridad y validez.

Almacenamiento seguro: Implementar sistemas para el almacenamiento seguro de evidencias, protegiéndolas contra accesos no autorizados y manipulaciones.

- **RSI-029 Material Físico (Impreso)**

Riesgo Identificado: Pérdida, robo o acceso no autorizado a documentos impresos confidenciales.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.3 Seguridad del cableado

Almacenamiento seguro: Implementar sistemas de almacenamiento físico seguro, como armarios con llave, para todos los documentos impresos confidenciales.

Acceso controlado: Limitar el acceso a las áreas donde se almacenan documentos impresos a personal autorizado mediante controles de acceso físicos.

Revisión periódica: Realizar auditorías periódicas del inventario de documentos impresos para asegurar que todos los documentos están donde deben estar y que no faltan.

A.7.2.2 Etiquetado y manejo de la información

Etiquetado claro: Etiquetar claramente todos los documentos impresos con su nivel de confidencialidad y las instrucciones de manejo adecuadas.

Procedimientos de manejo: Desarrollar y comunicar procedimientos claros para el manejo y la eliminación segura de documentos impresos.

Capacitación: Capacitar regularmente al personal sobre las políticas de etiquetado y manejo de información impresa.

A.10.7.3 Procedimientos de manipulación de la información

Destrucción segura: Implementar procedimientos para la destrucción segura de documentos impresos, como trituradores de papel certificados.

Registro de eliminación: Mantener un registro detallado de todos los documentos destruidos, incluyendo la fecha, el tipo de documento y la persona responsable.

Monitoreo continuo: Monitorear y revisar continuamente la efectividad de los procedimientos de destrucción y realizar mejoras según sea necesario.

A.6.1.5 Acuerdos de confidencialidad

Acuerdos firmados: Asegurarse de que todos los empleados firmen acuerdos de confidencialidad que incluyan el manejo de documentos impresos.

Revisión de acuerdos: Revisar y actualizar los acuerdos de confidencialidad regularmente para reflejar cualquier cambio en las políticas o procedimientos.

Seguimiento de cumplimiento: Realizar seguimientos regulares para asegurarse de que los empleados cumplan con los acuerdos de confidencialidad.

- **RSI-030 Información en Carpetas Compartidas en Red**

Riesgo Identificado: Acceso no autorizado, modificación o eliminación de información en carpetas compartidas en red.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.11.2.1 Registro de usuario

Control de acceso: Implementar controles de acceso basados en roles para las carpetas compartidas en red, garantizando que solo el personal autorizado pueda acceder.

Revisión de permisos: Realizar revisiones periódicas de los permisos de acceso para asegurar que solo los usuarios necesarios tienen acceso.

Revocación rápida: Establecer procedimientos para la revocación rápida de accesos cuando un empleado deja la organización o cambia de rol.

A.10.7.2 Retirada de soportes

Procedimientos de eliminación: Establecer procedimientos para la eliminación segura de información en carpetas compartidas cuando ya no es necesaria.

Copia de seguridad: Realizar copias de seguridad regulares de la información almacenada en carpetas compartidas para prevenir pérdida de datos.

Monitoreo de eliminación: Monitorear las actividades de eliminación para asegurar que se sigan los procedimientos adecuados.

A.10.8.4 Mensajería electrónica

Protección de transferencias: Utilizar métodos seguros para la transferencia de información sensible a través de carpetas compartidas, como cifrado.

Notificación de accesos: Implementar notificaciones automáticas para alertar a los administradores cuando se accede a información sensible.

Registro de auditoría: Mantener un registro de auditoría detallado de todos los accesos y modificaciones a las carpetas compartidas.

A.10.1.1 Documentación de los procedimientos de operación

Procedimientos documentados: Documentar todos los procedimientos relacionados con el acceso y manejo de información en carpetas compartidas.

Distribución controlada: Asegurar que solo el personal autorizado tenga acceso a los procedimientos documentados.

Actualización continua: Revisar y actualizar los procedimientos documentados regularmente para reflejar cambios en las políticas y tecnologías.

- **RSI-031 Información Disco**

Riesgo Identificado: Pérdida de datos, acceso no autorizado o corrupción de datos almacenados en discos duros.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.6 Reutilización o retirada segura de equipos

Destrucción segura: Implementar procedimientos para la destrucción segura de discos duros obsoletos o defectuosos, utilizando servicios certificados de destrucción.

Registro de destrucción: Mantener registros detallados de la destrucción de discos duros, incluyendo la fecha, el tipo de dispositivo y la persona responsable.

Reutilización segura: Antes de reutilizar cualquier disco duro, realizar un borrado completo de datos utilizando herramientas de borrado seguro.

A.12.3.1 Política de uso de los controles criptográficos

Cifrado de discos: Implementar cifrado completo del disco para proteger la información almacenada contra accesos no autorizados.

Gestión de claves: Establecer procedimientos para la gestión segura de claves de cifrado, asegurando que solo el personal autorizado tenga acceso a las claves.

Capacitación en cifrado: Capacitar al personal sobre la importancia del cifrado y los procedimientos para su implementación y gestión.

A.12.4.3 Control de acceso al código fuente de los programas

Acceso restringido: Restringir el acceso a los discos que contienen información crítica o sensible a personal autorizado mediante controles de acceso.

Monitoreo de acceso: Registrar y revisar el acceso a los discos y detectar cualquier actividad no autorizada.

Auditorías periódicas: Realizar auditorías periódicas del acceso a los discos para asegurar que se cumplen las políticas de acceso.

A.10.5.1 Copias de seguridad de la información

Política de copias de seguridad: Establecer una política de copias de seguridad que especifique la frecuencia, el tipo y la ubicación de las copias de seguridad de los datos.

Verificación de copias: Realizar pruebas regulares para verificar la integridad y la restaurabilidad de las copias de seguridad.

Almacenamiento seguro: Almacenar las copias de seguridad en ubicaciones seguras, preferiblemente fuera del sitio principal, para protegerlas contra desastres.

- **RSI-033 Datos de Identificación**

Riesgo Identificado: Uso indebido, robo o acceso no autorizado a datos de identificación personal.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.15.1.4 Protección de datos y privacidad de la información de carácter personal

Cifrado de datos: Implementar cifrado de datos para proteger los datos de identificación durante el almacenamiento y la transmisión.

Política de privacidad: Desarrollar y mantener una política de privacidad que detalle cómo se manejan, almacenan y protegen los datos de identificación.

Capacitación en privacidad: Capacitar al personal sobre las regulaciones de privacidad y las prácticas adecuadas para proteger los datos de identificación.

A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

Responsabilidad clara: Asignar responsabilidades claras para la gestión y protección de los datos de identificación a personal específico.

Monitoreo continuo: Implementar sistemas de monitoreo continuo para detectar y responder a cualquier acceso no autorizado a datos de identificación.

Revisión de roles: Revisar periódicamente las responsabilidades asignadas para asegurarse de que se mantienen actualizadas y relevantes.

A.11.2.3 Gestión de contraseñas de usuario

Contraseñas seguras: Exigir el uso de contraseñas seguras para acceder a los sistemas que manejan datos de identificación.

Cambio periódico: Implementar políticas que requieran el cambio periódico de contraseñas y la no reutilización de contraseñas antiguas.

Protección de contraseñas: Asegurar que las contraseñas se almacenan de manera segura y se protegen contra accesos no autorizados.

A.10.10.1 Registro de auditorias

Registro detallado: Mantener registros detallados de todas las actividades relacionadas con el acceso y el manejo de datos de identificación.

Revisión periódica: Revisar regularmente los registros de auditoría para identificar y responder a cualquier actividad sospechosa.

Almacenamiento seguro: Asegurar que los registros de auditoría se almacenan de manera segura y se protegen contra manipulaciones no autorizadas.

- **RSI-034 Información Financiera**

Riesgo Identificado: Pérdida, manipulación o acceso no autorizado a información financiera.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.5.1 Copias de seguridad de la información

Automatización de copias de seguridad: Implementar un sistema automatizado que realice copias de seguridad diarias de toda la información financiera.

Almacenamiento fuera de sitio: Guardar copias de seguridad en ubicaciones geográficas distintas para proteger contra desastres locales.

Pruebas regulares de restauración: Realizar pruebas periódicas de restauración de datos para asegurar la integridad y disponibilidad de las copias de seguridad.

A.11.2.2 Gestión de privilegios

Control de acceso basado en roles: Implementar un sistema de control de acceso basado en roles para restringir el acceso a la información financiera a personal autorizado.

Revisión periódica de accesos: Realizar auditorías trimestrales para revisar y ajustar los privilegios de acceso según las necesidades actuales.

Registro de accesos: Mantener un registro detallado de todas las actividades de acceso a la información financiera para detectar y responder a accesos no autorizados.

A.12.3.1 Política de uso de los controles criptográficos

Cifrado de datos en tránsito y en reposo: Usar cifrado fuerte para proteger la información financiera tanto en tránsito como en reposo.

Gestión segura de claves: Implementar políticas robustas para la generación, almacenamiento y rotación de claves criptográficas.

Auditorías de cifrado: Realizar auditorías periódicas para asegurar que todas las prácticas de cifrado se mantienen efectivas y actualizadas.

A.10.8.1 Políticas y procedimientos de intercambio de información

Protocolo seguro de intercambio: Establecer protocolos seguros (como SFTP) para el intercambio de información financiera con terceros.

Acuerdos de confidencialidad: Formalizar acuerdos de confidencialidad con todos los socios comerciales que manejen información financiera.

Capacitación en intercambio seguro: Capacitar al personal en los procedimientos seguros de intercambio de información para minimizar el riesgo de divulgación.

- **RSI-035 Información de Recursos Humanos**

Riesgo Identificado: Acceso no autorizado, pérdida o alteración de información de empleados.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.8.1.3 Términos y condiciones de contratación

Actualización de términos: Revisar y actualizar regularmente los términos y condiciones de contratación para reflejar cambios en las políticas de seguridad.

Capacitación en políticas de seguridad: Proveer capacitación a todos los empleados sobre las políticas de seguridad de la información y las consecuencias del incumplimiento.

A.9.1.3 Seguridad de oficinas, despachos e instalaciones

Control de acceso físico: Implementar sistemas de control de acceso físico, como tarjetas de identificación y biometría, para restringir el acceso a áreas donde se maneja información de recursos humanos.

Monitoreo y vigilancia: Instalar cámaras de vigilancia en áreas críticas y realizar monitoreo continuo para detectar actividades sospechosas.

Registro de visitantes: Mantener un registro detallado de todos los visitantes y sus accesos a las instalaciones de recursos humanos.

A.11.2.3 Gestión de contraseñas de usuario

Política de contraseñas seguras: Establecer una política de contraseñas robusta que requiera el uso de contraseñas complejas y la autenticación multifactor.

Cambio regular de contraseñas: Exigir el cambio de contraseñas a intervalos regulares (cada 90 días) para reducir el riesgo de acceso no autorizado.

Protección de contraseñas: Utilizar soluciones de almacenamiento seguro de contraseñas y educar a los empleados sobre la importancia de no compartir contraseñas.

A.7.2.1 Directrices de clasificación

Clasificación de información: Establecer directrices claras para la clasificación de la información de recursos humanos según su sensibilidad y criticidad.

Etiquetado de documentos: Etiquetar todos los documentos físicos y digitales con la clasificación adecuada para asegurar su manejo correcto.

Capacitación en manejo de información: Proveer capacitación continua al personal sobre cómo manejar y proteger información de acuerdo a su clasificación.

- **RSI-039 Internet**

Riesgo Identificado: Pérdida de datos, ataques de malware, y acceso no autorizado a través de internet.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.4.1 Controles contra el código malicioso

Software antivirus: Instalar y mantener actualizado el software antivirus en todos los dispositivos conectados a internet.

Filtrado de contenido: Implementar filtros de contenido para bloquear sitios web maliciosos o no seguros.

Educación de usuarios: Capacitar a los empleados sobre los riesgos del malware y las prácticas seguras de navegación en internet.

A.10.6.2 Seguridad de los servicios de red

Cortafuegos: Configurar cortafuegos para controlar y monitorear el tráfico de red entrante y saliente.

Sistemas de detección de intrusos: Implementar sistemas de detección y prevención de intrusos (IDS/IPS) para identificar y responder a amenazas en tiempo real.

Actualizaciones y parches: Asegurar que todos los dispositivos y servicios de red estén actualizados con los últimos parches de seguridad.

A.11.4.1 Política de uso de los servicios en red

Políticas de uso aceptable: Desarrollar y comunicar políticas claras sobre el uso aceptable de los servicios de internet.

Monitoreo del uso: Implementar herramientas para monitorear el uso de internet y detectar actividades sospechosas o no autorizadas.

Restricciones de acceso: Limitar el acceso a internet a sitios y servicios esenciales para el trabajo.

A.10.9.3 Información públicamente disponible

Gestión de la información pública: Asegurar que solo la información autorizada y revisada esté disponible públicamente en sitios web y otras plataformas en línea.

Control de cambios: Establecer un proceso de control de cambios para la información publicada públicamente.

Revisión periódica: Realizar revisiones periódicas del contenido público para garantizar su exactitud y seguridad.

- **RSI-040 Red Inalámbrica**

Riesgo Identificado: Intercepción de comunicaciones, acceso no autorizado y ataques de denegación de servicio en la red inalámbrica.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.6.1 Controles de red

Cifrado de comunicaciones: Usar cifrado WPA3 para asegurar las comunicaciones en la red inalámbrica.

Segmentación de red: Crear redes segmentadas (VLANs) para separar el tráfico de invitados del tráfico interno.

Filtrado de MAC: Implementar filtrado de direcciones MAC para limitar el acceso a dispositivos autorizados.

A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración

Protección de acceso remoto: Desactivar el acceso remoto no necesario y utilizar autenticación multifactor para acceso autorizado.

Cierre de puertos no utilizados: Desactivar puertos de configuración no necesarios para minimizar puntos de entrada potenciales.

Monitoreo de accesos: Implementar herramientas de monitoreo para detectar y alertar sobre intentos de acceso no autorizado.

A.9.2.3 Seguridad del cableado

Ubicación segura de puntos de acceso: Instalar puntos de acceso en ubicaciones seguras para prevenir el acceso físico no autorizado.

Protección del cableado: Asegurar el cableado de red para prevenir manipulaciones y accesos no autorizados.

Monitoreo de puntos de acceso: Monitorear continuamente los puntos de acceso para detectar y responder a anomalías.

- **RSI-041 Almacenamiento de Información**

Riesgo Identificado: Pérdida, acceso no autorizado o corrupción de datos almacenados.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.5.1 Copias de seguridad de la información

Automatización de backups: Establecer un sistema automatizado de copias de seguridad regulares y completas.

Almacenamiento seguro: Guardar copias de seguridad en ubicaciones seguras y fuera del sitio principal.

Pruebas de restauración: Realizar pruebas periódicas de restauración para garantizar la integridad y disponibilidad de los datos.

A.11.2.3 Gestión de contraseñas de usuario

Contraseñas robustas: Implementar políticas de contraseñas robustas que incluyan autenticación multifactor para acceder a datos sensibles.

Gestión de contraseñas: Utilizar herramientas de gestión de contraseñas para almacenar y manejar credenciales de forma segura.

Cambio periódico de contraseñas: Establecer una política de cambio regular de contraseñas para reducir el riesgo de accesos no autorizados.

A.9.2.6 Reutilización o retirada segura de equipos

Borrado seguro de datos: Implementar procedimientos para el borrado seguro de datos antes de la reutilización o disposición de equipos.

Registro de retirada: Mantener un registro detallado de la retirada y disposición de equipos de almacenamiento para auditoría y seguimiento.

A.12.3.1 Política de uso de los controles criptográficos

Cifrado de datos: Utilizar cifrado de datos tanto en tránsito como en reposo para proteger la información almacenada.

Gestión de claves: Implementar políticas robustas para la generación, almacenamiento y rotación de claves criptográficas.

Capacitación en criptografía: Capacitar al personal en el uso y manejo seguro de tecnologías criptográficas para proteger los datos.

- **RSI-042 Electricidad**

Riesgo Identificado: Interrupciones de energía que pueden causar pérdida de datos, daño a equipos y parálisis operativa.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.2 Instalaciones de suministro

Sistemas UPS: Instalar sistemas de alimentación ininterrumpida (UPS) para proteger equipos críticos contra apagones.

Generadores de respaldo: Implementar generadores de energía de respaldo para asegurar la continuidad de operaciones durante cortes prolongados.

Mantenimiento regular: Realizar mantenimiento periódico de los sistemas de energía para asegurar su funcionamiento óptimo en caso de emergencia.

A.9.1.4 Protección contra las amenazas externas y de origen ambiental

Supresores de picos: Utilizar supresores de picos de corriente para proteger los equipos electrónicos contra sobrevoltajes.

Estabilizadores de voltaje: Implementar estabilizadores de voltaje para asegurar una corriente eléctrica constante y segura.

Monitoreo de energía: Instalar sistemas de monitoreo para detectar y alertar sobre variaciones en el suministro eléctrico.

A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Plan de continuidad eléctrica: Desarrollar e implementar un plan de continuidad específico para la energía, incluyendo procedimientos de emergencia.

Simulacros regulares: Realizar simulacros periódicos para asegurar que el personal esté preparado para manejar cortes de energía.

Revisión y actualización: Revisar y actualizar regularmente el plan de continuidad para reflejar cambios en la infraestructura y tecnologías.

A.10.5.1 Copias de seguridad de la información

Backups regulares: Asegurar que se realicen copias de seguridad regulares de toda la información crítica para proteger contra la pérdida de datos debido a fallos eléctricos.

Almacenamiento externo: Guardar copias de seguridad en ubicaciones externas y seguras.

Pruebas de restauración: Realizar pruebas de restauración periódicas para asegurar la capacidad de recuperación de datos en caso de un corte de energía.

- **RSI-043 Instalaciones de la Organización**

Riesgo Identificado: Acceso no autorizado, robo, daño a instalaciones y equipos críticos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.1.1 Perímetro de seguridad física

Barreras físicas: Instalar barreras físicas, como cercas y muros, para proteger el perímetro de la organización.

Control de accesos: Implementar sistemas de control de acceso físico, como tarjetas de identificación y lectores biométricos.

Vigilancia y patrullaje: Mantener vigilancia constante y patrullajes regulares para detectar y disuadir intrusiones.

A.9.1.3 Seguridad de oficinas, despachos e instalaciones

Sistemas de alarmas: Instalar sistemas de alarmas para detectar accesos no autorizados y alertar al personal de seguridad.

Cámaras de vigilancia: Utilizar cámaras de vigilancia para monitorear áreas críticas y registrar actividades sospechosas.

Políticas de acceso: Desarrollar y comunicar políticas de acceso a las instalaciones, limitando el acceso a áreas sensibles solo a personal autorizado.

A.9.2.1 Emplazamiento y protección de equipos

Ubicación segura de equipos: Colocar equipos críticos en áreas seguras y restringidas para evitar accesos no autorizados.

Protección contra incendios: Instalar sistemas de detección y extinción de incendios en áreas donde se encuentran equipos críticos.

Climatización adecuada: Asegurar que los equipos estén en ambientes con temperatura y humedad controlada para prevenir daños.

A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

Responsables de seguridad: Designar personal específico responsable de la seguridad física de las instalaciones.

Capacitación en seguridad: Capacitar al personal en prácticas de seguridad física y protocolos de emergencia.

Revisión de responsabilidades: Revisar y actualizar periódicamente las responsabilidades de seguridad para reflejar cambios en la organización y amenazas.

- **RSI-044 Centro de Datos Principal**

Riesgo Identificado: Interrupciones en el funcionamiento del centro de datos, pérdida de datos, acceso no autorizado.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.1 Emplazamiento y protección de equipos

Ubicación segura: Seleccionar ubicaciones con bajo riesgo de desastres naturales y con infraestructura robusta.

Protección contra incendios: Implementar sistemas avanzados de detección y extinción de incendios.

Control ambiental: Mantener un control riguroso de temperatura y humedad para proteger los equipos del centro de datos.

A.9.1.3 Seguridad de oficinas, despachos e instalaciones

Control de acceso: Implementar sistemas de control de acceso biométrico y multifactor para el centro de datos.

Vigilancia continua: Instalar sistemas de videovigilancia y monitoreo 24/7 para detectar y responder a intrusiones.

Alarmas y sensores: Utilizar alarmas y sensores para detectar acceso no autorizado y situaciones de emergencia.

A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Planes de recuperación: Desarrollar y mantener un plan de recuperación ante desastres para el centro de datos.

Pruebas regulares: Realizar pruebas periódicas de los planes de recuperación para asegurar su efectividad.

Actualización continua: Actualizar los planes de continuidad y recuperación regularmente para reflejar cambios en la infraestructura y amenazas.

A.10.5.1 Copias de seguridad de la información

Backups automatizados: Establecer sistemas automatizados de copias de seguridad para los datos críticos del centro de datos.

Almacenamiento externo seguro: Guardar copias de seguridad en ubicaciones externas y seguras para protección adicional.

Verificación de backups: Implementar procedimientos para verificar regularmente la integridad y disponibilidad de las copias de seguridad.

- **RSI-045 Archivo Documental**

Riesgo Identificado: Pérdida, robo o acceso no autorizado a documentos físicos y electrónicos.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.6 Reutilización o retirada segura de equipos

Destrucción segura: Implementar procesos para la destrucción segura de documentos físicos sensibles.

Registro de disposición: Mantener registros detallados de la disposición de documentos y equipos para auditoría.

A.9.1.1 Perímetro de seguridad física

Control de acceso físico: Utilizar sistemas de control de acceso para limitar la entrada a áreas de archivo documental.

Sistemas de vigilancia: Instalar cámaras de seguridad para monitorear las áreas donde se almacenan documentos.

A.7.2.2 Etiquetado y manejo de la información

Clasificación de documentos: Establecer un sistema de clasificación y etiquetado de documentos según su sensibilidad.

Protocolos de manejo: Desarrollar y comunicar protocolos para el manejo seguro de documentos clasificados.

Auditorías de cumplimiento: Realizar auditorías periódicas para asegurar que los protocolos de manejo de información se sigan adecuadamente.

- **RSI-046 Red Eléctrica**

Riesgo Identificado: Interrupciones de energía que pueden afectar la operación de la organización.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.9.2.2 Instalaciones de suministro

Sistemas de UPS: Implementar sistemas de alimentación ininterrumpida (UPS) para proteger contra cortes de energía. Realizar pruebas periódicas de los UPS para garantizar su funcionamiento óptimo.

Generadores de emergencia: Instalar generadores de emergencia para asegurar la continuidad de operaciones críticas. Mantener los generadores regularmente y realizar simulacros de encendido para verificar su eficacia.

Mantenimiento preventivo: Realizar mantenimiento regular y pruebas de sistemas de suministro eléctrico. Programar inspecciones periódicas de las instalaciones eléctricas para identificar y corregir posibles problemas.

A.9.1.4 Protección contra las amenazas externas y de origen ambiental

Estabilizadores de voltaje: Utilizar estabilizadores para proteger equipos de sobrevoltajes y fluctuaciones de energía. Realizar análisis de calidad de energía para determinar la necesidad y ubicación de estabilizadores.

Supresores de picos: Implementar supresores de picos para mitigar el impacto de picos de energía. Capacitar al personal en la identificación y manejo de picos de energía para minimizar daños.

Monitorización continua: Instalar sistemas de monitoreo para detectar y alertar sobre problemas en el suministro eléctrico. Establecer protocolos de respuesta a alertas de monitoreo para acciones inmediatas.

A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Plan de emergencia eléctrica: Desarrollar y mantener un plan de respuesta a emergencias eléctricas. Realizar simulacros regulares para asegurar la efectividad del plan y entrenar al personal en su ejecución.

Simulacros y pruebas: Realizar simulacros y pruebas regulares para asegurar que el plan sea efectivo. Documentar lecciones aprendidas y realizar ajustes al plan según sea necesario.

Revisión y actualización: Revisar y actualizar el plan de continuidad y recuperación regularmente para reflejar cambios en la infraestructura y amenazas. Incorporar retroalimentación de simulacros y evaluaciones de riesgos en las actualizaciones.

- **RSI-047 Red de Datos**

Riesgo Identificado: Interrupción o compromiso de la red de datos que afecta la conectividad y la seguridad de la información.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.10.6.1 Controles de red

Firewalls de red: Implementar firewalls de red para filtrar el tráfico no autorizado y proteger la infraestructura de red. Configurar reglas de firewall basadas en políticas de seguridad para restringir el acceso no deseado.

Sistemas de detección de intrusiones (IDS): Desplegar sistemas de detección de intrusiones para monitorear el tráfico de red y detectar actividades maliciosas.

Segmentación de red: Dividir la red en segmentos lógicos para limitar el alcance de posibles ataques. Aplicar políticas de acceso basadas en roles para restringir el movimiento lateral de amenazas.

A.10.8.1 Políticas y procedimientos de intercambio de información

Política de uso aceptable de la red: Establecer políticas claras sobre el uso aceptable de la red para educar a los usuarios sobre prácticas seguras. Comunicar regularmente las políticas y realizar capacitaciones para garantizar el cumplimiento.

Protección de información en tránsito: Encriptar el tráfico de red sensible para proteger la confidencialidad durante la transmisión. Implementar protocolos de seguridad robustos, como SSL/TLS, para asegurar las comunicaciones.

Monitoreo de tráfico de red: Implementar herramientas de monitoreo de tráfico de red para identificar patrones anómalos y posibles amenazas. Establecer alertas para notificar al personal de seguridad sobre actividades sospechosas.

A.11.4.6 Control de la conexión a la red

Control de acceso basado en políticas (PBAC): Implementar PBAC para controlar el acceso a recursos de red según políticas definidas. Configurar reglas de PBAC para restringir el acceso a redes sensibles o segmentos críticos.

Registro de eventos de conexión: Registrar eventos de conexión para realizar seguimiento de actividades de red y detectar comportamientos anómalos. Establecer alertas para eventos de conexión inusual o no autorizado.

A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Plan de recuperación de red: Desarrollar un plan de recuperación de red para restaurar la conectividad en caso de interrupciones. Incluir procedimientos detallados de diagnóstico y resolución de problemas.

Pruebas de redundancia de red: Realizar pruebas regulares de redundancia de red para garantizar la disponibilidad de rutas alternativas en caso de fallo. Documentar y corregir debilidades identificadas durante las pruebas.

Respuesta a incidentes de red: Establecer un equipo de respuesta a incidentes de red para investigar y mitigar amenazas de seguridad. Capacitar al personal en la identificación y respuesta a incidentes de red de manera oportuna.

- **RSI-048 Personal Interno**

Riesgo Identificado: El riesgo de acceso no autorizado o uso inapropiado de la información por parte del personal interno.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.7.1 Responsabilidad sobre los activos

Establecer políticas claras de responsabilidad sobre los activos, incluyendo la información.

Realizar auditorías periódicas para asegurar el cumplimiento de las políticas de responsabilidad.

Implementar un sistema de seguimiento de activos para monitorear el acceso y el uso.

A.11 Control de acceso

Implementar un sistema de gestión de identidades y accesos (IAM) para asignar y controlar los privilegios de acceso.

Aplicar el principio de "menor privilegio", otorgando solo los permisos necesarios para realizar las funciones laborales.

Establecer procedimientos de revisión y revocación de accesos de forma regular y en caso de cambios en la posición laboral.

A.15 Cumplimiento

Desarrollar y difundir políticas claras de seguridad de la información, incluyendo normas de comportamiento y responsabilidades del personal interno.

Realizar sesiones de formación y concienciación regularmente para mantener al personal actualizado sobre las políticas y procedimientos de seguridad.

Establecer un mecanismo de reporte para que el personal pueda informar sobre incidentes de seguridad o violaciones de políticas de manera confidencial.

- **RSI-049 Directores de área**

Riesgo Identificado: El riesgo de falta de liderazgo en la implementación y cumplimiento de políticas de seguridad de la información por parte de los directores de área.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.6.1 Organización interna

Definir claramente las responsabilidades de los directores de área en lo que respecta a la seguridad de la información.

Establecer un comité de seguridad de la información liderado por los directores de área para coordinar y supervisar las iniciativas de seguridad.

Realizar reuniones periódicas de seguimiento para revisar el progreso y abordar cualquier problema relacionado con la seguridad de la información.

A.8 Seguridad ligada a los recursos humanos

Incluir la seguridad de la información como un criterio en la evaluación del desempeño de los directores de área.

Proporcionar formación específica sobre seguridad de la información a los directores de área para mejorar su comprensión y capacidad de liderazgo en este ámbito.

Establecer un proceso disciplinario claro y transparente para abordar las violaciones de políticas de seguridad por parte de los directores de área.

A.10 Gestión de comunicaciones y operaciones

Promover una cultura de comunicación abierta y transparente entre los directores de área para facilitar el intercambio de información relevante sobre seguridad.

Implementar un sistema de gestión de incidentes de seguridad que involucre activamente a los directores de área en la respuesta y mitigación de incidentes.

Realizar revisiones periódicas de los procesos y controles operativos para garantizar su eficacia y relevancia bajo la supervisión de los directores de área.

A.14 Gestión de la continuidad del negocio

Integrar la seguridad de la información en los planes de continuidad del negocio dirigidos por los directores de área.

Realizar simulacros de respuesta a incidentes y pruebas de continuidad del negocio con participación activa de los directores de área.

Mantener una comunicación regular con los directores de área para asegurar su compromiso continuo con la gestión de la continuidad del negocio y la seguridad de la información.

- **RSI-050 Personal Administrativo**

Riesgo Identificado: Acceso no autorizado a la información confidencial debido a la falta de controles adecuados sobre el personal administrativo.

Método de Tratamiento de Riesgos: Reducir

Controles Propuestos y Recomendaciones:

A.7.1 Responsabilidad sobre los activos

Realizar un inventario exhaustivo de los activos de información a los que el personal administrativo tiene acceso y mantenerlo actualizado regularmente.

Establecer claramente la propiedad de los activos de información y definir quién tiene la responsabilidad de protegerlos.

Establecer políticas y procedimientos para el uso aceptable de los activos de información, incluyendo pautas sobre el acceso y la manipulación de datos confidenciales.

A.8 Seguridad ligada a los recursos humanos

Proporcionar una formación integral en seguridad de la información al personal administrativo, incluyendo sesiones de concienciación sobre la importancia de proteger la información confidencial.

Establecer un proceso disciplinario claro para abordar cualquier violación de las políticas de seguridad de la información por parte del personal administrativo.

Implementar procedimientos efectivos para la gestión del cese del empleo, que incluyan la revocación de los derechos de acceso del personal que abandona la organización.

A.9 Seguridad física y ambiental

Garantizar que las áreas donde trabaja el personal administrativo estén físicamente seguras, con medidas como el control de acceso físico y la supervisión adecuada.

Implementar controles físicos de entrada para restringir el acceso no autorizado a las instalaciones donde se maneja información confidencial.

Establecer políticas y procedimientos Incluyendo medidas para prevenir el robo o la manipulación de dispositivos de almacenamiento externo.

A.11 Control de acceso

Implementar una política de control de acceso que defina claramente los roles y privilegios de acceso del personal administrativo a los sistemas y datos.

Establecer un proceso para el registro de usuarios que incluya la verificación de la identidad y la asignación de credenciales de acceso seguras.

Realizar revisiones periódicas de los derechos de acceso del personal administrativo para garantizar que estén alineados con sus funciones laborales y responsabilidades.

- **RSI-051 Administrador de Página Web**

Riesgo Identificado: Posible acceso no autorizado o manipulación de la página web debido a vulnerabilidades en su administración.

Método de Tratamiento de Riesgos: Reducir.

Controles Propuestos y Recomendaciones:

A.12.6.1 Control de las vulnerabilidades técnicas

Realizar análisis de vulnerabilidades periódicos utilizando herramientas especializadas para identificar posibles brechas de seguridad.

Implementar parches de seguridad y actualizaciones de software de forma regular para mitigar vulnerabilidades conocidas.

Establecer un plan de respuesta a incidentes que incluya acciones específicas para abordar y corregir las vulnerabilidades identificadas.

A.10.1 Responsabilidades y procedimientos de operación

Definir claramente las responsabilidades del personal encargado de administrar la página web, incluyendo la supervisión de actividades relacionadas con la seguridad.

Documentar los procedimientos operativos estándar para la gestión y mantenimiento de la página web, incluyendo la aplicación de parches de seguridad y la revisión de registros de actividad.

Establecer controles de acceso adecuados para limitar el número de personas autorizadas para realizar cambios en la página web y mantener un registro de las actividades realizadas.

A.11.4 Control de acceso a la red

Implementar medidas de autenticación sólidas, como contraseñas seguras o autenticación de dos factores, para acceder a los sistemas de administración de la página web.

Utilizar cortafuegos y filtros de paquetes para controlar el tráfico de red entrante y saliente hacia los servidores que alojan la página web.

Configurar listas de control de acceso (ACL) para restringir el acceso a los servicios de administración de la página web solo a direcciones IP autorizadas.

A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

Realizar auditorías periódicas de seguridad para verificar el cumplimiento de las políticas y normas establecidas para la administración de la página web.

Mantener registros detallados de las acciones realizadas en la administración de la página web, incluyendo cambios de configuración, actualizaciones de software y actividades de mantenimiento.

Capacitar al personal encargado de administrar la página web sobre las políticas de seguridad y las mejores prácticas para garantizar el cumplimiento continuo de los estándares de seguridad.

2.6 Aceptación del riesgo

Es crucial involucrar a las partes interesadas pertinentes en el proceso de aceptación de riesgos, donde se evalúan las opciones de tratamiento y se toman decisiones informadas sobre la tolerancia al riesgo [5].

Tras la evaluación de los riesgos asociados a los activos de la organización, se ha determinado que el riesgo residual de los activos que se encuentre en nivel bajo se aceptará sin tratamiento adicional. La decisión se fundamenta en los siguientes principios:

Criterios de aceptación de riesgos:

- **Criticidad del activo:** No todos los activos evaluados son críticos para la operación y seguridad de la organización.
- **Nivel de riesgo residual:** Algunos de los riesgos residuales evaluados caen dentro de los límites aceptables establecidos por la organización.
- **Política de seguridad de la información:** La política de seguridad de la organización permite la aceptación de ciertos riesgos cuando se considera que el costo de mitigación es mayor que el beneficio.

Justificación para la aceptación de riesgos:

Los siguientes riesgos han sido aceptados debido a su bajo impacto y/o baja probabilidad de ocurrencia, así como el alto costo o baja factibilidad de su mitigación:

- RSI-004 Dispositivos móviles
- RSI-008 Teléfonos
- RSI-013 Televisores
- RSI-016 Servidores Aplicaciones/ Contenedores
- RSI-018 Navegadores
- RSI-019 Office
- RSI-021 Licencias
- RSI-026 Solicitudes
- RSI-027 Formatos
- RSI-032 Información memorias USB
- RSI-036 Información Urbanística
- RSI-037 Capacitaciones

- RSI-038 Telefonía
- RSI-052 Proveedores

Justificación para la no aceptación de otros riesgos:

Todos los riesgos identificados durante el proceso de evaluación que no están en la lista de riesgos aceptados presentan un nivel de impacto o probabilidad que no satisface los criterios normales de aceptación de riesgos de la organización. En consecuencia, la organización ha decidido mitigar estos riesgos mediante el método de tratamiento, reducción del riesgo, al implementar controles y medidas de seguridad para disminuir la probabilidad y/o el impacto de los riesgos identificados.

El Comité de Evaluación ha concluido que, para asegurar un entorno seguro y confiable, no se aceptará ningún riesgo sin tratamiento si no está dentro del nivel de riesgo aceptable definido.

2.7 Comunicación del riesgo

La comunicación de riesgos juega un papel vital en la transparencia y la toma de decisiones informadas [5].

Este proceso implica el establecimiento de un mecanismo para la recepción y comunicación de la gestión de riesgos de seguridad de la información con todas las partes interesadas.

Objetivos de la comunicación del riesgo:

- **Transparencia:** Garantizar que todos los interesados estén al tanto de los riesgos identificados y las medidas adoptadas para mitigarlos.
- **Toma de decisiones informadas:** Proporcionar la información necesaria para que las partes interesadas puedan tomar decisiones informadas sobre la gestión de riesgos.

Mecanismo de recepción y comunicación:

Acta de recepción de riesgos: El propósito es documentar formalmente la recepción y aceptación de la evaluación de riesgos por parte de las partes interesadas.

Contenido del acta:

- Descripción del proceso de evaluación de riesgos.
- Listado de los activos evaluados y sus niveles de riesgo residual.
- Lista de riesgos aceptados.
- Propuestas de tratamiento de riesgos.
- Firmas de las partes interesadas, incluyendo miembros del comité de evaluación y representantes de la organización.

En la sección de Anexos se incluye el formato del acta de recepción de riesgos entregada a la empresa pública.

CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

3.1 Plan de evaluación

3.1.1 Objetivo

Validar la viabilidad de la propuesta de mejoras para la gestión de riesgos de seguridad de la información en la empresa pública, mediante la implementación de encuestas a expertos en seguridad de la información y basándose en normas nacionales.

3.1.2 Cronograma de actividades para el plan de evaluación

El cronograma de activadas se planificó en 4 semanas (del 10 de junio del 2024 al 05 de julio del 2024) para la realización de la evaluación del prototipo. El cronograma se puede observar en la Tabla 21:

Tabla 21: Cronograma de actividades para el plan de evaluación

Actividades	Semanas			
	Semana 10	Semana 11	Semana 12	Semana 13
Preparación y selección de expertos.				
Envío del formulario de la encuesta.				
Revisión de la documentación relevante por parte de los expertos.				
Recolección de respuestas de los expertos.				
Análisis de resultados de las encuestas.				
Elaboración del informe final.				
Revisión final del informe.				

3.1.3 Proceso

Preparación y selección de expertos en seguridad de la información: Se identifica y selecciona expertos en seguridad de la información con experiencia relevante para participar en la encuesta.

Envío del formulario de la encuesta a los expertos: Se envía el formulario online a los expertos, donde se incluye un enlace a un documento con la información relevante del proceso del proyecto para que la revisen antes de realizar la encuesta. El formulario también contiene preguntas específicas sobre el proceso de gestión de riesgos y la viabilidad de la propuesta de mejoras, solicitando su evaluación en diferentes aspectos.

Revisión de la documentación por parte de los expertos: Los expertos revisan la documentación proporcionada para comprender la propuesta de mejoras y prepararse para la encuesta.

Recolección de respuestas de los expertos: Se recolectan las respuestas de los expertos una vez que hayan revisado la documentación del proyecto y completado la encuesta.

Análisis de las respuestas de los expertos: Se analizan y sintetizan las respuestas de los expertos a la encuesta, identificando patrones y áreas de consenso o discrepancia.

Elaboración del informe final de evaluación: Se redacta el informe de evaluación, que resume los hallazgos y conclusiones de la encuesta siendo el resultado final del proceso de evaluación.

Revisión final del informe de evaluación: Se realiza una revisión final del informe de evaluación para garantizar su precisión y completitud.

3.1.4 Actividades

Las actividades realizadas en el plan de evaluación fueron las siguientes:

- Identificación de expertos en seguridad de la información.
- Establecimiento de contacto y coordinación con los expertos seleccionados.
- Envío del formulario en línea para la encuesta a los expertos.
- Revisión de la documentación por parte de los expertos.
- Recepción de las respuestas de los expertos a la encuesta.
- Análisis de las respuestas de los expertos para identificar patrones.
- Síntesis de los hallazgos y conclusiones preliminares.

- Preparación del informe final de evaluación con los resultados consolidados.
- Corrección de errores y ajustes en el informe.

3.1.5 Resultados esperados

Los resultados esperados incluyen la validación de la hipótesis planteada mediante la implementación de encuestas a expertos en seguridad de la información. Además, se busca identificar los puntos fuertes como los débiles presentes en la propuesta de mejoras, con el objetivo de analizar la gestión de los riesgos de seguridad de la información en la empresa pública. Por último, se busca validar el enfoque metodológico utilizado en el trabajo de titulación, asegurando su coherencia y efectividad en el trabajo de titulación.

3.2 Resultados de la evaluación

Los resultados de la evaluación de la propuesta de mejoras se obtuvieron a partir de una encuesta realizada a trabajadores de la empresa pública, estudiantes graduados de la carrera de Tecnologías de la Información de la Universidad Técnica de Machala y otros profesionales de áreas afines con conocimientos en normas como la ISO/IEC 27005 e ISO/IEC 27001. El formulario utilizó una escala de Likert con las siguientes cinco opciones:

1. Muy insatisfecho
2. Insatisfecho
3. Neutral
4. Satisfecho
5. Muy satisfecho

El cuestionario evaluó diversos aspectos del proceso de gestión de riesgos y la propuesta de mejoras en cuanto a su viabilidad y utilidad en la empresa pública. Un total de 14 personas respondieron a la encuesta. El formato del instrumento aplicado, realizado mediante Microsoft Forms, se incluye en la sección de Anexos.

A continuación, se detallan los resultados:

Para el registro de los encuestados, se solicitó ingresar su correo electrónico. De los participantes, 3 utilizaron correos con el dominio @hotmail.com, 9 con el dominio @gmail.com y 2 con el dominio @utmachala.edu.ec, como se muestra en la Figura 7.

14 Respuestas

ID ↑	Nombre	Respuestas
1	anonymous	lvsv2002@hotmail.com
2	anonymous	ferbenor@gmail.com
3	anonymous	ramoncitorogel@gmail.com
4	anonymous	snuneza21@gmail.com
5	anonymous	Aramirez5@utmachala.edu.ec
6	anonymous	luis20castillomu@gmail.com
7	anonymous	jeffersonp-2001@hotmail.com
8	anonymous	OZapata7@gmail.com
9	anonymous	david2001055@gmail.com
10	anonymous	kpambi2@utmachala.edu.ec
11	anonymous	danny261081@hotmail.com
12	anonymous	mercedesherreras27@gmail.com
13	anonymous	fbordonez@gmail.com
14	anonymous	waltermh@gmail.com

Figura 7: Personas que completaron el cuestionario

Identificación de los participantes

Como parte de los datos de identificación de los encuestados, se pidió que especificaran su rol. En la Figura 8, se detalla la distribución de los participantes: cinco personas (36%) son trabajadores de la empresa pública, dos personas (14%) son estudiantes graduados de la carrera de Tecnologías de la Información, y los otros siete encuestados (50%) pertenecen a otras profesiones de áreas afines con conocimientos sobre normas como la ISO/IEC 27005 e ISO/IEC 27001.

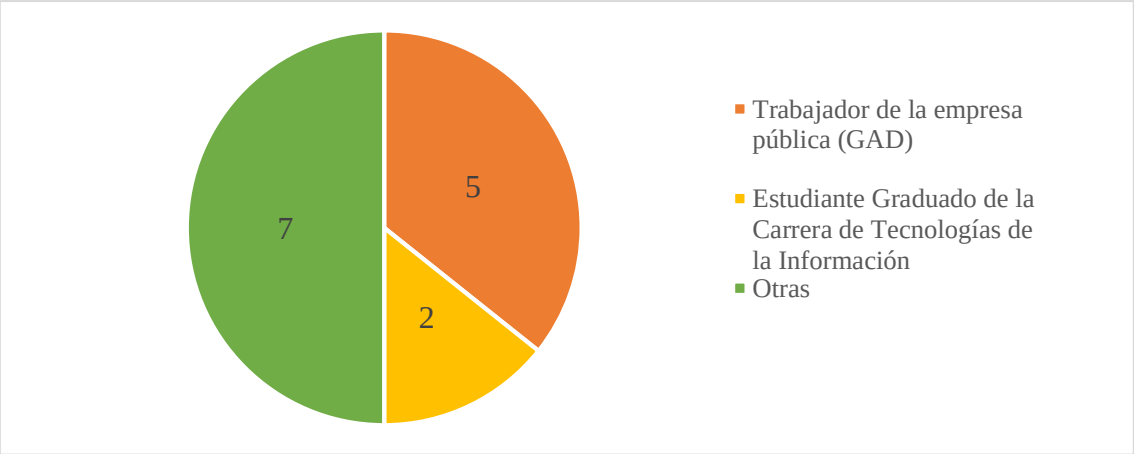


Figura 8: Identificación del participante

En la pregunta 1, "**¿Cómo evaluaría la relevancia y aplicabilidad de las normas nacionales (basadas en la ISO 27005) utilizadas como metodología para la gestión de riesgos en la propuesta?**", se observa que de los 14 encuestados, el 57.1% está completamente satisfecho con la relevancia y aplicabilidad de las normas nacionales en el trabajo. El 21.4% también está satisfecho con esta afirmación, mientras que el 21.4% restante mantiene una postura neutral. Nadie se sintió insatisfecho o muy insatisfecho con este criterio (Figura 9).

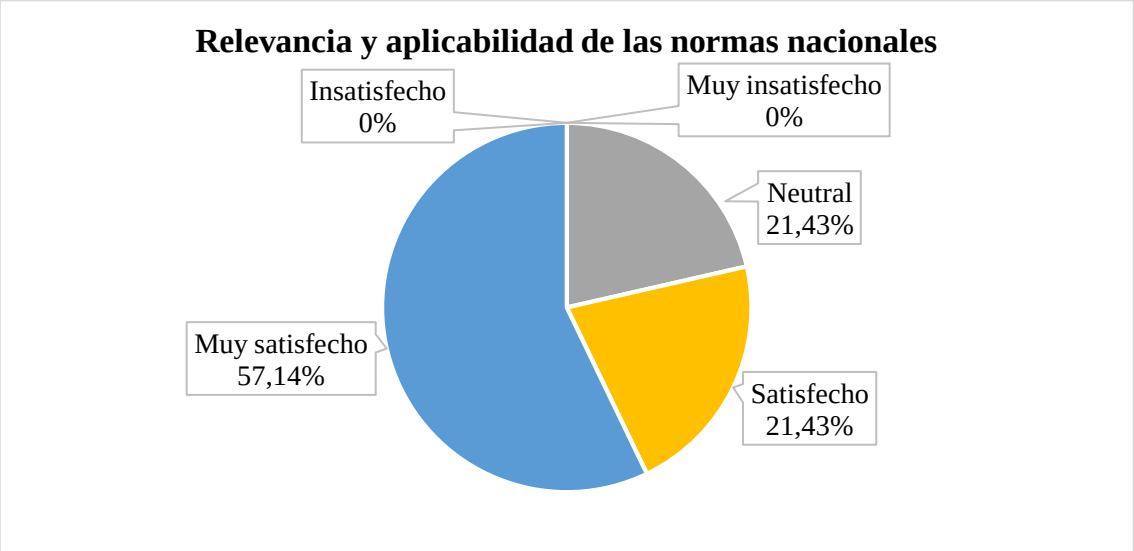


Figura 9: Resultados de la pregunta 1 de la encuesta

En la pregunta 2, "**¿Qué tan precisamente están identificados los activos críticos de seguridad de la información dentro de la empresa pública?**", se obtuvo que el 35.7% de los encuestados se encuentran muy satisfechos con la identificación de activos críticos, el 42.9% también está satisfecho con el proceso y el 21.4% se mantiene neutral. Ninguno de los encuestados expresó insatisfacción o mucha insatisfacción respecto a esta cuestión (Figura 10).

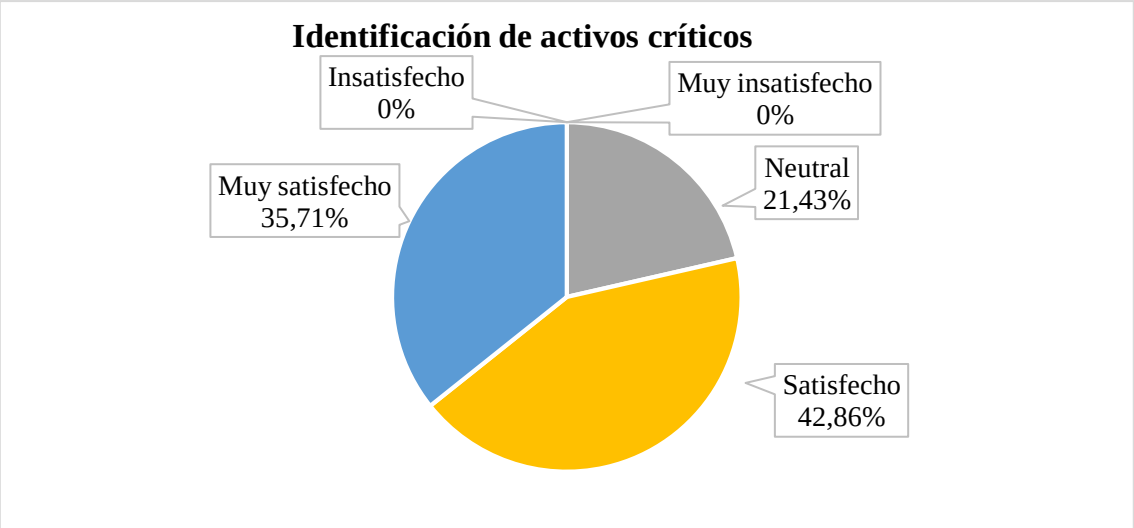


Figura 10: Resultados de la pregunta 2 de la encuesta

En la pregunta 3, "**¿En qué medida considera que los criterios de evaluación de riesgos establecidos (nivel de confidencialidad, integridad, disponibilidad, probabilidad de ocurrencia, nivel de efectividad de controles y mapa de calor) son adecuados y suficientes para analizar los riesgos asociados a la seguridad de la información**?", los resultados indican que el 42.9% de los encuestados están muy satisfechos con los criterios de evaluación de riesgos, el 42.9% también muestra satisfacción, y un 7.1% mantiene una postura neutral. Por otro lado, un 7.1% manifestó insatisfacción y no hubo encuestados muy insatisfechos en relación a esta pregunta (Figura 11).

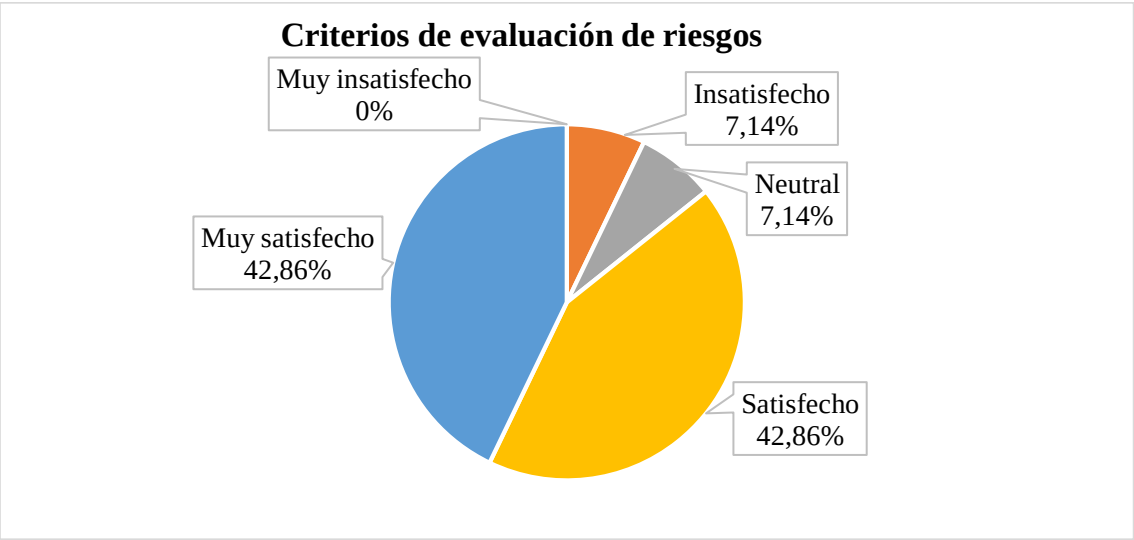


Figura 11: Resultados de la pregunta 3 de la encuesta

En la pregunta 4, "**¿Cómo evaluaría la calidad y precisión del análisis de vulnerabilidades y amenazas, así como del proceso de evaluación de riesgos de seguridad de la información?**", los datos muestran que el 28.6% de los encuestados están muy satisfechos con

la calidad del análisis de vulnerabilidades, amenazas y riesgos. Otro 35.7% se muestra satisfecho con dichos criterios, y un 21.4% mantiene una posición neutral al respecto. Además, un 14.3% indicó algún grado de insatisfacción, mientras que ningún encuestado reportó estar muy insatisfecho con estos aspectos (Figura 12).

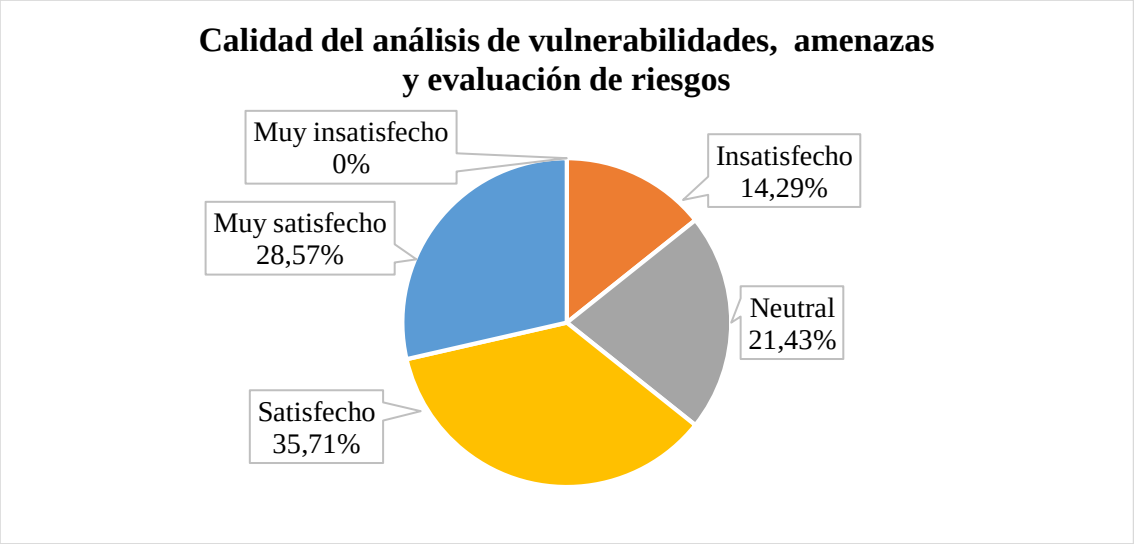


Figura 12: Resultados de la pregunta 4 de la encuesta

En la pregunta 5, "**¿Cómo evaluaría la adecuación de los controles y recomendaciones planteados en la propuesta de mejoras, en términos de su capacidad para tratar los riesgos de seguridad de la información de los activos identificados?**", se observa que el 35.7% de los encuestados están muy satisfechos con la adecuación de los controles y recomendaciones, otro 28.6% muestra satisfacción con el criterio establecido, y un 28.6% se muestra neutral al respecto. En contraste, un 7.1% expresó insatisfacción, y ninguno se mostró muy insatisfecho con esta pregunta (Figura 13).

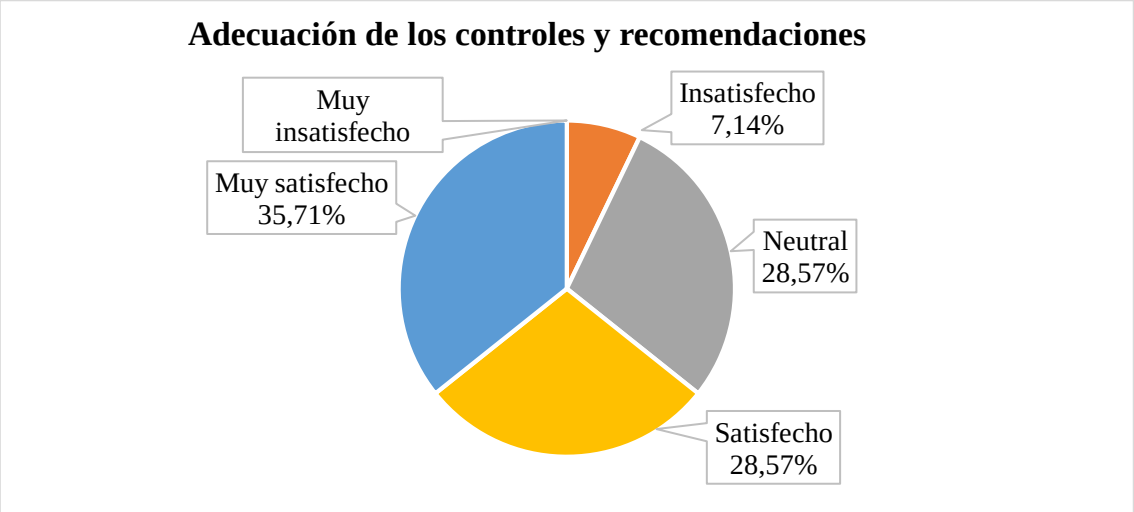


Figura 13: Resultados de la pregunta 5 de la encuesta

En la pregunta 6, "**¿En qué medida considera adecuada la aceptación de los riesgos de seguridad de la información que no pueden ser mitigados y no tienen controles adicionales?**", se evidencia que el 42.9% de los encuestados están muy satisfechos con la aceptación de riesgos, otro 42.9% se muestra satisfecho, y un 7.1% se encuentra en una posición neutral al respecto. Por otro lado, un 7.1% mostró insatisfacción, y ninguno señaló estar muy insatisfecho con este criterio (Figura 14).

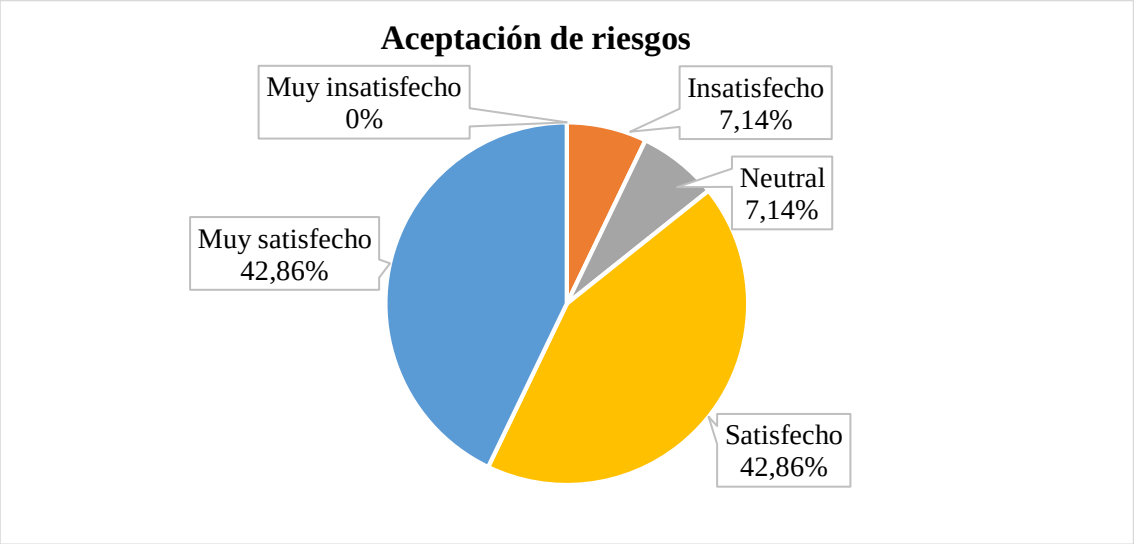


Figura 14: Resultados de la pregunta 6 de la encuesta

En la pregunta 7, "**¿En qué medida encuentra viable implementar la propuesta de mejoras basada en la gestión de riesgos de seguridad de la información identificados en la empresa pública?**", se observa que el 50% de los encuestados están muy satisfechos con la viabilidad de implementación, mientras que otro 42.9% se muestra satisfecho. No hubo encuestados que mantuvieran una postura neutral. Por otra parte, un 7.1% afirmó estar insatisfecho, y ninguno comunicó estar muy insatisfecho con este aspecto (Figura 15).

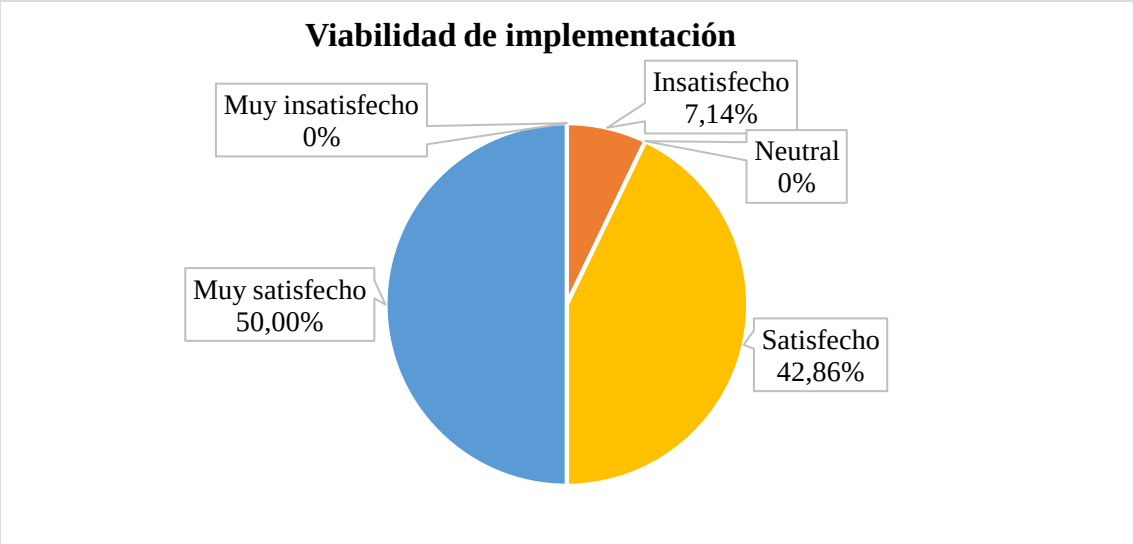


Figura 15: Resultados de la pregunta 7 de la encuesta

Por último, en la pregunta 8, "**¿Qué tan útil considera que será la propuesta de mejoras para fortalecer la postura general de seguridad de la información de la empresa pública?**", resulta evidente que el 64.3% de los encuestados están muy satisfechos con la utilidad de la propuesta de mejoras, mientras que otro 28.6% se declara satisfecho con el criterio establecido. No hubo encuestados que se mantuvieran neutrales. Asimismo, un 7.1% manifestó insatisfacción, y ninguno señaló estar muy insatisfecho con esta cuestión (Figura 16).

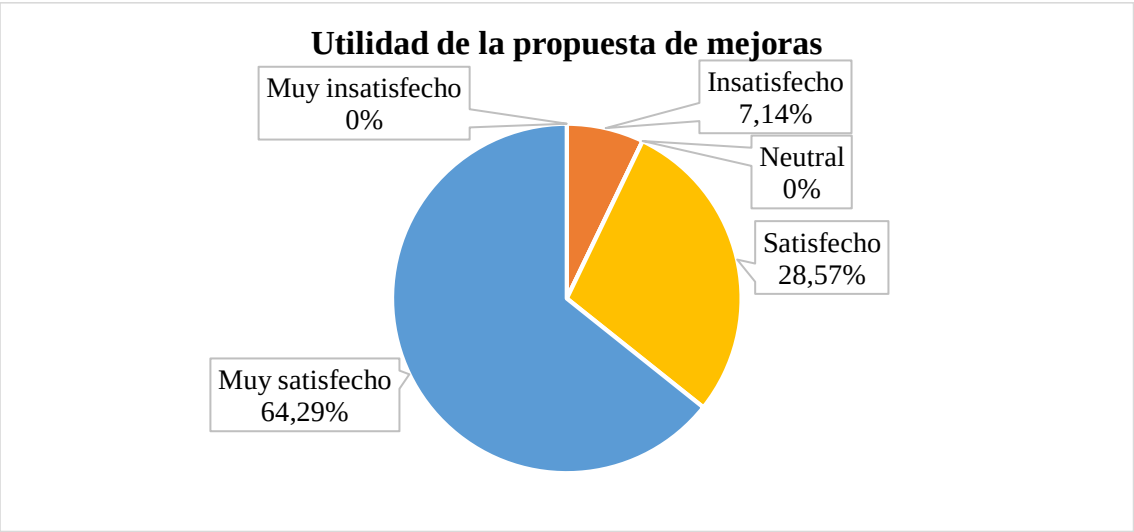


Figura 16: Resultados de la pregunta 8 de la encuesta

A continuación, en la Tabla 22, se presenta el análisis de satisfacción de las respuestas obtenidas en la encuesta. Este tipo de análisis permite cuantificar y cualificar el nivel de satisfacción de los encuestados respecto a diferentes aspectos de la propuesta, identificando áreas de fortaleza y aspectos que podrían necesitar mejoras.

Tabla 22: Análisis de conformidad de los resultados de la encuesta

Pregunta	% Muy insatisfecho	% Insatisfecho	% Neutral	% Satisfecho	% Muy satisfecho	**% Conformidad**	**% Insatisfacción**	**% Satisfacción General**
Pregunta 1	0.0	0.0	21.43	21.43	57.14	78.57	0.0	100.0
Pregunta 2	0.0	0.0	21.43	42.86	35.71	78.57	0.0	100.0
Pregunta 3	0.0	7.14	7.14	42.86	42.86	85.71	7.14	92.86
Pregunta 4	0.0	14.29	21.43	35.71	28.57	64.29	14.29	85.71
Pregunta 5	0.0	7.14	28.57	28.57	35.71	64.29	7.14	92.86
Pregunta 6	0.0	7.14	7.14	42.86	42.86	85.71	7.14	92.86
Pregunta 7	0.0	7.14	0.0	42.86	50.0	92.86	7.14	92.86
Pregunta 8	0.0	7.14	0.0	28.57	64.29	92.86	7.14	92.86

Los resultados de la encuesta indican un alto nivel de satisfacción y conformidad general entre los encuestados respecto a la propuesta de mejoras derivada del proceso de gestión de riesgos de seguridad de la información. La conformidad, definida como la suma de los porcentajes de "Satisfecho" y "Muy satisfecho", varía entre el 64.29% y el 92.86%. La insatisfacción, definida como la suma de "Insatisfecho" y " Muy insatisfecho", no supera el 14.29%. Estos datos permiten concluir que la mayoría de los participantes considera la propuesta efectiva y adecuada. La satisfacción general, que incluye respuestas neutrales, satisfechas y muy satisfechas, es alta en todas las preguntas, con un mínimo del 85.71%. Estos resultados reflejan una fuerte aceptación del proyecto y sugieren que los objetivos del mismo han sido cumplidos con éxito. La elevada conformidad indica que los criterios y controles establecidos son percibidos como viables y beneficiosos, confirmando la eficacia de la propuesta y su alineación con las expectativas y necesidades de los encuestados.

Para demostrar la validez de la hipótesis, se ha definido un umbral de aceptación. En estudios de satisfacción, generalmente se considera que un 70% de respuestas positivas (entre satisfecho o muy satisfecho) indica una fuerte aceptación. Superar este valor se interpreta como una señal robusta de viabilidad y apoyo. Basándonos en los resultados de la pregunta 7 de la encuesta, que se refiere a la viabilidad del plan de mejoras para la seguridad de la información en la empresa pública, donde el 92.86% de los encuestados muestran conformidad, lo que supera ampliamente el umbral del 70%, podemos concluir que la hipótesis es válida. La gran mayoría considera que la propuesta de mejoras es viable, lo que confirma que gestionar los riesgos usando normas nacionales permite proponer un plan de mejoras viable para la seguridad de la información de una empresa pública.

CONCLUSIONES

La elaboración del plan de gestión de riesgos de seguridad de la información basado en normas nacionales como la Norma Técnica Ecuatoriana ISO/IEC 27005 y la Guía para la gestión de riesgos de seguridad de la información de MINTEL ha permitido a la empresa pública no solo cumplir con estándares nacionales de seguridad, sino también establecer un marco estructurado para identificar, evaluar y tratar los riesgos de seguridad de la información. La propuesta de mejoras desarrollada ofrece una guía de los controles que pueden fortalecen la postura de seguridad de la organización.

- El desarrollo del estado del arte sobre la gestión de riesgos de seguridad de la información en empresas, con un enfoque en normas nacionales y mejores prácticas, ha proporcionado una comprensión profunda del panorama actual. Esto ha permitido identificar los enfoques más efectivos y adaptarlos a las necesidades específicas de la empresa, garantizando que el plan de gestión de riesgos esté alineado con las mejores prácticas y estándares nacionales e internacionales.

- La identificación de vulnerabilidades en la infraestructura tecnológica de la empresa ha sido un paso crucial en el proceso. Se han detectado debilidades en áreas clave como hardware, software, bases de datos, redes, servicios, etc., lo que ha permitido focalizar los esfuerzos en los puntos más críticos. Esta identificación detallada ha sentado las bases para el diseño de un plan de tratamiento de riesgos más efectivo y específico.

- El diseño del prototipo de la propuesta de mejoras, que incluye estrategias para la gestión de riesgos de seguridad de la información, ha resultado en un plan detallado y práctico. Las estrategias propuestas están alineadas con los controles de la ISO/IEC 27001, proporcionando una hoja de ruta para la implementación de mejoras específicas que mitigarán los riesgos identificados. Este prototipo ha sido fundamental para visualizar y planificar la implementación de los controles.

- La validación del plan de mejoras a través de la revisión por parte de expertos ha confirmado la efectividad y viabilidad del proyecto. Los resultados de la encuesta reflejaron alta satisfacción con las mejoras propuestas y los controles establecidos, con poca insatisfacción o neutralidad. Esto permite validar la hipótesis de que la gestión de riesgos basada en normas nacionales fue efectiva para identificar y evaluar riesgos, resultando en un plan de mejoras viable para la seguridad de la información en la empresa pública.

RECOMENDACIONES

Para futuros trabajos sobre gestión de riesgos de seguridad de la información en empresas nacionales, se sugiere utilizar la Norma Técnica Ecuatoriana ISO/IEC 27005 y la Guía para la gestión de riesgos de seguridad de la información de MINTEL como marcos de referencia. Estas normas brindan directrices estructuradas y reconocidas a nivel nacional, lo que asegura un enfoque sistemático y consistente en la identificación, evaluación y tratamiento de riesgos.

- Al desarrollar el estado del arte sobre la gestión de riesgos de seguridad de la información, es aconsejable realizar una revisión exhaustiva de las normas nacionales e internacionales, así como de las mejores prácticas en la industria. En particular, se recomienda el uso de las versiones más recientes de las normas para asegurarse de que las soluciones propuestas estén alineadas con los estándares y prácticas más actuales. Esto permite identificar los enfoques más efectivos y adaptarlos a las necesidades específicas del contexto del estudio.

- Para la identificación de vulnerabilidades en la infraestructura tecnológica, resulta útil utilizar herramientas y metodologías avanzadas de análisis de vulnerabilidades. Además, es crucial llevar a cabo una evaluación integral que considere todas las áreas clave como hardware, software, bases de datos, redes, personas, servicios e información. Esto proporciona una visión completa y detallada de las debilidades presentes, facilitando el diseño de planes de tratamiento de riesgos más efectivos y específicos.

- Al diseñar prototipos de propuestas de mejoras, es conveniente alinearse con los controles y requisitos establecidos por la ISO/IEC 27001. Esta norma proporciona un conjunto de buenas prácticas para la gestión de la seguridad de la información, asegurando que las estrategias propuestas sean robustas y efectivas. Además, la creación de planes de mejoras detallados y prácticos facilita la visualización de la implementación de medidas correctivas y preventivas.

- Se sugiere seguir el enfoque de validar el plan de mejoras a través de la revisión por parte de expertos. Este método de evaluación ha demostrado ser crucial para confirmar tanto la efectividad como la viabilidad de iniciativas similares. Además, es importante mantener informados y realizar reuniones periódicas con los interesados dentro de la empresa para asegurar el alineamiento del plan de mejoras con las necesidades organizacionales.

REFERENCIAS BIBLIOGRÁFICAS

[1] V. P. Castro-Rivera, R. A. Herrera-Acuña, y M. A. Villalobos-Abarca, «Desarrollo de un software web para la generación de planes de gestión de riesgos de software», *Inf. Tecnológica*, vol. 31, n.º 3, pp. 135-148, jun. 2020, doi: 10.4067/S0718-07642020000300135.

[2] C. A. Pazmiño Zabala, A. K. Serrano Castro, y M. M. González Rivera, «Las Tics como herramienta para la gestión de riesgos», *RECIMUNDO Rev. Científica Investig. El Conoc.*, vol. 4, n.º Extra 1 (ESP), pp. 182-190, 2020.

[3] M. A. Velepucha Sánchez, J. Morales Carrillo, y M. F. Pazmiño Campuzano, «Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO/IEC 27002: Caso de estudio Distribuidora Bravel», *Informática Sist. Rev. Tecnol. Informática Las Comun.*, vol. 6, n.º 1, pp. 63-78, jun. 2022, doi: 10.33936/isrtic.v6i1.4473.

[4] *NTE INEN-ISO/IEC 27005:2012*, 1, 2012. [En línea]. Disponible en: https://app.virtualex.ec/documentos/nte_inen_iso_iec_27005.pdf

[5] «Guía para la gestión de riesgos de seguridad de la información». Ministerio de Telecomunicaciones y de la sociedad de la información, 2020. [En línea]. Disponible en: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

[6] Diligent Corporation, «Tabla de resumen», jul. 2024. Accedido: 21 de diciembre de 2023. [En línea]. Disponible en: https://help.highbond.com/helpdocs/highbond/es/Content/results/visualizations/charts/summary_table.htm

[7] J. Del Carpio Gallegos, «Gestión de riesgos en proyectos de tecnología de información en el Perú», *Ind. Data*, vol. 11, n.º 2, p. 045, mar. 2014, doi: 10.15381/idata.v11i2.6049.

[8] J. C. Alfaro-Campos, «Metodología para la gestión de riesgos de TI basada en COBIT 5», *Univ. Costa Rica*, 2017, Accedido: 22 de mayo de 2024. [En línea]. Disponible en: https://repositoriotec.tec.ac.cr/handle/2238/11060

[9] R. R. Gómez-García, «Gestión y prevención de riesgos con tecnologías de información y comunicaciones», *Cienc. Holguín*, vol. 28, n.º 2, pp. 76-87, 2022.

[10] B. M. Martínez Herrera y I. E. Martínez Michel, «Diagnóstico de la gestión actual de manejo de riesgos con el uso de las tecnologías de información para asegurar una correcta presentación de la prima de riesgo de trabajo», *Interconectando Saberes*, vol. 8, n.º 15, Art. n.º 15, mar. 2023, doi: 10.25009/is.v0i15.2780.

[11] I. Velitchkov, «Integration of IT strategy and enterprise architecture models», en *Proceedings of the 9th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, en CompSysTech '08. New York, NY, USA: Association for Computing Machinery, jun. 2008, p. V.7-1. doi: 10.1145/1500879.1500955.

[12] Y. A. Viteri Alcívar, M. T. Cano Montesdeoca, A. D. Zambrano Rendón, y C. G. Minaya Vera, «EVALUACIÓN DE LAS INCIDENCIAS Y RIESGOS PRESENTES EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ-ECUADOR», *Univ. Cienc. Tecnol.*, vol. 23, n.º 94, Art. n.º 94, ago. 2019.

[13] B. Oviedo, E. Zhuma, y A. Gracia, «ANÁLISIS DE HERRAMIENTAS DE CÓDIGOS ABIERTOS QUE PERMITAN LA SEGURIDAD DE LA DATA EN LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO», *Univ. Cienc. Tecnol.*, vol. 23, n.º 94, Art. n.º 4, 2018, Accedido: 21 de diciembre de 2023. [En línea]. Disponible en: https://uctunexpo.autanabooks.com/index.php/uct/article/view/21

[14] Z. Ping, W. Zhipeng, L. Wenjing, y N. Jiang, «Modelo de calidad del servicio en la nube IEEE», 2018.

[15] «Plan de Tratamiento de Riesgos de Seguridad Digital». 2020. [En línea]. Disponible en: https://www.ani.gov.co/sites/default/files/plan_de_tratamiento_de_riesos_de_seguridad_de_la_informacion_v5_15-4-2020.pdf

[16] Ministerio de Ambiente y Desarrollo Sostenible, «Plan de Tratamiento de Riesgos - 2023», Ministerio de Ambiente y Desarrollo Sostenible, DS-E-GET-27, ene. 2023. [En línea]. Disponible en: https://www.minambiente.gov.co/wp-content/uploads/2023/01/Plan-de-tratamiento-de-riesgos-2023-DS-E-GET-27.pdf

[17] D. L. Carvajal, A. Cardona, y F. J. Valencia, «Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana», *Entre Cienc. E Ing.*, vol. 13, n.º 25, pp. 68-76, jun. 2019, doi: 10.31908/19098367.4016.

[18] M. J. Aguilar Quintanilla y A. del P. Letona, «Diseño de procedimientos de un sistema de gestión de la seguridad de información para la pequeña empresa, aplicado al caso de la Asociación Protectora de Créditos de El Salvador (PROCREDITO)», *CONIA, Congreso de Ingeniería y Arquitectura 2018. "Ciencia y tecnología para una mejor calidad de vida"*, 2019, Accedido: 9 de mayo de 2024. [En línea]. Disponible en: http://repositorio.uca.edu.sv/jspui/handle/11674/6086

[19] D. E. Duran-Romero, J. I. Lechuga-Cardozo, E. Y. Guisao-Giraldo, y O. Leyva-Cordero, «Gestión de la seguridad de las empresas prestadoras de servicio logístico en Colombia», *Pensam. Amp Gest.*, n.º 48, pp. 12-37, jun. 2020.

[20] *NTE INEN-ISO/IEC 27001:2011*, 1, 2011.

[21] A. A. Enríquez Collaguazo, «Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 aplicada a la clínica médica fértil», bachelorThesis, Universidad Técnica del Norte, Ibarra, 2018. Accedido: 4 de enero de 2024. [En línea]. Disponible en: http://repositorio.utn.edu.ec/handle/123456789/8572

[22] M. Á. Álvarez Roldán y H. F. Montoya Vargas, «Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos», *Ing. Desarro.*, vol. 38, n.º 2, pp. 279-297, dic. 2020, doi: 10.14482/inde.38.2.006.31.

[23] O. M. Cohaila Bravo, «Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad en la compañía de seguros SECREX», *Esc. Posgrado Newman - EPN*, dic. 2023, Accedido: 9 de mayo de 2024. [En línea]. Disponible en: https://repositorio.epnewman.edu.pe/handle/20.500.12892/870

[24] E. J. Guaña Moya, «La importancia de la seguridad informática en la educación digital: retos y soluciones», *RECIMUNDO Rev. Científica Investig. El Conoc.*, vol. 7, n.º 1, pp. 609-616, 2023.

[25] J.-M. Aguilar-Antonio, «Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad», *URVIO Rev. Latinoam. Estud. Segur.*, n.º 25, Art. n.º 25, nov. 2019, doi: 10.17141/urvio.25.2019.4007.

[26] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez, y D. Lévano Rodríguez, «Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú», *Enfoque UTE*, vol. 12, n.º 2, pp. 69-79, jun. 2021, doi: 10.29019/enfoqueute.743.

[27] N. Hernández Díaz, M. Yelandy Leyva, y B. Cuza García, «Modelos causales para la Gestión de Riesgos», *Rev. Cuba. Cienc. Informáticas*, vol. 7, n.º 4, pp. 58-74, dic. 2013.

[28] R. M. Llanos y E. M. Díaza, «Las variaciones de la satisfacción vital según edad y clima organizacional en trabajadores de la salud», *Gerenc. Políticas Salud*, vol. 18, n.º 36, Art. n.º 36, abr. 2019, doi: 10.11144/Javeriana.rgsp18-36.vsve.

[29] E. P. Alvarado, «Gestión de riesgos para la seguridad sostenible en edificaciones públicas: revisión sistemática», *Cent. Rev. Científica Univ.*, vol. 11, n.º 1, pp. 50-73, 2022.

[30] I. Cienfuegos, «Desarrollo de un modelo comprensivo de madurez de prácticas de gestión de riesgos para municipios neerlandeses», *Gest. Política Pública*, vol. 28, n.º 1, Art. n.º 1, ene. 2019, doi: 10.29265/gypp.v28i1.544.

[31] B. D. Valencia Jara y C. I. Narváez Zurita, «La gestión de riesgos financieros y su incidencia en la toma de decisiones», *CIENCIAMATRIA*, vol. 7, n.º 2, Art. n.º 2, sep. 2021, doi: 10.35381/cm.v7i2.526.

[32] P. P. Miranda, V. C. Atia, R. S. Herrera, y A. E. Pérez, «Dirección estratégica para la innovación en pequeñas y medianas empresas de la ciudad de Barranquilla –Colombia», *Rev. Venez. Gerenc.*, vol. 25, n.º 89, Art. n.º 89, mar. 2020, doi: 10.37960/revista.v25i89.31380.

[33] E. A. Ramírez Camargo y M. A. Rincón, «La importancia de la seguridad de la información en el sector público en Colombia», *RISTI Rev. Ibérica Sist. E Tecnol. Informação*, n.º 46, pp. 87-99, 2022.

[34] M. E. Rios Yanza, «Gestión del riesgo del área informática del Centro de Educación Continua de la Universidad Técnica de Machala». 2019. Accedido: 27 de diciembre de 2023. [En línea]. Disponible en: http://repositorio.utmachala.edu.ec/handle/48000/14971

[35] J. Llerena Izquierdo, O. Barcia Ayala, y R. Ayala Carabajo, «Faculty Training through Crowdlearning for Emerging Online Education», en *2020 IEEE ANDESCON*, oct. 2020, pp. 1-7. doi: 10.1109/ANDESCON50619.2020.9272103.

[36] J. N. Miranda Jiménez, «Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos», bachelorThesis, Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, 2021. Accedido: 4 de enero de 2024. [En línea]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/20966

[37] J. L. M. Loor, J. A. B. Mera, H. F. M. Cedeño, y K. M. M. Vega, «ANÁLISIS DE LA GESTIÓN DE RIESGOS EN LAS UNIDADES DE TECNOLOGÍA DE LA INFORMACIÓN DE LAS INSTITUCIONES PÚBLICAS DE MANABÍ-ECUADOR», *Univ. Cienc. Tecnol.*, vol. 1, n.º 1, pp. 6-6, 2019.

[38] W. A. Apaza Chávez, «Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera», *Innov. Softw.*, vol. 2, n.º 2, pp. 27-43, sep. 2021, doi: 10.48168/innosoft.s6.a39.

[39] E. Guerra, H. Neira, J. L. Díaz, y J. Patiño, «Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias», *Inf. Tecnológica*, vol. 32, n.º 5, pp. 145-156, oct. 2021, doi: 10.4067/S0718-07642021000500145.

[40] P. A. Sánchez-Sánchez, J. R. García-González, A. Triana, y L. Perez-Coronell, «Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia», *Inf. Tecnológica*, vol. 32, n.º 5, pp. 121-128, oct. 2021, doi: 10.4067/S0718-07642021000500121.

[41] R. M. Cedeño Zambrano y L. M. Morell González, «La gestión de riesgos en Ecuador: una aproximación evolutiva desde el control interno», *Cofin Habana*, vol. 12, n.º 2, pp. 306-318, dic. 2018.

[42] Constitución de la República del Ecuador, *Asamblea Nacional Constituyente*. 2008.

[43] O. Ñañez Campos, «Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú.», oct. 2019, Accedido: 4 de enero de 2024. [En línea]. Disponible en: http://repositorio.unprg.edu.pe/handle/20.500.12893/6110

[44] *Tecnología de la información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información*, Quito, Ecuador., 2023. [En línea]. Disponible en: https://www.normalizacion.gob.ec/

[45] M. A. Castillo Palma, J. K. Molina Jiménez, y L. Freire C., «Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005», masterThesis, ESPOL. FIEC, 2020. Accedido: 28 de febrero de 2024. [En línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/50317

[46] H. A. Tapiero Tapiero y H. Suarez Ramirez, «Modelo de gestión de riesgos de la seguridad de la información en empresas del sector asegurador utilizando la norma ISO/IEC 27005», dic. 2016, Accedido: 28 de febrero de 2024. [En línea]. Disponible en: http://repository.udistrital.edu.co/handle/11349/8322

[47] S. M. Escobar Rivera y S. C. León Aguirre, «Diseño de un sistema de gestión de riesgos en la seguridad de la información, orientado al gobierno de TI en base a la norma NTE INEN-ISO/IEC 27005:2012, para la Dirección Nacional de Desarrollo Tecnológico en Telecomunicaciones (DTT), de la Superintendencia de Telecomunicaciones», bachelorThesis, Quito, 2016., 2016. Accedido: 28 de febrero de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/15189

ANEXOS

Anexo 1: Matriz de consistencia

Tabla 23: Matriz de consistencia

Problema, objeto y campo	Objetivo	Marco Teórico	Hipótesis	Variables	Metodología
Problema: Necesidad de proponer mejoras significativas en la gestión de riesgos de seguridad de la información en una empresa pública, mediante el cumplimiento de normativas nacionales. **Problemas específicos:** - ¿Cómo se pueden identificar y definir de manera exhaustiva los activos críticos para la seguridad de la información que deben ser evaluados en el proceso de gestión de riesgos? - ¿Cuáles son las herramientas y metodologías más adecuadas para realizar un escaneo completo de vulnerabilidades en los activos identificados? - ¿Cómo se puede realizar una valoración precisa del nivel de riesgo asociado a las vulnerabilidades identificadas en los activos, considerando tanto impactos como probabilidades?	**Objetivo General:** - Elaborar un plan de gestión de riesgos en una empresa pública, basado en normas nacionales, para la propuesta de mejoras de seguridad de la información. **Objetivos Específicos:** - Desarrollar el estado del arte sobre la gestión de riesgos de seguridad de la información en empresas, enfocado en normas nacionales y mejores prácticas. - Identificar las vulnerabilidades existentes en la infraestructura tecnológica de la empresa. - Diseñar un prototipo de la propuesta de mejoras que incluya estrategias para la gestión de riesgos de seguridad de la información. - Validar el plan de mejoras a través de la revisión por parte de expertos.	**Antecedentes históricos a nivel internacional y nacional del objeto, campo:** La gestión de riesgos de seguridad de la información en una empresa pública es un proceso crucial para salvaguardar la eficiencia y eficacia de los proyectos y procesos relacionados con la tecnología. La implementación de una política de gestión de riesgos de TI adaptada a las normativas y estándares gubernamentales vigentes, como la Norma Técnica Ecuatoriana INEN-ISO/IEC 27001:2014 es esencial. Este enfoque busca mitigar posibles eventos adversos que podrían afectar la calidad, seguridad y continuidad de los servicios públicos, contribuyendo así a mejorar el desempeño y la seguridad de los sistemas de información, al tiempo que reduce pérdidas, costos y demoras asociados a los riesgos **Fundamentos Teóricos de objeto, campo y variables:** - Gestión de la seguridad de la información - Modelos de gestión de riesgos	**Hipótesis General:** - Si se gestionan los riesgos usando normas nacionales, se podrá proponer un plan de mejoras viable para la seguridad de la información de una empresa pública. **Hipótesis específicas o preguntas científicas:** - RQ1. ¿Cuáles son los principales riesgos de seguridad de la información que enfrentan las empresas del sector público en Ecuador? - RQ1.1. ¿Cómo se pueden aplicar las normas ecuatorianas de seguridad de la información para mejorar la gestión de riesgos en las empresas públicas? - RQ1.2. ¿Cuáles son las mejores prácticas para la gestión de riesgos de seguridad de la información en las empresas públicas? - RQ1.3. ¿Cuáles son las técnicas más efectivas para el análisis de riesgos de seguridad de la	**Variable 1 / Independiente:** - Gestión de riesgos usando normas nacionales Dimensiones o categorías: - Implementación de normas nacionales basadas en normas ISO. - Grado de adopción de normas. - Plan de Gestión - Documentación de procesos normativos **Variable 2 / Dependiente:** - Propuesta de mejoras	**Enfoque:** cuantitativo **Alcance:** descriptivo y explicativo **Diseño:** no experimental transversal **Unidades de análisis:** **Población:** Infraestructura tecnológica de la empresa pública. **Muestra:** No aplica, se analizarán todos los activos de la empresa entre estos se incluye: Sistemas informáticos, página web, equipos clave y segmentos de la red

- ¿Cuáles son los enfoques estratégicos para diseñar planes de mitigación efectivos que aborden las vulnerabilidades y reduzcan el riesgo a niveles aceptables en los activos críticos para la seguridad de la información? **Objeto de estudio:** Gestión de riesgos de seguridad de la información en una empresa pública. **Campo de Acción:** Aplicación de normativas nacionales para mejorar la seguridad de la información en la empresa.		- Enfoque estructurado de la gestión de riesgos en las organizaciones - Procedimiento diseñado para la gestión de riesgos integrado al sistema de gestión de la calidad - Amenazas y Vulnerabilidades - ISO/IEC 27005:2012 - Guía para la gestión de riesgos de seguridad de la información - Seguridad de la Información - Principios de seguridad de la información	información en las empresas públicas? - RQ1.4. ¿Cómo se pueden mejorar los procesos de gestión de riesgos de seguridad de la información en las empresas públicas utilizando tecnologías de la información? - RQ2 ¿Cuáles son los principales desafíos que enfrentan las empresas públicas en Ecuador en la gestión de riesgos de seguridad de la información?	Dimensiones o categorías: - Grado de efectividad de las propuestas. - Alineación con estándares y normativas. - Integración con procesos existentes de la empresa.	LAN, representantes dentro del personal **Técnicas e instrumentos de recolección de datos:** - Análisis de Documentos - Entrevistas - Encuestas - Análisis de Vulnerabilidades **Técnicas de procesamiento de datos:** - Análisis Descriptivo - Análisis Inferencial - Análisis de Regresión - Identificación de áreas críticas

Anexo 2: Instrumento de recopilación de información de la Empresa Pública (GAD)

Entrevista al comité de evaluación

Sección 1: Identificación de Activos de Información

- ¿Cuáles son los activos de información más importantes en su departamento?
- ¿Qué tipo de información maneja cada uno de estos activos?
- ¿Cómo clasifica los activos en términos de confidencialidad, integridad y disponibilidad, calificando entre alto, medio y bajo?

Sección 2: Identificación de Vulnerabilidades

- ¿Qué vulnerabilidades han sido identificadas en relación con los activos de información?

Sección 3: Identificación de Amenazas

- ¿Cuáles son las principales amenazas que podrían afectar los activos de información?
- ¿Qué probabilidad de ocurrencia entre improbable, medianamente probable y muy probable existe de que las amenazas afecten los activos?
- ¿Qué impacto tendría en la empresa la pérdida, alteración o acceso no autorizado a estos activos?
- ¿Ha habido incidentes de seguridad en el pasado relacionados con estas amenazas?

Sección 4: Controles y Medidas de Seguridad

- ¿Qué controles y medidas de seguridad están implementados actualmente para proteger los activos de información?
- ¿Cuál es el nivel de efectividad de los controles actuales calificando entre muy alta, alta y muy baja?

Anexo 3: Acta de recepción de riesgos entregada a la empresa pública

Santa Rosa, 08 de julio de 2024

Acta de Recepción de Riesgos

Mediante esta acta se lleva a cabo la recepción oficial de los resultados del proceso de evaluación de riesgos de seguridad de la información de la empresa pública (GAD). El jefe del departamento de Tecnologías de la Información, en calidad de representante del comité de evaluación y de la organización, será la persona responsable de receptar este documento.

Participantes:

- Jefe unidad de TIC, miembro del comité de evaluación
- Responsable de TIC, miembro del comité de evaluación
- Directora talento humano, miembro del comité de evaluación
- Soriano Herrera Roger Hitler, miembro del comité de desarrollo
- Velásquez Porras Diana Maribel, miembro del comité de desarrollo

Descripción del Proceso de Gestión de Riesgos:

El proceso de gestión de riesgos de seguridad de la información se ha realizado conforme a las directrices establecidas en la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2011 y en la Guía para la gestión de riesgos de seguridad de la información de MINTEL, estableciendo las siguientes fases:

- **Establecimiento del Contexto:** Durante esta fase, se recopilaron datos a través de entrevistas, revisiones y evaluación del entorno tecnológico del departamento de informática. El alcance del proyecto incluye el análisis del equipo de informática, la documentación, la estructura tecnológica y la información generada, alineado con las necesidades de la entidad. Se estableció un comité especializado que gestione la evaluación y el desarrollo de medidas de tratamiento de riesgos, también se consideran restricciones legales para proteger la información y garantizar la confidencialidad.
- **Valoración del Riesgo de seguridad de la información:**
    - **Identificación de los activos:** Se identifican y valoran los activos críticos de la organización, distinguiéndose en tipos como Hardware, Software, Información Electrónica, Información Física, Base de Datos, Medio de Almacenamiento, Sitio, Servicio, Red y Persona. Cada activo es evaluado en términos de confiabilidad, integridad y disponibilidad según la Guía para la gestión de riesgos de seguridad de la información (MINTEL). La valoración del impacto se calcula con el promedio de estas tres dimensiones.
    - **Identificación de las amenazas y vulnerabilidades:** Durante esta fase, se evalúan posibles amenazas y vulnerabilidades que pueden afectar la integridad, confidencialidad y accesibilidad de los activos de información. Las amenazas se clasifican como deliberadas, accidentales o ambientales, y se identifican vulnerabilidades como falta de controles de acceso, políticas inadecuadas o fallas en la gestión de actualizaciones y monitoreo.

Figura 17: Acta de recepción de riesgos firmada 1 - 8

- **Evaluación del Riesgo:** Se emplean métodos cuantitativos y cualitativos para evaluar el riesgo de los activos identificados. Para determinar el riesgo inherente se evalúa la valoración del impacto y la probabilidad de ocurrencia. Para determinar el riesgo actual se establece el nivel de efectividad de los controles. Se emplean mapas de calor para determinar el riesgo inherente y el riesgo actual. Finalmente, se determina el riesgo residual para determinar el método de tratamiento y un posible plan de tratamiento.

- **Tratamiento del Riesgo:** Se propusieron mejoras con controles para cada activo con riesgo residual medio o alto, basándose en los controles propuestos por la ISO 27001. Cada control propuesto incluye recomendaciones específicas para su implementación.
- **Aceptación del Riesgo:** El comité decidió aceptar los riesgos de nivel residual bajo sin aplicar controles adicionales, basándose en la evaluación del impacto y la probabilidad de ocurrencia de los riesgos.
- **Comunicación del Riesgo:** Se estableció un acta de recepción como mecanismo formal para la comunicación de los riesgos identificados con las partes interesadas.

Listado de los Activos Evaluados y sus Niveles de Riesgo Residual:

A continuación, se presenta un resumen de los activos evaluados junto con sus niveles de riesgo residual. El listado completo se encuentra detallado en el documento "Gestión de Riesgos de Seguridad de la Información de la Empresa Pública.xlsx".

Activos Evaluados:

ID RIESGO	Activo	Nivel Riesgo Residual
RSI-001	Servidores	MEDIO
RSI-002	Computadores de escritorio	ALTO
RSI-003	Portátiles	ALTO
RSI-004	Dispositivos móviles	BAJO
RSI-005	Impresoras	MEDIO
RSI-006	Equipos multifuncional	MEDIO
RSI-007	Routers	MEDIO
RSI-008	Teléfonos	BAJO
RSI-009	Modems	MEDIO
RSI-010	Memoria USB	MEDIO
RSI-011	Discos Portables	MEDIO
RSI-012	Cámaras de Seguridad	ALTO
RSI-013	Televisores	BAJO
RSI-014	Sistemas Operativos	MEDIO
RSI-015	Antivirus	MEDIO
RSI-016	Servidores Aplicaciones/ Contenedores	BAJO
RSI-017	Página WEB	MEDIO
RSI-018	Navegadores	BAJO
RSI-019	Office	BAJO
RSI-020	Motor de Base de Datos	ALTO
RSI-021	Licencias	BAJO
RSI-022	Base de Datos	MEDIO

Figura 18: Acta de recepción de riesgos firmada 2 - 8

ID RIESGO	Activo	Nivel Riesgo Residual
RSI-023	Archivos de Datos	MEDIO
RSI-024	Manuales de Usuario	MEDIO
RSI-025	Documentación del sistema	MEDIO
RSI-026	Solicitudes	BAJO
RSI-027	Formatos	BAJO
RSI-028	Documentos internos	MEDIO
RSI-029	Material Físico (Impreso)	MEDIO
RSI-030	Información en carpetas compartidas en red	MEDIO
RSI-031	Información Disco	MEDIO
RSI-032	Información memorias USB	BAJO
RSI-033	Datos de identificación	MEDIO
RSI-034	Información Financiera	MEDIO
RSI-035	Información de Recursos Humanos	MEDIO
RSI-036	Información Urbanística	BAJO
RSI-037	Capacitaciones	BAJO
RSI-038	Telefonía	BAJO
RSI-039	Internet	MEDIO
RSI-040	Red Inalámbrica	MEDIO
RSI-041	Almacenamiento de información	MEDIO
RSI-042	Electricidad	MEDIO
RSI-043	Instalaciones de la Organización	ALTO
RSI-044	Centro de datos principal	ALTO
RSI-045	Archivo documental	MEDIO
RSI-046	Red eléctrica	MEDIO
RSI-047	Red de datos	MEDIO
RSI-048	Personal Interno	MEDIO
RSI-049	Directores de área	MEDIO
RSI-050	Personal Administrativo	MEDIO
RSI-051	Administrador de Página Web	MEDIO
RSI-052	Proveedores	BAJO

Lista de Riesgos Aceptados:

Los siguientes riesgos han sido aceptados sin aplicar controles adicionales debido a su nivel de riesgo residual bajo:

- RSI-004 Dispositivos móviles
- RSI-008 Teléfonos
- RSI-013 Televisores
- RSI-016 Servidores Aplicaciones/ Contenedores
- RSI-018 Navegadores
- RSI-019 Office
- RSI-021 Licencias
- RSI-026 Solicitudes
- RSI-027 Formatos
- RSI-032 Información memorias USB
- RSI-036 Información Urbanística
- RSI-037 Capacitaciones

Figura 19: Acta de recepción de riesgos firmada 3 - 8

- RSI-038 Telefonía
- RSI-052 Proveedores

Propuestas de Tratamiento de Riesgos

Todos los riesgos no aceptados serán tratados mediante estrategias de reducción del riesgo. Se detallan las propuestas de mejoras con controles basados en la ISO 27001 y las recomendaciones correspondientes por cada control identificado. Las acciones específicas para mitigar estos riesgos se detallan en el informe del proyecto de integración curricular.

ID RIESGO	Activo	Riesgo	Controles
RSI-001	Servidores	Fallas en el dispositivo debido a manipulación no autorizada.	A.9.2.1 Emplazamiento y protección de equipos A.9.1.1 Perímetro de seguridad física A.10.4.1 Controles contra el código malicioso A.12.6.1 Gestión de vulnerabilidades técnicas
RSI-002	Computadores de escritorio	Acceso no autorizado a la información.	A.11.5.2 Identificación y autenticación de usuario A.11.3.1 Uso de contraseñas A.10.5.1 Copias de seguridad de la información A.9.2.3 Seguridad del cableado
RSI-003	Portátiles	Pérdida o robo de dispositivos.	A.11.7.1 Equipos portátiles y comunicaciones móviles A.9.2.5 Seguridad de los equipos fuera de las instalaciones A.10.4.1 Controles contra el código malicioso A.9.2.6 Reutilización o retirada segura de equipos
RSI-005	Impresoras	Acceso no autorizado.	A.9.2.1 Emplazamiento y protección de equipos A.10.4.1 Controles contra el código malicioso A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.6.1 Gestión de vulnerabilidades técnicas
RSI-006	Equipos multifuncionales	Acceso no autorizado a documentos y datos almacenados.	A.9.2.1 Emplazamiento y protección de equipos A.10.4.1 Controles contra el código malicioso A.11.7.1 Equipos portátiles y comunicaciones móviles A.12.6.1 Control de las vulnerabilidades técnicas
RSI-007	Routers	Acceso no autorizado a la red y compromisos de seguridad.	A.11.4.1 Política de uso de los servicios en red A.10.6.1 Controles de red A.10.4.1 Controles contra el código malicioso A.10.10.1 Registro de auditorias
RSI-009	Modems	Acceso no autorizado a la red y compromisos de seguridad.	A.11.4.1 Política de uso de los servicios en red A.10.6.1 Controles de red A.10.4.1 Controles contra el código malicioso A.10.10.1 Registro de auditorias
RSI-010	Memoria USB	Pérdida de datos y compromisos de seguridad por dispositivos portátiles.	A.10.7.1 Gestión de soportes extraíbles A.10.4.1 Controles contra el código malicioso A.9.2.6 Reutilización o retirada segura de equipos A.10.8.1 Políticas y procedimientos de intercambio de información
RSI-011	Discos Portables	Pérdida de datos y compromisos de seguridad por dispositivos portátiles.	A.10.7.1 Gestión de soportes extraíbles A.10.4.1 Controles contra el código malicioso A.9.2.6 Reutilización o retirada segura de equipos A.10.8.1 Políticas y procedimientos de intercambio de información

Figura 20: Acta de recepción de riesgos firmada 4 - 8

ID RIESGO	Activo	Riesgo	Controles
RSI-012	Cámaras de Seguridad	Compromiso de la seguridad física y privacidad por acceso no autorizado a las cámaras.	A.9.1.1 Perímetro de seguridad física A.10.10.1 Registro de auditorias A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.12.3.1 Polítca de uso de los controles criptográficos
RSI-014	Sistemas Operativos	Vulnerabilidades de seguridad y ataques debido a sistemas operativos desactualizados o mal configurados.	A.12.6.1 Control de las vulnerabilidades técnicas A.10.1.1 Documentación de los procedimientos de operación A.11.5.2 Identificación y autenticación de usuario A.10.10.4 Registros de administración y operación
RSI-015	Antivirus	Infecciones de malware y pérdida de datos debido a la falta de protección antivirus adecuada.	A.10.4.1 Controles contra el código malicioso A.11.2.3 Gestión de contraseñas de usuario A.10.10.1 Registro de auditorias A.8.2.2 Concienciación, formación y capacitación en seguridad de la información
RSI-017	Página WEB	Exposición a ataques cibernéticos, como inyecciones.	A.10.4.1 Controles contra el código malicioso A.12.1.1 Análisis y especificación de los requisitos de seguridad A.11.5.2 Identificación y autenticación de usuario A.10.10.1 Registro de auditorias
RSI-020	Motor de Base de Datos	Falla o vulnerabilidad en el motor de base de datos que comprometa la integridad y disponibilidad de los datos.	A.12.6.1 Gestión de vulnerabilidades técnicas A.10.5.1 Copias de seguridad de la información A.9.2.4 Mantenimiento de los equipos A.12.5.1 Procedimientos de control de cambios
RSI-022	Base de Datos	Pérdida, corrupción o acceso no autorizado a la base de datos.	A.10.5.1 Copias de seguridad de la información A.11.6.1 Restricción del acceso a la información A.12.3.1 Política de uso de los controles criptográficos A.12.4.3 Control de acceso al código fuente de los programas
RSI-023	Archivos de Datos	Pérdida, corrupción o acceso no autorizado a archivos de datos.	A.10.5.1 Copias de seguridad de la información A.9.2.6 Reutilización o retirada segura de equipos A.11.6.1 Restricción del acceso a la información A.12.3.1 Política de uso de los controles criptográficos
RSI-024	Manuales de Usuario	Acceso no autorizado y manipulación de los manuales de usuario.	A.7.2.2 Etiquetado y manejo de la información A.9.2.3 Seguridad del cableado A.10.5.1 Copias de seguridad de la información A.11.2.1 Registro de usuario
RSI-025	Documentación del sistema	Divulgación de información.	A.7.2.2 Etiquetado y manejo de la información A.10.8.1 Políticas y procedimientos de intercambio de información A.11.3.1 Uso de contraseñas A.8.2.2 Concienciación, formación y capacitación en seguridad de la información

Figura 21: Acta de recepción de riesgos firmada 5 - 8

ID RIESGO	Activo	Riesgo	Controles
RSI-028	Documentos internos	Fuga, robo o pérdida de información.	A.7.2.2 Etiquetado y manejo de la información A.8.2.2 Concienciación, formación y capacitación en seguridad de la información A.10.1.1 Documentación de los procedimientos de operación A.13.2.3 Recopilación de evidencias
RSI-029	Material Físico (Impreso)	Pérdida, robo o acceso no autorizado a documentos impresos confidenciales.	A.9.2.3 Seguridad del cableado A.7.2.2 Etiquetado y manejo de la información A.10.7.3 Procedimientos de manipulación de la información A.6.1.5 Acuerdos de confidencialidad
RSI-030	Información en Carpetas Compartidas en Red	Acceso no autorizado, modificación o eliminación de información en carpetas compartidas en red.	A.11.2.1 Registro de usuario A.10.7.2 Retirada de soportes A.10.8.4 Mensajería electrónica A.10.1.1 Documentación de los procedimientos de operación
RSI-031	Información Disco	Pérdida de datos, acceso no autorizado o corrupción de datos almacenados en discos duros.	A.9.2.6 Reutilización o retirada segura de equipos A.12.3.1 Política de uso de los controles criptográficos A.12.4.3 Control de acceso al código fuente de los programas A.10.5.1 Copias de seguridad de la información
RSI-033	Datos de Identificación	Uso indebido, robo o acceso no autorizado a datos de identificación personal.	A.15.1.4 Protección de datos y privacidad de la información de carácter personal A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información A.11.2.3 Gestión de contraseñas de usuario A.10.10.1 Registro de auditorias
RSI-034	Información Financiera	Pérdida, manipulación o acceso no autorizado a información financiera.	A.10.5.1 Copias de seguridad de la información A.11.2.2 Gestión de privilegios A.12.3.1 Política de uso de los controles criptográficos A.10.8.1 Políticas y procedimientos de intercambio de información
RSI-035	Información de Recursos Humanos	Acceso no autorizado, pérdida o alteración de información de empleados.	A.8.1.3 Términos y condiciones de contratación A.9.1.3 Seguridad de oficinas, despachos e instalaciones A.11.2.3 Gestión de contraseñas de usuario A.7.2.1 Directrices de clasificación
RSI-039	Internet	Pérdida de datos, ataques de malware, y acceso no autorizado a través de internet.	A.10.4.1 Controles contra el código malicioso A.10.6.2 Seguridad de los servicios de red A.11.4.1 Política de uso de los servicios en red A.10.9.3 Información públicamente disponible
RSI-040	Red Inalámbrica	Intercepción de comunicaciones, acceso no autorizado y ataques de	A.10.6.1 Controles de red A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración A.9.2.3 Seguridad del cableado

Figura 22: Acta de recepción de riesgos firmada 6 - 8

ID RIESGO	Activo	Riesgo	Controles
		denegación de servicio en la red inalámbrica.	
RSI-041	Almacenamiento de Información	Pérdida, acceso no autorizado o corrupción de datos almacenados.	A.10.5.1 Copias de seguridad de la información A.11.2.3 Gestión de contraseñas de usuario A.9.2.6 Reutilización o retirada segura de equipos A.12.3.1 Política de uso de los controles criptográficos
RSI-042	Electricidad	Interrupciones de energía que pueden causar pérdida de datos, daño a equipos y parálisis operativa.	A.9.2.2 Instalaciones de suministro A.9.1.4 Protección contra las amenazas externas y de origen ambiental A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información A.10.5.1 Copias de seguridad de la información
RSI-043	Instalaciones de la Organización	Acceso no autorizado, robo, daño a instalaciones y equipos críticos.	A.9.1.1 Perímetro de seguridad física A.9.1.3 Seguridad de oficinas, despachos e instalaciones A.9.2.1 Emplazamiento y protección de equipos A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información
RSI-044	Centro de Datos Principal	Interrupciones en el funcionamiento del centro de datos, pérdida de datos, acceso no autorizado.	A.9.2.1 Emplazamiento y protección de equipos A.9.1.3 Seguridad de oficinas, despachos e instalaciones A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información A.10.5.1 Copias de seguridad de la información
RSI-045	Archivo Documental	Pérdida, robo o acceso no autorizado a documentos físicos y electrónicos.	A.9.2.6 Reutilización o retirada segura de equipos A.9.1.1 Perímetro de seguridad física A.7.2.2 Etiquetado y manejo de la información
RSI-046	Red Eléctrica	Interrupciones de energía que pueden afectar la operación de la organización.	A.9.2.2 Instalaciones de suministro A.9.1.4 Protección contra las amenazas externas y de origen ambiental A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información
RSI-047	Red de Datos	Interrupción o compromiso de la red de datos que afecta la conectividad y la seguridad de la información.	A.10.6.1 Controles de red A.10.8.1 Políticas y procedimientos de intercambio de información A.11.4.6 Control de la conexión a la red A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información
RSI-048	Personal Interno	El riesgo de acceso no autorizado o uso inapropiado de la información por parte del personal interno.	A.7.1 Responsabilidad sobre los activos A.11 Control de acceso A.15 Cumplimiento
RSI-049	Directores de área	El riesgo de falta de liderazgo en la implementación y cumplimiento de políticas de	A.6.1 Organización interna A.8 Seguridad ligada a los recursos humanos A.10 Gestión de comunicaciones y operaciones A.14 Gestión de la continuidad del negocio

Figura 23: Acta de recepción de riesgos firmada 7 - 8

ID RIESGO	Activo	Riesgo	Controles
		seguridad de la información por parte de los directores de área.	
RSI-050	Personal Administrativo	Acceso no autorizado a la información confidencial debido a la falta de controles adecuados sobre el personal administrativo.	A.7.1 Responsabilidad sobre los activos A.8 Seguridad ligada a los recursos humanos A.9 Seguridad física y ambiental A.11 Control de acceso
RSI-051	Administrador de Página Web	Posible acceso no autorizado o manipulación de la página web debido a vulnerabilidades en su administración.	A.12.6.1 Control de las vulnerabilidades técnicas A.10.1 Responsabilidades y procedimientos de operación A.11.4 Control de acceso a la red A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

Con esta acta, se formaliza la entrega y aceptación del documento de gestión de riesgos de seguridad de la información de la empresa pública, junto con la propuesta detallada de mejoras y controles para mitigar los riesgos identificados. Este documento establece una base sólida para mantener un entorno seguro y protegido, salvaguardando la integridad, confidencialidad y disponibilidad de la información crítica.

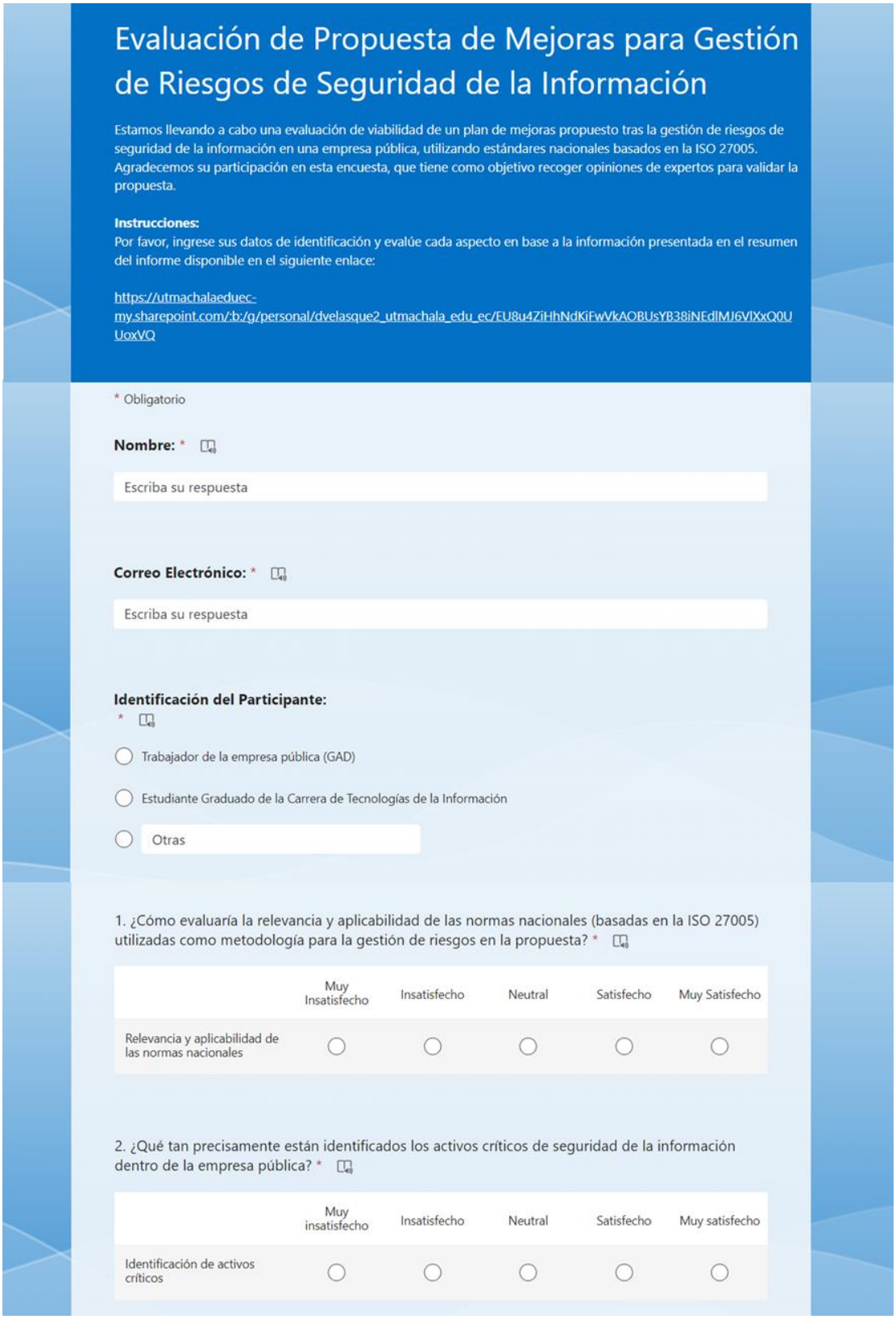
GAD. MUNICIPAL DEL CANTÓN * DPTO. DE INFORMÁTICA

(Entrega)
Soriano Herrera Roger Hitler
Representante del comité de desarrollo
Estudiante de Tecnologías de la Información
C.I.: 0706467115

(Recibe)
Ing. [redacted]
Representante del comité de evaluación
Jefe unidad de TIC de la empresa pública (GAD)
C.I.: [redacted]

Figura 24: Acta de recepción de riesgos firmada 8 - 8

Anexo 4: Formato de encuesta en línea enviada para la evaluación de la propuesta de mejoras, realizada en Microsoft Forms.



Evaluación de Propuesta de Mejoras para Gestión de Riesgos de Seguridad de la Información

Estamos llevando a cabo una evaluación de viabilidad de un plan de mejoras propuesto tras la gestión de riesgos de seguridad de la información en una empresa pública, utilizando estándares nacionales basados en la ISO 27005. Agradecemos su participación en esta encuesta, que tiene como objetivo recoger opiniones de expertos para validar la propuesta.

Instrucciones:
Por favor, ingrese sus datos de identificación y evalúe cada aspecto en base a la información presentada en el resumen del informe disponible en el siguiente enlace:

https://utmachalaeduec-my.sharepoint.com/:b:/g/personal/dvelasque2_utmachala_edu_ec/EU8u4ZiHhNdKiFwVkAOBUsYB38iNEdlMJ6VlXxQ0UUoxVQ

* Obligatorio

Nombre: *

Escriba su respuesta

Correo Electrónico: *

Escriba su respuesta

Identificación del Participante: *

- Trabajador de la empresa pública (GAD)
- Estudiante Graduado de la Carrera de Tecnologías de la Información
- Otras

1. ¿Cómo evaluaría la relevancia y aplicabilidad de las normas nacionales (basadas en la ISO 27005) utilizadas como metodología para la gestión de riesgos en la propuesta? *

	Muy Insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy Satisfecho
Relevancia y aplicabilidad de las normas nacionales	○	○	○	○	○

2. ¿Qué tan precisamente están identificados los activos críticos de seguridad de la información dentro de la empresa pública? *

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Identificación de activos críticos	○	○	○	○	○

Figura 25: Formato de instrumento de evaluación 1 - 2

3. ¿En qué medida considera que los criterios de evaluación de riesgos establecidos (nivel de confidencialidad, integridad, disponibilidad, probabilidad de ocurrencia, nivel de efectividad de controles y mapa de calor) son adecuados y suficientes para analizar los riesgos asociados a la seguridad de la información?
*

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Criterios de evaluación de riesgos	○	○	○	○	○

4. ¿Cómo evaluaría la calidad y precisión del análisis de vulnerabilidades y amenazas, así como del proceso de evaluación de riesgos de seguridad de la información?
*

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Calidad del análisis de vulnerabilidades, amenazas y evaluación de riesgos	○	○	○	○	○

5. ¿Cómo evaluaría la adecuación de los controles y recomendaciones planteados en la propuesta de mejoras, en términos de su capacidad para tratar los riesgos de seguridad de la información de los activos identificados?
*

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Adecuación de los controles y recomendaciones	○	○	○	○	○

6. ¿En qué medida considera adecuada la aceptación de los riesgos de seguridad de la información que no pueden ser mitigados y no tienen controles adicionales?
*

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Aceptación de riesgos	○	○	○	○	○

7. ¿En qué medida encuentra viable y factible implementar la propuesta de mejoras basada en la gestión de riesgos de seguridad de la información identificados en la empresa pública? *

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Viabilidad de implementación	○	○	○	○	○

8. ¿Qué tan útil considera que será la propuesta de mejoras para fortalecer la postura general de seguridad de la información de la empresa pública?
*

	Muy insatisfecho	Insatisfecho	Neutral	Satisfecho	Muy satisfecho
Utilidad de la propuesta de mejoras	○	○	○	○	○

Enviar

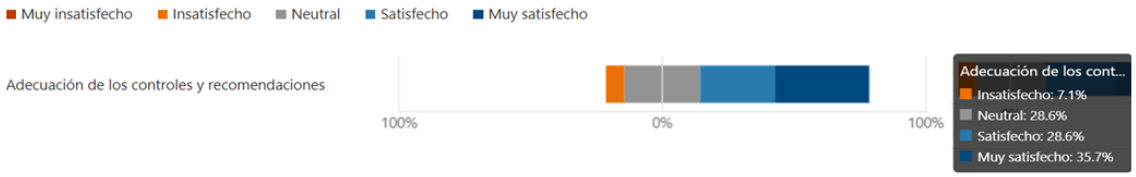
Figura 26: Formato de instrumento de evaluación 1 - 2

Anexo 5: Resultados de la encuesta en línea generados en Microsoft Forms.

Figura 27: Resultados de encuesta de evaluación del prototipo 1 - 2

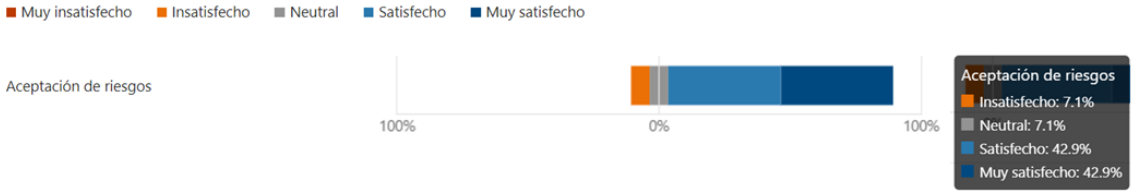
5. ¿Cómo evaluaría la adecuación de los controles y recomendaciones planteados en la propuesta de mejoras, en términos de su capacidad para tratar los riesgos de seguridad de la información de los activos identificados?

Más detalles



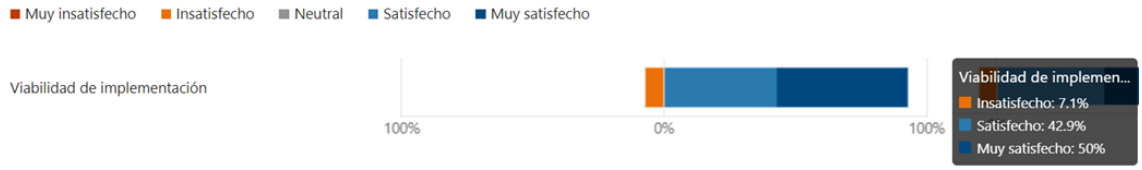
6. ¿En qué medida considera adecuada la aceptación de los riesgos de seguridad de la información que no pueden ser mitigados y no tienen controles adicionales?

Más detalles



7. ¿En qué medida encuentra viable y factible implementar la propuesta de mejoras basada en la gestión de riesgos de seguridad de la información identificados en la empresa pública?

Más detalles



8. ¿Qué tan útil considera que será la propuesta de mejoras para fortalecer la postura general de seguridad de la información de la empresa pública?

Más detalles

Figura 28: Resultados de encuesta de evaluación del prototipo 2 - 2