UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de riesgos de seguridad de la información de una empresa y propuesta de mejoras utilizando normas y estándares internacionales

LUZURIAGA REY EDWIN PAUL
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MARIN RAMON JUAN ANDRES
INGENIERO 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 de una empresa y propuesta de mejoras utilizando normas y estándares internacionales

LUZURIAGA REY EDWIN PAUL
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MARIN RAMON JUAN ANDRES
INGENIERO 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 de una empresa y propuesta de mejoras utilizando normas y estándares internacionales

LUZURIAGA REY EDWIN PAUL
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MARIN RAMON JUAN ANDRES
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

LOJA MORA NANCY MAGALY

MACHALA
2024

Gestión de riesgos de seguridad de la información de una empresa y propuesta de mejoras utilizando normas y estándares internacionales

por Nancy Magaly Loja Mora

Fecha de entrega: 23-jul-2024 08:53p.m. (UTC-0500)

Identificador de la entrega: 2421570420

Nombre del archivo: TRABAJO_DE_PROYECTO_DE_INTEGRACI_N_CURRICULAR_Final_4.docx (3.08M)

Total de palabras: 32611

Total de caracteres: 185603

Gestión de riesgos

INFORME DE ORIGINALIDAD

8%	7%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repository.unipiloto.edu.co Fuente de Internet	3%
2	repositorioacademico.upc.edu.pe Fuente de Internet	1%
3	repositorio.ug.edu.ec Fuente de Internet	<1%
4	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1%
5	repositorio.unne.edu.ar Fuente de Internet	<1%
6	hdl.handle.net Fuente de Internet	<1%
7	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	<1%
8	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%

9	repositorio.unab.cl Fuente de Internet	<1 %
10	repositorio.unprg.edu.pe Fuente de Internet	<1 %
11	repository.udistrital.edu.co Fuente de Internet	<1 %
12	es.scribd.com Fuente de Internet	<1 %
13	repositorio.pucesa.edu.ec Fuente de Internet	<1 %
14	repositorio.ufpso.edu.co Fuente de Internet	<1 %
15	Jorge Merchan-Lima, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez, Dorys Quiroz. "Information Security Management Frameworks in Higher Education Institutions: An Overview", 2019 3rd Cyber Security in Networking Conference (CSNet), 2019 Publicación	<1 %
16	Ratna Ika Puspitasari, DYAH TITISARI, Lamidi Lamidi. "Development of Monitoring Parameters of Oxygen Concentration, Oxygen Flow Rate, Temperature and Humidity in IoT-Based CPAP Bubble (Oxygen	<1 %

and Humidity Concentration)", Jurnal Teknokes, 2023
Publicación

17	repository.unad.edu.co Fuente de Internet	<1 %
18	Ocheme Anthony Ekle, Denis Ulybyshev. "Cyber Risk Evaluation for Android-based Devices", 2023 IEEE Conference on Dependable and Secure Computing (DSC), 2023 Publicación	<1 %
19	Mildred Sena-Vittini, Victor Gomez-Valenzuela, Katerin Ramirez. "Social perceptions and conservation in protected areas: Taking stock of the literature", Land Use Policy, 2023 Publicación	<1 %
20	Oludele Awodele, Chibueze Ogbonna, Emmanuel O. Ogu, Johnson O. Hinmikaiye, Jide E. T. Akinsola. "Characterization and Risk Assessment of Cyber Security Threats in Cloud Computing: A Comparative Evaluation of Mitigation Techniques", Acadlore Transactions on AI and Machine Learning, 2024 Publicación	<1 %
21	Emmanuel Muragijimana, T.N. Shankar, Naween Kumar, Basant Sah, Sasmita Padhy. "Digital Crimes in Cloud Environment and the	<1 %

Analysis via Blockchain", 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), 2022
Publicación

22	Mar Díaz-Millón. "What do experts think about transcreation training? A Delphi method approach", The Interpreter and Translator Trainer, 2023 Publicación	<1 %
23	Submitted to Universidad de Santiago de Chile Trabajo del estudiante	<1 %
24	Submitted to Universidad de Lima Trabajo del estudiante	<1 %
25	reunir.unir.net Fuente de Internet	<1 %
26	Cataldo Basile, Bjorn De Sutter, Daniele Canavese, Leonardo Regano, Bart Coppens. "Design, implementation, and automation of a risk management approach for man-at-the-End software protection", Computers & Security, 2023 Publicación	<1 %
27	openaccess.uoc.edu Fuente de Internet	<1 %
28	repositorio.utn.edu.ec Fuente de Internet	<1 %

29	Leidy Angamarca. "Estrategias de auditoría informática en la era de la transformación digital", Technology Rain Journal, 2022 Publicación	<1 %
30	Submitted to Universidad Europea de Madrid Trabajo del estudiante	<1 %
31	Submitted to Universidad Privada Boliviana Trabajo del estudiante	<1 %
32	repositorio.espe.edu.ec 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, LUZURIAGA REY EDWIN PAUL y MARIN RAMON JUAN ANDRES, en calidad de autores del siguiente trabajo escrito titulado Gestión de riesgos de seguridad de la información de una empresa y propuesta de mejoras utilizando normas y estándares internacionales, 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.

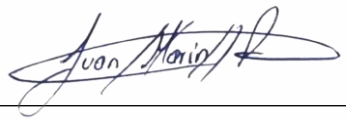
Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

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.

LUZURIAGA REY EDWIN PAUL

0704628825



MARIN RAMON JUAN ANDRES

0150255479

DEDICATORIA

Quiero dedicarle este trabajo primero a Dios, por ser mi guía y fortaleza en cada momento de mi vida, por darme la sabiduría y el valor necesarios para enfrentar y superar todos los desafíos. También a mis padres, por su amor incondicional, apoyo constante y por creer en mí siempre. Gracias por ser mi inspiración y por enseñarme los valores que me han formado como persona. Y, por último, a mi familia en general, por estar siempre a mi lado, brindándome ánimo y apoyo incondicional. Cada uno de ustedes ha sido fundamental en este logro.

Edwin Paul Luzuriaga Rey

Dedico este logro a mi madre por su incalculable fortaleza, dedicación, amor y sacrificio, que han sido una fuente de inspiración constante en mi vida, motivándome a nunca rendirme y perseguir mis metas con determinación. A mis hermanos, por su constante apoyo y siempre estar en los momentos más difíciles. A mis familiares cercanos, por su constante apoyo y cariño, que me han dado la fuerza para seguir adelante. Gracias por estar siempre a mi lado, por creer en mí y por compartir este camino conmigo

Juan Andrés Marín Ramon

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas e instituciones que hicieron posible la realización de este trabajo de titulación. A los ingenieros Fausto Redrován y Bertha Mazón, por su invaluable apoyo y guía durante todo este proceso. Su conocimiento y experiencia fueron fundamentales para el desarrollo de este proyecto. A la ingeniera Nancy Loja, mi tutora, por su dedicación, paciencia y consejos. Su orientación fue esencial para superar los obstáculos y lograr los objetivos planteados. Al ingeniero Rodrigo Morocho, mi cotutor, por su constante apoyo y contribuciones significativas que enriquecieron este trabajo. Al ingeniero Wilmer Rivas, especialista en el área, por su colaboración y aportes técnicos que ayudaron a mejorar la calidad de este proyecto. Finalmente, agradecer a la empresa que nos brindó la oportunidad y nos abrió sus puertas, permitiéndonos trabajar junto a ellos. Su colaboración y disposición fueron importantes para llevar a cabo esta investigación y obtener resultados valiosos. A todos ustedes, mi más profundo agradecimiento por haber creído en mí y en este proyecto.

Edwin Paul Luzuriaga Rey

Quiero expresar mi más sincero agradecimiento a todos los docentes de las instituciones que colaboraron en el desarrollo de este trabajo de titulación. Agradezco de manera especial al ingeniero Fausto Redrován por su apoyo y orientación a lo largo de este proyecto. Asimismo, deseo agradecer a la ingeniera Nancy Loja, por su guía fue crucial para superar los obstáculos y alcanzar los objetivos propuestos. Además, expreso mi gratitud al ingeniero Rodrigo Morocho por su constante apoyo y valiosas contribuciones en este trabajo. También quiero agradecer al ingeniero Wilmer Rivas por su colaboración y aportes técnicos que contribuyeron a mejorar la calidad de este proyecto. Agradezco a mis compañeros y amigos por su constante apoyo y motivación, convirtiendo este trayecto en una experiencia enriquecedora y llevadera. Por último, quiero expresar mi gratitud a la empresa que nos ofreció la oportunidad de colaborar con ellos, permitiéndonos llevar a cabo este trabajo de titulación. A todos ustedes, mi más sincero agradecimiento por creer en mí y en este proyecto.

Juan Andrés Marín Ramon

RESUMEN

El presente trabajo de titulación aborda la gestión de riesgos de la seguridad de la información en una empresa y propone mejoras utilizando normas y estándares internacionales, específicamente la norma ISO/IEC 27005 y la metodología NIST SP 800-30. El objetivo principal es identificar, evaluar y mitigar los riesgos de seguridad de la información, fortaleciendo la continuidad del negocio.

Para alcanzar este objetivo, se llevó a cabo una exhaustiva investigación sobre normas internacionales que abordan políticas, procedimientos y controles de seguridad. Se formó un comité de seguridad de la información para realizar una evaluación de riesgos detallada que incluyó la identificación y tasación de activos de toda empresa, así como la identificación de amenazas y vulnerabilidades asociadas. Posteriormente, se priorizaron los activos de las áreas identificadas como críticas en función de su impacto y probabilidad, y se definieron controles y propuestas de mejora específicas para su tratamiento.

Los resultados de la evaluación demuestran que la realización de un marco de gestión de riesgos basado en la norma ISO/IEC 27005 y la metodología NIST SP 800-30 es eficaz para mitigar incidentes de seguridad y reducir la exposición a amenazas. Las propuestas de mejora incluyen controles específicos que abordan las áreas críticas identificadas, tales como la protección de datos sensibles, la gestión de accesos y la capacitación del personal, asegurando la protección de los activos de la empresa y mejorando su postura de seguridad.

Las conclusiones confirman la hipótesis de que una gestión de riesgos adecuada, respaldada por normas y estándares internacionales, no solo cumple con los aspectos requeridos para la mitigación de incidentes de seguridad, sino que también proporciona una guía clara para la implementación de buenas prácticas. Este trabajo no solo aporta una solución integral para la seguridad de la información en la empresa, sino que también establece un referente de buenas prácticas que pueden ser adoptadas por otras organizaciones en busca de mejorar su seguridad de la información.

PALABRAS CLAVE

Normas internacionales, activos, amenazas, vulnerabilidades, gestión de riesgos, mitigación, propuestas de mejora, seguridad de la información.

ABSTRACT

This thesis addresses the management of information security risks in a company and proposes improvements using international standards and frameworks, specifically ISO/IEC 27005 and the NIST SP 800-30 methodology. The primary objective is to identify, assess, and mitigate information security risks, thereby strengthening business continuity.

To achieve this objective, an exhaustive investigation into international standards that address security policies, procedures, and controls was conducted. An information security committee was formed to carry out a detailed risk assessment, which included the identification and valuation of company-wide assets, as well as the identification of associated threats and vulnerabilities. Subsequently, the assets within the identified critical areas were prioritized based on their impact and likelihood, and specific controls and improvement proposals were defined for their treatment.

The evaluation results demonstrate that establishing a risk management framework based on ISO/IEC 27005 and the NIST SP 800-30 methodology is effective in mitigating security incidents and reducing exposure to threats. The proposed improvements include specific controls that address the identified critical areas, such as sensitive data protection, access management, and personnel training, ensuring the protection of the company's assets and enhancing its security posture.

The conclusions confirm the hypothesis that adequate risk management, supported by international standards and frameworks, not only meets the required aspects for mitigating security incidents but also provides clear guidance for the implementation of best practices. This work not only offers a comprehensive solution for information security within the company but also establishes a benchmark of best practices that can be adopted by other organizations seeking to improve their information security.

KEYWORDS

International standards, assets, threats, vulnerabilities, risk management, mitigation, improvement proposals, information security.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

GLOSARIO

- **Metodología NIST SP 800-30:** Proceso estructurado desarrollado por el Instituto Nacional de Sta.
- **Mitigación:** Acciones o medidas tomadas para reducir la probabilidad de ocurrencia o el impacto de un riesgo de seguridad de la información
- **Normas Internacionales:** Conjunto de directrices, estándares y prácticas reconocidas internacionalmente que establecen requisitos para la gestión de la seguridad de la información.
- **Vulnerabilidad:** Una debilidad o fallo en un sistema que puede ser explotado por una amenaza para comprometer la seguridad de la información.
- **Tasación de Activos:** Es un proceso crucial en la gestión de riesgos de seguridad de la información, que implica asignar un valor a cada activo de la organización.

INTRODUCCIÓN

En la era digital actual, las Tecnologías de la Información (TI) han alcanzado una presencia importante en el tejido empresarial, desempeñando roles críticos en la ejecución eficiente de las operaciones diarias. La rápida evolución de estas tecnologías para adaptarse a las cambiantes necesidades organizativas ha sido un factor clave en su adopción generalizada. Sin embargo, esta creciente dependencia de las TI ha traído consigo desafíos significativos, especialmente en lo que respecta a la seguridad de la información[1].

La integridad, confidencialidad y disponibilidad de los datos se han convertido en pilares fundamentales para la continuidad y el éxito de cualquier empresa en el panorama actual. La amenaza constante de ciberataques, el aumento de las regulaciones de privacidad de datos y la sofisticación de las vulnerabilidades informáticas plantean desafíos cada vez mayores para garantizar la protección adecuada de la información sensible.

En este contexto, la gestión de riesgos de seguridad de la información emerge como una disciplina indispensable. Su enfoque proactivo y sistemático para identificar, evaluar y mitigar las amenazas a la seguridad de la información se convierte en un componente crítico de la estrategia empresarial. Además, la gestión de riesgos no solo se trata de minimizar las amenazas, sino también de fortalecer la resiliencia organizativa frente a incidentes potenciales[2].

Este proyecto se centra en ofrecer una solución integral para la gestión de riesgos de seguridad de la información en el contexto específico de una empresa. Basándose en las normas y estándares internacionales ISO/IEC 27005, y en la metodología NIST SP 800-30, se propone un marco sólido y estructurado para abordar los desafíos de seguridad de la información de manera efectiva.

Este proyecto tiene como objetivo ofrecer una aproximación integral y orientada a resultados para la gestión de riesgos de seguridad de la información, con el fin de garantizar la protección de la empresa en un entorno empresarial cada vez más digitalizado y amenazante.

Al adoptar esta gestión de riesgos, no solo se busca resolver problemas inmediatos de seguridad de la información, sino también preparar a la organización para enfrentar de manera proactiva los desafíos futuros en un entorno digital en constante evolución. La implementación de esta estrategia no solo protege los activos críticos de información, sino que también fortalece la posición competitiva y la reputación de la empresa en el mercado.

i. Declaración y formulación del Problema

En la actualidad, la empresa se enfrenta a desafíos significativos en cuanto a la seguridad de la información, evidenciados por la creciente de amenazas y vulnerabilidades existentes. La falta de una gestión de riesgos específica y estructurada compromete la integridad, confidencialidad y disponibilidad de los activos, lo que se traduce en potenciales pérdidas financieras, daño a la reputación y riesgos operativos. La ausencia de un marco normativo claro y la ineficiente identificación y tratamiento de riesgos específicos amenazan la seguridad de la información, afectando la continuidad operativa. Ante este panorama, se plantea la necesidad de proponer una gestión de riesgos respaldado por normativas internacionales, como ISO/IEC 27005 y NIST SP 800-30, para fortalecer la postura de la empresa. En la Figura 1, se presenta las causas y efectos del problema de estudio en este trabajo.

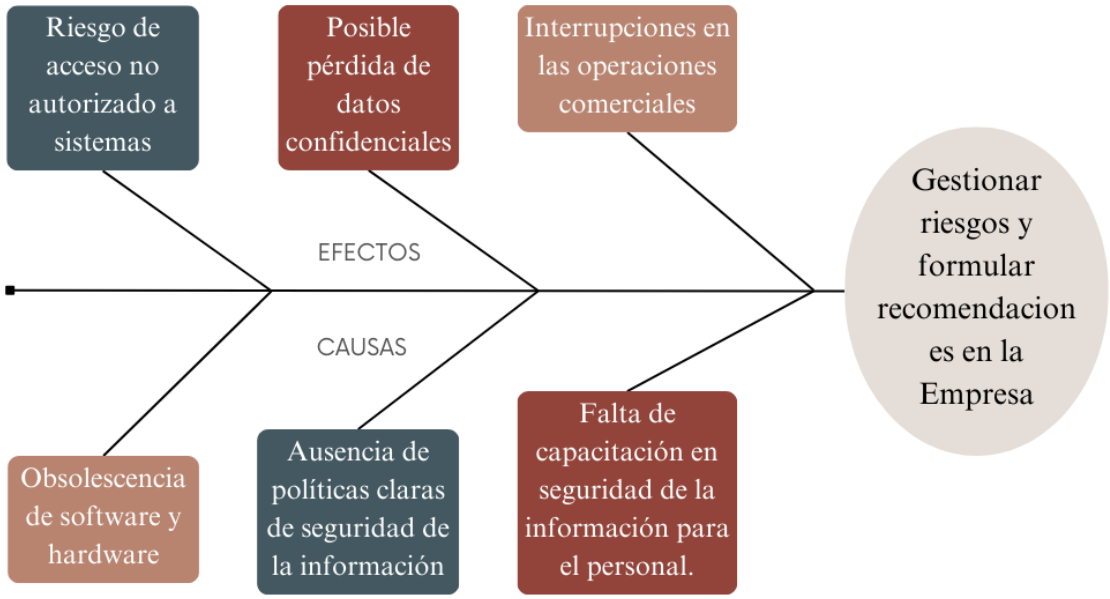


Figura 1 *Causas y efectos del problema*

Formulación del problema

- **Problema principal:**
    - ¿Cómo gestionar los riesgos en la empresa?

- **Problemas específicos:**
    - ¿Cuál es el protocolo de respuesta ante incidentes de seguridad?
    - ¿Cómo realiza la empresa una evaluación continua de riesgos?
    - ¿Se realizan análisis periódicos de riesgos en base a la seguridad de la información?
    - ¿Qué herramientas ayudan a gestionar los riesgos en la seguridad de la información?

- ¿Qué programas de capacitación en seguridad de la información existen para los empleados?
- ¿Existen procesos establecidos para la revisión de seguridad de sistemas antes de su implementación?

ii. Objeto de estudio y Campo de acción

Objeto de estudio

- Gestionar los riesgos dentro de una empresa privada.

Campo de acción

- Gestionar el cumplimiento de las normas internacionales.

iii. Objetivos

Objetivo General

- Gestionar los riesgos de la seguridad de la información para la propuesta de mejoras, mediante normas y estándares internacionales.

Objetivos específicos

- Investigar las normas internacionales, abarcando políticas, procedimientos y controles de seguridad para una buena gestión de riegos en la empresa.
- Realizar una evaluación de riesgos mediante la identificación de activos de la empresa.
- Formular controles de seguridad y propuestas de mejora, abordando las áreas identificadas como críticas dentro de la organización.
- Realizar el tratamiento de los riesgos para la reducción del impacto de las amenazas identificadas dentro de la empresa.
- Evaluar si la gestión de riesgos cumple con los aspectos requeridos en la norma ISO/IEC 27005 y la metodología NIST-SP 800-30 mediante la aplicación de una encuesta a expertos en el área.

iv. Hipótesis y variables o Preguntas de investigación

Hipótesis principal

- Si se realiza una gestión de riesgos de la seguridad de la información, se cumplirán los aspectos de las normas y estándares internacionales para la mitigación de incidentes de seguridad dentro de una empresa.

Variables y dimensionamiento

Tabla 1 Variables y Dimensionamiento

Variable	Definición Teórica	Categorías	Indicadores	Ítems
Variable Independiente: Normas y estándares internacionales.	Propuesta de mejoras aplicando normas y estándares internacionales.	**1.** Normas y Estándares Internacionales. **2.** Metodologías. **3.** Herramientas.	**1.** Aplicación de normas y estándares internacionales. **2.** Aplicación de metodologías **3.** Aplicación de herramientas.	**1.** Investigar para definir las normas y estándares a utilizar. **2.** Análisis de la correcta aplicación de las metodologías.
Variable dependiente: Gestión de riesgos y fortalecimiento de la seguridad de la información de la empresa.	La gestión adecuada de los riesgos puede proponer mejoras para reforzar la seguridad de la información de la empresa.	**1.** Evaluación de los riesgos. **2.** Tratamiento de los riesgos.	**1.** Políticas de seguridad. **2.** Propuesta de mejoras de acuerdo a los riesgos.	**1.** Utilización apropiada de herramientas para detectar riesgos. **2.** Evaluación de la gestión de riesgos a expertos en el área.

v. Justificación

La empresa una posición vulnerable ante la creciente amenazas cibernéticas, cuya magnitud y diversidad presentan riesgos significativos para la integridad de la información sensible y la continuidad operativa del negocio. En este contexto, la ausencia de una metodología estructurada para la gestión de riesgos se convierte en un factor crítico que intensifica la exposición a posibles ataques. Esta investigación se manifiesta en la urgente necesidad de no solo identificar y abordar las amenazas inminentes, sino también en la implementación de prácticas de gestión de riesgos que ofrecerán soluciones sostenibles y eficaces. Por ende, la innovación radica en la capacidad de integrar conocimientos avanzados sobre seguridad de la información y adaptar las mejores prácticas reconocidas internacionalmente a la estructura específica de la empresa. Aportando beneficios derivados al proyecto que están trascendiendo los confines de la empresa para impactar directamente en sus clientes y la comunidad en general. La implementación exitosa de la gestión de riesgos de seguridad de la información no solo resguardará la información crítica, sino que también fortalecerá la confianza de los clientes, un activo invaluable en cualquier empresa. En un plano más amplio, la contribución activa a la seguridad de la información a nivel local posiciona a la empresa como un enfoque proactivo en la protección de la información digital en su entorno. Al convertirse en un referente en buenas prácticas, la empresa puede inspirar y motivar a otras entidades locales a seguir un camino similar, generando así un impacto positivo expansivo en la seguridad de la información de la comunidad empresarial. La participación activa y la disposición de la empresa para colaborar estrechamente en este estudio no solo validan la necesidad imperante de este proyecto, sino que también certifica que las recomendaciones resultantes sean prácticas, aplicables y se alineen de manera precisa con las condiciones y desafíos específicos que enfrenta la empresa.

CAPÍTULO I. MARCO TEÓRICO

En este primer capítulo, se llevó a cabo una revisión de la literatura centrada en la seguridad de la información y la gestión de riesgos. Se formularon preguntas de investigación para abordar aspectos clave como la identificación de normas internacionales relevantes para la gestión de riesgos, la estructuración y la aplicación de políticas de seguridad. Se establecieron palabras clave y cadenas de búsqueda para abarcar diversas fuentes académicas, y se formularon criterios de inclusión y exclusión para ayudar a seleccionar investigaciones centradas en la gestión de riesgos informáticos, la seguridad de la información y las normas internacionales. Además, el proceso de búsqueda en diversas bases de datos académicas arrojó resultados significativos, que contribuyeron al desarrollo de la investigación. En cuanto a los antecedentes históricos, teóricos y contextuales, estos aspectos exploraron los acontecimientos históricos relevantes, las teorías fundamentales asociadas y el contexto aplicativo, incluido el ámbito de aplicación y el establecimiento de requisitos.

1.1 Antecedentes de la Investigación

En esta sección se presenta una revisión de literatura (SRL) en lo que se refiere al tema de seguridad de la información y gestión de riesgos en la seguridad de la información. El proceso consiste en buscar, evaluar y resumir los resultados de estudios anteriores para reorientar la investigación de este trabajo. Se emplea métodos para minimizar los sesgos en el proceso de investigación, incluyendo el análisis, la medición, la síntesis y la redacción[3].

a) Preguntas de investigación

A continuación, se presenta las interrogantes de investigación formuladas en la tabla 2 para realizar una búsqueda sobre la seguridad de la información.

Tabla 2 *Interrogantes de investigación*

Pregunta	**Descripción y motivación**
¿Cuáles son las normas y estándares internacionales más relevantes para la gestión de riesgos en seguridad de la información?	La pregunta busca identificar e investigar los estándares y normas internacionales que son comúnmente empleados en la gestión de riesgos.
¿Cómo se estructuran y aplican las políticas de seguridad en organizaciones que gestionan riesgos informáticos de acuerdo con normas internacionales?	La pregunta busca comprender la estructuración y aplicación de políticas de seguridad, abarcando aspectos como acceso, privacidad y respuesta a incidentes, según normas internacionales
¿Qué resultado se obtendrá con la implantación de la gestión de riesgos de la seguridad de la información en la empresa?	La pregunta busca evidenciar los beneficios y resultados que se obtendrá al implantar la gestión de riesgos
¿Cuáles son las herramientas que ayudarán en la gestión de riesgos para la mitigación de incidentes de seguridad en la empresa?	La pregunta busca identificar y comprender las herramientas específicas que son útiles en el proceso de gestión de riesgos

b) Palabras claves y Cadena(s) de búsqueda

Se utilizó palabras claves y cadenas de búsqueda para encontrar en varias bases de datos académicas publicaciones relacionadas con el tema de este trabajo.

Cadena de búsqueda en español

- (Gestión de riesgos de seguridad de la información) AND (Normas ISO/IEC) OR (Estándares internacionales de seguridad informática)
- (Gestión de incidentes de seguridad informática) OR (Análisis de riesgos informáticos) AND (Estándares internacionales de seguridad informática ISO/IEC 27005)
- (Cumplimiento con ISO/IEC) OR (Implementación de estándares de seguridad) OR (Certificación ISO/IEC)

Cadenas de búsqueda en inglés.

- (Information security risk management) AND (ISO/IEC Standards) OR (International computer security standards)
- (Computer security incident management) OR (Computer risk analysis) AND (International computer security standards ISO/IEC)
- (ISO/IEC Compliance) OR (Implementation of Safety Standards) OR (ISO/IEC Certification)

c) Criterios de inclusión y exclusión

__Tabla 3__ Criterios de inclusión y exclusión

#	**Criterios de inclusión**
1	Investigaciones primarias
2	Investigaciones a partir del 2018
3	Investigaciones asociadas a gestión de riesgos informáticos
4	Investigaciones asociadas a seguridad de la información
5	Investigaciones asociadas a las normas internacionales ISO/IEC 27005
#	**Criterios de exclusión**
1	Investigaciones secundarias
2	Investigaciones anteriores al 2018
3	Investigaciones duplicadas
4	Investigaciones inaccesibles
5	Investigaciones menores a 3 páginas.

d) Proceso y resultados de la búsqueda

Mediante una búsqueda en diversas bases de datos académicas, pudimos obtener varios estudios refrentes a nuestro proyecto. Siguiendo el proceso descrito en la Figura 2, obtuvimos estudios que contribuyen al proyecto.

Estudios de la búsqueda

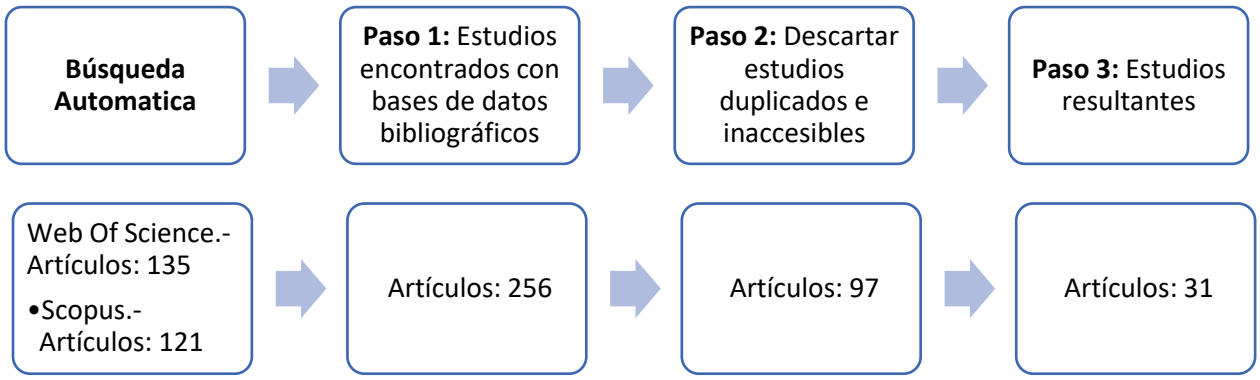


Figura 2 *Proceso y Resultados de la Búsqueda*

Los hallazgos de trabajos relacionados por año de publicación (Figura 3)

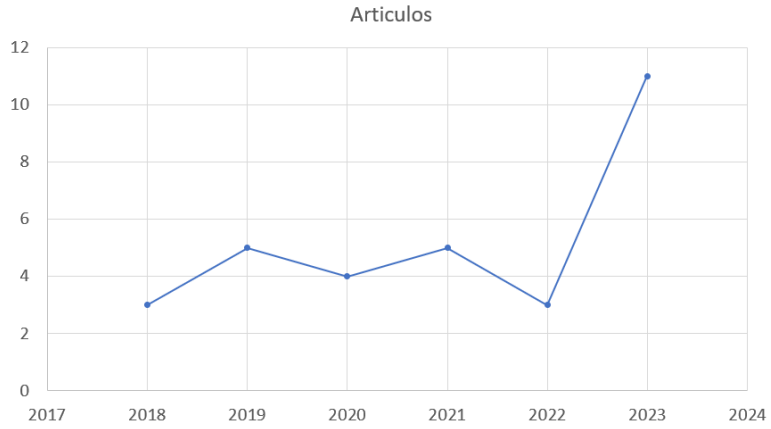


Figura 3 *Estudios de la Búsqueda, diagrama de cantidad de estudios por año*

1.2 Antecedentes históricos

La norma ISO/IEC 27001 y la norma ISO/IEC 27005 han evolucionado a lo largo del tiempo para adaptarse a las necesidades cambiantes de las organizaciones en cuanto a la gestión de la seguridad de la información. Las normas individuales de la serie ISO 27000 abordan diversos aspectos en el ámbito de la seguridad de la información. La norma ISO/IEC 27001 establece los requisitos para un sistema de gestión de seguridad de la información, ha sido actualizada en varias ocasiones, siendo la versión más reciente la ISO/IEC 27001:2013. Esta versión incluye cambios significativos en la estructura y el contenido de la norma, como la inclusión de un enfoque basado en el riesgo y la integración de la gestión de la seguridad de la información en los procesos de negocio de la organización[4].

la norma internacional ISO 27001 establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), por otro lado, la ISO 27005 proporciona orientación para la gestión de riesgos relacionados con la seguridad de la información[5]. Las normas complementarias incluyen la ISO/IEC 27002, que ofrece un código de buenas prácticas para el

control de la seguridad de la información, proporcionando directrices detalladas para implementar controles de seguridad[6].

La transición de ISO/IEC 27001 a ISO/IEC 27005 representó un cambio significativo, ya que mientras la primera se enfoca en establecer un Sistema de Gestión de la Seguridad de la Información (SGSI), la segunda se especializa en la gestión detallada de riesgos asociados con la seguridad de la información. Esta evolución permitió una mayor claridad y especialización al proporcionar pautas más detalladas para abordar de manera efectiva los riesgos específicos en este ámbito, brindando a las organizaciones un marco más preciso para la gestión de riesgos en seguridad de la información[7].

En la actualidad con la ayuda de estas normas, las organizaciones pueden llevar a cabo una gestión de riesgos de la seguridad de la información de manera más eficiente y efectiva. La ISO/IEC 27001 proporciona una base sólida para establecer y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI), asegurando que la seguridad sea una parte integral de los procesos de negocio. La ISO/IEC 27005 complementa esto al ofrecer directrices detalladas para identificar, evaluar y tratar los riesgos específicos relacionados con la seguridad de la información. Adicionalmente, normas como la ISO/IEC 27002, con sus buenas prácticas para el control de la seguridad, permiten a las organizaciones implementar controles de seguridad sólidos y coherentes. Esta integración de normas proporciona un marco robusto que ayuda a las organizaciones a no solo proteger sus activos de información, sino también a cumplir con los requisitos regulatorios, mejorar la confianza de los clientes y fortalecer su resiliencia ante posibles amenazas.

1.3 Antecedentes Teóricos

En la figura 4 se muestran los temas y subtemas que se abordan en este literal:

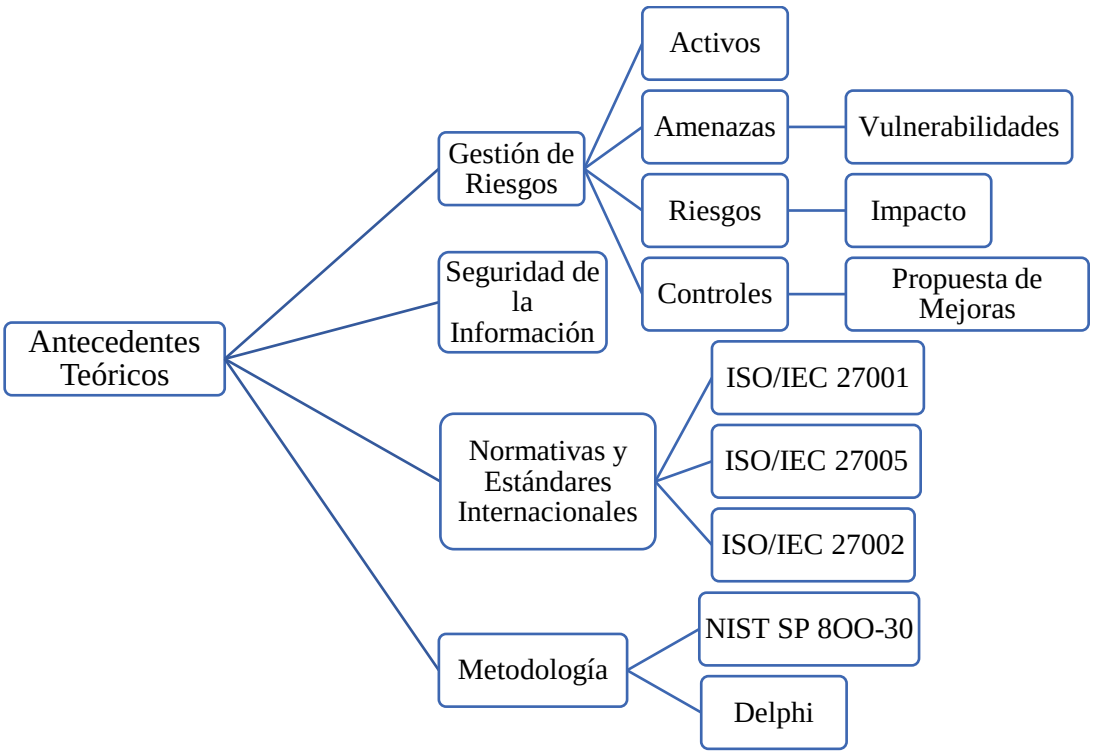


Figura 4 *Antecedentes Teóricos*

1.3.1 Gestión de Riesgos

Gestionar el riesgo es el proceso coordinado de dirigir y controlar una organización. Su objetivo es desarrollar controles e indicadores que ayuden a proteger la información. Esto se logra mediante la implementación de medidas de seguridad efectivas que mitiguen los posibles riesgos a los que está expuesta la organización[8]. El propósito de la gestión de riesgos es reducir la probabilidad de que ocurran eventos negativos o adversos mediante la detección, evaluación, corrección, monitoreo y control de los riesgos. La gestión de riesgos de seguridad de TI con llevar las principales tareas que consisten en identificar y clasificar los riesgos de seguridad informática de la organización como también la evaluación de riesgos e identificar las técnicas adecuadas para reducir los riesgos. Por ende, antes de tomar decisiones sobre la inversión en seguridad, se debe considerar la gestión de riesgos de TI [9].

La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable[10]. La aplicación de medidas de seguridad informática implica implementar un conjunto de normas y procedimientos que regulan el manejo de la información. Estos criterios de seguridad deben ser capaces de salvaguardar los datos de diversas organizaciones frente a múltiples riesgos ineludibles[11].

La gestión de riesgos es una estrategia que ayuda a los encargados de tecnología de la información a encontrar el equilibrio entre el costo y la efectividad de las medidas de seguridad. Esto permite fortalecer la capacidad de las organizaciones para proteger sus sistemas y datos de TI, que son fundamentales para cumplir sus objetivos[12].

Activo

Un activo se define como cualquier recurso, tangible o intangible, que posee valor para una organización y cuya pérdida, daño o mal uso podría tener un impacto negativo en su capacidad para operar eficazmente. Estos activos pueden abarcar desde propiedades físicas, como instalaciones y equipos, hasta activos financieros, información, capital humano e intangibles como la reputación y la propiedad intelectual. Identificar, evaluar y proteger estos activos es fundamental para mitigar riesgos y garantizar la continuidad del negocio, mediante la implementación de medidas de seguridad y controles adecuados[13]. Los activos de información son elementos indispensables dentro de la misma para la seguridad de la información. Por lo tanto, la decisión de implementar un sistema de gestión de la seguridad de la información depende de la relevancia que estos activos tienen para la organización[14].

Amenaza

En el ámbito de gestión de riesgos una amenaza se refiere a cualquier evento o circunstancia potencial que pueda causar daño, pérdida o interrupción a los activos de una organización o a sus operaciones. Estas amenazas pueden manifestarse de diversas formas, incluyendo desastres naturales, fallos en sistemas tecnológicos, ciberataques, errores humanos, cambios en el entorno regulatorio, o incluso crisis de reputación[15]. Identificar y comprender estas amenazas son fundamentales para una gestión eficaz de riesgos, permitiendo a las organizaciones implementar medidas preventivas y de mitigación adecuadas para proteger sus activos, garantizar la continuidad del negocio. Es importante distinguir las amenazas y precisar el impacto de cada una con el propósito de ejercer medidas necesarias para evitar ataques[16].

Vulnerabilidad

Las vulnerabilidades son debilidades o deficiencias relacionadas a una amenaza en específico que son provocados por procesos, infraestructuras o controles de una organización que podrían ser explotadas para causar daño, pérdida o interrupción en las operaciones o en los activos de la organización. Estas vulnerabilidades pueden surgir debido a diversos factores, como fallas en la seguridad de la información, deficiencias en los procedimientos operativos, carencias en la capacitación del personal, falta de mantenimiento de equipos o sistemas obsoletos[17]. La identificación y comprensión de las vulnerabilidades en una gestión de riesgos permiten a las organizaciones tomar medidas proactivas para fortalecer sus defensas, implementar controles de seguridad adecuados y reducir la probabilidad de que las amenazas que exploten estas debilidades. Para identificar y definir los parámetros, que serán base para el proceso de análisis de riesgos, se hace necesario determinar el valor de los activos y la vulnerabilidad del proceso, esto se logró por medio de las actividades de observación directa y revisión documenta[18].

Riesgos

Los riesgos es una posibilidad de que ocurran eventos o situaciones que tengan un impacto negativo en los objetivos, activos o intereses de una organización. Estos eventos pueden incluir desde pérdidas financieras, daños materiales, interrupciones en las operaciones, hasta daños a la reputación o incumplimientos regulatorios. Los riesgos se derivan de la combinación de amenazas que explotan vulnerabilidades, y pueden ser internos o externos, conocidos o desconocidos[19]. Una gestión de riesgos ayuda a identificar, evaluar y priorizar estos riesgos, así como desarrollar estrategias y controles para mitigarlos o gestionarlos de manera efectiva, con el objetivo de proteger los activos y promover la continuidad del negocio en un entorno cambiante y potencialmente peligroso. El estudio de riesgo, ezse determina la técnica para el análisis del riesgo, la cual puede ser cualitativa, cuantitativa o una combinación de ambas y finalmente se determina el nivel del riesgo[20].

Impacto

El impacto se refiere a la medida en que un evento adverso podría afectar directamente con pérdidas o daños a una organización, sus activos o sus objetivos. La evaluación del impacto ayuda a las organizaciones a comprender las posibles consecuencias de los riesgos identificados y a priorizar la asignación de recursos para mitigarlos o gestionarlos de manera efectiva. Comprender el impacto potencial de los riesgos permite a las organizaciones tomar decisiones informadas y proactivas para protegerse contra las amenazas y mantener la resiliencia en un entorno empresarial [21].

Controles

Los controles son medidas o acciones diseñadas para reducir la probabilidad de que ocurran eventos adversos o para mitigar su impacto en caso de que se materialicen. Estas medidas pueden incluir políticas, procedimientos, prácticas, tecnologías, equipos, herramientas o cualquier otra acción destinada a proteger los activos de una organización, garantizar el cumplimiento de regulaciones y normativas, para promover la continuidad del negocio. Los controles pueden ser preventivos o correctivos, y se seleccionan y aplican según la naturaleza y el nivel de los riesgos identificados[22]. La implementación efectiva de controles adecuados ayuda a las organizaciones a gestionar los riesgos de manera más eficiente, protegiendo sus activos y salvaguardando su capacidad para alcanzar sus objetivos estratégicos.

Propuesta de mejoras

Una propuesta de mejora es un documento o plan que describe una serie de acciones específicas destinadas a mejorar un proceso, producto, servicio o sistema dentro de una organización. Estas propuestas suelen surgir como resultado de la identificación de áreas de oportunidad o debilidades en la operación actual, ya sea a través de la retroalimentación de los clientes, la observación interna, el análisis de datos o la evaluación de desempeño[23]. Una propuesta de mejora generalmente incluye objetivos claros, acciones concretas, un cronograma de implementación, asignación de recursos necesarios y una estimación de los beneficios esperados. Su objetivo es impulsar la eficiencia, la calidad, la productividad o la satisfacción del cliente, contribuyendo así al crecimiento y éxito continuo de la organización.

1.3.2 Seguridad de la Información

La seguridad de la información implica salvaguardar la confidencialidad, integridad y disponibilidad de los datos, la información, los sistemas de información y sus componentes esenciales frente al acceso, uso, exposición y modificación no autorizados[24]. La escalada de ciberamenazas y ataques que pueden comprometer información sensible, causar importantes pérdidas económicas y dañar la reputación de una organización han hecho que la seguridad de la información sea cada vez más crítica, por lo tanto, es un componente crucial de las operaciones de cualquier organización.

La seguridad de la información involucra procesos, prácticas y metodologías para proteger la información y los sistemas de accesos no autorizados. En esencia, esto implica la necesidad de salvaguardar los datos y los recursos de infraestructura tecnológica de aquellos individuos que pretendan hacer un uso indebido de los mismos[25].

la seguridad de la información se orienta a proteger los activos de información sin importar su forma o estado, valiéndose de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, para la aplicación y gestión de las medidas de seguridad apropiadas en cada caso. teniendo en cuenta se debe desarrollar correctamente para asegurar el éxito de una organización[26].

1.3.3 Normas y estándares Internacionales

ISO/IEC 27001

La norma ISO 27001:2013 establece un marco internacional para los sistemas de gestión de seguridad de la información (SGSI), con el objetivo de garantizar la confidencialidad, integridad y disponibilidad continua de la información, así como el cumplimiento legal. La certificación según la ISO 27001 es crucial para salvaguardar los activos más importantes, como la información de clientes y empleados, la reputación empresarial y otros datos privados [27]. Esta norma adopta un enfoque basado en procesos para implementar, operar y mantener un SGSI.
La adopción de la ISO 27001 se presenta como la solución óptima para satisfacer los requisitos legales y las demandas de los clientes, incluyendo el RGPD, así como para hacer frente a diversas amenazas potenciales, como el cibercrimen, la violación de datos personales, el vandalismo/terrorismo, incendios, mal uso intencional, robo y ataques de virus. la norma proporciona un proceso sistemático y estructurado para identificar, evaluar y gestionar los riesgos de seguridad de la información de una organización. Este enfoque se basa en el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar), lo que permite a las organizaciones adaptarse de manera eficaz a los cambios en el entorno de seguridad y a las nuevas amenazas que puedan surgir[28].

la adopción de la norma ISO 27001 no solo es una forma efectiva de cumplir con los requisitos legales y las expectativas de los clientes en materia de seguridad de la información, sino que también puede ser un catalizador para la mejora continua y la excelencia operativa en toda la organización.

ISO/IEC 27005

La Norma y estándar internacional ISO/IEC 27005 forma parte de la serie ISO/IEC 27000. ISO 27005 es un estándar que proporciona directrices para la gestión de riesgos de seguridad de la información, la norma internacional da una contribución a emplear correctamente la seguridad de la información basada en una gestión de riesgos y respalda los términos generales descritos en ISO/IEC 27001. La ISO/IEC 27005 consta de varios pasos, como el establecimiento del contexto, la evaluación del riesgo la cual está conformado por: identificación, análisis y evaluación; el tratamiento del riesgo, la aceptación del riesgo, la comunicación, consulta del riesgo, la supervisión y revisión del riesgo [29].

La norma ISO/IEC 27005 se estructura en varios pasos clave:

1. **Establecimiento del contexto**: Definir el ámbito y los criterios para la gestión de riesgos, identificando los activos de información, las amenazas, las vulnerabilidades y las consecuencias potenciales.

2. **Evaluación del riesgo**: Este proceso se divide en tres subpasos:
    - **Identificación del riesgo**: Reconocer las posibles amenazas que puedan afectar a los activos de información y las vulnerabilidades que puedan ser explotadas.
    - **Análisis del riesgo**: Evaluar la probabilidad y el impacto de los riesgos identificados para determinar su nivel de riesgo.
    - **Evaluación del riesgo**: Comparar los niveles de riesgo encontrados con los criterios de riesgo establecidos para decidir si los riesgos son aceptables o requieren tratamiento.

3. **Tratamiento del riesgo**: Seleccionar e implementar medidas adecuadas para mitigar los riesgos a niveles aceptables. Esto puede incluir la implementación de controles de seguridad adicionales, la transferencia del riesgo a terceros, la aceptación del riesgo o la evitación del riesgo mediante cambios en los procesos o sistemas.

4. **Aceptación del riesgo**: Decidir formalmente sobre la aceptación de los riesgos residuales después de que se hayan aplicado las medidas de tratamiento del riesgo.

5. **Comunicación y consulta del riesgo**: Informar y consultar a las partes interesadas relevantes sobre los riesgos y las medidas adoptadas para gestionarlos, asegurando una comprensión compartida y el apoyo a las decisiones tomadas.

6. **Supervisión y revisión del riesgo**: Monitorear continuamente los riesgos y la efectividad de los controles implementados, revisando y actualizando el proceso de gestión de riesgos para reflejar cambios en el entorno interno y externo[30].

ISO/IEC 27002

La ISO/IEC 27002 es una norma internacional que proporciona directrices y mejores prácticas para la implementación de controles de seguridad de la información. Es una extensión de la ISO/IEC 27001 y se utiliza para ayudar a las organizaciones a seleccionar y aplicar los controles adecuados para proteger sus activos de información. Mientras que la ISO/IEC 27001 especifica los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), la ISO/IEC 27002 se enfoca en los controles detallados que pueden ser implementados dentro de ese sistema[31].

Para mantener y mejorar el desarrollo futuro, es crucial analizar y evaluar regularmente el rendimiento del Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27001 es clave en la gestión de riesgos de seguridad, ya que busca controlar y reducir el riesgo de violaciones de datos de manera aceptable. Los controles de seguridad y designa a los responsables, mientras que la norma ISO/IEC 27002 brinda instrucciones para implementar dichos controles de manera efectiva[32].

Cuadro comparativo de las Normas y Metodologías

Tabla 4 *Cuadro comparativo de las normas*

Aspecto	ISO 27001	ISO 27005	ISO 31000	NIST SP 800-30
Objetivo principal	Establecer un sistema de gestión de seguridad de la información (SGSI)[28].	Proporcionar directrices para la gestión de riesgos específicamente relacionados con la seguridad de la información[30].	Ofrecer un enfoque genérico para la gestión del riesgo en cualquier ámbito organizacional[33].	Identificar, evaluar y gestionar los riesgos de seguridad de la información en una organización[34].
Enfoque	Diseñado especialmente para proteger la información.	Específico para la gestión de riesgos de SGSI	Genérico, aplicable a todo tipo de riesgos y organizaciones.	Basado en la evaluación de riesgos utilizando un proceso sistemático y estructurado.
Alcance	Su enfoque principal es garantizar la seguridad de los datos.	El enfoque se centra en identificar y valorar los riesgos de seguridad de la información.	Cubre la gestión del riesgo en todos los aspectos y actividades organizacionales.	Aplicable a todas las organizaciones que manejan información sensible.

Requisitos	Establece requisitos para un SGSI efectivo.	Proporciona directrices y recomendaciones para la gestión de riesgos de seguridad de la información.	No establece requisitos específicos, solo ofrece principios y directrices.	No hay requisitos específicos, pero se espera que las organizaciones implementen evaluación de riesgos de acuerdo con las pautas establecidas.
Certificación	Es posible obtener la certificación ISO 27001.	No se emite una certificación específica bajo ISO 27005.	No se emite una certificación específica bajo ISO 31000.	No hay una certificación específica bajo la metodología NIST SP 800-30.
Relación	Puede ser utilizada junto con ISO 27005 para gestionar riesgos específicos de seguridad de la información	Puede complementar la implementación de un SGSI conforme a ISO 27001	Puede ser utilizada en conjunto con ISO 27001 y ISO 27005 para una gestión integral de la seguridad de la información y otros riesgos	Se puede utilizar en conjunto con ISO 27005 ya que ambos se centran en la evaluación de riesgos.
Aplicación	Principalmente en entornos donde la SGSI es crítica	Específicamente en la gestión de riesgos de SGSI	En cualquier ámbito organizacional y tipo de riesgo	Se aplica en la identificación, evaluación y gestión de riesgos de seguridad de la información en una variedad de contextos organizacionales.

Para este proyecto, de todas las normas de la familia de las ISO/IEC 27000 descritas en la tabla 4, se decidió utilizar la ISO/IEC 27005 ya que se centra específicamente en la gestión de riesgos relacionados con la seguridad de la información. Al utilizar esta norma, una empresa puede beneficiarse de directrices y mejores prácticas específicas diseñadas para abordar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información sensible. La ISO 27005 promueve un enfoque sistemático y basado en el riesgo para la gestión de la seguridad de la información. Esto significa que la empresa puede identificar, evaluar y tratar los riesgos de manera proactiva, enfocando sus recursos en las áreas donde el impacto potencial de los riesgos es mayor. También permite a las empresas adaptar sus procesos y controles según sus necesidades específicas, lo que significa que una empresa puede personalizar su enfoque de gestión de riesgos para que se ajuste mejor a su entorno operativo, tamaño y naturaleza de los datos. Finalmente, La ISO/IEC 27005 proporciona un enfoque detallado para la gestión de riesgos de seguridad de la información, mientras que la metodología NIST SP 800-30 ofrece un marco específico para la evaluación de riesgos. Combinar ambas metodologías permite cubrir tanto la gestión continua de riesgos como la evaluación detallada.

1.3.4 Metodología

NIST SP 800-30

La Metodología NIST SP 800-30 fue creada por el Instituto Nacional de Estándares y Tecnología (NIST), se presenta como un complemento a las directrices NIST SP 800-39, con el propósito de ofrecer una evaluación de riesgos para la información en sistemas de organizaciones y entidades gubernamentales y privadas. En sintonía con la norma ISO 27005, NIST 800-30 se destaca como una guía completa para la realización de evaluaciones de riesgos. Este marco proporciona los cimientos necesarios para establecer un programa efectivo de gestión de riesgos, ofreciendo definiciones claras y orientaciones prácticas para evaluar y mitigar los riesgos presentes en los sistemas de tecnología de la información. Sus nueve etapas de evaluación abarcan desde la caracterización del sistema y la identificación de amenazas y vulnerabilidades, hasta el análisis de control, la determinación de probabilidad, el análisis de impacto, y la emisión de sugerencias de control, culminando en un informe detallado de la evaluación de riesgos. Este enfoque estructurado y completo se rige como un recurso fundamental para fortalecer la seguridad de la información en diversos contextos organizacionales[29].

NIST SP 800-30 aboga por un enfoque continuo y dinámico en la gestión de riesgos, subrayando la importancia de la supervisión y revisión periódica de los riesgos y controles implementados. Asimismo, la guía incluye técnicas y herramientas específicas para la evaluación de riesgos, como matrices de riesgo y métodos de evaluación cualitativa y cuantitativa, que permiten a las organizaciones adaptar la evaluación a sus necesidades específicas y niveles aceptables de riesgo[35].

Delphi

La Metodología Delphi es una forma estructurada para la obtención de consensos y la toma de decisiones informadas, basada en la consulta iterativa a un panel de expertos. Esta técnica, desarrollada por primera vez por la corporación RAND en la década de 1950, ha sido ampliamente empleada en una variedad de campos, como la evaluación de políticas públicas, la previsión tecnológica, la investigación de mercado y la planificación estratégica[36].

El método Delphi fue diseñado para la investigación práctica, estableciéndose en el pragmatismo de John Dewey, el cual se considera un puente entre el paradigma interpretativo, que valora el subjetivismo y el contexto, y el paradigma post-positivista, que busca la objetividad y la generalización. Por esta razón, el uso apropiado del método dentro del contexto adecuado tiende a producir buenos resultados, mientras que no hacerlo puede generar dudas sobre el rigor científico de la investigación realizada y, en consecuencia, sobre el valor científico de los resultados obtenidos. Delphi es una técnica de recopilación de información fiable de un panel de expertos a través de una serie de rondas de interacción cíclicas en las que se mantiene el anonimato de los participantes[37].

El investigador selecciona a un grupo de expertos con un cierto nivel de experiencia en el tema de estudio y compila un cuestionario con una lista de declaraciones que se les presenta para que expresen sus opiniones al respecto. A partir de las respuestas de los expertos a cada tema presentado, el investigador crea nuevas interrogantes sobre el mismo tema, basándose en la evaluación inicial del panel. Posteriormente, el investigador retroalimenta a los expertos con análisis estadísticos de las respuestas y les presenta un nuevo grupo de preguntas[38].

Después de recibir los comentarios, los miembros del grupo pueden revisar sus respuestas al cuestionario. El nivel de acuerdo entre los evaluadores sobre las preguntas planteadas se examina después de uno o más ciclos de respuestas a las preguntas replanteadas. El uso adecuado del método Delphi en el contexto adecuado tiende a generar buenos resultados; por otro lado, no hacerlo puede generar incertidumbre sobre el rigor científico de la investigación llevada a cabo y, por ende, sobre el valor científico de los resultados obtenidos[38].

1.4 Antecedentes Contextuales

En un entorno empresarial cada vez más digitalizado, la gestión eficaz de los riesgos para la seguridad de la información se convierte en una necesidad imperiosa. La creciente complejidad y sofisticación de las ciberamenazas contemporáneas plantean retos sustanciales para salvaguardar la información en las organizaciones. En respuesta a esta realidad, la adopción de normas y estándares internacionales surge como un componente esencial para reforzar la postura de las empresas frente a posibles vulnerabilidades. La aplicación de estos marcos de referencia no solo proporciona directrices claras para evaluar y mitigar los riesgos, sino que también establece un enfoque unificado y sólido para hacer frente a las amenazas emergentes. En este contexto, comprender los antecedentes contextuales se vuelve crucial, ya que permite a las organizaciones adaptarse de forma proactiva a un panorama de riesgos dinámico, garantizando así la integridad y la continuidad operativa en un mundo empresarial cada vez más interconectado.

1.4.1 Ámbito de aplicación

Se ha desarrollado una gestión de riesgos de seguridad de la información en el entorno corporativo. Esta propuesta de gestión permite a las empresas identificar, evaluar y mitigar los riesgos dentro de la organización, no solo refuerza la seguridad de la información, sino que también fomenta la concienciación y la colaboración, lo que beneficia a empleados y directivos al proporcionar una mejor postura de seguridad para la empresa.

1.4.2 Establecimiento de requerimientos

En el proceso de establecimiento de requisitos para la gestión de riesgos de seguridad de la información en la empresa, se pretende implantar requisitos que aborden aspectos cruciales para que la gestión de riesgos sea proactiva, eficaz y alineada con las mejores prácticas internacionales.

1. **Definición del Alcance:**
    - La organización deberá establecer y documentar claramente el alcance de su sistema de gestión de riesgos de seguridad de la información, identificando los límites y contextos pertinentes.
2. **Identificación de Activos:**
    - La organización deberá mantener un inventario actualizado de todos los activos de información, incluyendo procesos, datos, sistemas, personal y recursos físicos.
3. **Tasación de Activos:**
    - Se deben establecer métodos y criterios claros para la tasación de activos, considerando su importancia en términos de confidencialidad, integridad y disponibilidad.
4. **Identificación de Amenazas y Vulnerabilidades:**
    - Se deberá implementar procesos para identificar y documentar amenazas y vulnerabilidades relevantes para sus activos de información.

5. **Evaluación de Riesgos:**
    - Se deberá realizar una evaluación sistemática de los riesgos, considerando la probabilidad e impacto, para determinar la magnitud y prioridad de cada riesgo.
6. **Definición de Controles de Seguridad:**
    - Se deberá definir controles de seguridad de los activos, que aborden de manera específica los riesgos identificados.
7. **Formulación de Propuestas de Mejora:**
    - Se deberá proponer estrategias y controles específicos para mitigar los riesgos identificados, asegurando una protección adecuada de los activos.
8. **Comunicación de Resultados:**
    - La comunicación de los resultados de la evaluación de riesgos deberá ser clara, detallada y comprensible.
9. **Evaluación de la gestión de riesgos a expertos en el área:**
    - Se realizará una encuesta a un grupo seleccionado de expertos en el área para evaluar si la gestión de riesgos cumple con los aspectos de la norma ISO/IEC 27005 y la metodología NIST-SP 800-30.

CAPÍTULO II. DESARROLLO DEL PROTOTIPO

2.1 Definición del prototipo

En la siguiente figura 5 se puede observar el proceso de gestión de riesgos de seguridad de la información, basados en la combinación de en la ISO 27005 y la metodología NIST SP 800-30. Se inicia con la definición precisa del alcance y la identificación detallada de activos, como también la evaluación de riesgos que se lleva a cabo considerando la probabilidad y el impacto, respaldado por la elaboración de informes detallados. La formulación de resultados se centra en controles específicos, asegurando una propuesta de mejoras efectiva respaldada por normas internacionales. Este enfoque proporciona una base sólida para gestionar los riesgos de la seguridad de la información dentro de la organización.

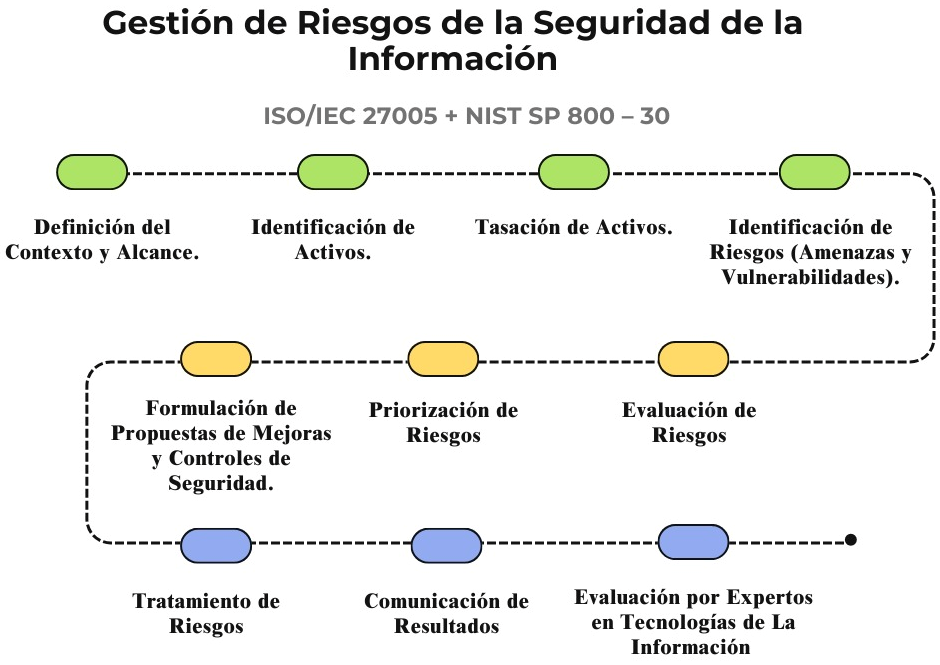


Figura 5 *Prototipo de la gestión de riesgos de la seguridad de la información*

2.2 Metodología de desarrollo del prototipo

2.2.1 Enfoque, alcance y diseño de investigación

Este proyecto adoptó un enfoque cuantitativo que permite gestionar los riesgos en la seguridad de la información de la empresa. Se basó en la recopilación y el análisis de datos que permitieron medir objetivamente la seguridad de la información, identificando los riesgos y proporcionando recomendaciones específicas. Las métricas de rendimiento obtenidas durante este proceso sirvieron de base para comprobar la hipótesis propuesta y evaluar si se cumplen los aspectos de las normas y estándares internacionales utilizados.

El alcance de esta investigación se inicia con un estudio descriptivo centrado en comprender en detalle los procesos actuales de gestión de riesgos en la empresa planteada. Posteriormente, el estudio avanzó hacia un enfoque correlacional con el propósito de demostrar que la implantación de una gestión de riesgos puede influir positivamente en la mejora de la seguridad de la información. El alcance de esta investigación permitió no solo describir los procesos existentes, sino también establecer relaciones entre la propuesta de controles y mejoras y los resultados observados en términos de seguridad de la información.

El diseño de la investigación se planteó como cuasi experimental, con el propósito de validar la hipótesis centrada en el cumplimiento de las normas de la gestión de riesgos de la seguridad de la información a través de un grupo de expertos en el área de TI ajenos a la organización, trabajando para mitigar los riesgos dentro de la empresa.

2.2.2 Unidades de análisis

Población (universo)

La población mostrada en la tabla 5 que se utilizó para esta investigación está compuesta por el personal de la empresa, que asciende a 10 individuos, y está estructurada de la siguiente manera.

Tabla 5 *Población del personal de la empresa*

Personal de la Empresa	
Gerente General	1 personas
Área de Tecnologías	2 personas
Área de Contabilidad	2 personas
Área de Operadores	3 personas
Área de Auxiliares	2 personas

Muestra

Dado que la población de estudio está conformada por menos de 30 individuos, se adoptó un enfoque particular en la selección de la muestra. En este caso, la muestra, por conveniencia, se establecerá con el mismo tamaño que la población, representando proporcionalmente el 33.33%

del total de elementos. Esto se traduce en una muestra compuesta por 10 individuos, lo que facilitó un análisis detallado y representativo de toda la población.

2.2.3 Técnicas e instrumentos de recopilación de datos

En el marco de la gestión de riesgos de seguridad de la información, la técnica y los instrumentos de recolección de datos se basaron en una serie de instrucciones para la recolección de datos, que incluyen:

.

- Revisión documental, analizando manuales de seguridad, informes previos de incidentes y cualquier documentación relevante.
- Un análisis detallado de la información existente, incluyendo reportes de incidentes pasados.

Este enfoque permitió comprender los últimos incidentes y procedimientos actuales para la gestión de riesgos en la empresa, con la finalidad de identificar áreas críticas más susceptibles a amenazas y establecer una base para la implementación de mejoras en la seguridad de la información.

2.2.4 Técnicas de procesamiento de datos para la obtención de resultados

Este proyecto aplica métodos que se centraron en herramientas visuales, como gráficos, documentos, estadísticas e informes. Estas herramientas proporcionaron un enfoque para analizar la información recogida durante el proceso de gestión de riesgo. Los gráficos permitieron la representación visual de patrones y tendencias clave, facilitando una comprensión rápida y eficaz de la complejidad de los datos. Los documentos, como los manuales de seguridad y las políticas existentes, sirvieron como fuentes fundamentales para contextualizar la información y establecer referencias en el análisis. Además, se utilizaron análisis estadísticos para evaluar la magnitud de los riesgos identificados. Los informes proporcionaron información enriqueciendo el análisis con las perspectivas directas del personal implicado. Este enfoque de la herramientas visuales y analíticas garantizó una interpretación completa de la información, apoyando decisiones y recomendaciones basadas en la gestión de riesgos informáticos.

2.2.5 Metodología o métodos específicos

Para realizar el presente trabajo, se utilizaron las metodologías NIST SP 800-30 y la norma ISO/IEC 27005, que ayudan a la gestión de riesgos en la organización al mejorar la seguridad de la información de la empresa mediante el uso de mejores prácticas.
La metodología de gestión de riesgos más utilizada es el NIST SP 800-30, que ayuda a las empresas a mejorar sus capacidades para evitar, identificar y responder a los ciberataques. Esta estrategia se emplea comúnmente para disminuir la exposición al riesgo, el proceso de gestión de riesgos utilizando el NIST SP 800-30 abarca varios pasos secuenciales[35]. Según su planteamiento, la metodología consta con fases de identificación de riesgos, fases de mitigación de riesgos y una fase de evaluación de riesgos, todas ellas estructuradas y adaptadas para garantizar la seguridad y la gestión de riesgos de seguridad de la información. En la figura 6 se puede observar la estructura que está conformada la metodología NIST SP 800-30.

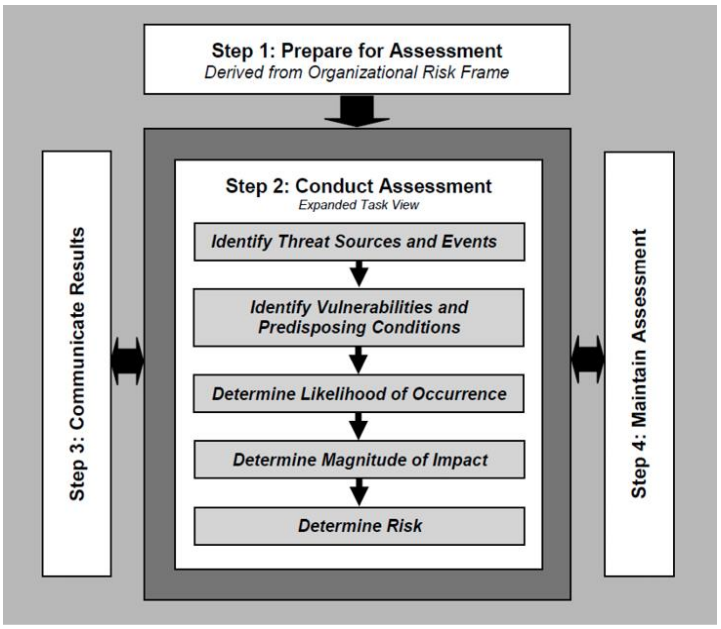


Figura 6 *Metodología NIST SP 800-30[29]*

La norma internacional ISO 27005 está compuesta por procesos de gestión de riesgos de la información que consta de siete elementos principales: instalación del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, consultoría del riesgo, monitoreo del riesgo y revisión del riesgo[39]. Según la norma ISO/IEC, la figura 7 muestra un enfoque de gestión de riesgos de ciberseguridad, el procedimiento genera suficiente información para establecer las necesarias para reducir los riesgos a un nivel aceptable, el trabajo está terminado y se puede comenzar el tratamiento de los riesgos. la información es insuficiente, se realiza la evaluación de riesgos[40].

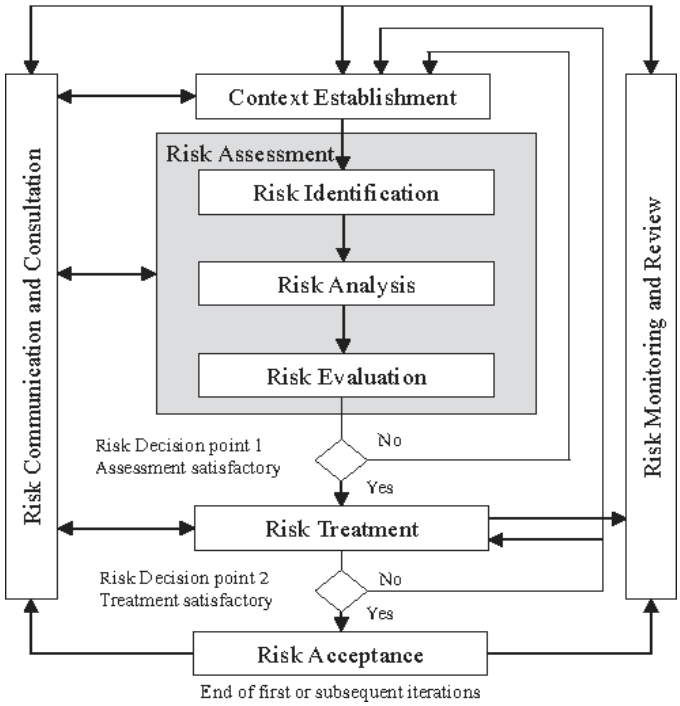


Figura 7 *Norma internacional ISO 27005[40]*

2.2.6 Herramientas y/o Materiales

La tabla 6 contiene las herramientas que se emplearon en el desarrollo de este proyecto.

Tabla 6 Herramientas y/o Materiales

Categorías	Herramientas y/o Materiales
Normas y Estándares Internacionales	• ISO/IEC 27001 • ISO/IEC 27002 • ISO/IEC 27005
Metodologías	• NIST SP 800-30 • Delphi
Encuestas	• Google Forms • Gmail

2.3 Desarrollo del prototipo

2.3.1 Definición del Contexto y Alcance

Descripción general de la Empresa

Reseña Histórica

La empresa fue fundada el 7 de abril de 2021 en la ciudad de Machala, Ecuador, es el resultado del esfuerzo conjunto de tres accionistas visionarios. Desde sus inicios, la compañía se ha destacado en la industria de la tecnología, enfocándose en servicios como la Asistencia en Desarrollo de Proyectos, Call Center Inteligente y Desarrollo de Software y Aplicaciones.

Con un enfoque claro en la innovación y la excelencia en el servicio al cliente, la empresa ha logrado posicionarse como un referente en su sector en la región. Su compromiso con la calidad y la satisfacción del cliente ha sido fundamental para su crecimiento continuo y su éxito en un mercado altamente competitivo.

A lo largo de los años, la empresa ha demostrado su capacidad para adaptarse a las cambiantes demandas del mercado y aprovechar las oportunidades emergentes en la industria de la tecnología. Su equipo altamente capacitado y su enfoque en la mejora continua le han permitido mantenerse a la vanguardia de la innovación y seguir ofreciendo soluciones a sus clientes.

Objetivo Estratégico

Nuestro objetivo es mantener altos estándares de disciplina, actitud, calidad y empatía en todas nuestras operaciones. Nos esforzamos por superar expectativas, ofreciendo productos y servicios de calidad, mientras nos comprometemos a entender y apoyar las necesidades de nuestros clientes y comunidad.

Misión

La empresa tiene como misión propia “Somos una empresa que ofrecemos diferentes servicios para el sector empresarial, brindando soluciones diseñadas a las medidas de sus necesidades y en tiempo real, a través de una atención de excelencia, optimización de recursos e innovación constante”.

Visión

La empresa tiene como visión “Ser reconocidos como una de la mejores que brinde diferentes servicios a nivel nacional e internacional, con tecnología de punta y equipo humano altamente calificado”.

Organigrama

La siguiente figura 8 representa visualmente la estructura organizativa de la empresa, demostrando la relación entre los distintos departamentos de la organización. Este diagrama proporciona una visión clara y ordenada de la distribución de responsabilidades y autoridades, permitiendo una fácil comprensión de la estructura interna de la empresa.

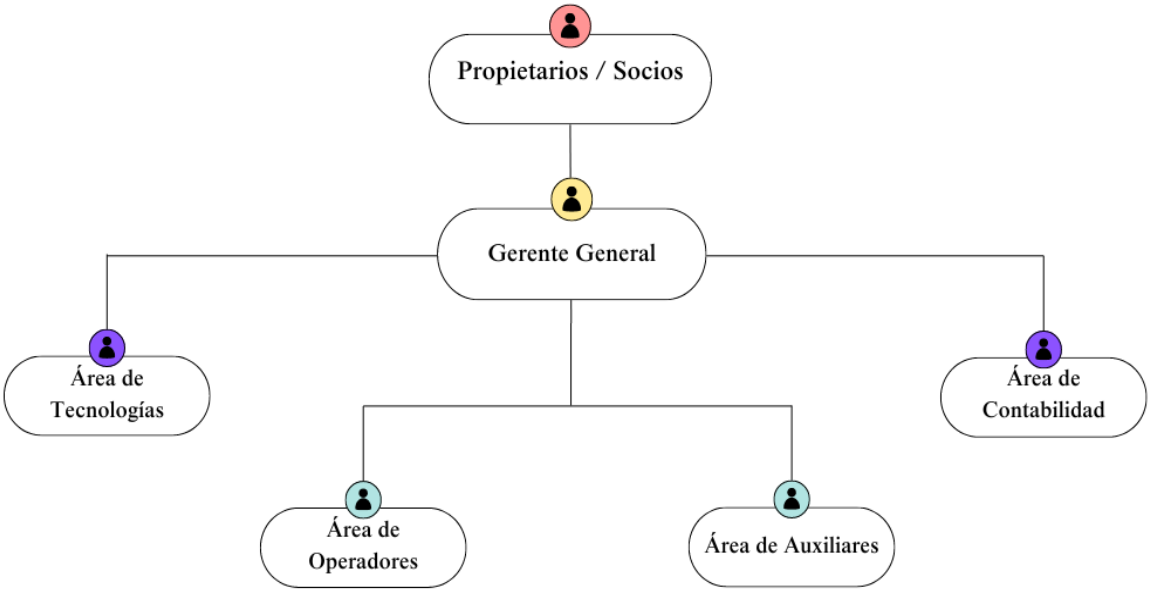


Figura 8 *Estructura organizativa de la empresa*

Alcance

En el desarrollo del proyecto de gestión de riesgos para la seguridad de la información en la empresa, se estableció un claro alcance que permitió aplicar estrategias de seguridad adaptadas a las necesidades específicas de la organización alineadas con normativas y estándares

internacionales. Esto implicó la identificación, evaluación y propuesta de mejoras destinadas a mitigar los riesgos críticos que puedan poner en peligro los activos y la integridad de la empresa.

2.3.2 Identificación

Comité de Seguridad de la Información

En la tabla 7 se encuentra el comité de seguridad de la información, conformado por 3 miembros del personal de la empresa y 2 miembros externos, se encarga de definir valores durante toda la gestión de riesgos y también se encarga de la aprobación de todas las etapas de la gestión de riesgos.

__Tabla 7__ Comité de Seguridad de la Información

Cargo	Nombre y Apellido
Gerente General	Eco. Danessa Serrano
Área de TI	Ing. Milton Valarezo Pardo
Área de Operadores	Srta. Mayerli Balcázar
Desarrollador de Gestión de Riesgos	Sr. Edwin Luzuriaga Rey
Desarrollador de Gestión de Riesgos	Sr. Juan Marín Ramon

Identificación de Activos

Para el registro de los activos que se identificaron, se procedió a clasificarlos en categorías de software, hardware, redes y comunicación, personal de la empresa y servicios, permitiendo tener un orden y una idea clara de los activos involucrados en la gestión de riesgos. El Anexo 1 evidencia que se estuvo identificando los activos personalmente en la empresa. A continuación, en la tabla 8 se detallan los siguientes activos.

Tabla 8 *Registro de activos generales*

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN					
Nro. Activo	**Sub Proceso**	**Tipo de Activo**	**Nombre del Activo**	**Descripción del Activo**	**Ubicación**
000001	Infraestructura	Hardware	CPU CORE I5 4TH GEN 4GB 500 GB HDD DVD-RW WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED- MÁS TECLADO	Computadora de escritorio con procesador Core i5 de 4ta generación, 4GB de RAM, disco duro de 500GB, unidad de DVD-RW, sistema operativo Windows 10 Pro, monitor de 19 pulgadas, y se incluye un mouse y teclado nuevos. Utilizado para tareas generales.	Área de Operadores
000002		Hardware	COMPUTADOR TODO EN 1 21-B0002LA CELERON 4GB 1TB 20.7 PLG WINDOWS 10	Computadora todo en uno con procesador Celeron, 4GB de RAM, disco duro de 1TB, pantalla de 20.7 pulgadas y sistema operativo Windows 10. Asignado para el uso en el departamento de gerencia.	Gerente General
000003		Hardware	CPU CORE I5 4TH GEN 4GB 500 GB HDD DVD-RW-WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED. - CONTADORA	Computadora de escritorio con procesador Core i5 de 4ta generación, 4GB de RAM, disco duro de 500GB, unidad de DVD-RW, sistema operativo Windows 10 Pro, monitor de 19 pulgadas, y se incluye un mouse	Área de Contabilidad

				y teclado nuevos. Utilizado para tareas generales.	
000004		Hardware	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS) MAS TECLADO QUASAD COMPUTER QC-4400U Y MAUSE	Torre de computadora con fuente de alimentación de 750W, 2 puertos USB 2.0, salida de audio. Utilizado como servidor de llamadas. Se incluye teclado y mouse.	Área de Tecnologías
000005		Hardware	CPU CORE I7 16GB 500 GB SSD WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED.	Computadora de escritorio con procesador Core i5 de 4ta generación, 4GB de RAM, disco duro de 500GB, unidad de DVD-RW, sistema operativo Windows 10 Pro, monitor de 19 pulgadas, y se incluye un mouse y teclado nuevos. Utilizado para tareas generales.	Área de Tecnologías
000006		Hardware	CPU CORE I5 4TA GENERACION 4GB, 500 GB	Computadora de escritorio con procesador Core i5 de 4ta generación, 4GB de RAM, disco duro de 500GB, unidad de DVD-RW, sistema operativo Windows 10 Pro, monitor de 19 pulgadas.	Área de Operadores
000007		Hardware	CELULAR SAMSUNG A04E SM-A04EM	Teléfono móvil Samsung modelo A04E en color azul.	Área de Operadores

000008	Redes y comunicación	Redes	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Teléfono Yeanlink de una línea, modelo YE-SIP-T30-E2	Gerente General
000009		Redes	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Teléfono Yeanlink de una línea, modelo YE-SIP-T30-E2	Área de Operadores
000010		Redes	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Teléfono Yeanlink de una línea, modelo YE-SIP-T30-E2	Área de Tecnologías
000011		Redes	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM- OFICINA	Cámara de seguridad IP marca EZVIZ, modelo Tubo Sellada, resolución de 2MP, lente de 4mm. Instalada en la oficina.	Área de Operadores
000012		Redes	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Cámara de seguridad IP marca EZVIZ, modelo Pantil, resolución de 2MP, lente de 2.8mm.	Área de Contabilidad
000013		Redes	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Cámara de seguridad IP marca EZVIZ, modelo Pantil, resolución de 2MP, lente de 2.8mm.	Área de Tecnologías
000014		Redes	NVR DE 4CH CAPACIDAD 20MB 1HDD	Grabador de video en red con capacidad para 4 canales y 1 disco duro de 20MB.	Área de Operadores
000015		Redes	Cerradura Biométrica Inteligente X2 Tuya Smart desbloqueo	Cerradura inteligente biométrica de marca Tuya Smart, con capacidad de	Matriz

				desbloqueo mediante huella digital. Dos unidades.	
000016		Redes	TELÉFONO IP 1 LINEAS POE	Teléfono IP de una línea con alimentación a través de Ethernet (PoE).	Área de Contabilidad
000017		Redes	TELÉFONO IP 1 LINEAS POE	Teléfono IP de una línea con alimentación a través de Ethernet (PoE).	Área de Operadores
000018		Redes	16- PORT GIGABIT RACKMOUNT SWITCH	Switch de montaje en rack con 16 puertos Gigabit Ethernet.	Área de Tecnologías
000019		Redes	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM	Gateway Openvox para 8 canales GSM.	Área de Tecnologías
000020	Software Informático	Software	ISSABEL	Plataforma web para recopilar grabaciones e información del cliente.	Área de Tecnologías
000021		Software	FORMULARIO GENERAL	Plataforma para registrar información del cliente.	Matriz
000022	Talento Humano	Personal	GERENTE GENERAL	Personal de alta dirección encargado de la gestión general de la empresa.	Matriz
000023		Personal	PERSONAL DE TECNOLOGÍAS	Personal especializado en tecnologías de la información.	Matriz
000024		Personal	PERSONAL DE CONTABILIDAD	Personal encargado de las operaciones contables de la empresa.	Matriz

000025		Personal	PERSONAL DE OPERACIONES	Personal encargado de las operaciones diarias de la empresa.	Matriz
000026		Personal	PERSONAL AUXILIAR	Personal de apoyo en diversas áreas de la empresa.	Matriz
000027	Servicios y Procesos	Servicios	ASISTENCIA DE DESARROLLO DE PROYECTOS	Maximizar la eficiencia y la efectividad en la ejecución de proyectos, asegurando que se alcancen los objetivos establecidos dentro del plazo y el presupuesto definidos.	Matriz
000028		Servicios	CALL CENTER INTELIGENTE	Sistema de enrutamiento inteligente que dirige las llamadas al agente más adecuado según diversos criterios, como la habilidad, la disponibilidad y la prioridad del cliente.	Matriz
000029		Servicios	DESARROLLO DE SOFTWARE Y APLICACIONES	Abarca todo el ciclo de vida del desarrollo de software, desde la concepción de la idea hasta el mantenimiento y la actualización continua.	Matriz

2.3.3 Tasación de Activos

Para llevar a cabo la tasación de activos en la gestión de riesgos de seguridad de la información, se buscó una evaluación del impacto de cada componente crítico para la organización. Este proceso, apoyado en una escala, simplifica la evaluación cuantitativa de los activos, permitiendo asignar niveles de riesgo claros. Cada activo, desde el hardware, software, redes, servicios y el personal, se clasifica teniendo en cuenta su impacto potencial en aspectos fundamentales como la confidencialidad, la integridad y la disponibilidad. Además, se puede evidenciar en el Anexo 2 la tasación de los activos dentro de la empresa.

La estrategia seleccionada para realizar la evaluación adopta en un enfoque cuantitativo, utilizando una escala de tres niveles para caracterizar la gravedad del impacto, asignando valores representativos de "bajo, medio, alto".

Para comprender mejor los criterios de cálculo de la valoración del impacto según la confidencialidad, se gestionó según la tabla 9**.**

Tabla 9 *Nivel de Confidencialidad*

Nivel	Valor	Confidencialidad (C)
Bajo	1	La difusión de información sin la debida autorización tiene un efecto nulo en la empresa.
Medio	2	La difusión de información sin la debida autorización tiene un limitado en la empresa.
Alto	3	La difusión de información sin la debida autorización tiene un efecto critico en la empresa.

Para comprender mejor los criterios de cálculo de la valoración del impacto según la integridad, se gestionó según la tabla 10**.**

Tabla 10 *Nivel de Integridad*

Nivel	Valor	Integridad (I)
Bajo	1	La eliminación o alteración no autorizada de información tiene un impacto reducido en la empresa.
Medio	2	La eliminación o alteración no autorizada de información tiene un impacto importante en la empresa.
Alto	3	La eliminación o alteración no autorizada de información tiene un impacto grave en la empresa.

Para comprender mejor los criterios de cálculo de la valoración del impacto según la disponibilidad, se gestionó según la tabla 11**.**

Tabla 11 Nivel de Disponibilidad

Nivel	Valor	Disponibilidad (D)
Bajo	1	La interrupción del acceso a la información o a los sistemas puede tener un efecto mínimo en la empresa.
Medio	2	La interrupción del acceso a la información o a los sistemas puede tener un efecto importante en la empresa.
Alto	3	La interrupción del acceso a la información o a los sistemas puede tener un efecto grave en la empresa.

El cálculo del impacto consiste en obtener la media a partir del valor asignado según la confidencialidad, la integridad y la disponibilidad. Para calcular la valoración del impacto, se utilizó la siguiente fórmula.

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

Con respecto a las tablas mencionadas, la confidencialidad, la integridad y la disponibilidad, son los aspectos que se tomaron en cuenta para la valoración del impacto, tal y como se puede observar en la tabla 12.

Tabla 12 Tasación de los activos

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN							
Nro. Activo	Nombre de Activo	Tipo de Soporte	Ubicación	Valoración del impacto			
				C	I	D	VA
000001	COMPUTADOR (CPU CORE I5 4TH GEN 4GB 500 GB)	Físico y Lógico	Área de Operadores	3	3	3	3
000002	COMPUTADOR TODO EN 1 21-B0002LA CELERON 4GB 1TB	Físico y Lógico	Gerente General	3	3	3	3
000003	COMPUTADOR (CPU CORE I5 4TH GEN 4GB 500 GB)	Físico y Lógico	Área de Contabilidad	3	3	3	3
000004	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS)	Físico y Lógico	Área de Tecnologías	3	3	3	3
000005	CPU CORE I7 16GB 500 GB SSD WIN 10	Físico y Lógico	Área de Tecnologías	3	3	3	3
000006	CPU CORE I5 4TA GENERACION 4GB, 500 GB	Físico y Lógico	Área de Operadores	3	3	3	3
000007	CELULAR SAMSUNG A04E SM-A04EM	Físico y Lógico	Área de Operadores	2	1	2	1,66666667
000008	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Físico y Lógico	Gerente General	3	3	3	3
000009	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Físico y Lógico	Área de Operadores	2	2	2	2

000010	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Físico y Lógico	Área de Tecnologías	1	2	3	2
000011	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM-OFICINA	Físico y Lógico	Área de Operadores	2	3	3	2,66666667
000012	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Físico y Lógico	Área de Contabilidad	2	3	3	2,66666667
000013	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Físico y Lógico	Área de Tecnologías	2	3	3	2,66666667
000014	NVR DE 4CH CAPACIDAD 20MB 1HDD	Físico y Lógico	Área de Operadores	3	3	3	3
000015	CERRADURA BIOMÉTRICA INTELIGENTE X2 TUYA SMART DESBLOQUEO	Físico y Lógico	Matriz	3	3	3	3
000016	TELÉFONO IP 1 LINEAS POE	Físico y Lógico	Área de Contabilidad	3	3	3	3
000017	TELÉFONO IP 1 LINEAS POE	Físico y Lógico	Área de Operadores	3	3	3	3
000018	16- PORT GIGABIT RACKMOUNT SWITCH	Lógico	Área de Tecnologías	3	3	3	3
000019	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM	Lógico	Área de Tecnologías	3	3	3	3
000020	ISSABEL	Lógico	Área de Tecnologías	3	3	3	3
000021	FORMULARIO GENERAL	Físico y Lógico	Matriz	3	3	3	3
000022	GERENTE GENERAL	Físico	Matriz	3	3	3	3
000023	PERSONAL DE TECNOLOGÍAS	Físico	Matriz	3	3	3	3
000024	PERSONAL DE CONTABILIDAD	Físico	Matriz	3	3	3	3
000025	PERSONAL DE OPERACIONES	Físico	Matriz	3	3	3	3
000026	PERSONAL AUXILIAR	Físico	Matriz	2	1	2	1,66666667
000027	ASISTENCIA DE DESARROLLO DE PROYECTOS	Lógico	Matriz	2	3	3	2,66666667
000028	CALL CENTER INTELIGENTE	Físico y Lógico	Matriz	3	3	3	3
000029	DESARROLLO DE SOFTWARE Y APLICACIONES	Lógico	Matriz	3	2	3	2,66666667

2.3.4 Identificación de Amenazas

Después de evaluar el impacto de cada activo, es de suma importancia identificar las amenazas potenciales y su origen, tal y como se observa en la tabla 13, ya que pueden representar una causa grave de daños a los activos de la empresa. Estas amenazas pueden variar desde ciberataques maliciosos hasta errores humanos involuntarios. Al comprender la naturaleza y el origen de estas amenazas, la empresa puede desarrollar estrategias de mitigación eficaces para proteger sus activos y salvaguardar la información vital contra cualquier daño o compromiso potencial.

__Tabla 13__ Identificación de Amenazas

IDENTIFICACIÓN DE AMENAZAS			
Nro. Activo	Nombre del Activo	Categoría	Amenazas
000001 000003 000006	3- COMPUTADOR (CPU CORE I5 4TH GEN 4GB 500 GB)	Hardware (Computadoras)	Errores de mantenimiento
000002	COMPUTADOR TODO EN 1 21-B0002LA CELERON 4GB 1TB		Fallas en el hardware
000005	CPU CORE I7 16GB 500 GB SSD WIN 10		Acceso remoto no autorizado
000004	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS)	Hardware (Servidor)	Fallas en el Hardware
			Ataque de DoS
			Explotación de configuración débil de seguridad
000007	CELULAR SAMSUNG A04E SM-A04EM	Hardware (Celular)	Pérdida o robo del dispositivo
			Fallas en el hardware

000008 000009 000010	3- TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Redes (Teléfonos IP)	Falsificación de llamadas (spoofing)
			Intercepción de llamadas
000016 000017	2- TELÉFONO IP 1 LINEAS POE		Manipulación de la configuración
000011	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM- OFICINA	Redes (Cámaras)	Acceso no autorizado
000012 000013	2 - CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM		Eliminación y alteración del dispositivo
000014	NVR DE 4CH CAPACIDAD 20MB 1HDD	Redes (Dispositivo de Grabación)	Acceso no autorizado
			Fallas en el hardware
000015	CERRADURA BIOMÉTRICA INTELIGENTE X2 TUYA SMART DESBLOQUEO	Redes (Dispositivo de Seguridad Inteligente)	Fuga de credenciales
			Acceso no autorizado

000018	16- PORT GIGABIT RACKMOUNT SWITCH	Redes (Infraestructura)	Firmware desactualizado
			Acceso lógico no autorizado a los servicios de red
000019	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM		Manipulación de la configuración
			Fallas en el hardware
000020	ISSABEL	Software	Acceso no autorizado
			Fallas en el software
000021	FORMULARIO GENERAL		Cambios no autorizados de la configuración del sistema
			Acceso no autorizado
000022	GERENTE GENERAL	Talento Humano	Ataque informático
000023	PERSONAL DE TECNOLOGÍAS		Alteración accidental de la información
000024	PERSONAL DE CONTABILIDAD		

000025	PERSONAL DE OPERACIONES		Divulgación de información
000026	PERSONAL AUXILIAR		
000027	ASISTENCIA DE DESARROLLO DE PROYECTOS	Servicios	Ataques de ingeniería social
			Acceso no autorizado a archivos de los proyectos
000028	CALL CENTER INTELIGENTE		Escuchas no autorizadas
			Fallas en la comunicación
000029	DESARROLLO DE SOFTWARE Y APLICACIONES		Fuga de información durante el proceso de despliegue
			Fallas en la validación de entradas

2.3.5 Identificación de Vulnerabilidades

La identificación de vulnerabilidades específicas es importante, ya que representan puntos de entrada potenciales para las amenazas. Es necesario reconocer y supervisar las vulnerabilidades, incluso aquellas que no tienen una amenaza correspondiente inmediata, para garantizar la correcta implementación de controles que minimicen los riesgos de explotación. Es relevante señalar que un control implementado incorrectamente o que funcione de forma defectuosa también puede constituir una vulnerabilidad en sí mismo. A continuación, en la tabla 14 se procedió a identificar vulnerabilidades de cada activo.

Tabla 14 *Identificación de Vulnerabilidades*

IDENTIFICACIÓN DE VULNERABILIDADES					
Nro. Activo	Cantidad	Nombre del Activo	Categoría	Amenazas	Vulnerabilidades
000001 000003 000006	3	COMPUTADOR (CPU CORE I5 4TH GEN 4GB 500 GB)	Hardware (Computadoras)	Errores de mantenimiento	Uso de antivirus obsoletos
					Inyección por malware
000002	1	COMPUTADOR TODO EN 1 21-B0002LA CELERON 4GB 1TB		Fallas en el hardware	Pérdida de datos
					Maltrato de equipos
					Puertos expuestos
000005	1	CPU CORE I7 16GB 500 GB SSD WIN 10		Acceso remoto no autorizado	Contraseñas débiles
					Credenciales expuestas
000004	1	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS)	Hardware (Servidor)	Ataque de DoS	Falta de mitigación de tráfico malicioso
					Infraestructura débil del protocolo de red
				Fallas en el Hardware	Pérdida de datos
					Daño físico o lógico
				Explotación de configuración débil de seguridad	Falta de cifrado
					Puertos abiertos innecesarios
					Servicios de red mal configurados
000007	1	CELULAR SAMSUNG A04E SM-A04EM	Hardware (Celular)	Pérdida o robo del dispositivo	Suplantación de identidad
					Fuga de información corporativa
				Fallas en el hardware	Pérdida de información
					Maltrato del dispositivo
000008 000009 000010	3	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Redes (Teléfonos IP)	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing
					Ataques de phishing
				Intercepción de llamadas	Tráfico sin cifrar
					Red inalámbrica no segura

000016 000017	2	TELÉFONO IP 1 LINEAS POE		Manipulación de la configuración	Redirección del tráfico de red Puertos Expuestos Falta de controles establecidos para la administración
000011	1	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM-OFICINA	Redes (Cámaras)	Acceso no autorizado	Contraseñas débiles Red inalámbrica no segura
000012 000013	2	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM		Eliminación y alteración del dispositivo	Daño físico o destrucción Dificultad para detectar intrusiones Compromiso de la integridad de la información
000014	1	NVR DE 4CH CAPACIDAD 20MB 1HDD	Redes (Dispositivo de Grabación)	Acceso no autorizado	Exposición a Internet Credenciales predeterminadas o débiles
				Fallas en el hardware	Daño físico Pérdida de información Fallo en la infraestructura de red
000015	1	Cerradura Biométrica Inteligente X2 Tuya Smart desbloqueo	Redes (Dispositivo de Seguridad Inteligente)	Fuga de credenciales	Ataques de fuerza bruta Falta de protocolo de privilegios
				Acceso no autorizado	Falla en la autenticación Contraseñas débiles o predeterminadas
000018	1	16- PORT GIGABIT RACKMOUNT SWITCH	Redes (Infraestructura)	Firmware desactualizado	Compatibilidad con protocolos obsoletos Falta de parches de seguridad
				Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos Acceso a través de puertos de gestión mal configurados
000019	1	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM		Manipulación de la configuración	Filtración de información confidencial Puertos expuestos Desactivación de protocolos de seguridad
				Fallas en el hardware	Daño físico o lógico Pérdida de comunicación entre dispositivos Mala manipulación de los equipos

000020	1	Issabel	Software	Acceso no autorizado	Contraseñas débiles o predeterminadas
					Falta de expiración adecuada de sesiones
				Fallas en el software	Inyección de código
					Mala utilización del sistema
000021	1	Formulario General		Cambios no autorizados de la configuración del sistema	Alteración de información
					Exposición de datos sensibles
					Falta de auditoría de cambios
				Acceso no autorizado	Falta de gestión de sesiones
					Contraseñas débiles o predeterminadas
000022	1	Gerente General	Talento Humano	Ataque informático	Instalación de software no autorizado
					Falta de entrenamiento en seguridad de la información
000023	2	Personal de Tecnologías		Alteración accidental de la información	Malentendidos en la comunicación
000024	2	Personal de Contabilidad			Falta de capacitación en procesos
000025	3	Personal de Operaciones		Divulgación de información	Fuga de datos confidenciales de los clientes
000026	2	Personal Auxiliar			Compartir credenciales de acceso
					Uso inapropiado de correo electrónico
000027	1	Asistencia de Desarrollo de Proyectos	Servicios	Ataques de ingeniería social	Correos electrónicos de phishing
					Llamadas fraudulentas
				Acceso no autorizado a archivos de los proyectos	Robo de documentación importante
					Filtración de información confidencial a terceros
000028	1	Call Center Inteligente		Escuchas no autorizadas	Privacidad de conversaciones comprometidas
					Fuga de información confidencial de los clientes
				Fallas en la comunicación	Falta de cifrado de extremo a extremo
					Interrupción del servicio
000029	1	Desarrollo de software y aplicaciones		Fuga de información durante el proceso de despliegue	Exposición de claves de las API
					Credenciales de bases de datos expuestas
				Fallas en la validación de entradas	SQL injection
					XSS (cross-site scripting)

2.3.6 Evaluación de Riesgos

La presente evaluación de activos en el proceso de valoración está diseñada para establecer un análisis que pueda definir el nivel de riesgos con mayor precisión. Esto implica la evaluación del impacto, el nivel de probabilidad de las amenazas y el nivel de vulnerabilidades asociadas a cada activo de la empresa, lo que permite una evaluación proactiva de los riesgos potenciales. Cada activo, desde el hardware, el software, redes y el talento humano, se somete a un riguroso escrutinio, considerando la asignación de niveles de riesgo en base a una escala que proporciona una clasificación cuantitativa que servirá de base para priorizar los riesgos de mayor escala e implementar estrategias de mitigación y fortalecimiento. Se puede observar en el Anexo 3 que se realizó la evaluación de riesgos junto al comité de seguridad de la información.

Criterios de Probabilidad

En las siguientes tablas 15 y 16, se detallaron criterios de probabilidad de ocurrencia para deducir y valorizar los niveles de amenazas y vulnerabilidades que puedan afectar a los diferentes activos involucrados. Estos criterios se basan en la probabilidad y la posibilidad de ocurrencia de eventos adversos, permitiendo una evaluación más precisa del riesgo potencial.

Criterio de probabilidad de ocurrencia de amenazas

Tabla 15 *Nivel de Amenaza*

Nivel de Amenaza			
Nivel	**Valor**	**Criterio por probabilidad**	**Periodicidad**
Bajo	1	La ocurrencia es menos probable	No ha sucedido
Medio	2	La ocurrencia es probable	Ha ocurrido o podría ocurrir en un período a largo plazo (1 año)
Alto	3	La ocurrencia es muy probable	Ha ocurrido o podría ocurrir en un período a corto plazo

Criterio de probabilidad de ocurrencia de vulnerabilidades

Tabla 16 *Nivel de Vulnerabilidad*

Nivel de Vulnerabilidad			
Nivel	**Valor**	**Criterio por probabilidad**	**Periodicidad**
Bajo	1	La ocurrencia es menos probable	No ha sucedido
Medio	2	La ocurrencia es probable	Ha ocurrido o podría ocurrir en un período a largo plazo (1 año)
Alto	3	La ocurrencia es muy probable	Ha ocurrido o podría ocurrir en un período a corto plazo

Criterio de Evaluación de Riesgos

Para realizar la evaluación de riesgos, la cual se encuentra en la tabla 18, se utilizó la combinación de la probabilidad de que ocurra una amenaza, la probabilidad de que se explote una vulnerabilidad y el valor del impacto del activo de la información (CID) determina el nivel de riesgo asociado a cada activo.

Nivel de Riesgo = CID + Nivel de amenazas + Nivel de vulnerabilidades

Según el valor de riesgo, descrito en la tabla 17, se determina el nivel de riesgo basado en la escala ya determinada.

Tabla 17 *Nivel de Riesgo*

Nivel de Riesgo	
Nivel	**Valor**
Bajo	1 – 3
Medio	4 - 8
Alto	9 - 20

Tabla 18 *Evaluación de Riesgos*

EVALUACIÓN DE RIESGOS												
Nro. Activo	Cantidad	Nombre Activo	Áreas	Categoría	Amenaza	Vulnerabilidades	Controles Implementados existentes	Impacto	Probabilidad		Cálculo de Evaluación de Riesgos	Nivel de Riesgo
								CID	Nivel de Amenazas	Nivel de Vulnerabilidades		
000001 000003 000006	3	COMPUTADOR (CPU CORE I5 4TH GEN 4GB 500 GB)	Área de Operadores	Hardware (Computadoras)	Errores de mantenimiento	Uso de antivirus obsoletos	Ninguno	3	2	2	12	Alto
			Área de Contabilidad			Inyección por malware	Parches de seguridad			1	6	Medio
000002	1	COMPUTADOR TODO EN 1 21-B0002LA CELERON 4GB 1TB	Gerencia		Fallas en el hardware	Pérdida de Datos	Almacenamiento en la nube de Google			1	6	Medio
						Maltrato de equipos	Ninguno			3	18	Alto
						Puertos expuestos	Ninguno			3	18	Alto
000005	1	CPU CORE I7 16GB 500 GB SSD WIN 10	Área de Tecnologías		Acceso remoto no autorizado	Contraseñas débiles	Ninguno		1	3	9	Alto
						Credenciales expuestas	Ninguno			3	9	Alto
#000004	1	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS)	Área de Tecnologías	Hardware (Servidor)	Ataque de DoS	Falta de mitigación de tráfico malicioso	Firewall	3	1	1	3	Bajo
						Infraestructura débil del protocolo de red	Tecnología de cifrado SSL			1	3	Bajo
					Fallas en el Hardware	Pérdida de Datos	Almacenamiento en la nube de Google		2	1	6	Medio
						Daño físico o lógico	Ninguno			3	18	Alto
					Explotación de configuración débil de seguridad	Falta de cifrado	Tecnología de cifrado SSL		2	1	6	Medio
						Puertos abiertos innecesarios	Firewall			3	18	Alto
						Servicios de red mal configurados	Revisión continua de los servicios de red			1	6	Medio
000007	1	CELULAR SAMSUNG A04E SM-A04EM	Área de Operadores	Hardware (Celular)	Pérdida o robo del dispositivo	Suplantación de identidad	Ninguno	1,66666667	1	1	2	Bajo

						Fuga de información corporativa	Ninguno			2	3	Bajo
					Fallas en el hardware	Pérdida de información	Ninguno		2	3	10	Alto
						Maltrato del dispositivo	Ninguno			3	10	Alto
000009 000010	2	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Área de Operadores	Redes (Teléfonos IP)	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	Autenticación fuerte para verificar la identidad de los usuarios y dispositivos	2	2	1	4	Medio
						Ataques de phishing	Software Antivirus			1	4	Medio
					Intercepción de llamadas	Tráfico sin cifrar	Tecnología de cifrado SSL		1	1	2	Bajo
						Red inalámbrica no segura	Red inalámbrica con cifrado WPA2 o WPA3			1	2	Bajo
			Área de Tecnologías		Manipulación de la configuración	Redirección de tráfico de red	Tecnología de cifrado SSL		1	1	2	Bajo
						Puertos Expuestos	Ninguno			3	6	Medio
						Falta de controles establecidos para la administración	Autenticación multifactor para acceder a la configuración del teléfono.			1	2	Bajo
#000008	1	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Gerencia		Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	Autenticación fuerte para verificar la identidad de los usuarios y dispositivos	2	2	1	4	Medio
						Ataques de phishing	Software Antivirus			1	4	Medio
000016 000017	2	TELÉFONO IP 1 LINEAS POE	Área de Operadores		Intercepción de llamadas	Tráfico sin cifrar	Tecnología de cifrado SSL		1	1	2	Bajo
						Red inalámbrica no segura	Red inalámbrica con cifrado WPA2 o WPA3			1	2	Bajo
			Área de Tecnologías		Manipulación de la configuración	Puertos Expuestos	Ninguno		1	3	6	Medio
						Redirección de tráfico de red	Tecnología de cifrado SSL			1	2	Bajo
						Falta de controles establecidos para la administración	Autenticación multifactor para acceder a la configuración del teléfono.			1	2	Bajo
000011	1	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM- OFICINA	Área de Operadores	Redes (Cámaras)	Acceso no autorizado	Contraseñas débiles	Ninguno	2,66666667	1	3	8	Medio
						Red inalámbrica no segura	Cifrado WPA2 o WPA3			1	3	Bajo
000012 000013	2	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Área de Contabilidad		Eliminación y alteración del dispositivo	Daño físico o destrucción	Ninguno		1	2	5	Medio
						Dificultad para detectar intrusiones	Ninguno			2	5	Medio
			Área de Tecnologías			Compromiso de la integridad de la información	Ninguno			2	5	Medio

000014	1	NVR DE 4CH CAPACIDAD 20MB 1HDD	Área de Operadores	Redes (Dispositivo de Grabación)	Acceso no autorizado	Exposición a Internet	Firewall	3	2	1	6	Medio
						Credenciales predeterminadas o débiles	Ninguno			3	18	Alto
					Fallas en el hardware	Pérdida de información	Almacenamiento en la nube de Google		1	1	3	Bajo
						Daño físico	Ninguno			2	6	Medio
						Fallo en la infraestructura de red	Revisión continua de los servicios de red			1	3	Bajo
000015	1	Cerradura Biométrica Inteligente X2 Tuya Smart desbloqueo	Matriz	Redes (Dispositivo de Seguridad Inteligente)	Fuga de credenciales	Ataques de fuerza bruta	Mecanismo de bloqueo temporal después de un número determinado de intentos fallidos	3	2	1	6	Medio
						Falta de protocolo de privilegios	Ninguno			2	12	Alto
					Acceso no autorizado	Falla en la autenticación	Contraseña y una verificación biométrica		1	2	6	Medio
						Contraseñas débiles o predeterminadas	Ninguno			3	9	Medio
000018	1	16- PORT GIGABIT RACKMOUNT SWITCH	Área de Tecnologías	Redes (Infraestructura)	Firmware desactualizado	Compatibilidad con protocolos obsoletos	Actualización regular del firmware	3	2	1	6	Medio
						Falta de parches de seguridad	Evaluación, la aplicación y la verificación regular de parches de seguridad.			1	6	Medio
					Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos	Ninguno		1	2	6	Medio
						Acceso a través de puertos de gestión mal configurados	Utilización de VLANs			1	3	Bajo
000019	1	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM			Manipulación de la configuración	Filtración de información confidencial	Firewall		1	1	3	Bajo
						Puertos expuestos	Ninguno			2	6	Medio
						Desactivación de protocolos de seguridad	Utilización de cifrado y autenticación fuerte			1	3	Bajo
					Fallas en el hardware	Pérdida de comunicación entre dispositivos	Revisión continua de los servicios de red		2	2	12	Alto
						Daño físico o lógico	Ninguno			2	12	Alto

						Mala manipulación de los equipos	Ninguno			3	18	Alto
000020	1	Issabel	Matriz	Software	Acceso no autorizado	Contraseñas débiles o predeterminadas	Ninguno	3	2	3	18	Alto
						Falta de expiración adecuada de sesiones	Ninguno			2	12	Alto
					Fallas en el software	Inyección de código	Funciones de enmascaramiento de datos		2	1	6	Medio
						Mala utilización del sistema	Formación y documentación clara sobre cómo utilizar correctamente el sistema.			2	12	Alto
000021	1	Formulario General	Matriz	Software	Cambios no autorizados de la configuración del sistema	Alteración de información	Ninguno		2	3	18	Alto
						Filtración de datos sensibles	Ninguno			3	18	Alto
						Falta de auditoría de cambios	Ninguno			3	18	Alto
					Acceso no autorizado	Falta de gestión de sesiones	Ninguno		3	3	27	Alto
						Contraseñas débiles o predeterminadas	Ninguno			3	27	Alto
000022	1	Gerente General	Gerencia	Talento Humano	Ataque informático	Instalación de software no autorizado	Aprobación previa para la instalación de software en los dispositivos de la empresa.	3	1	1	3	Bajo
						Falta de entrenamiento en seguridad de la información	Ninguno			2	6	Medio
000023	2	Personal de Tecnologías	Área de Tecnologías		Alteración accidental de la información	Malentendidos en la comunicación	Ninguno		2	3	18	Alto
000024	2	Personal de Contabilidad	Área de Contabilidad			Falta de capacitación en procesos	Formación detallada sobre los procesos internos de la empresa			2	12	Alto
000025	3	Personal de Operaciones	Área de Operadores		Divulgación de información	Fuga de datos confidenciales de los clientes	Ninguno		1	3	9	Alto
						Uso inapropiado de correo electrónico	Formación sobre el uso seguro del correo electrónico			2	6	Medio
000026	2	Personal Auxiliar	Matriz		Ataque Informático	Instalación de software no autorizado	Aprobación previa para la instalación de software en los dispositivos de la empresa.	1,66666667	1	1	2	Bajo
						Falta de entrenamiento en	Ninguno			3	5	Medio

						seguridad de la información						
					Alteración accidental de la información	Malentendidos en la comunicación	Cultura de comunicación abierta y transparente		2	2	7	Medio
						Falta de capacitación en procesos	Formación detallada sobre los procesos internos de la empresa			2	7	Medio
					Divulgación de información	Compartir credenciales de acceso	Ninguno		2	3	10	Alto
						Uso inapropiado de correo electrónico	Formación sobre el uso seguro del correo electrónico			2	7	Medio
000027	1	Asistencia de Desarrollo de Proyectos	Área de Tecnologías	Servicios	Ataques de ingeniería social	Correos electrónicos de phishing	Formación sobre el uso seguro del correo electrónico	2,66666667	1	1	3	Bajo
						Llamadas fraudulentas	Sistema de identificación de llamadas			2	5	Medio
					Acceso no autorizado a archivos de los proyectos	Robo de documentación importante	Cámaras de seguridad		1	1	3	Bajo
						Filtración de información confidencial a terceros	Ninguno			3	8	Medio
000029	1	Desarrollo de software y aplicaciones			Fuga de información durante el proceso de despliegue	Exposición de claves de las API	Controles de acceso basados en roles.		1	1	3	Bajo
						Credenciales de bases de datos expuestas	Ninguno			2	5	Medio
					Fallas en la validación de entradas	SQL injection	Procedimientos almacenados		1	1	3	Bajo
						XSS (cross-site scripting)	Ninguno			2	5	Medio
000028	1	Call Center Inteligente	Área de Operaciones		Ataques de ingeniería social	Correos electrónicos de phishing	Formación sobre el uso seguro del correo electrónico	3	2	1	6	Medio
						Llamadas fraudulentas	Sistema de identificación de llamadas			2	12	Alto
					Escuchas no autorizadas	Privacidad de conversaciones comprometidas	Acceso a las grabaciones de llamadas solo a personal autorizado		1	1	3	Bajo
						Fuga de información confidencial de los clientes	Ninguno			2	6	Medio

					Fallas en la comunicación	Falta de cifrado de extremo a extremo	Tecnología de cifrado SSL		2	1	6	Medio
						Interrupción del servicio	Ninguno			2	12	Alto

2.3.7 Priorización de los Riesgos

Conforme con el comité de evaluación de riesgos de la empresa, se ha determinado en la tabla 19 que la gestión de riesgos en materia de seguridad de la información se enfocará primordialmente en los activos involucrados dentro de las áreas de Operaciones y Tecnologías. Estas áreas han sido identificadas como críticas debido a su papel esencial en el funcionamiento diario y la infraestructura tecnológica de la organización. La intervención en estos activos se llevará a cabo de manera prioritaria, con el objetivo de salvaguardar la integridad, disponibilidad y confidencialidad de la información, así como proteger los activos de la empresa.

Tabla 19 *Priorización de los Riesgos*

Nro. Activo	Área	Activo
#000001	Área de Operadores	CPU CORE I5 4TH GEN 4GB 500 GB HDD DVD-RW WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED- MAS TECLADO
#000006		CPU CORE I5 4TA GENERACION 4GB, 500 GB
#000007		CELULAR SAMSUNG A04E SM-A04EM
#000009		TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2
#000011		CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM- OFICINA
#000014		NVR DE 4CH CAPACIDAD 20MB 1HDD
#000017		TELÉFONO IP 1 LINEAS POE
#000025		Personal de Operaciones
#000028		Call Center Inteligente
#000004	Área de Tecnologías	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS) MAS TECLADO QUASAD COMPUTER QC-4400U Y MAUSE
#000005		CPU CORE I7 16GB 500 GB SSD WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED.
#000010		TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2

#000013		CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-
#000018		16- PORT GIGABIT RACKMOUNT SWITCH
#000019		OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM
#000023		Personal de Tecnologías
#000027		Asistencia de Desarrollo de Proyectos
#000029		Desarrollo de Software y Aplicaciones
#000020		Issabel
#000021		Formulario General

2.3.8 Definición de Controles y Propuestas de Mejora

Una vez realizada con éxito la evaluación de riesgos, es necesario definir controles y propuestas de mejora para mitigar los riesgos identificados en los activos de la empresa. Tal y como se observa en la tabla 20, los objetivos de control y controles fueron tomados de la norma ISO/IEC 27002:2013 y a partir de esos controles se definieron las propuestas de mejora.

Tabla 20 *Controles y Propuesta de Mejoras*

Nro. Activo	Activo	Área	Amenaza	Vulnerabilidad	Objetivo de Control	Control sugerido	Propuesta de Mejoras
#000001	CPU CORE I5 4TH GEN 4GB 500 GB HDD DVD-RW WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED - MÁS TECLADO	Área de Operadores	Errores de Mantenimiento	Uso de antivirus obsoletos	A7.2/A12.2	A7.2.2/A12.2.1	A7.2.2.1/A12.2.1.1
				Inyección por malware	A12.2	A12.2.1	A12.2.1.2
			Fallas en el hardware	Pérdida de Datos	A11.2/A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Maltrato de equipos	A11.2	A11.2.1/A11.2.2/A11.2.4	A11.2.1.1/A11.2.2.1/A11.2.2.2/A11.2.4.1
				Puertos expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
			Acceso remoto no autorizado	Contraseñas débiles	A9.4	A9.4.3	A9.4.3.1
				Credenciales expuestas	A9.3/A9.4	A9.3.1/A9.4.2	A9.3.1.1/A9.4.2.1
#000004	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS) MAS TECLADO QUASAD COMPUTER QC-4400U Y MAUSE	Área de Tecnologías	Ataque de DoS	Falta de mitigación de tráfico malicioso	A13.1	A13.1.1	A13.1.1.2
				Infraestructura débil del protocolo de red	A13.1	A13.1.1/A13.1.2	A13.1.1.2/A13.1.2.1
			Fallas en el Hardware	Pérdida de Datos	A11.2-A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Daño físico o lógico	A11.2/A12.2	A11.2.2/A11.2.4/A11.2.6/A12.2.1	A11.2.2.1/A11.2.2.2A11.2.4.1/A11.2.6.1/A12.2.1.1
			Explotación de configuración débil de seguridad	Falta de cifrado	A13.2	A13.2.1	A13.2.1.1
				Puertos abiertos innecesarios	A12.6	A12.6.1	A12.6.1.1
				Servicios de red mal configurados	A13.1	A13.1.1/A13.1.2	A13.1.1.1/A13.1.2.2
#000005	CPU CORE I7 16GB 500		Errores de Mantenimiento	Uso de antivirus obsoletos	A7.2/A12.2	A7.2.2/A12.2.1	A7.2.2.1/A12.2.1.1

	GB SSD WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED.	Área de Tecnologías		Inyección por malware	A12.2	A12.2.1	A12.2.1.2
			Fallas en el hardware	Pérdida de Datos	A11.2/A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Maltrato de equipos	A11.2	A11.2.1/A11.2.2/A11.2.4	A11.2.1.1/A11.2.2.1/A11.2.2.2/A11.2.4.1
				Puertos expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
			Acceso remoto no autorizado	Contraseñas débiles	A9.4	A9.4.3	A9.4.3.1
				Credenciales expuestas	A9.3/A9.4	A9.3.1/A9.4.2	A9.3.1.1/A9.4.2.1
#000006	CPU CORE I5 4TA GENERACION 4GB, 500 GB	Área de Operadores	Errores de Mantenimiento	Uso de antivirus obsoletos	A7.2/A12.2	A7.2.2/A12.2.1	A7.2.2.1/A12.2.1.1
				Inyección por malware	A12.2	A12.2.1	A12.2.1.2
			Fallas en el hardware	Pérdida de Datos	A11.2/A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Maltrato de equipos	A11.2	A11.2.1/A11.2.2/A11.2.4	A11.2.1.1/A11.2.2.1/A11.2.2.2/A11.2.4.1
				Puertos expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
			Acceso remoto no autorizado	Contraseñas débiles	A9.4	A9.4.3	A9.4.3.1
				Credenciales expuestas	A9.3/A9.4	A9.3.1/A9.4.2	A9.3.1.1/A9.4.2.1
#000007	CELULAR SAMSUNG A04E SM-A04EM	Área de Operadores	Pérdida o robo del dispositivo	Suplantación de identidad	A9.3	A9.3.1	A9.3.1.2
				Fuga de información corporativa	A9.3	A9.3.1	A9.3.1.3
			Fallas en el hardware	Pérdida de información	A11.2/A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Maltrato del dispositivo	A11.2	A11.2.1/A11.2.4	A11.2.1.1/A11.2.4.1
#000009	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Área de Operadores	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	A12.6/A13.1	A12.6.1/A13.1.2	A12.6.1.2/A13.1.2.3
				Ataques de phishing	A13.1/A13.2	A13.1.2/A13.2.1/A13.2.4	A13.1.2.4/A13.2.1.2/A13.2.4.1
			Intercepción de llamadas	Tráfico sin cifrar	A13.2	A13.2.1	A13.2.1.1
				Red inalámbrica no segura	A9.1/A13.1	A9.1.2/A13.1.1/A13.1.2	A9.1.2.1/A13.1.1.2/A13.1.2.1

			Manipulación de la configuración	Redirección de tráfico de red	A9.1/A14.2	A9.1.2/A14.2.2	A9.1.2.1/A14.2.2.1
				Puertos Expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
				Falta de controles establecidos para la administración	A14.2	A14.2.2	A14.2.2.2
#000010	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Área de Tecnologías	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	A12.6/A13.1	A12.6.1/A13.1.2	A12.6.1.2/A13.1.2.3
				Ataques de phishing	A13.1/A13.2	A13.1.2/A13.2.1/A13.2.4	A13.1.2.4/A13.2.1.2/A13.2.4.1
			Intercepción de llamadas	Tráfico sin cifrar	A13.2	A13.2.1	A13.2.1.1
				Red inalámbrica no segura	A9.1/A13.1	A9.1.2/A13.1.1/A13.1.2	A9.1.2.1/A13.1.1.2/A13.1.2.1
			Manipulación de la configuración	Redirección de tráfico de red	A9.1/A14.2	A9.1.2/A14.2.2	A9.1.2.1/A14.2.2.1
				Puertos Expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
				Falta de controles establecidos para la administración	A14.2	A14.2.2	A14.2.2.2
#000011	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM-OFICINA	Área de Operadores	Acceso no autorizado	Contraseñas débiles	A9.4	A9.4.3	A9.4.3.1
				Red inalámbrica no segura	A9.1/A13.1	A9.1.2/A13.1.1/A13.1.2	A9.1.2.1/A13.1.1.2/A13.1.2.1
			Eliminación y alteración del dispositivo	Daño físico o destrucción	A11.2	A11.2.1/A11.2.3	A11.2.1.1/A11.2.3.1
				Dificultad para detectar intrusiones	A12.4	A12.4.1/A12.4.2	A12.4.1.1/A12.4.2.1
				Compromiso de la integridad de la información	A12.3	A12.3.1	A12.3.1.1
#000013	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Área de Tecnologías	Acceso no autorizado	Contraseñas débiles	A9.4	A9.4.3	A9.4.3.1
				Red inalámbrica no segura	A9.1/A13.1	A9.1.2/A13.1.1/A13.1.2	A9.1.2.1/A13.1.1.2/A13.1.2.1
			Eliminación y alteración del dispositivo	Daño físico o destrucción	A11.2	A11.2.1/A11.2.3	A11.2.1.1/A11.2.3.1
				Dificultad para detectar intrusiones	A12.4	A12.4.1/A12.4.2	A12.4.1.1/A12.4.2.1

				Compromiso de la integridad de la información	A12.3	A12.3.1	A12.3.1.1
#000014	NVR DE 4CH CAPACIDAD 20MB 1HDD	Área de Operadores	Acceso no autorizado	Exposición a Internet	A13.1	A13.1.1	A13.1.1.3
				Credenciales predeterminadas o débiles	A9.3/A9.4	A9.3.1/A9.4.2/A9.4.3	A9.3.1.1/A9.4.2.1/A9.4.3.1
			Fallas en el hardware	Pérdida de información	A11.2/A12.3	A11.2.7/A12.3.1	A11.2.7.1/A12.3.1.1
				Daño físico	A11.2	A11.2.1/A11.2.2/A11.2.4	A11.2.1.1/A11.2.2.1/A11.2.2.2/A11.2.4.1
				Fallo en la infraestructura de red	A13.1	A13.1.1/A13.1.2	A13.1.1.1/A13.1.2.2
#000017	TELÉFONO IP 1 LINEAS POE	Área de Operadores	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	A12.6/A13.1	A12.6.1/A13.1.2	A12.6.1.2/A13.1.2.3
				Ataques de phishing	A13.1/A13.2	A13.1.2/A13.2.1/A13.2.4	A13.1.2.4/A13.2.1.2/A13.2.4.1
			Intercepción de llamadas	Tráfico sin cifrar	A13.2	A13.2.1	A13.2.1.1
				Red inalámbrica no segura	A9.1/A13.1	A9.1.2/A13.1.1/A13.1.2	A9.1.2.1/A13.1.1.2/A13.1.2.1
			Manipulación de la configuración	Redirección de tráfico de red	A9.1/A14.2	A9.1.2/A14.2.2	A9.1.2.1/A14.2.2.1
				Puertos Expuestos	A12.6/A13.1	A12.6.1/A13.1.1	A12.6.1.1/A13.1.1.1
				Falta de controles establecidos para la administración	A14.2	A14.2.2	A14.2.2.2
#000018	16- PORT GIGABIT RACKMOUNT SWITCH	Área de Tecnologías	Firmware desactualizado	Compatibilidad con protocolos obsoletos	A7.2/A12.6	A7.2.2/A12.6.1	A7.2.2.1/A12.6.1.3
				Falta de parches de seguridad	A7.2	A7.2.2	A7.2.2.1
			Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos	A9.3/A9.4	A9.3.1/A9.4.2/A9.4.3	A9.3.1.1/A9.4.2.1/A9.4.3.1
				Acceso a través de puertos de gestión mal configurados	A12.4/A13.1	A12.4.1/A13.1.1	A12.4.1.2/A13.1.1.4

			Manipulación de la configuración	Filtración de información confidencial	A13.2	A13.2.1	A13.2.1.1
				Puertos expuestos	A13.1	A13.1.2	A13.1.2.5
				Desactivación de protocolos de seguridad	A13.1/A14.2	A13.1.2/A14.2.2	A13.1.2.2/A14.2.2.1
			Fallas en el hardware	Pérdida de comunicación entre dispositivos	A11.2	A11.2.3	A11.2.3.1
				Daño físico o lógico	A11.2/A12.2	A11.2.2/A11.2.4/A11.2.6/A12.2.1	A11.2.2.1/A11.2.2.2/A11.2.4.1/A11.2.6.1/A12.2.1.1
				Mala manipulación de los equipos	A11.2	A11.2.1/A11.2.4	A11.2.1.1/A11.2.1.2/A11.2.4.1
#000019	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM	Área de Tecnologías	Firmware desactualizado	Compatibilidad con protocolos obsoletos	A7.2/A12.6	A7.2.2/A12.6.1	A7.2.2.1/A12.6.1.3
				Falta de parches de seguridad	A7.2	A7.2.2	A7.2.2.1
			Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos	A9.3/A9.4	A9.3.1/A9.4.2/A9.4.3	A9.3.1.1/A9.4.2.1/A9.4.3.1
				Acceso a través de puertos de gestión mal configurados	A12.4/A13.1	A12.4.1/A13.1.1	A12.4.1.2/A13.1.1.4
			Manipulación de la configuración	Filtración de información confidencial	A13.2	A13.2.1	A13.2.1.1
				Configuración de puertos inseguros	A13.1	A13.1.2	A13.1.2.5
				Desactivación de protocolos de seguridad	A13.1/A14.2	A13.1.2/A14.2.2	A13.1.2.2/A14.2.2.1
			Fallas en el hardware	Pérdida de comunicación entre dispositivos	A11.2	A11.2.3	A11.2.3.1
				Daño físico o lógico	A11.2/A12.2	A11.2.2/A11.2.4/A11.2.6/A12.2.1	A11.2.2.1/A11.2.2.2/A11.2.4.1/A11.2.6.1/A12.2.1.1
				Mala manipulación de los equipos	A11.2	A11.2.1/A11.2.4	A11.2.1.1/A11.2.1.2/A11.2.4.1
#000020	Issabel	Área de Tecnologías	Acceso no autorizado	Contraseñas débiles o predeterminadas	A9.3/A9.4	A9.3.1/A9.4.2/A9.4.3	A9.3.1.1/A9.4.2.1/A9.4.3.1
				Falta de expiración adecuada de sesiones	A9.2/A9.4	A9.2.5/A9.4.2	A9.2.5.1/A9.4.2.2

			Fallas en el software	Inyección de código	A14.1	A14.1.1	A14.1.1.1
				Mala utilización del sistema	A7.2/A14.2	A7.2.2/A14.2.2	A7.2.2.2/A14.2.2.3
#000021	Formulario General	Área de Tecnologías	Cambios no autorizados de la configuración del sistema	Alteración de información	A12.1	A12.1.2	A12.1.2.1/A12.1.2.2
				Filtración de datos sensibles	A10.1/A13.2	A10.1.1/A13.2.4	A10.1.1.1/A13.2.4.1
				Falta de auditoría de cambios	A12.1	A12.1.2	A12.1.2.3
			Acceso no autorizado	Falta de gestión de sesiones	A9.2/A9.4	A9.2.5/A9.4.2	A9.2.5.1/A9.4.2.2
				Contraseñas débiles o predeterminadas	A9.3/A9.4	A9.3.1/A9.4.2/A9.4.3	A9.3.1.1/A9.4.2.1/A9.4.3.1
#000023	Personal de Tecnologías	Área de Tecnologías	Ataque Informático	Instalación de software no autorizado	A9.4/A12.5	A9.4.4/A12.5.1	A9.4.4.1/A12.5.1.1
				Falta de entrenamiento en seguridad de la información	A7.2	A7.2.2	A7.2.2.1/A7.2.2.2
			Alteración accidental de la información	Malentendidos en la comunicación	A7.2	A7.2.2	A7.2.2.3/A7.2.2.4
				Falta de capacitación en procesos	A7.2	A7.2.2	A7.2.2.1/A7.2.2.5
			Divulgación de información	Fuga de datos confidenciales de los clientes	A7.2/A13.2	A7.2.3/A13.2.4	A7.2.3.1/A7.2.3.2/A13.2.4.1
				Uso inapropiado de correo electrónico	A7.2	A7.2.2	A7.2.2.6
#000025	Personal de Operaciones	Área de Operadores	Ataque informático	Instalación de software no autorizado	A9.4/A12.5	A9.4.4/A12.5.1	A9.4.4.1/A12.5.1.1
				Falta de entrenamiento en seguridad de la información	A7.2	A7.2.2	A7.2.2.1/A7.2.2.2
			Alteración accidental de la información	Malentendidos en la comunicación	A7.2	A7.2.2	A7.2.2.3/A7.2.2.4
				Falta de capacitación en procesos	A7.2	A7.2.2	A7.2.2.1/A7.2.2.5
			Divulgación de información	Fuga de datos confidenciales de los clientes	A7.2/A13.2	A7.2.3/A13.2.4	A7.2.3.1/A7.2.3.2/A13.2.4.1

				Uso inapropiado de correo electrónico	A7.2	A7.2.2	A7.2.2.6
#000027	Asistencia de Desarrollo de Proyectos	Área de Tecnologías	Ataques de ingeniería social	Correos electrónicos de phishing	A7.2/A13.2	A7.2.2/A13.2.1	A7.2.2.7/A13.2.1.2
				Llamadas fraudulentas	A7.2	A7.2.2	A7.2.2.8
			Acceso no autorizado a archivos de los proyectos	Robo de documentación importante	A7.2/A9.1/A13.2	A7.2.3/A9.1.1/A13.2.4	A7.2.3.1/A7.2.3.2/A9.1.1.1/A13.2.4.1
				Filtración de información confidencial a terceros	A7.2/A13.2	A7.2.3/A13.2.4	A7.2.3.1/A7.2.3.2/A13.2.4.1
#000028	Call Center Inteligente	Área de Operadores	Ataques de ingeniería social	Correos electrónicos de phishing	A7.2/A13.2	A7.2.2/A13.2.1	A7.2.2.7/A13.2.1.2
				Llamadas fraudulentas	A7.2	A7.2.2	A7.2.2.8
			Escuchas no autorizadas	Privacidad de conversaciones comprometidas	A11.1	A11.1.5	A11.1.5.1
				Fuga de información confidencial de los clientes	A7.2/A13.2	A7.2.3/A13.2.4	A7.2.3.1/A7.2.3.2/A13.2.4.1
			Fallas en la comunicación	Falta de cifrado de extremo a extremo	A13.2	A13.2.1	A13.2.1.1
				Interrupción del servicio	A11.2	A11.2.2/A11.2.3/A11.2.4	A11.2.2.1/A11.2.2.2/A11.2.3.1/A11.2.4.1
#000029	Desarrollo de Software y Aplicaciones	Área de Tecnologías	Fuga de información durante el proceso de despliegue	Exposición de claves de las API	A13.2/A14.2	A13.2.4/A14.2.1	A13.2.4.1/A14.2.1.1
				Credenciales de bases de datos expuestas	A14.2	A14.2.1	A14.2.1.1/A14.2.1.2
			Fallas en la validación de entradas	SQL injection	A14.2	A14.2.1/A14.2.8	A14.2.1.3/A14.2.8.1
				XSS (cross-site scripting)	A14.2	A14.2.1/A14.2.8	A14.2.1.4/A14.2.1.5/A14.2.8.2

POLÍTICAS, CONTROLES Y PROPUESTA DE MEJORAS EN BASE A LA NORMA ISO/IEC 27002:2013

A7 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

A7.2 Durante la ejecución del empleo.

Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan[41].

A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.

Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo[41].

Propuesta de mejoras:

A7.2.2.1 Implementar un programa de concientización sobre seguridad que incluya sesiones de formación específicas sobre la identificación y el manejo de software, protocolos o procesos obsoletos. Se fomentará una cultura de seguridad donde todos los empleados comprendan su responsabilidad en la protección de la infraestructura de TI.

A7.2.2.2 Proporcionar programas de educación y formación en seguridad de la información para garantizar que los empleados comprendan las políticas, procedimientos y mejores prácticas relacionadas con el uso adecuado de los sistemas.

A7.2.2.3 Proporcionar capacitación regular en comunicación segura en materia de seguridad de la información para todo el personal de la organización. La capacitación incluye técnicas de comprensión de la terminología específica de seguridad de la información y promueve la comunicación efectiva, abierta y transparente entre el personal.

A7.2.2.4 Establecer canales de comunicación abiertos y transparentes para que los empleados puedan hacer preguntas, plantear inquietudes y solicitar aclaraciones sobre temas de generales. fomentando una cultura de apertura y colaboración para facilitar la comunicación efectiva en toda la organización.

A7.2.2.5 Desarrollar programas de capacitación específicos para todos los procesos, diseñados para proporcionar a los empleados el conocimiento y las habilidades necesarias para desempeñar sus funciones de manera segura y eficiente.

A7.2.2.6 Establecer que el correo electrónico solo debe utilizarse para fines comerciales legítimos y relacionados con el trabajo. Además, no se permite el uso del correo electrónico para actividades personales no relacionadas con el trabajo, como el envío de correos electrónicos personales o el acceso a sitios web no relacionados con el trabajo.

A7.2.2.7 Proporcionar capacitación periódica sobre el uso seguro y apropiado del correo electrónico, incluyendo la identificación de correos electrónicos de phishing y otras amenazas de seguridad.

A7.2.2.8 Proporcionar formación regular sobre los riesgos asociados con las llamadas fraudulentas y cómo identificarlas. Los empleados serán informados sobre las técnicas comunes utilizadas por los estafadores en llamadas telefónicas fraudulentas y se les enseñará cómo responder adecuadamente.

A7.2.3 Proceso disciplinario.

Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información[41].

Propuesta de mejoras:

A7.2.3.1 Establecer un proceso disciplinario claro y transparente para abordar los incumplimientos relacionados con la fuga de datos confidenciales.

A7.2.3.2 Definir las acciones disciplinarias apropiadas, que pueden incluir advertencias formales, suspensión temporal, terminación de empleo y acciones legales según la gravedad del incumplimiento.

A9 POLÍTICAS DE CONTROL DE ACCESO

A9.1 Requisitos del negocio para control de acceso.

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información[41].

A9.1.1 Política de control de acceso

Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información[41].

Propuesta de mejoras:

A9.1.1.1 Establecer sistemas de control de acceso lógico para restringir el acceso a personal autorizado a la documentación importante almacenada en oficinas, sistemas informáticos y bases de datos. Se asignarán permisos de acceso de manera específica y limitada, de acuerdo con los roles y responsabilidades de cada usuario.

A9.1.2 Política sobre el uso de los servicios de red

Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente[41].

Propuesta de mejoras:

A9.1.2.1 Establecer estándares de seguridad para todas las redes inalámbricas utilizadas en la organización que debe incluir la autenticación adecuada, el cifrado de datos, la segmentación de red y otras medidas de seguridad necesarias para proteger la integridad y la confidencialidad de la información transmitida a través de redes inalámbricas.

A9.2 Gestión de acceso de usuarios.

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios[41].

A9.2.5 Revisión de los derechos de acceso de usuarios.

Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares[41].

Propuesta de mejoras:

A9.2.5.1 Se deben realizar revisiones periódicas de los derechos de acceso de todo el personal, asegurando que los permisos de los usuarios sean apropiados para sus funciones actuales y que las sesiones de acceso expiren adecuadamente tras un período de inactividad.

A9.3 Responsabilidades del personal

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación[41].

A9.3.1 Uso de información de autenticación secreta.

Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta[41].

Propuesta de mejoras:

A9.3.1.1 Proporcionar capacitación regular al personal sobre la importancia de utilizar contraseñas seguras y sobre los riesgos asociados con las contraseñas comprometidas. Se enfatizará la necesidad de seguir las políticas de contraseñas establecidas por la organización.

A9.3.1.2 Promover el uso de aplicaciones de autenticación de doble factor confiables, como Google Authenticator o Microsoft Authenticator, para generar códigos de verificación, todos los empleados deben activar y configurar la autenticación de doble factor en sus dispositivos móviles corporativos utilizados para acceder a recursos críticos de la empresa.

A9.3.1.3 El personal encargado deberá hacerse con la responsabilidad de establecer un lugar fijo para mantener seguro el dispositivo, evitando así la pérdida o robo del mismo para salvaguardar la información corporativa de la empresa.

A9.4 Control de acceso a sistemas y aplicaciones.

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones[41].

A9.4.2 Procedimiento de ingreso seguro.

Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro[41].

Propuesta de mejoras:

A9.4.2.1 Proporcionar capacitación periódica al personal sobre la importancia de no exponer ni divulgar contraseñas debido al alto riesgo de comprometer la seguridad de la información de los datos de los clientes.

A9.4.2.2 Todos los sistemas de información deben estar configurados para establecer tiempos de sesión para el personal y administradores. Los tiempos de sesión deben basarse en las mejores prácticas de seguridad y en las necesidades operativas de la organización.

A9.4.3 Sistema de gestión de contraseñas.

Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas[41].

Propuesta de mejoras:

A9.4.3.1 Establecer requisitos para la complejidad de las contraseñas, como la inclusión de una longitud mínima de 8 caracteres sean alfanuméricos, símbolos, mayúsculas y minúsculas. A la vez establecer un intervalo de tiempo donde los usuarios deben cambiar sus contraseñas periódicamente.

A9.4.4 Uso de programas utilitarios privilegiados.

Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones[41].

Propuesta de mejoras:

A9.4.4.1 Establecer consecuencias claras para cualquier empleado que instale software no autorizado en los sistemas operativos, lo que puede incluir medidas disciplinarias según las políticas de la organización.

A10 POLÍTICAS DE CRIPTOGRAFÍA

A10.1 Controles criptográficos.

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información[41].

A10.1.1 Política sobre el uso de controles criptográficos.

Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información[41].

Propuesta de mejoras:

A10.1.1.1 Implementar herramientas de prevención de pérdida de datos (DLP) como Endpoint Protector, McAfee, etc. para monitorear y controlar la transferencia de datos sensibles dentro y fuera de la red de la organización.

A11 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

A11.1 Áreas seguras.

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización[41].

A11.1.5 Trabajo en áreas seguras.

Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras[41].

Propuesta de mejoras:

A11.1.5.1 Todas las conversaciones que involucren información confidencial o sensible deben realizarse exclusivamente dentro de las áreas seguras designadas.

A11.2 Equipos.

Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización[41].

A11.2.1 Política de ubicación y protección de los equipos.

Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado[41].

Propuesta de mejoras:

A11.2.1.1 Implementar medidas de protección física como también inspecciones regulares para verificar el estado y la funcionalidad del equipo, así como para identificar y abordar cualquier problema de seguridad o daño físico.

A11.2.1.2 Se deben llevar a cabo campañas periódicas de concientización para destacar la importancia de proteger los equipos de TI y fomentar una cultura de seguridad en toda la organización

A11.2.2 Servicios de suministro.

Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro[41].

Propuesta de mejoras:

A11.2.2.1 Establecer procedimientos claros para la respuesta a fallas de energía seleccionando un UPS con capacidad suficiente para mantener estos equipos operativos durante un tiempo determinado, permitiendo la transición a generadores de respaldo o el apagado seguro.

A11.2.2.2 Instalar generadores de respaldo para proporcionar energía continua en caso de interrupciones prolongadas del suministro eléctrico.

A11.2.3 Seguridad del cableado.

Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño[41].

Propuesta de mejoras:

A11.2.3.1 Todo cableado de red o energética debe ser instalado de manera segura para prevenir daños físicos. Se deben utilizar conductos y canalizaciones adecuadas para proteger el cableado contra daños o exposición a elementos externos. También se debe realizar inspecciones periódicas del cableado para identificar y abordar cualquier signo de deterioro.

A11.2.4 Mantenimiento de equipos.

Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas[41].

Propuesta de mejoras:

A11.2.4.1 Establecer un programa de mantenimiento regular para todos los equipos críticos, con el fin de garantizar su correcto funcionamiento y disponibilidad continua. Este programa deberá

incluir inspecciones periódicas, actualizaciones de software y hardware según sea necesario, así como la reparación o reemplazo oportuno de componentes defectuosos.

A11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones[41].

Propuesta de mejoras:

A11.2.6.1 Se debe implementar medidas de seguridad específicas para proteger los activos de información cuando sean utilizados fuera o dentro de las instalaciones de la empresa. Esto incluye el uso de conexiones seguras, cifrado de datos sensibles, autenticación de usuarios y dispositivos, y el uso de herramientas de gestión remota para garantizar la seguridad y la integridad de la información en todo momento.

A11.2.7 Disposición segura o reutilización de equipos.

Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización[41].

Propuesta de mejoras:

A11.2.7.1 Verificación de la eliminación segura de datos de todos los equipos antes de su disposición o reutilización. Esto incluye la realización de un proceso de borrado seguro o destrucción física de los medios de almacenamiento de datos, así como la documentación adecuada para demostrar que se han tomado las medidas necesarias para proteger la información confidencial antes de deshacerse de los equipos.

A12 POLÍTICAS DE SEGURIDAD EN EL ÁREA DE OPERACIONES

A12.1 Procedimientos operacionales y responsabilidades.

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información[41].

A12.1.2 Gestión de cambios

Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información[41].

Propuesta de mejoras:

A12.1.2.1 Se establece que el equipo de gestión de cambios es responsable de administrar el proceso de gestión de cambios y garantizar que se implementen controles efectivos para prevenir la alteración no autorizada de la información.

A12.1.2.2 Se establece que los empleados que utilicen los sistemas de información son responsables de informar cualquier actividad sospechosa que pueda indicar una posible alteración de la información.

A12.1.2.3 Se asignarán responsabilidades claras para la realización de auditorías de cambios, incluyendo la revisión de los registros de cambios y la identificación de posibles desviaciones o anomalías.

A12.2 Protección contra códigos maliciosos

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos[41].

A12.2.1 Controles contra códigos maliciosos

Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos[41].

Propuesta de mejoras:

A12.2.1.1 Programación de análisis periódicos configurando el software antivirus para que realice análisis periódicos del sistema en busca de posibles amenazas. Esto puede ayudar a detectar y eliminar malware de forma proactiva.

A12.2.1.2 Capacitación en concienciación sobre seguridad proporcionando formación al personal sobre las prácticas seguras de navegación por internet, descarga de archivos y apertura de correos electrónicos para reducir la probabilidad de caer en trampas de malware.

A12.3 Copias de respaldo

Objetivo: Proteger contra la perdida de datos[41].

A12.3.1 Controles de respaldo de información

Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada[41].

Propuesta de mejoras:

A12.3.1.1 Realizar copias de respaldo de la información crítica y comprobación de la misma. Esto puede incluir la programación regular de copias de seguridad automáticas, la verificación de la integridad de las copias de seguridad y la garantía de que las copias se almacenen de forma segura.

A12.4 Registro y seguimiento.

Objetivo: Registrar eventos y generar evidencia[41].

A12.4.1 Registro de eventos.

Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información[41].

Propuesta de mejoras:

A12.4.1.1 Implementar un procedimiento para el registro y almacenamiento seguro de todos los eventos de seguridad, incluyendo detalles relevantes como la fecha y hora, la naturaleza del evento, y la dirección IP involucrada.

A12.4.1.2 Utilizar herramientas de monitoreo de red y registro de eventos para verificar el tráfico en los puertos de gestión y alertar sobre actividades sospechosas, como intentos de acceso desde direcciones IP no autorizadas o a través de protocolos inusuales.

A12.4.2 Protección de la información de registro.

Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado[41].

Propuesta de mejoras:

A12.4.2.1 Implementar controles de acceso y almacenamiento seguro para garantizar que solo personal autorizado pueda acceder, modificar o eliminar registros de eventos.

A12.5 Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales[41].

A12.5.1 Instalación de software en sistemas operativos.

Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos[41].

Propuesta de mejoras:

A12.5.1.1 Establecer un proceso formal para solicitar y aprobar la instalación de nuevo software en los sistemas operativos. Cualquier solicitud de instalación de software deberá ser presentada a través de un formulario de solicitud de cambios y solicitar la aprobación de un supervisor o departamento responsable designado.

A12.6 Gestión de la vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas[41].

A12.6.1 Controles de gestión de las vulnerabilidades técnicas.

Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado[41].

Propuesta de mejoras:

A12.6.1.1 Cierre de puertos no utilizados en todos los sistemas de información de la organización. Los puertos que no sean necesarios para el funcionamiento de los servicios y aplicaciones serán cerrados para reducir la superficie de ataque y minimizar el riesgo de explotación.

A12.6.1.2 Establecer que todos los teléfonos IP deben ser regularmente monitoreados y actualizados con las últimas versiones de firmware y parches de seguridad disponibles. Esto ayuda a mitigar las vulnerabilidades conocidas que podrían ser explotadas por herramientas o técnicas maliciosas.

A12.6.1.3 Establecer un proceso formal de evaluación de riesgos que incluya la identificación de sistemas y servicios que dependen de protocolos obsoletos. Se priorizarán las acciones de mitigación en función del riesgo identificado.

A13 POLÍTICAS DE LA SEGURIDAD DE LAS COMUNICACIONES

A13.1 Gestión de la seguridad de las redes.

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte[41].

A13.1.1 Controles de redes.

Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones[41].

Propuesta de mejoras:

A13.1.1.1 Se implementarán firewalls de seguridad perimetral para proteger la red contra accesos no autorizados, ataques maliciosos y filtrado de tráfico no deseado.

A13.1.1.2 Establecer filtros de tráfico en puntos estratégicos de la red para bloquear el acceso no autorizado y prevenir la propagación de malware. Cada filtro debe actualizarse regularmente para adaptarse a las nuevas amenazas y patrones de ataque y llevar monitoreo continuo de tráfico de red para detectar patrones inusuales o comportamientos sospechosos.

A13.1.1.3 Se debe establecer una red interna segregada y protegida, limitando el acceso desde Internet y promoviendo conexiones seguras y autenticadas desde la red interna.

A13.1.1.4 Implementar enrutadores que filtren el tráfico entre las diferentes zonas de la red y bloqueen el acceso no autorizado a los puertos de gestión desde redes externas o menos confiables.

A13.1.2 Seguridad de los servicios de red.

Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente[41].

Propuesta de mejoras:

A13.1.2.1 Se debe priorizar la actualización o eliminación de protocolos obsoletos o vulnerables que puedan exponer la red a riesgos de seguridad. A la vez se deben implementar mecanismos de seguridad, como firewalls, sistemas de detección de intrusos (IDS), para proteger la red contra intrusiones y ataques.

A13.1.2.2 Establecer un proceso formal para gestionar cambios en la configuración de los servicios de red, que incluya la evaluación de impacto en la seguridad, la aprobación por parte de autoridades competentes y la documentación adecuada de los cambios realizados.

A13.1.2.3 Establecer que los teléfonos IP deben estar en una red separada o en segmentos de red dedicados para reducir la superficie de ataque y limitar el alcance de cualquier intento malicioso que pueda ocurrir en la red.

A13.1.2.4 Mantener actualizados los dispositivos y aplicaciones del teléfono IP con los últimos parches de seguridad para mitigar las vulnerabilidades conocidas que podrían ser explotadas en ataques de phishing.

A13.1.2.5 Todos los equipos de red, incluidos switches, routers y dispositivos de acceso, deben tener la función de Port Security habilitada en todos los puertos. Esta función debe estar configurada para aprender automáticamente las direcciones MAC y asignarlas al puerto correspondiente para evitar conexiones no deseadas a los equipos o puertos en cuestión ejecutando una acción en el momento que esta violación de seguridad ocurra.

A13.2 Transferencia de información.

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa[41].

A13.2.1 Políticas y procedimientos de transferencia de información.

Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación[41].

Propuesta de mejoras:

A13.2.1.1 Las transferencias de información, dentro de la organización o hacia entidades externas, deben estar cifradas utilizando algoritmos y protocolos de cifrado. Se deben utilizar canales de comunicación seguros y confiables para la transferencia de información sensible. Esto puede incluir el uso de conexiones VPN (Redes Privadas Virtuales), protocolos de transferencia segura como HTTPS o SFTP, entre otros.

A13.2.1.2 Establecer un procedimiento formal para que el personal notifique inmediatamente cualquier incidente de phishing al equipo de seguridad de la información o al equipo de respuesta a incidentes de la organización.

A13.2.4 Acuerdos de confidencialidad o de no divulgación.

Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información[41].

Propuesta de mejoras:

A13.2.4.1 Reforzar los acuerdos de confidencialidad o de no divulgación para incluir disposiciones específicas sobre la protección de la información confidencial ante ataques informáticos o de ingeniería social, prohibiendo la divulgación de información importante para la empresa.

A14 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

A14.1 Requisitos de seguridad de los sistemas de información.

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas[41].

A14.1.1 Análisis y especificación de requisitos de seguridad de la información.

Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes[41].

Propuesta de mejoras:

A14.1.1.1 Se deben implementar controles de acceso adecuados para restringir el acceso a sistemas y aplicaciones solo a usuarios autorizados. Esto puede ayudar a prevenir la inyección de código mediante la limitación de puntos de entrada potenciales.

A14.2 Seguridad en los procesos de desarrollo y de soporte.

Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información[41].

A14.2.1 Política de desarrollo seguro.

Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización[41].

Propuesta de mejoras:

A14.2.1.1 Todos los códigos fuente deben ser revisados por pares o a través de revisiones automáticas para garantizar que no se incluyan claves de API en el código de manera insegura.

A14.2.1.2 Se debe prohibir almacenar claves de API o credenciales en el código fuente sin cifrado. En su lugar, se deben utilizar mecanismos seguros de servicios de gestión de secretos o variables de entorno protegido como AWS Secrets Manager, Azure Key Vault o HashiCorp Vault, para almacenar y gestionar las claves de las API de manera segura.

A14.2.1.3 Todas las entradas de usuarios deben ser validadas y saneadas antes de ser procesadas por la aplicación. Se deben utilizar listas blancas de caracteres permitidos y rechazar cualquier entrada que no cumpla con los criterios establecidos. Utilizar funciones de escape específicas del lenguaje de programación y del sistema de gestión de bases de datos (DBMS) para neutralizar cualquier código SQL malicioso.

A14.2.1.4 Todas las entradas de usuarios, incluyendo datos de formularios, URL y cookies, deben ser validadas y escapadas antes de ser mostradas en la interfaz de usuario. Se deben utilizar funciones de escape específicas del contexto (HTML, atributo HTML, JavaScript, etc.) para evitar la ejecución de código malicioso.

A14.2.1.5 Configurar cabeceras HTTP de seguridad, como Content-Security-Policy (CSP), para mitigar el riesgo de XSS al restringir el origen de los recursos cargados en la página.

A14.2.2 Procedimientos de control de cambios en sistemas.

Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios[41].

Propuesta de mejoras:

A14.2.2.1 Se deben utilizar herramientas de gestión de configuración de red como Ansible, Puppet o Chef para realizar un seguimiento de todos los cambios realizados en la configuración de la red. Los cambios críticos en la configuración de la red deben ser revisados por el equipo de seguridad de la información antes de su implementación.

A14.2.2.2 Todos los procesos o cambios de la red deben ser solicitados mediante un formulario de solicitud de cambio (RFC) y aprobados por el equipo de administración encargado.

A14.2.2.3 El equipo de seguridad de la información es responsable de supervisar la implementación de controles para prevenir la mala utilización del sistema y tomar medidas correctivas según sea necesario.

A14.2.8 Prueba de seguridad de sistemas.

Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad[41].

Propuesta de mejoras:

A14.2.8.1 Realizar pruebas de inyección SQL como parte de las pruebas de seguridad estándar para todas las aplicaciones que interactúan con bases de datos. Utilizar herramientas de pruebas de seguridad automatizadas (DAST) como Burp Suite, Netsparker o Acunetix para identificar posibles puntos de inyección SQL en las aplicaciones.

A14.2.8.2 Realizar pruebas automatizadas de XSS como parte de las pruebas de seguridad estándar para todas las aplicaciones web. Utilice herramientas de escaneo de vulnerabilidades que puedan identificar de manera automática y precisa las vulnerabilidades de XSS como Burp Suite, Netsparker, Acunetix.

2.3.9 Tratamiento de los Riesgos

El tratamiento de riesgos, que se encuentra en la tabla 22, se realizó para identificar, evaluar y mitigar los riesgos asociados a la seguridad de la información de una organización. Este proceso es esencial para proteger la confidencialidad, integridad y disponibilidad de la información, y prevenir posibles amenazas y vulnerabilidades. Al gestionar adecuadamente los riesgos, la organización pudo minimizar el impacto de los incidentes de seguridad, asegurar la continuidad del negocio y fortalecer la confianza de las partes interesadas. Se evidencia en el Anexo 4 la realización del tratamiento de riesgos junto al comité de seguridad de la información de la empresa.

Escala de Aceptación

A continuación, la tabla 21 muestra la escala de aceptación, la cual describe si el riesgo residual es aceptable o no dependiendo si su nivel es bajo, medio o alto.

Tabla 21 *Escala de Aceptación*

Escala de Aceptación	
Nivel de Riesgo Residual	**ACEPTABLE(SI/NO)**
Bajo	SI
Medio	SI
Alto	NO

Tabla 22 Tratamiento de Riesgos

EVALUACIÓN DE RIESGOS									TRATAMIENTO DE RIESGOS								
Nro. Activo	Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad		Cálculo de Evaluación de Riesgo	Nivel de Riesgo	Método de tratamiento de riesgos	Tipo de Control	Controles a Implementar	Nivel de Amenaza	Nivel de Vulnerabilidad	Cálculo de Evaluación de Riesgos con el Control Implementado	Nivel de Riesgo con el Control Implementado	Nivel de Riesgo Residual	ACEPTABLE(SI/NO)
				CID	Nivel de Amenazas	Nivel de Vulnerabilidades											
#000001	CPU CORE I5 4TH GEN 4GB 500 GB HDD DVD-RW WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED- MÁS TECLADO	Errores de Mantenimiento	Uso de antivirus obsoletos	3	2	2	12	Alto	REDUCIR	CORRECTIVO	A7.2.2/A12.2.1	1	1	3	BAJO	BAJO	SI
			Inyección por malware			1	6	Medio	REDUCIR	PREVENTIVO	A12.2.1	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de Datos			1	6	Medio	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	3	BAJO	BAJO	SI
			Maltrato de equipos			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.2/A11.2.4	1	2	6	MEDIO	MEDIO	SI
			Puertos expuestos			3	18	Alto	REDUCIR	CORRECTIVO	A12.6.1/A13.1.1	1	1	3	BAJO	BAJO	SI
		Acceso remoto no autorizado	Contraseñas débiles		1	3	9	Alto	REDUCIR	PREVENTIVO	A9.4.3	1	1	3	BAJO	BAJO	SI
			Credenciales expuestas			3	9	Alto	REDUCIR	CORRECTIVO	A9.3.1/A9.4.2	1	1	3	BAJO	BAJO	SI
#000004	CASE XCASE 176 ATX / PSU 750W / 2*USB 2.0 / AUDIO (SERVIDOR DE LLAMADAS) MAS TECLADO QUASAD COMPUTER QC-4400U Y MAUSE	Ataque de DoS	Falta de mitigación de tráfico malicioso	3	1	1	3	Bajo	REDUCIR	PREVENTIVO	A13.1.1	1	1	3	BAJO	BAJO	SI
			Infraestructura débil del protocolo de red			1	3	Bajo	REDUCIR	PREVENTIVO	A13.1.1/A13.1.2	1	1	3	BAJO	BAJO	SI
		Fallas en el Hardware	Pérdida de Datos		2	1	6	Medio	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	3	BAJO	BAJO	SI
			Daño físico o lógico			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.2/A11.2.4/A11.2.6/A12.2.1	1	1	3	BAJO	BAJO	SI
		Explotación de configuración débil de seguridad	Falta de cifrado		2	1	6	Medio	REDUCIR	PREVENTIVO	A13.2.1	1	1	3	BAJO	BAJO	SI
			Puertos abiertos innecesarios			3	18	Alto	REDUCIR	PREVENTIVO	A12.6.1	1	1	3	BAJO	BAJO	SI
			Servicios de red mal configurados			1	6	Medio	REDUCIR	PREVENTIVO	A13.1.1/A13.1.2	1	1	3	BAJO	BAJO	SI
#000005	CPU CORE I7 16GB 500 GB SSD WIN 10 PRO 19" MONITOR BRAND NEW MOUSE Y KB INCLUDED.	Errores de Mantenimiento	Uso de antivirus obsoletos	3	2	2	12	Alto	REDUCIR	CORRECTIVO	A7.2.2/A12.2.1	1	1	3	BAJO	BAJO	SI
			Inyección por malware			1	6	Medio	REDUCIR	PREVENTIVO	A12.2.1	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de Datos			1	6	Medio	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	3	BAJO	BAJO	SI
			Maltrato de equipos			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.2/A11.2.4	1	2	6	MEDIO	MEDIO	SI
			Puertos expuestos			3	18	Alto	REDUCIR	CORRECTIVO	A12.6.1/A13.1.1	1	1	3	BAJO	BAJO	SI
		Acceso remoto no autorizado	Contraseñas débiles		1	3	9	Alto	REDUCIR	PREVENTIVO	A9.4.3	1	1	3	BAJO	BAJO	SI
			Credenciales expuestas			3	9	Alto	REDUCIR	CORRECTIVO	A9.3.1/A9.4.2	1	1	3	BAJO	BAJO	SI
#000006	CPU CORE I5 4TA GENERACION 4GB, 500 GB	Errores de Mantenimiento	Uso de antivirus obsoletos	3	2	2	12	Alto	REDUCIR	CORRECTIVO	A7.2.2/A12.2.1	1	1	3	BAJO	BAJO	SI
			Inyección por malware			1	6	Medio	REDUCIR	PREVENTIVO	A12.2.1	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de Datos			1	6	Medio	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	3	BAJO	BAJO	SI

			Maltrato de equipos			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.2/A11.2.4	1	2	6	MEDIO	MEDIO	SI
			Puertos expuestos			3	18	Alto	REDUCIR	CORRECTIVO	A12.6.1/A13.1.1	1	1	3	BAJO	BAJO	SI
		Acceso remoto no autorizado	Contraseñas débiles		1	3	9	Alto	REDUCIR	PREVENTIVO	A9.4.3	1	1	3	BAJO	BAJO	SI
			Credenciales expuestas			3	9	Alto	REDUCIR	CORRECTIVO	A9.3.1/A9.4.2	1	1	3	BAJO	BAJO	SI
#000007	CELULAR SAMSUNG A04E SM-A04EM	Pérdida o robo del dispositivo	Suplantación de identidad	1,66666667	1	1	2	Bajo	REDUCIR	PREVENTIVO	A9.3.1	1	1	1,666666667	BAJO	BAJO	SI
			Fuga de información corporativa			2	3	Bajo	REDUCIR	PREVENTIVO	A9.3.1	1	1	1,666666667	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de información		2	3	10	Alto	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	1,666666667	BAJO	BAJO	SI
			Maltrato del dispositivo			3	10	Alto	REDUCIR	PREVENTIVO	A11.2.1/A11.2.4	1	2	3,333333333	BAJO	BAJO	SI
#000009	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	2	2	1	4	Medio	REDUCIR	PREVENTIVO	A12.6.1/A13.1.2	1	1	2	BAJO	BAJO	SI
			Ataques de phishing			1	4	Medio	REDUCIR	PREVENTIVO	A13.1.2/A13.2.1/A13.2.4	1	1	2	BAJO	BAJO	SI
		Intercepción de llamadas	Tráfico sin cifrar		1	1	2	Bajo	REDUCIR	PREVENTIVO	A13.2.1	1	1	2	BAJO	BAJO	SI
			Red inalámbrica no segura			1	2	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A13.1.1/A13.1.2	1	1	2	BAJO	BAJO	SI
		Manipulación de la configuración	Redirección de tráfico de red		1	1	2	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A14.2.2	1	1	2	BAJO	BAJO	SI
			Puertos Expuestos			3	6	Medio	REDUCIR	CORREGIR	A12.6.1/A13.1.1	1	1	2	BAJO	BAJO	SI
			Falta de controles establecidos para la administración			1	2	Bajo	REDUCIR	PREVENTIVO	A14.2.2	1	1	2	BAJO	BAJO	SI
#000010	TELÉFONO YEANLINK 1 LINEA YE-SIP-T30-E2	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	2	2	1	4	Medio	REDUCIR	PREVENTIVO	A12.6.1/A13.1.2	1	1	2	BAJO	BAJO	SI
			Ataques de phishing			1	4	Medio	REDUCIR	PREVENTIVO	A13.1.2/A13.2.1/A13.2.4	1	1	2	BAJO	BAJO	SI
		Intercepción de llamadas	Tráfico sin cifrar		1	1	2	Bajo	REDUCIR	PREVENTIVO	A13.2.1	1	1	2	BAJO	BAJO	SI
			Red inalámbrica no segura			1	2	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A13.1.1/A13.1.2	1	1	2	BAJO	BAJO	SI
		Manipulación de la configuración	Redirección de tráfico de red		1	1	2	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A14.2.2	1	1	2	BAJO	BAJO	SI
			Puertos Expuestos			3	6	Medio	REDUCIR	CORREGIR	A12.6.1/A13.1.1	1	1	2	BAJO	BAJO	SI
			Falta de controles establecidos para la administración			1	2	Bajo	REDUCIR	PREVENTIVO	A14.2.2	1	1	2	BAJO	BAJO	SI
#000011	CÁMARA IP EZVIZ TUBO SELLADA 2MP L 4MM-OFICINA	Acceso no autorizado	Contraseñas débiles	2,66666667	1	3	8	Medio	REDUCIR	PREVENTIVO	A9.4.3	1	1	2,666666667	BAJO	BAJO	SI
			Red inalámbrica no segura			1	3	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A13.1.1/A13.1.2	1	1	2,666666667	BAJO	BAJO	SI
		Eliminación y alteración del dispositivo	Daño físico o destrucción		1	2	5	Medio	REDUCIR	CORRECTIVO	A11.2.1/A11.2.3	1	1	2,666666667	BAJO	BAJO	SI
			Dificultad para detectar intrusiones			2	5	Medio	REDUCIR	PREVENTIVO	A12.4.1/A12.4.2	1	1	2,666666667	BAJO	BAJO	SI

			Compromiso de la integridad de la información			2	5	Medio	REDUCIR	PREVENTIVO	A12.3.1	1	1	2,666666667	BAJO	BAJO	SI
#000013	CÁMARA IP PANTIL EZVIZ 2MP L 2.8MM-	Acceso no autorizado	Contraseñas débiles	2,666666667	1	3	8	Medio	REDUCIR	PREVENTIVO	A9.4.3	1	1	2,666666667	BAJO	BAJO	SI
			Red inalámbrica no segura			1	3	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A13.1.1/A13.1.2	1	1	2,666666667	BAJO	BAJO	SI
		Eliminación y alteración del dispositivo	Daño físico o destrucción		1	2	5	Medio	REDUCIR	CORRECTIVO	A11.2.1/A11.2.3	1	1	2,666666667	BAJO	BAJO	SI
			Dificultad para detectar intrusiones			2	5	Medio	REDUCIR	PREVENTIVO	A12.4.1/A12.4.2	1	1	2,666666667	BAJO	BAJO	SI
			Compromiso de la integridad de la información			2	5	Medio	REDUCIR	PREVENTIVO	A12.3.1	1	1	2,666666667	BAJO	BAJO	SI
#000014	NVR DE 4CH CAPACIDAD 20MB 1HDD	Acceso no autorizado	Exposición a Internet	3	2	1	6	Medio	REDUCIR	PREVENTIVO	A13.1.1	1	1	3	BAJO	BAJO	SI
			Credenciales predeterminadas o débiles			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A9.3.1/A9.4.2/A9.4.3	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de información		1	1	3	Bajo	REDUCIR	PREVENTIVO	A11.2.7/A12.3.1	1	1	3	BAJO	BAJO	SI
			Daño físico			2	6	Medio	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.2/A11.2.4	1	1	3	BAJO	BAJO	SI
			Fallo en la infraestructura de red			1	3	Bajo	REDUCIR	PREVENTIVO	A13.1.1/A13.1.2	1	1	3	BAJO	BAJO	SI
#000017	TELÉFONO IP 1 LINEAS POE	Falsificación de llamadas (spoofing)	Uso de herramientas de spoofing	2	2	1	4	Medio	REDUCIR	PREVENTIVO	A12.6.1/A13.1.2	1	1	2	BAJO	BAJO	SI
			Ataques de phishing			1	4	Medio	REDUCIR	PREVENTIVO	A13.1.2/A13.2.1/A13.2.4	1	1	2	BAJO	BAJO	SI
		Intercepción de llamadas	Tráfico sin cifrar		1	1	2	Bajo	REDUCIR	PREVENTIVO	A13.2.1	1	1	2	BAJO	BAJO	SI
			Red inalámbrica no segura			1	2	Bajo	REDUCIR	PREVENTIVO	A9.1.2/A13.1.1/A13.1.2	1	1	2	BAJO	BAJO	SI
		Manipulación de la configuración	Redirección de tráfico de red		1	3	6	Medio	REDUCIR	PREVENTIVO	A9.1.2/A14.2.2	1	1	2	BAJO	BAJO	SI
			Puertos Expuestos			1	2	Bajo	REDUCIR	CORRECTIVO	A12.6.1/A13.1.1	1	1	2	BAJO	BAJO	SI
			Falta de controles establecidos para la administración			1	2	Bajo	REDUCIR	PREVENTIVO	A14.2.2	1	1	2	BAJO	BAJO	SI
#000018	16- PORT GIGABIT RACKMOUNT SWITCH	Firmware desactualizado	Compatibilidad con protocolos obsoletos	3	2	1	6	Medio	REDUCIR	PREVENTIVO	A7.2.2/A12.6.1	1	1	3	BAJO	BAJO	SI
			Falta de parches de seguridad			1	6	Medio	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos		1	2	6	Medio	REDUCIR	CORRECTIVO/PREVENTIVO	A9.3.1/A9.4.2/A9.4.3	1	1	3	BAJO	BAJO	SI
			Acceso a través de puertos de gestión mal configurados			1	3	Bajo	REDUCIR	PREVENTIVO	A12.4.1/A13.1.1	1	1	3	BAJO	BAJO	SI

		Manipulación de la configuración	Filtración de información confidencial		1	1	3	Bajo	REDUCIR	PREVENTIVO	A13.2.1	1	1	3	BAJO	BAJO	SI
			Puertos expuestos			2	6	Medio	REDUCIR	CORRECTIVO	A13.1.2	1	1	3	BAJO	BAJO	SI
			Desactivación de protocolos de seguridad			1	3	Bajo	REDUCIR	PREVENTIVO	A13.1.2/A14.2.2	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de comunicación entre dispositivos		2	2	12	Alto	REDUCIR	CORRECTIVO	A11.2.3	1	1	3	BAJO	BAJO	SI
			Daño físico o lógico			2	12	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.2/A11.2.4/A11.2.6/A12.2.1	1	1	3	BAJO	BAJO	SI
			Mala manipulación de los equipos			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.4	1	2	6	MEDIO	MEDIO	SI
#000019	OPENVOX GATEWAY GSM SWG-3008G / 8 CANALES GSM	Firmware desactualizado	Compatibilidad con protocolos obsoletos	3	2	1	6	Medio	REDUCIR	PREVENTIVO	A7.2.2/A12.6.1	1	1	3	BAJO	BAJO	SI
			Falta de parches de seguridad			1	6	Medio	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Acceso lógico no autorizado a los servicios de red	Credenciales débiles o defectuosos		1	2	6	Medio	REDUCIR	CORRECTIVO/PREVENTIVO	A9.3.1/A9.4.2/A9.4.3	1	1	3	BAJO	BAJO	SI
			Acceso a través de puertos de gestión mal configurados			1	3	Bajo	REDUCIR	PREVENTIVO	A12.4.1/A13.1.1	1	1	3	BAJO	BAJO	SI
		Manipulación de la configuración	Filtración de información confidencial		1	1	3	Bajo	REDUCIR	PREVENTIVO	A13.2.1	1	1	3	BAJO	BAJO	SI
			Configuración de puertos inseguros			2	6	Medio	REDUCIR	CORRECTIVO	A13.1.2	1	1	3	BAJO	BAJO	SI
			Desactivación de protocolos de seguridad			1	3	Bajo	REDUCIR	PREVENTIVO	A13.1.2/A14.2.2	1	1	3	BAJO	BAJO	SI
		Fallas en el hardware	Pérdida de comunicación entre dispositivos		2	2	12	Alto	REDUCIR	CORRECTIVO	A11.2.3	1	1	3	BAJO	BAJO	SI
			Daño físico o lógico			2	12	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.2/A11.2.4/A11.2.6/A12.2.1	1	1	3	BAJO	BAJO	SI
			Mala manipulación de los equipos			3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.1/A11.2.4	1	2	6	MEDIO	MEDIO	SI
#000020	Issabel	Acceso no autorizado	Contraseñas débiles o predeterminadas	3	2	3	18	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A9.3.1/A9.4.2/A9.4.3	1	1	3	BAJO	BAJO	SI
			Falta de expiración adecuada de sesiones			2	12	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A9.2.5/A9.4.2	1	1	3	BAJO	BAJO	SI
		Fallas en el software	Inyección de código		2	1	6	Medio	REDUCIR	PREVENTIVO	A14.1.1	1	1	3	BAJO	BAJO	SI
			Mala utilización del sistema			2	12	Alto	REDUCIR	CORRECTIVO	A7.2.2/A14.2.2	1	1	3	BAJO	BAJO	SI
#000021	Formulario General	Cambios no autorizados de la configuración del sistema	Alteración de información	3	2	3	18	Alto	REDUCIR	CORRECTIVO	A12.1.2	1	2	6	MEDIO	MEDIO	SI
			Filtración de datos sensibles			3	18	Alto	REDUCIR	CORRECTIVO	A10.1.1/A13.2.4	1	2	6	MEDIO	MEDIO	SI
			Falta de auditoría de cambios			3	18	Alto	REDUCIR	CORRECTIVO	A12.1.2	1	1	3	BAJO	BAJO	SI

		Acceso no autorizado	Falta de gestión de sesiones		3	3	27	Alto	ACEPTAR/EVITAR	CORRECTIVO	A9.2.5/A9.4.2	2	1	6	MEDIO	MEDIO	SI
			Contraseñas débiles o predeterminadas			3	27	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A9.3.1/A9.4.2/A9.4.3	1	2	6	MEDIO	MEDIO	SI
#000023	Personal de Tecnologías	Ataque Informático	Instalación de software no autorizado	3	1	1	3	Bajo	REDUCIR	CORRECTIVO/PREVENTIVO	A9.4.4/A12.5.1	1	1	3	BAJO	BAJO	SI
			Falta de entrenamiento en seguridad de la información			2	6	Medio	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Alteración accidental de la información	Malentendidos en la comunicación		2	3	18	Alto	REDUCIR	PREVENTIVO	A7.2.2	1	2	6	MEDIO	MEDIO	SI
			Falta de capacitación en procesos			2	12	Alto	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Divulgación de información	Fuga de datos confidenciales de los clientes		1	3	9	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A7.2.3/A13.2.4	1	1	3	BAJO	BAJO	SI
			Uso inapropiado de correo electrónico			2	6	Medio	REDUCIR	CORRECTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
#000025	Personal de Operaciones	Ataque Informático	Instalación de software no autorizado	3	1	1	3	Bajo	REDUCIR	CORRECTIVO/PREVENTIVO	A9.4.4/A12.5.1	1	1	3	BAJO	BAJO	SI
			Falta de entrenamiento en seguridad de la información			2	6	Medio	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Alteración accidental de la información	Malentendidos en la comunicación		2	3	18	Alto	REDUCIR	PREVENTIVO	A7.2.2	1	2	6	MEDIO	MEDIO	SI
			Falta de capacitación en procesos			2	12	Alto	REDUCIR	PREVENTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
		Divulgación de información	Fuga de datos confidenciales de los clientes		1	3	9	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A7.2.3/A13.2.4	1	1	3	BAJO	BAJO	SI
			Uso inapropiado de correo electrónico			2	6	Medio	REDUCIR	CORRECTIVO	A7.2.2	1	1	3	BAJO	BAJO	SI
#000027	Asistencia de Desarrollo de Proyectos	Ataques de ingeniería social	Correos electrónicos de phishing	2,66666667	1	1	3	Bajo	REDUCIR	PREVENTIVO	A7.2.2/A13.2.1	1	1	2,66666667	BAJO	BAJO	SI
			Llamadas fraudulentas			2	5	Medio	REDUCIR	PREVENIR	A7.2.2	1	1	2,66666667	BAJO	BAJO	SI
		Acceso no autorizado a archivos de los proyectos	Robo de documentación importante		1	1	3	Bajo	REDUCIR	CORRECTIVO/PREVENTIVO	A7.2.3/A9.1.1/A13.2.4	1	1	2,66666667	BAJO	BAJO	SI
			Filtración de información confidencial a terceros			3	8	Medio	REDUCIR	CORRECTIVO/PREVENTIVO	A7.2.3/A13.2.4	1	1	2,66666667	BAJO	BAJO	SI
#000028	Call Center Inteligente	Ataques de ingeniería social	Correos electrónicos de phishing	3	2	1	6	Medio	REDUCIR	PREVENTIVO	A7.2.2/A13.2.1	1	1	3	BAJO	BAJO	SI
			Llamadas fraudulentas			2	12	Alto	REDUCIR	PREVENIR	A7.2.2	1	1	3	BAJO	BAJO	SI
		Escuchas no autorizadas	Privacidad de conversaciones comprometidas		1	1	3	Bajo	REDUCIR	PREVENIR	A11.1.5	1	1	3	BAJO	BAJO	SI
			Fuga de información confidencial de los clientes			2	6	Medio	REDUCIR	CORRECTIVO/PREVENTIVO	A7.2.3/A13.2.4	1	1	3	BAJO	BAJO	SI
		Fallas en la comunicación	Falta de cifrado de extremo a extremo		2	1	6	Medio	REDUCIR	PREVENTIVO	A13.2.1	1	1	3	BAJO	BAJO	SI

			Interrupción del servicio			2	12	Alto	REDUCIR	CORRECTIVO/PREVENTIVO	A11.2.2/A11.2.3/A11.2.4	1	2	6	MEDIO	MEDIO	SI
#000029	Desarrollo de Software y Aplicaciones	Fuga de información durante el proceso de despliegue	Exposición de claves de las API	2,66666667	1	1	3	Bajo	REDUCIR	PREVENTIVO	A13.2.4/A14.2.1	1	1	2,666666667	BAJO	BAJO	SI
			Credenciales de bases de datos expuestas			2	5	Medio	REDUCIR	PREVENTIVO	A14.2.1	1	1	2,666666667	BAJO	BAJO	SI
		Fallas en la validación de entradas	SQL injection		1	1	3	Bajo	REDUCIR	CORRECTIVO	A14.2.1/A14.2.8	1	1	2,666666667	BAJO	BAJO	SI
			XSS (cross-site scripting)			2	5	Medio	REDUCIR	CORRECTIVO	A14.2.1/A14.2.8	1	1	2,666666667	BAJO	BAJO	SI

2.3.10 Comunicación de Resultados

La fase de Comunicación de Resultados es importante para garantizar que todas las partes interesadas comprendan plenamente las decisiones y acciones adoptadas para mitigar los riesgos identificados. Esta fase implica la presentación de los hallazgos, análisis y medidas implementadas para gestionar los riesgos de manera efectiva. La claridad y la transparencia en esta comunicación no solo refuerzan la confianza ante la empresa, sino que también aseguran la alineación de los objetivos planteados en la gestión de riesgos de la seguridad de la Información.

Declaración de aplicabilidad

La declaración de aplicabilidad en la gestión de riesgos de seguridad de la información permite a la empresa adaptar y seleccionar controles específicos a su contexto, proporcionando claridad y transparencia sobre las decisiones tomadas. Facilita el cumplimiento de la norma ISO/IEC 27005, y demuestra un enfoque sistemático en la mitigación de riesgos. Además, ayuda en la asignación de responsabilidades y recursos, asegurando una protección eficaz de la información y permitiendo ajustes conforme evolucionan las amenazas. Esta etapa de la gestión de riesgos se puede evidenciar en el Anexo 5, donde el comité de seguridad de la información discute sobre si los controles propuestos son aplicables o no.

En la siguiente tabla 23 se muestran los controles de la norma que se van a utilizar junto a la propuesta de mejoras, la cual fue hecha a partir de los controles. Junto a eso se encuentra la aplicabilidad, donde la empresa ha decidido aplicar todos los controles marcados con un “SI” con su respectiva justificación, tal y como se ve en el Anexo 6 donde se evidencia la revisión de la declaración de la aplicabilidad junto a la gerente general de la empresa. Toda esta documentación fue entregada formalmente a la empresa junto a un oficio de entrega y recepción, el cual fue firmado por la gerente general. Como evidencia de este proceso, dicho oficio firmado se encuentra en el Anexo 7, proporcionando una referencia formal y verificable de la comunicación y aprobación de los resultados.

Tabla 23 Declaración de Aplicabilidad

Numeral	Dominio	Objetivo de Control	Control	Propuesta de Mejoras	Aplicabilidad SI/NO	Justificación
A.7	**POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS**	A.7.2 Durante la ejecución del empleo	A.7.2.2 Control de toma de conciencia, educación y formación en la seguridad de la información.	A.7.2.2.1 Implementar un programa de concientización sobre seguridad que incluya sesiones de formación específicas sobre la identificación y el manejo de software, protocolos o procesos obsoletos. Se fomentará una cultura de seguridad donde todos los empleados comprendan su responsabilidad en la protección de la infraestructura de TI.	SI	Este control educa a los empleados para reconocer y gestionar riesgos de seguridad, reduciendo la probabilidad de que el uso de software obsoleto comprometa la infraestructura de TI.
				A.7.2.2.2 Proporcionar programas de educación y formación en seguridad de la información para garantizar que los empleados comprendan las políticas, procedimientos y mejores prácticas relacionadas con el uso adecuado de los sistemas.	SI	Este control asegura que los empleados entiendan y sigan las políticas y mejores prácticas de seguridad, minimizando riesgos y protegiendo los sistemas de información de la empresa.
				A.7.2.2.3 Proporcionar capacitación regular en comunicación segura en materia de seguridad de la información para todo el personal de la organización. La capacitación incluye técnicas de comprensión de la terminología específica de seguridad de la información y promueve la comunicación efectiva, abierta y transparente entre el personal.	SI	Este control ayuda a que el personal comprenda y utilice correctamente el lenguaje y las prácticas de seguridad de la información, promoviendo una comunicación efectiva y transparente en la organización
				A.7.2.2.4 Establecer canales de comunicación abiertos y transparentes para que los empleados puedan hacer preguntas, plantear inquietudes y solicitar aclaraciones sobre temas de generales. fomentando una cultura de apertura y colaboración para facilitar la comunicación efectiva en toda la organización.	SI	Este control facilita la colaboración y confianza donde los empleados se sienten cómodos compartiendo preocupaciones y preguntas, lo que promueve la resolución rápida de problemas y fortalece la seguridad de la información al permitir una comunicación efectiva en toda la organización.
				A.7.2.2.5 Desarrollar programas de capacitación específicos para todos los procesos, diseñados para proporcionar a los empleados el conocimiento y las habilidades necesarias para desempeñar sus funciones de manera segura y eficiente.	SI	Este control permite que los empleados adquieran el conocimiento y las habilidades necesarias para llevar a cabo sus funciones de forma segura y eficiente.
				A.7.2.2.6 Establecer que el correo electrónico solo debe utilizarse para fines comerciales legítimos y relacionados con el trabajo. Además, no se permite el uso del correo electrónico para actividades	SI	Este control limita el uso del correo electrónico a actividades laborales, reduciendo el riesgo de amenazas cibernéticas y manteniendo un

				personales no relacionadas con el trabajo, como el envío de correos electrónicos personales o el acceso a sitios web no relacionados con el trabajo.		ambiente de trabajo enfocado y seguro
				A.7.2.2.7 Proporcionar capacitación periódica sobre el uso seguro y apropiado del correo electrónico, incluyendo la identificación de correos electrónicos de phishing y otras amenazas de seguridad.	SI	Este control ayuda al personal para reconocer y evitar amenazas cibernéticas como el phishing, fortaleciendo la protección de los datos de la organización y reduciendo el riesgo de violaciones de seguridad.
				A.7.2.2.8 Proporcionar formación regular sobre los riesgos asociados con las llamadas fraudulentas y cómo identificarlas. Los empleados serán informados sobre las técnicas comunes utilizadas por los estafadores en llamadas telefónicas fraudulentas y se les enseñará cómo responder adecuadamente.	SI	Este control ayuda al personal para identificar y responder adecuadamente a técnicas comunes de estafadores en llamadas telefónicas, reduciendo así el riesgo de divulgación de información confidencial o de caer en esquemas de fraude
			A.7.2.3 Control de proceso disciplinario.	A7.2.3.1 Establecer un proceso disciplinario claro y transparente para abordar los incumplimientos relacionados con la fuga de datos confidenciales.	SI	Este control define consecuencias claras para el incumplimiento de las políticas de seguridad de la información, fomentando la responsabilidad y disuadiendo el comportamiento negligente o malicioso, lo que fortalece la protección de los datos confidenciales de la organización
				A7.2.3.2 Definir las acciones disciplinarias apropiadas, que pueden incluir advertencias formales, suspensión temporal, terminación de empleo y acciones legales según la gravedad del incumplimiento.	SI	Este control establece medidas disciplinarias proporcionales a la gravedad de los incumplimientos, asegurando una respuesta justa y consistente a las violaciones de seguridad de datos.
A.9	**POLÍTICAS DE CONTROL DE ACCESO**	A.9.1 Requisitos del negocio para control de acceso.	A.9.1.1 Política de control de acceso.	A.9.1.1.1 Establecer sistemas de control de acceso lógico para restringir el acceso a personal autorizado a la documentación importante almacenada en oficinas, sistemas informáticos y bases de datos. Se asignarán permisos de acceso de manera específica y limitada, de acuerdo con los roles y responsabilidades de cada usuario.	SI	Este control protege la información restringiendo el acceso solo a personal autorizado según roles y responsabilidades, reduciendo así el riesgo de exposición de datos sensibles.
			A.9.1.2 Control de acceso a redes y a servicios de red.	A.9.1.2.1 Establecer estándares de seguridad para todas las redes inalámbricas utilizadas en la organización que debe incluir la autenticación adecuada, el cifrado de datos, la segmentación de red y otras medidas de seguridad necesarias para proteger la	SI	Este control protege la integridad y confidencialidad de la información transmitida a través de redes inalámbricas mediante la implementación de medidas de seguridad como autenticación,

				integridad y la confidencialidad de la información transmitida a través de redes inalámbricas.		cifrado de datos y segmentación de red, asegurando una protección adecuada contra amenazas.
		A.9.2 Gestión de acceso de usuarios.	A9.2.5 Revisión de los derechos de acceso de usuarios.	A.9.2.5.1 Se deben realizar revisiones periódicas de los derechos de acceso de todo el personal, asegurando que los permisos de los usuarios sean apropiados para sus funciones actuales y que las sesiones de acceso expiren adecuadamente tras un período de inactividad.	SI	Este control proporciana permisos de acceso de los usuarios se ajusten a sus funciones actuales, reduciendo el riesgo de acceso no autorizado.
		A.9.3 Responsabilidades del personal	A.9.3.1 Control sobre el uso de información de autenticación secreta.	A.9.3.1.1 Proporcionar capacitación regular al personal sobre la importancia de utilizar contraseñas seguras y sobre los riesgos asociados con las contraseñas comprometidas. Se enfatizará la necesidad de seguir las políticas de contraseñas establecidas por la organización.	SI	Este control Educa al personal sobre la importancia de usar contraseñas seguras y los riesgos de contraseñas comprometidas.
				A.9.3.1.2 Promover el uso de aplicaciones de autenticación de doble factor confiables, como Google Authenticator o Microsoft Authenticator, para generar códigos de verificación, todos los empleados deben activar y configurar la autenticación de doble factor en sus dispositivos móviles corporativos utilizados para acceder a recursos críticos de la empresa.	SI	Este control refuerza la seguridad de los sistemas al requerir que todos los empleados activen y configuren la autenticación de doble factor en sus dispositivos móviles corporativos.
				A.9.3.1.3 El personal encargado deberá hacerse con la responsabilidad de establecer un lugar fijo para mantener seguro el dispositivo, evitando así la pérdida o robo del mismo para salvaguardar la información corporativa de la empresa.	SI	Este control reduce el riesgo de pérdida o robo de dispositivos al asignar responsabilidad al personal para mantenerlos seguros en un lugar fijo. Esto ayuda a salvaguardar la información corporativa de la empresa al prevenir el acceso no autorizado a los datos almacenados en los dispositivos perdidos o robados.
		A.9.4 Control de acceso a sistemas y aplicaciones.	A.9.4.2 Control de procedimiento de ingreso seguro.	A.9.4.2.1 Proporcionar capacitación periódica al personal sobre la importancia de no exponer ni divulgar contraseñas debido al alto riesgo de comprometer la seguridad de la información de los datos de los clientes.	SI	Este control educa al personal sobre el riesgo de seguridad asociado con la exposición o divulgación de contraseñas, especialmente en lo que respecta a la protección de los datos de los clientes.
				A.9.4.2.2 Todos los sistemas de información deben estar configurados para establecer tiempos de sesión para el personal y administradores. Los tiempos de sesión deben basarse en las mejores prácticas de	SI	Este control mejora la seguridad de los sistemas al limitar el tiempo que los usuarios y administradores pueden permanecer conectados.

				seguridad y en las necesidades operativas de la organización.		
			A.9.4.3 Control de sistema de gestión de contraseñas	A.9.4.3.1 Establecer requisitos para la complejidad de las contraseñas, como la inclusión de una longitud mínima de 8 caracteres sean alfanuméricos, símbolos, mayúsculas y minúsculas. A la vez establecer un intervalo de tiempo donde los usuarios deben cambiar sus contraseñas periódicamente.	SI	Este control refuerza la seguridad de los sistemas al exigir contraseñas robustas que incluyan una combinación de caracteres alfanuméricos, símbolos, mayúsculas y minúsculas, con una longitud mínima de 8 caracteres.
			A.9.4.4 Uso de programas utilitarios privilegiados.	A.9.4.4.1 Establecer consecuencias claras para cualquier empleado que instale software no autorizado en los sistemas operativos, lo que puede incluir medidas disciplinarias según las políticas de la organización.	SI	Este control promueve la responsabilidad y el cumplimiento de las políticas de seguridad al definir medidas disciplinarias para aquellos empleados que instalen software no autorizado en los sistemas operativos
A.10	**POLÍTICAS DE CRIPTOGRAFÍA**	A.10.1 Revisiones de seguridad de la información.	A.10.1.1 Cumplimiento con las políticas y normas de seguridad	A.10.1.1.1 Implementar herramientas de prevención de pérdida de datos (DLP) como Endpoint Protector, McAfee, etc. para monitorear y controlar la transferencia de datos sensibles dentro y fuera de la red de la organización.	SI	Este control mejora la seguridad de la organización al monitorear y controlar la transferencia de datos sensibles dentro y fuera de la red.
A.11	**POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO**	A.11.1 Áreas seguras.	A.11.1.5 Trabajo en áreas seguras.	A.11.1.5.1 Todas las conversaciones que involucren información confidencial o sensible deben realizarse exclusivamente dentro de las áreas seguras designadas.	SI	Este control protege la confidencialidad de la información al evitar conversaciones sobre datos sensibles en áreas no seguras, reduciendo así el riesgo de divulgación no autorizada.
		A.11.2 Equipos.	A.11.2.1 Política de ubicación y protección de los equipos.	A.11.2.1.1 Implementar medidas de protección física como también inspecciones regulares para verificar el estado y la funcionalidad del equipo, así como para identificar y abordar cualquier problema de seguridad o daño físico.	SI	Este control refuerza la seguridad de los activos de la organización al proteger físicamente el equipo y verificar su estado y funcionalidad de manera regular.
				A.11.2.1.2 Se deben llevar a cabo campañas periódicas de concientización para destacar la importancia de proteger los equipos de TI y fomentar una cultura de seguridad en toda la organización	SI	Este control promueve una cultura de seguridad en toda la organización al destacar la importancia de proteger los equipos de TI.
			A.11.2.2 Servicios de suministro.	A.11.2.2.1 Establecer procedimientos claros para la respuesta a fallas de energía seleccionando un UPS con capacidad suficiente para mantener estos equipos operativos durante un tiempo determinado,	SI	Este control garantiza la continuidad operativa al tener procedimientos definidos para responder a fallas de energía.

				permitiendo la transición a generadores de respaldo o el apagado seguro.		
				A.11.2.2.2 Instalar generadores de respaldo para proporcionar energía continua en caso de interrupciones prolongadas del suministro eléctrico.	SI	Este control asegura la continuidad operativa al proporcionar una fuente de energía continua en caso de interrupciones prolongadas del suministro eléctrico
			A.11.2.3 Política de seguridad del cableado.	A.11.2.3.1 Todo cableado de red o energética debe ser instalado de manera segura para prevenir daños físicos. Se deben utilizar conductos y canalizaciones adecuadas para proteger el cableado contra daños o exposición a elementos externos. También se debe realizar inspecciones periódicas del cableado para identificar y abordar cualquier signo de deterioro.	SI	Este control evita daños físicos y protege la integridad del cableado al instalarlo de forma segura y utilizar conductos adecuados para protegerlo contra daños o exposición a elementos externos.
			A.11.2.4 Controles de mantenimiento de equipos.	A.11.2.4.1 Establecer un programa de mantenimiento regular para todos los equipos críticos, con el fin de garantizar su correcto funcionamiento y disponibilidad continua. Este programa deberá incluir inspecciones periódicas, actualizaciones de software y hardware según sea necesario, así como la reparación o reemplazo oportuno de componentes defectuosos.	SI	Este control asegura el correcto funcionamiento y la disponibilidad continua de los equipos críticos mediante inspecciones periódicas, actualizaciones de software y hardware según sea necesario, y la reparación o reemplazo oportuno de componentes defectuosos.
			A.11.2.6 Controles de seguridad de los equipos y activos fuera de las instalaciones.	A.11.2.6.1 Se debe implementar medidas de seguridad específicas para proteger los activos de información cuando sean utilizados fuera o dentro de las instalaciones de la empresa. Esto incluye el uso de conexiones seguras, cifrado de datos sensibles, autenticación de usuarios y dispositivos, y el uso de herramientas de gestión remota para garantizar la seguridad y la integridad de la información en todo momento.	SI	Este control proporciana la seguridad y la integridad de la información en todo momento al utilizar conexiones seguras, cifrado de datos sensibles, autenticación de usuarios y dispositivos, y herramientas de gestión remota.
			A.11.2.7 Controles de disposición segura o reutilización de equipos.	A.11.2.7.1 Verificación de la eliminación segura de datos de todos los equipos antes de su disposición o reutilización. Esto incluye la realización de un proceso de borrado seguro o destrucción física de los medios de almacenamiento de datos, así como la documentación adecuada para demostrar que se han tomado las medidas necesarias para proteger la información confidencial antes de deshacerse de los equipos.	SI	Este control Asegura la protección de la información confidencial al realizar un proceso de borrado seguro o destrucción física de los medios de almacenamiento de datos.

A.12	**POLÍTICAS DE SEGURIDAD EN EL ÁREA DE OPERACIONES**	A.12.1 Procedimientos operacionales y responsabilidades.	A.12.1.2 Gestión de cambios	A.12.1.2.1 Se establece que el equipo de gestión de cambios es responsable de administrar el proceso de gestión de cambios y garantizar que se implementen controles efectivos para prevenir la alteración no autorizada de la información.	SI	Este control asegura que se implementen controles efectivos para prevenir la alteración no autorizada de la información al asignar la responsabilidad al equipo de gestión de cambios.
				A.12.1.2.2 Se establece que los empleados que utilicen los sistemas de información son responsables de informar cualquier actividad sospechosa que pueda indicar una posible alteración de la información.	SI	Este control promueve una cultura de seguridad al hacer que los empleados sean responsables de identificar y reportar cualquier actividad sospechosa
				A.12.1.2.3 Se asignarán responsabilidades claras para la realización de auditorías de cambios, incluyendo la revisión de los registros de cambios y la identificación de posibles desviaciones o anomalías.	SI	Este control asegura la integridad de los sistemas al establecer responsabilidades específicas para la auditoría de cambios.
		A.12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos	A.12.2.1.1 Programación de análisis periódicos configurando el software antivirus para que realice análisis periódicos del sistema en busca de posibles amenazas. Esto puede ayudar a detectar y eliminar malware de forma proactiva.	SI	Este control ayuda a detectar y eliminar malware de manera proactiva al realizar análisis regulares en busca de posibles amenazas.
				A.12.2.1.2 Capacitación en concienciación sobre seguridad proporcionando formación al personal sobre las prácticas seguras de navegación por internet, descarga de archivos y apertura de correos electrónicos para reducir la probabilidad de caer en trampas de malware.	SI	Este control reduce la probabilidad de caer en trampas de malware al educar al personal sobre las mejores prácticas de seguridad en línea.
		A.12.3 Copias de respaldo	A.12.3.1 Controles de respaldo de información	A.12.3.1.1 Realizar copias de respaldo de la información crítica y comprobación de la misma. Esto puede incluir la programación regular de copias de seguridad automáticas, la verificación de la integridad de las copias de seguridad y la garantía de que las copias se almacenen de forma segura.	SI	Este control asegura la disponibilidad y la integridad de la información crítica al realizar copias de seguridad regulares y verificar su integridad.
		A.12.4 Registro y seguimiento.	A.12.4.1 Registro de eventos.	A.12.4.1.1 Implementar un procedimiento para el registro y almacenamiento seguro de todos los eventos de seguridad, incluyendo detalles relevantes como la fecha y hora, la naturaleza del evento, y la dirección IP involucrada.	SI	Este control ayuda a la trazabilidad y la capacidad de respuesta ante incidentes al registrar y almacenar de manera segura todos los eventos de seguridad.
				A.12.4.1.2 Utilizar herramientas de monitoreo de red y registro de eventos para verificar el tráfico en los puertos de gestión y alertar sobre actividades sospechosas, como intentos de acceso desde direcciones	SI	Este control mejora la seguridad de la red al monitorear el tráfico en los puertos de gestión y detectar actividades sospechosas.

				IP no autorizadas o a través de protocolos inusuales.		
			A.12.4.2 Protección de la información de registro.	A.12.4.2.1 Implementar controles de acceso y almacenamiento seguro para garantizar que solo personal autorizado pueda acceder, modificar o eliminar registros de eventos.	SI	Este control protege la integridad y la confidencialidad de los registros de eventos al limitar el acceso solo a personal autorizado.
		A.12.5 Control de software operacional	A.12.5.1 Control de instalación de software en sistemas operativos	A.12.5.1.1 Establecer un proceso formal para solicitar y aprobar la instalación de nuevo software en los sistemas operativos. Cualquier solicitud de instalación de software deberá ser presentada a través de un formulario de solicitud de cambios y solicitar la aprobación de un supervisor o departamento responsable designado.	SI	Este control ayuda a un control adecuado sobre la instalación de nuevo software en los sistemas operativos al requerir un proceso formal de solicitud y aprobación.
		A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1 Controles de gestión de las vulnerabilidades técnicas.	A.12.6.1.1 Cierre de puertos no utilizados en todos los sistemas de información de la organización. Los puertos que no sean necesarios para el funcionamiento de los servicios y aplicaciones serán cerrados para reducir la superficie de ataque y minimizar el riesgo de explotación.	SI	Este control reduce la superficie de ataque y minimiza el riesgo de explotación al cerrar los puertos que no son necesarios para el funcionamiento de los servicios y aplicaciones.
				A.12.6.1.2 Establecer que todos los teléfonos IP deben ser regularmente monitoreados y actualizados con las últimas versiones de firmware y parches de seguridad disponibles. Esto ayuda a mitigar las vulnerabilidades conocidas que podrían ser explotadas por herramientas o técnicas maliciosas.	SI	Este control ayuda a proteger los sistemas de comunicación de la organización contra posibles ataques y asegura que estén equipados con las defensas más recientes contra amenazas cibernéticas.
				A.12.6.1.3 Establecer un proceso formal de evaluación de riesgos que incluya la identificación de sistemas y servicios que dependen de protocolos obsoletos. Se priorizarán las acciones de mitigación en función del riesgo identificado.	SI	Este control permite identificar y abordar de manera proactiva los sistemas y servicios que dependen de protocolos obsoletos, los cuales pueden representar vulnerabilidades de seguridad significativas.
A.13	**POLÍTICAS DE LA SEGURIDAD DE LAS COMUNICACIONES**	A.13.1 Gestión de la seguridad de las redes.	A.13.1.1 Controles de redes.	A.13.1.1.1 Se implementarán firewalls de seguridad perimetral para proteger la red contra accesos no autorizados, ataques maliciosos y filtrado de tráfico no deseado.	SI	Este control ayuda a filtran el tráfico no deseado, bloquean accesos no autorizados y previenen ataques maliciosos, contribuyendo así a mantener la integridad y la seguridad de los sistemas de información de la organización.
				A.13.1.1.2 Establecer filtros de tráfico en puntos estratégicos de la red para bloquear el acceso no autorizado y prevenir la propagación de malware. Cada filtro debe actualizarse regularmente para adaptarse a las nuevas amenazas y patrones de ataque y	SI	Este control proporciona filtros de tráfico en puntos estratégicos de la red ayudan a prevenir el acceso no autorizado y la propagación de malware al bloquear tráfico malicioso.

				llevar monitoreo continuo de tráfico de red para detectar patrones inusuales o comportamientos sospechosos.		
				A.13.1.1.3 Se debe establecer una red interna segregada y protegida, limitando el acceso desde Internet y promoviendo conexiones seguras y autenticadas desde la red interna.	SI	Este control propone conexiones seguras y autenticadas desde la red interna refuerza la seguridad al garantizar que solo usuarios autorizados puedan acceder a recursos y datos sensibles, reduciendo así el riesgo de acceso no autorizado y mitigando posibles ataques desde el exterior.
				A.13.1.1.4 Implementar enrutadores que filtren el tráfico entre las diferentes zonas de la red y bloqueen el acceso no autorizado a los puertos de gestión desde redes externas o menos confiables.	SI	Este control propone enrutadores que filtran el tráfico entre diferentes zonas de la red ayudan a controlar y proteger el flujo de datos, previniendo accesos no autorizados entre distintas partes de la red.
			A.13.1.2 Control de seguridad de los servicios de red.	A.13.1.2.1 Se debe priorizar la actualización o eliminación de protocolos obsoletos o vulnerables que puedan exponer la red a riesgos de seguridad. A la vez se deben implementar mecanismos de seguridad, como firewalls, sistemas de detección de intrusos (IDS), para proteger la red contra intrusiones y ataques.	SI	Este control propone actualizaciones o eliminaciones de protocolos obsoletos o vulnerables es esencial para reducir la exposición de la red a riesgos de seguridad conocidos.
				A.13.1.2.2 Establecer un proceso formal para gestionar cambios en la configuración de los servicios de red, que incluya la evaluación de impacto en la seguridad, la aprobación por parte de autoridades competentes y la documentación adecuada de los cambios realizados.	SI	Este control propone un proceso formal de gestión de cambios en la configuración de los servicios de red garantiza que cualquier modificación se realice de manera controlada y segura.
				A.13.1.2.3 Establecer que los teléfonos IP deben estar en una red separada o en segmentos de red dedicados para reducir la superficie de ataque y limitar el alcance de cualquier intento malicioso que pueda ocurrir en la red.	SI	Este control ayuda a proteger los sistemas de comunicación de la organización y a garantizar la disponibilidad y seguridad de los servicios de voz sobre IP (VoIP).
				A.13.1.2.4 Mantener actualizados los dispositivos y aplicaciones del teléfono IP con los últimos parches de seguridad para mitigar las vulnerabilidades conocidas que podrían ser explotadas en ataques de phishing.	SI	Este control fortalece la seguridad de los sistemas de comunicación de la organización y reduce el riesgo de compromisos de seguridad y pérdida de datos debido a ataques maliciosos

				A.13.1.2.5 Todos los equipos de red, incluidos switches, routers y dispositivos de acceso, deben tener la función de Port Security habilitada en todos los puertos. Esta función debe estar configurada para aprender automáticamente las direcciones MAC y asignarlas al puerto correspondiente para evitar conexiones no deseadas a los equipos o puertos en cuestión ejecutando una acción en el momento que esta violación de seguridad ocurra.	SI	Este control ayuda a prevenir accesos no autorizados y protege la integridad y la seguridad de la red al tomar medidas proactivas contra posibles violaciones de seguridad
		A.13.2 Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información.	A.13.2.1.1 Las transferencias de información, dentro de la organización o hacia entidades externas, deben estar cifradas utilizando algoritmos y protocolos de cifrado. Se deben utilizar canales de comunicación seguros y confiables para la transferencia de información sensible. Esto puede incluir el uso de conexiones VPN (Redes Privadas Virtuales), protocolos de transferencia segura como HTTPS o SFTP, entre otros.	SI	Este control asegura la confidencialidad y la integridad de los datos durante su tránsito, protegiéndolos contra accesos no autorizados y posibles interceptaciones.
				A.13.2.1.2 Establecer un procedimiento formal para que el personal notifique inmediatamente cualquier incidente de phishing al equipo de seguridad de la información o al equipo de respuesta a incidentes de la organización.	SI	Este control establece un procedimiento formal de notificación de incidentes de phishing, se fomenta una respuesta rápida y efectiva ante posibles ataques de phishing.
			A.13.2.4 Acuerdos de confidencialidad o de no divulgación.	A.13.2.4.1 Reforzar los acuerdos de confidencialidad o de no divulgación para incluir disposiciones específicas sobre la protección de la información confidencial ante ataques informáticos o de ingeniería social, prohibiendo la divulgación de información importante para la empresa.	SI	Este control refuerza los acuerdos de confidencialidad o de no divulgación con disposiciones específicas relacionadas con la protección de la información confidencial frente a ataques informáticos o de ingeniería social ayuda a garantizar que el personal comprenda la importancia de mantener la confidencialidad de la información crítica de la empresa.
A.14	**POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	A.14.1 Requisitos de seguridad de los sistemas de información.	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información.	A.14.1.1.1 Se deben implementar controles de acceso adecuados para restringir el acceso a sistemas y aplicaciones solo a usuarios autorizados. Esto puede ayudar a prevenir la inyección de código mediante la limitación de puntos de entrada potenciales.	SI	Este control ayuda a implementar controles de acceso adecuados, se limita el acceso a sistemas y aplicaciones únicamente a usuarios autorizados, reduciendo así la superficie de ataque y mitigando el riesgo de inyección de código.
		A.14.2 Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1 Política de desarrollo seguro.	A.14.2.1.1 Todos los códigos fuente deben ser revisados por pares o a través de revisiones automáticas para garantizar que	SI	Este control propone realizar revisiones por pares o revisiones automáticas, se aumenta la probabilidad de detectar estos errores

				no se incluyan claves de API en el código de manera insegura.		antes de que se desplieguen en producción, lo que ayuda a proteger la seguridad y la integridad de los sistemas de la organización
				A.14.2.1.2 Se debe prohibir almacenar claves de API o credenciales en el código fuente sin cifrado. En su lugar, se deben utilizar mecanismos seguros de servicios de gestión de secretos o variables de entorno protegido como AWS Secrets Manager, Azure Key Vault o HashiCorp Vault, para almacenar y gestionar las claves de las API de manera segura.	SI	Este control propone almacenar claves de API o credenciales en el código fuente sin cifrado representa un riesgo de seguridad significativo, ya que estos pueden ser expuestos accidentalmente o comprometidos por atacantes.
				A.14.2.1.3 Todas las entradas de usuarios deben ser validadas y saneadas antes de ser procesadas por la aplicación. Se deben utilizar listas blancas de caracteres permitidos y rechazar cualquier entrada que no cumpla con los criterios establecidos. Utilizar funciones de escape específicas del lenguaje de programación y del sistema de gestión de bases de datos (DBMS) para neutralizar cualquier código SQL malicioso.	SI	Este control ayuda validar y sanear las entradas de usuarios es fundamental para prevenir ataques de inyección de código, como los ataques SQL, que pueden comprometer la seguridad y la integridad de la aplicación y la base de datos
				A.14.2.1.4 Todas las entradas de usuarios, incluyendo datos de formularios, URL y cookies, deben ser validadas y escapadas antes de ser mostradas en la interfaz de usuario. Se deben utilizar funciones de escape específicas del contexto (HTML, atributo HTML, JavaScript, etc.) para evitar la ejecución de código malicioso.	SI	Este control ayuda a la validación y escape de las entradas de usuarios antes de mostrarlas en la interfaz de usuario ayuda a prevenir ataques de inyección de código, como los ataques de scripting entre sitios (XSS), que pueden comprometer la seguridad de la aplicación y los datos del usuario.
				A.14.2.1.5 Configurar cabeceras HTTP de seguridad, como Content-Security-Policy (CSP), para mitigar el riesgo de XSS al restringir el origen de los recursos cargados en la página.	SI	Este control propone la configuración de cabeceras HTTP de seguridad, como Content-Security-Policy (CSP), ayuda a mitigar el riesgo de ataques de scripting entre sitios (XSS) al restringir el origen de los recursos cargados en la página web.
			A.14.2.2 Procedimientos de control de cambios en sistemas.	A.14.2.2.1 Se deben utilizar herramientas de gestión de configuración de red para realizar un seguimiento de todos los cambios realizados en la configuración de la red. Los cambios críticos en la configuración de la red deben ser revisados por el equipo de seguridad de la información antes de su implementación.	SI	Este control propone el seguimiento de los cambios en la configuración de la red mediante herramientas de gestión de configuración ayuda a garantizar la integridad y la seguridad de la infraestructura de red.

				A.14.2.2.2 Todos los procesos o cambios de la red deben ser solicitados mediante un formulario de solicitud de cambio (RFC) y aprobados por el equipo de administración encargado.	SI	Este control propone la implementación de un proceso formal de solicitud y aprobación de cambios en la red mediante RFCs ayuda a garantizar que los cambios sean planificados, documentados y aprobados por las partes interesadas pertinentes antes de su implementación.
				A.14.2.2.3 El equipo de seguridad de la información es responsable de supervisar la implementación de controles para prevenir la mala utilización del sistema y tomar medidas correctivas según sea necesario.	SI	Este control propone la supervisión por parte del equipo de seguridad de la información es esencial para garantizar que los controles de seguridad implementados en la red estén funcionando adecuadamente y para detectar cualquier actividad sospechosa o mala utilización del sistema.
			A.14.2.8 Prueba de seguridad de sistemas.	A.14.2.8.1 Realizar pruebas de inyección SQL como parte de las pruebas de seguridad estándar para todas las aplicaciones que interactúan con bases de datos. Utilizar herramientas de pruebas de seguridad automatizadas (DAST) como Burp Suite, Netsparker o Acunetix para identificar posibles puntos de inyección SQL en las aplicaciones.	SI	Este control ayuda a realizar pruebas de inyección SQL son cruciales para identificar y mitigar vulnerabilidades en las aplicaciones web que interactúan con bases de datos.
				A.14.2.8.2 Realizar pruebas automatizadas de XSS como parte de las pruebas de seguridad estándar para todas las aplicaciones web. Utilice herramientas de escaneo de vulnerabilidades que puedan identificar de manera automática y precisa las vulnerabilidades de XSS como Burp Suite, Netsparker, Acunetix.	SI	Este control ayuda a realizar pruebas automatizadas de XSS son fundamentales para identificar y mitigar vulnerabilidades en las aplicaciones web que podrían ser explotadas por atacantes para ejecutar scripts maliciosos en el navegador del usuario.

CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

3.1 Plan de evaluación

Metodología Delphi

1. Preparación

a. Definición del Objetivo

- Evaluar si la gestión de riesgos cumple con los aspectos requeridos en la norma ISO/IEC 27005 y la metodología NIST-SP 800-30 mediante la aplicación de una encuesta a expertos en el área.

b. Selección de Expertos

- Identificar y seleccionar un panel de expertos en seguridad de la información y gestión de riesgos con experiencia en las normas ISO 27000.
- En total son 5 expertos en el área de TI. La información de los expertos se encuentra en el Anexo 8.

2. Desarrollo de la Encuesta

a. Diseño de la Encuesta Inicial

- Crear un cuestionario con preguntas cerradas y abiertas sobre la gestión de riesgos en seguridad de la información.
- Preguntas deben abordar aspectos como efectividad, factibilidad, aplicabilidad, y esfuerzo de implementación. En el Anexo 10 se pueden ver las preguntas de la encuesta inicial antes de realizar la prueba piloto.

b. Piloto

- Realizar un piloto del cuestionario con el especialista 2, cotutor y el encargado del seminario de titulación para identificar fallas y mejorar las preguntas. En el Anexo 9 se puede ver la información de los docentes encuestados y en el Anexo 10 las correcciones de la encuesta inicial.
- Se debe corregir la encuesta en base a la prueba piloto aplicada a los docentes para obtener la encuesta final que se aplicará a los expertos seleccionados.

3. Ronda de Encuestas

a. Distribución del Cuestionario

- Enviar la encuesta final a los expertos seleccionados. La encuesta final se la puede visualizar en el Anexo 11.
- Asegurarse de proporcionar un plazo claro para las respuestas.

b. Recopilación de Respuestas

- Recopilar las respuestas y realizar un análisis cuantitativo preliminar.

4. Análisis y Retroalimentación

a. Análisis de Resultados

- Analizar las respuestas para identificar áreas de consenso y discrepancias.
- Preparar un resumen de los resultados.

5. Informe Final

a. Redacción del Informe

- Preparar un informe detallado con los resultados finales, incluyendo gráficos y tablas que resumen los hallazgos.

b. Recomendaciones

- Incluir recomendaciones específicas basadas en el consenso de los expertos.

Cronograma

Tabla 24 Cronograma de evaluación

Actividad	Duración	Fecha de inicio	Fecha de finalización
Definición de objetivo y alcance	1 semana	10/06/2024	14/06/2024
Piloto de encuestas	1 semana	10/06/2024	14/06/2024
Encuesta final	1 semana	10/06/2024	14/06/2024
Distribución de encuestas	2 semanas	17/06/2024	28/07/2024
Recopilación de respuestas	1 semanas	01/07/2024	05/07/2024
Análisis de resultados	2 semana	08/07/2024	19/07/2024
Redacción de informe	1 semana	22/07/2024	26/07/2024

3.2 Resultados de la evaluación

Encuesta aplicada a expertos en el área de TI y sus resultados

1. ¿Considera usted que se han clasificado adecuadamente los activos de la empresa?

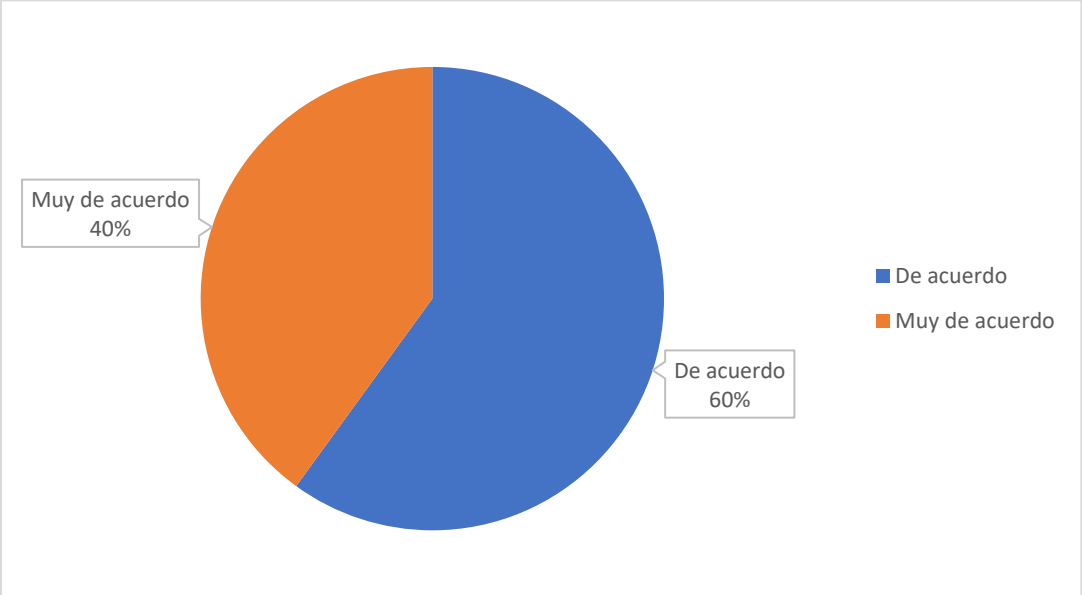


Figura 9 Resultados pregunta 1 de encuesta a expertos

La mayoría de los expertos consideran que la clasificación de los activos de la empresa se ha realizado adecuadamente, con tres personas que están "De acuerdo" y dos que están "Muy de acuerdo", tal y como se observa en la figura 9. No se reportaron respuestas en desacuerdo o en neutralidad, lo que sugiere una percepción positiva generalizada sobre la clasificación de los activos en la empresa.

2. ¿Se han identificado las posibles amenazas de seguridad de la información a los activos de la empresa?

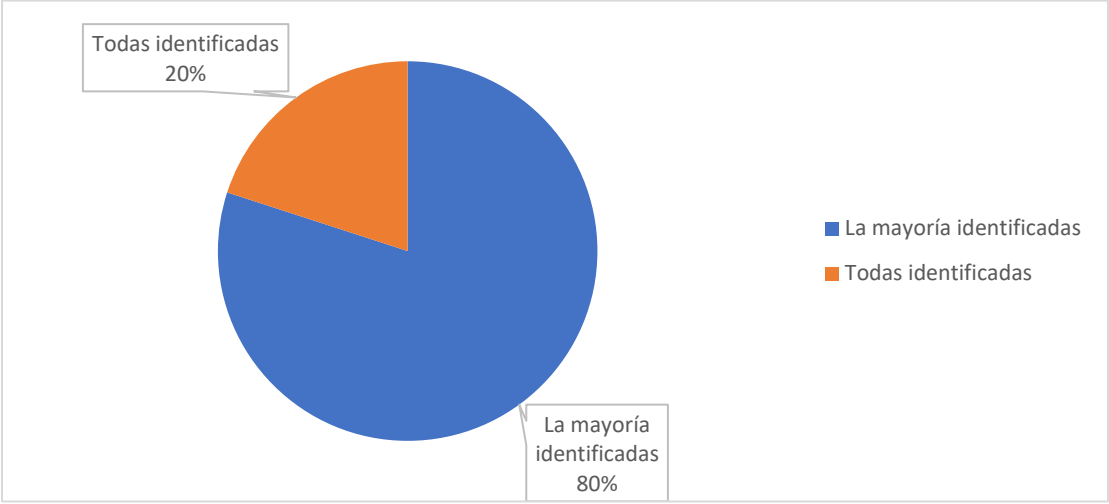


Figura 10 *Resultados pregunta 2 de encuesta a expertos*

De acuerdo con los resultados obtenidos, se observa en la figura 10 que una mayoría significativa de los expertos encuestados, representando el 80%, considera que "La mayoría" de las amenazas han sido identificadas. Solo un 20% de los participantes afirma que "Todas" las amenazas han sido identificadas.

3. ¿Se han considerado las posibles vulnerabilidades involucradas para la seguridad de la información?

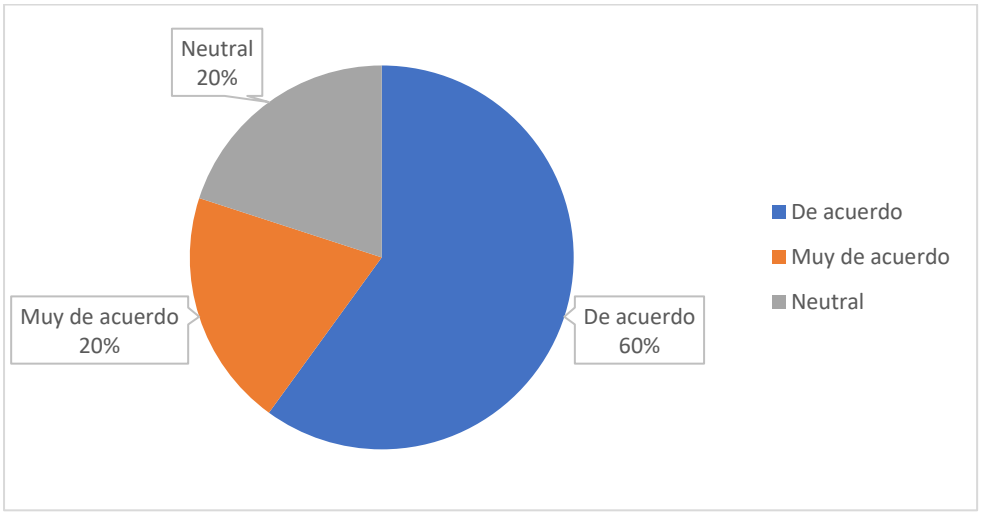


Figura 11 *Resultados pregunta 3 de encuesta a expertos*

Los resultados de la figura 11 muestran que la mayoría de los expertos se sienten confiados en que se han tenido en cuenta todas las vulnerabilidades. Específicamente, el 60% de los encuestados están "De acuerdo" con esta afirmación, mientras que un 20% está "Muy de acuerdo" y otro 20% se mantiene "Neutral". Estos datos indican una percepción positiva general sobre la consideración de las vulnerabilidades, aunque la presencia de respuestas neutrales sugiere que puede haber ciertas dudas o áreas que podrían mejorarse.

4. ¿Cree que se han considerado adecuadamente los impactos potenciales de los riesgos?

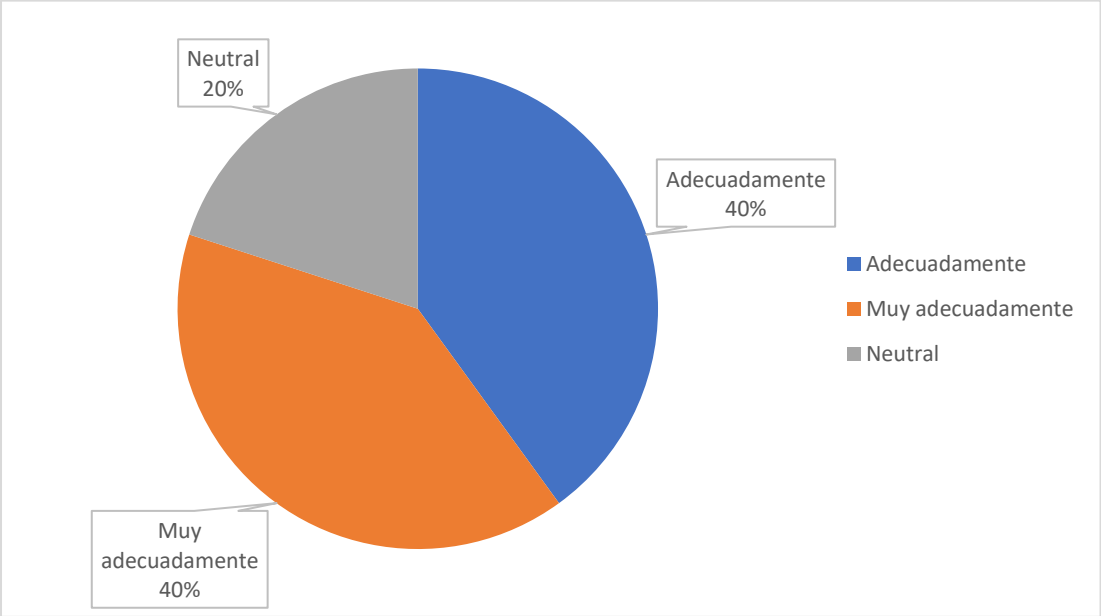


Figura 12 *Resultados pregunta 4 de encuesta a expertos*

Los resultados vistos en la figura 12 reflejan una percepción mayoritariamente positiva sobre la consideración de los impactos de los riesgos. El 40% de los encuestados considera que los impactos se han considerado "Adecuadamente" y otro 40% cree que se han considerado "Muy adecuadamente". Sin embargo, un 20% de los participantes se mantiene "Neutral", lo que indica que, aunque hay un reconocimiento general del buen manejo de los impactos potenciales, aún hay una pequeña porción de la población que no está completamente convencida.

5. ¿Cómo calificaría la precisión para evaluar el análisis cuantitativo de los riesgos?

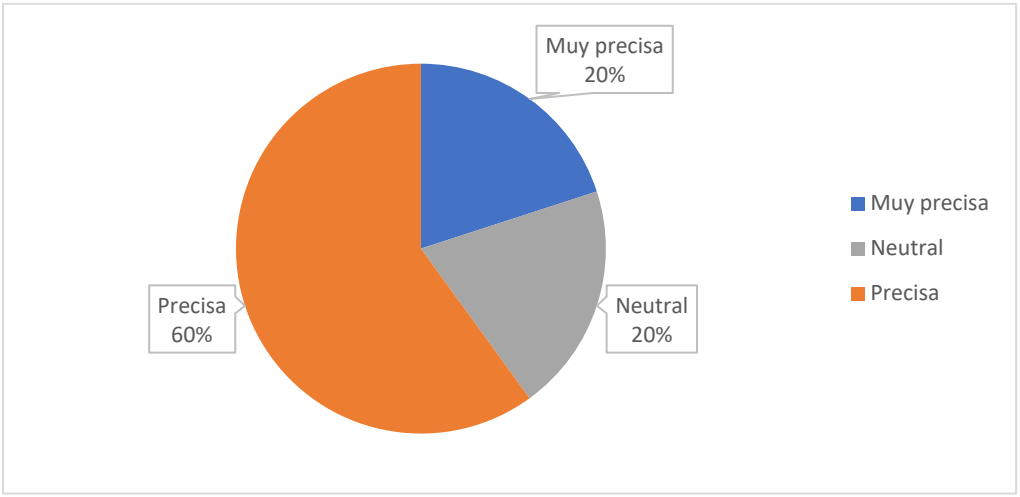


Figura 13 *Resultados pregunta 5 de encuesta a expertos*

La figura 13 muestra resultados que indican una percepción predominantemente positiva sobre la precisión del análisis cuantitativo de riesgos. El 60% de los encuestados considera que el análisis es "Preciso", mientras que un 20% lo califica como "Muy preciso". Sin embargo, un 20% de los participantes se muestra "Neutral", lo que sugiere que, aunque la mayoría está satisfecha con la precisión del análisis, existe una minoría que no está totalmente convencida de su exactitud.

6. ¿Cree que se ha utilizado un criterio adecuado para la priorización de riesgos?

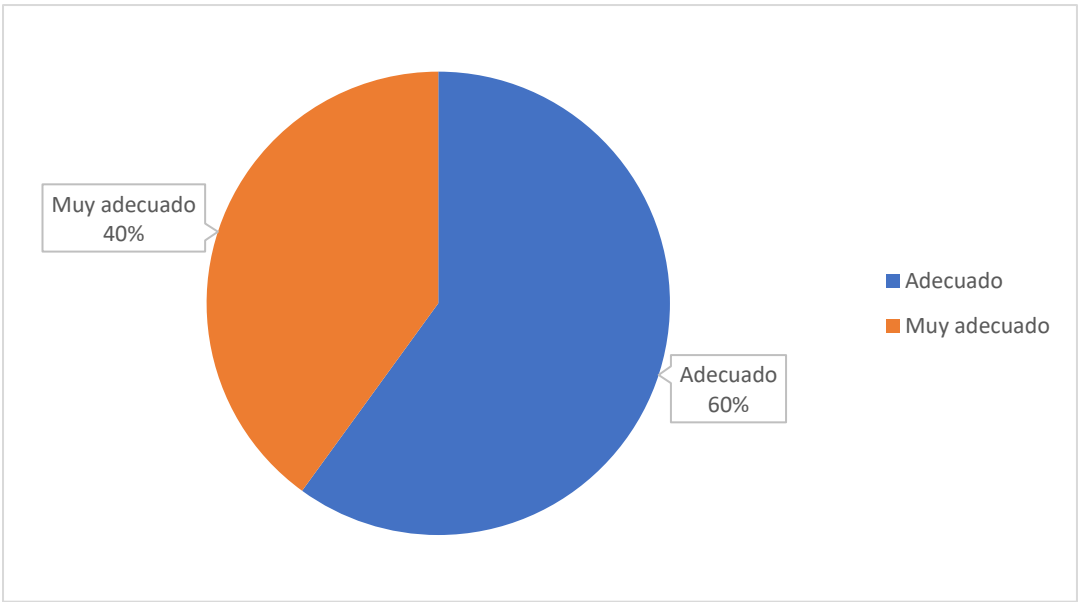


Figura 14 *Resultados pregunta 6 de encuesta a expertos*

Los resultados que se pueden observar en la figura 14, muestran una valoración muy positiva por parte de los encuestados. El 60% de los participantes considera que el criterio utilizado es "Adecuado" y un 40% lo califica como "Muy adecuado". Estos resultados indican un alto grado

de satisfacción y confianza en el criterio de priorización de riesgos empleado. No se registraron respuestas negativas o neutrales, lo que sugiere que el método actual para priorizar riesgos es efectivo y bien recibido.

7. ¿Considera que se ha dado suficiente importancia a los riesgos de alto impacto?

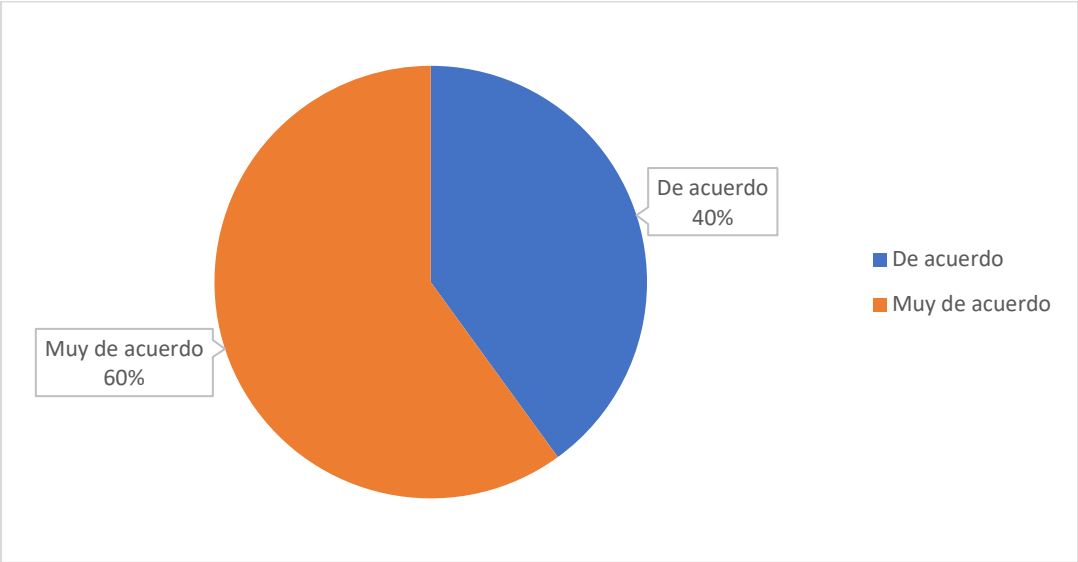


Figura 15 *Resultados pregunta 7 de encuesta a expertos*

Los resultados reflejados en la figura 15, dan una percepción muy positiva entre los encuestados. El 40% de los participantes está "De acuerdo" con que se ha dado suficiente importancia a estos riesgos, mientras que un 60% está "Muy de acuerdo". No se registraron respuestas negativas o neutrales, lo que indica un alto nivel de satisfacción respecto a la atención prestada a los riesgos de alto impacto. Esta fuerte aprobación sugiere que los esfuerzos y estrategias implementadas para gestionar los riesgos de mayor impacto están bien fundamentados y son efectivos.

8. ¿Cómo evalúa la adecuación de los controles propuestos, basados en la norma ISO/IEC 27002:2013, para reducir los riesgos?

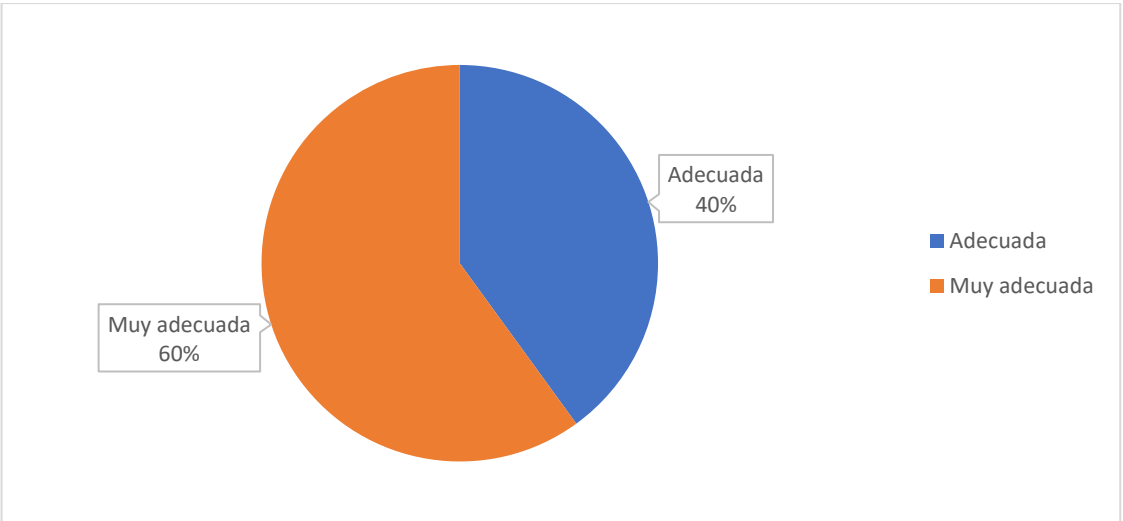


Figura 16 *Resultados pregunta 8 de encuesta a expertos*

Los resultados vistos en la figura 16 indican una evaluación muy positiva de los controles propuestos. El 40% de los encuestados considera que los controles son "Adecuados" y el 60% los califica como "Muy adecuados". No se registraron respuestas negativas o neutrales, lo que demuestra una fuerte aprobación de los controles implementados según la norma ISO/IEC 27002:2013. Estos resultados sugieren que los expertos tienen un nivel de satisfacción alto en que los controles actuales son efectivos para mitigar los riesgos.

9. ¿Está de acuerdo con la factibilidad de implementar los controles sugeridos?

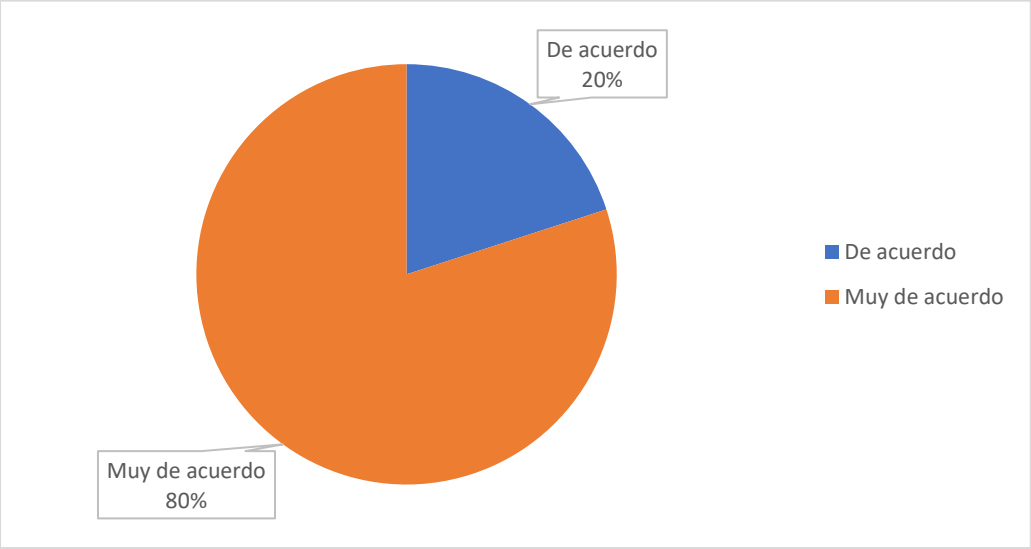


Figura 17 *Resultados pregunta 9 de encuesta a expertos*

Los resultados mostrados en la figura 17 dan una percepción muy favorable entre los expertos con respecto a la factibilidad de implementar los controles sugeridos. Los encuestados indicaron estar de acuerdo 20% o muy de acuerdo el 80% con esta afirmación. Este alto nivel de acuerdo refleja una fuerte confianza en la viabilidad y eficacia de las medidas propuestas. La falta de respuestas neutrales o negativas sugiere un respaldo unánime hacia la implementación de estos controles, destacando su importancia para la gestión efectiva de riesgos en la organización.

10. ¿Considera que las estrategias de tratamiento de riesgos (evitar, transferir, reducir, aceptar) son adecuadas?

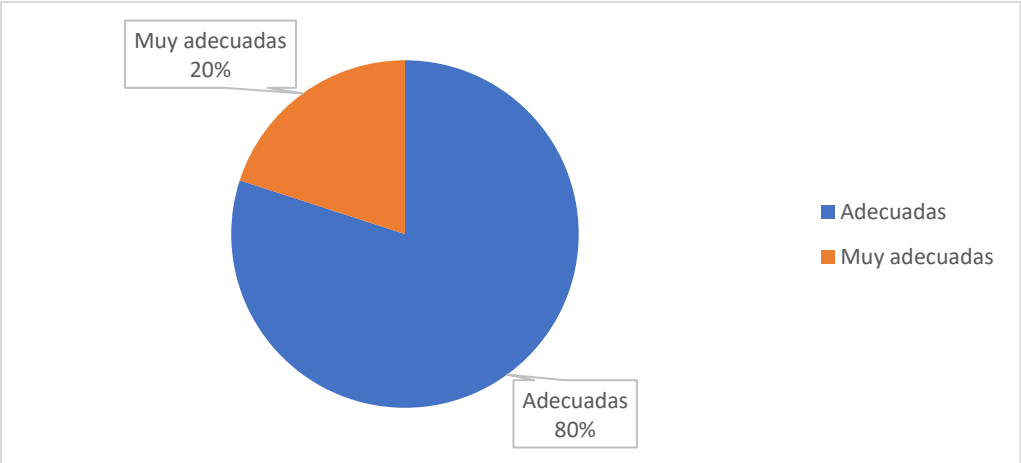


Figura 18 *Resultados pregunta 10 de encuesta a expertos*

Los resultados muestran una evaluación positiva por parte de los encuestados respecto a las estrategias de tratamiento de riesgos implementadas. Como se puede ver en la figura 18, el 40% de los participantes considera que estas estrategias son "Adecuadas", mientras que el 60% las califica como "Muy adecuadas". No se registraron respuestas negativas, lo que indica un fuerte respaldo hacia la efectividad y pertinencia de las estrategias adoptadas. Esta alta aprobación sugiere que las estrategias actuales son percibidas como eficaces para gestionar los riesgos identificados, lo cual es fundamental para reducir impactos adversos en la organización.

11. ¿En qué medida considera que la gestión de riesgos cumple con los principios de la norma ISO/IEC 27005?

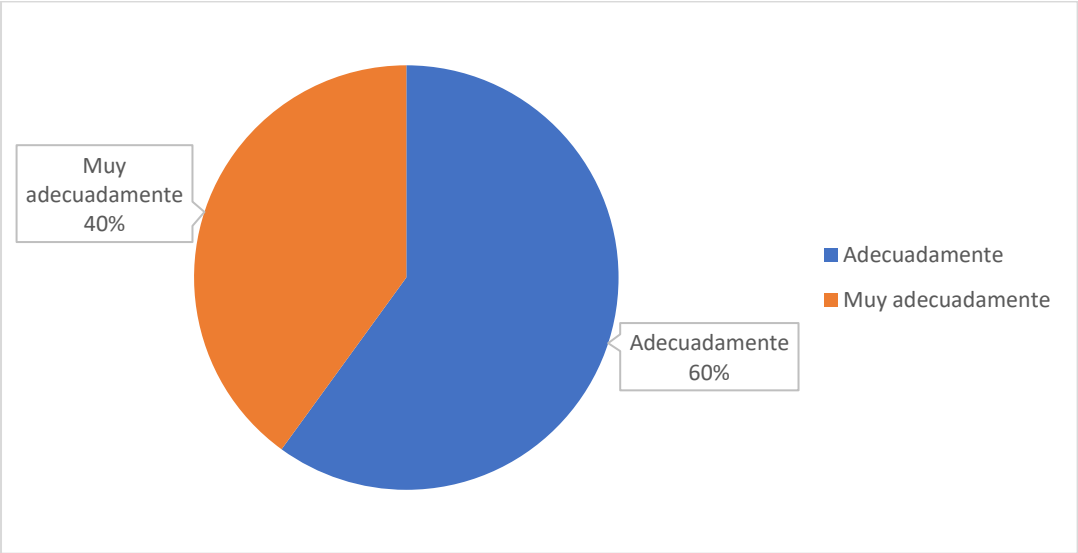


Figura 19 *Resultados pregunta 11 de encuesta a expertos*

Según la figura 19, los encuestados tienen una percepción favorable sobre la gestión de riesgos en relación con los principios de la norma ISO/IEC 27005. El 60% considera que la gestión de riesgos cumple "Adecuadamente" con estos principios, mientras que el 40% la califica como "Muy adecuadamente". No se registraron respuestas que indiquen una percepción negativa, lo que sugiere un respaldo generalizado hacia la alineación de la gestión de riesgos con los estándares establecidos. Esta evaluación positiva indica que las prácticas actuales de gestión de riesgos están bien fundamentadas y son consistentes con los requisitos normativos, lo cual es esencial para garantizar la seguridad de la información y la protección de los activos críticos de la organización.

12. ¿Considera que la comunicación de resultados ha sido clara y comprensible para la organización?

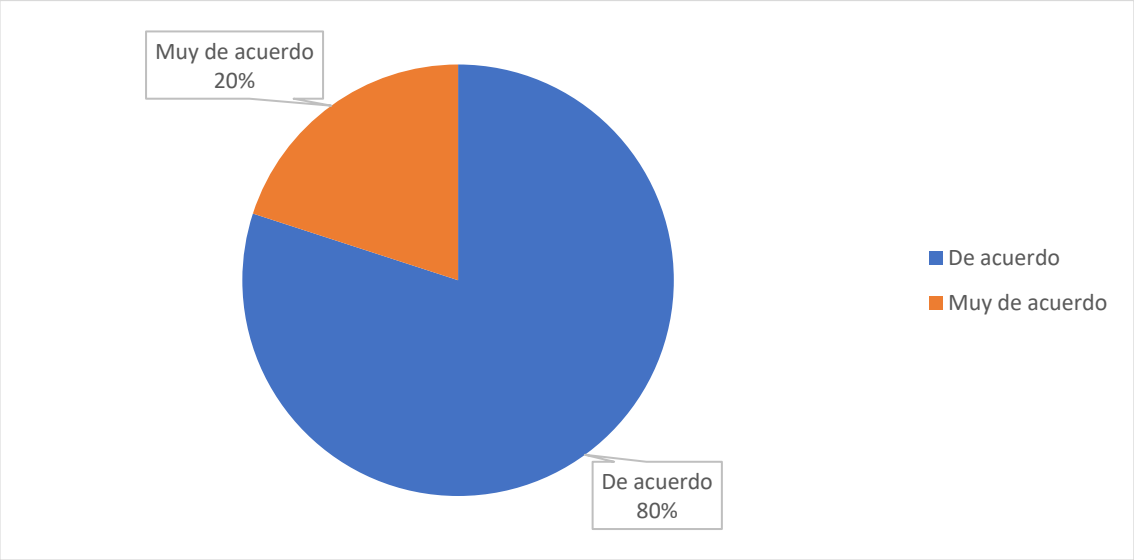


Figura 20 *Resultados pregunta 12 de encuesta a expertos*

Los resultados muestran una percepción positiva entre los expertos respecto a la claridad y comprensibilidad de la comunicación de resultados dentro de la organización. Tal y como se observa en la figura 20, el 20% de los participantes está "De acuerdo" con la claridad de la comunicación, mientras que el 80% está "Muy de acuerdo". La falta de respuestas neutrales o negativas indica un fuerte respaldo hacia la efectividad de la comunicación de resultados. La alta aprobación sugiere que la organización ha logrado transmitir información de manera clara y comprensible, lo cual es crucial para asegurar que todos los niveles de la organización estén informados y puedan actuar adecuadamente en base a los resultados presentados.

13. ¿Cree que las medidas propuestas, basadas en la norma ISO/IEC 27002:2013, mejorarán significativamente la seguridad de la información de la empresa?

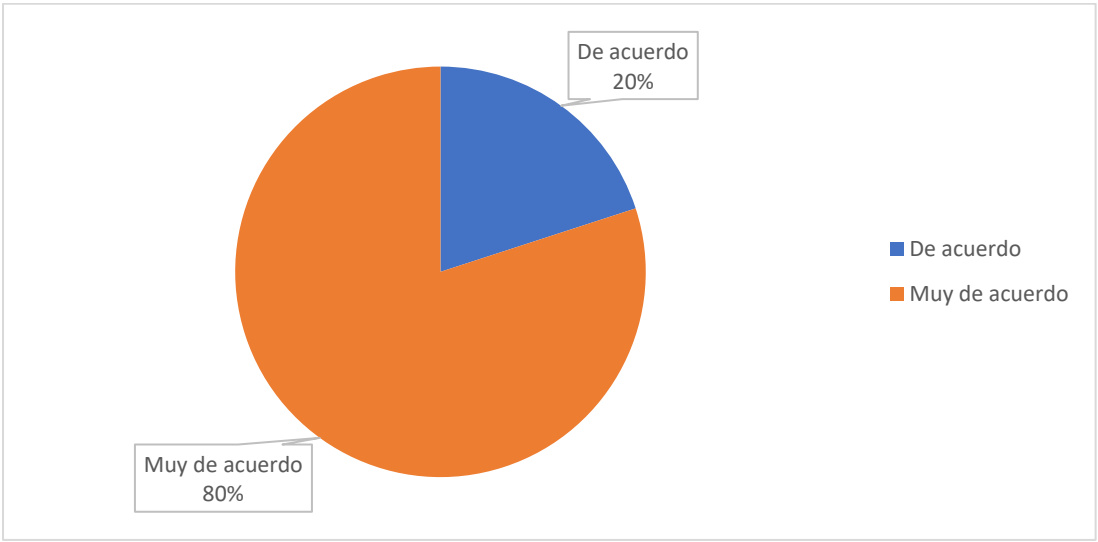


Figura 21 *Resultados pregunta 13 de encuesta a expertos*

Los resultados de la encuesta revelan una percepción muy positiva entre los encuestados con respecto a las medidas propuestas basadas en la norma ISO/IEC 27002:2013. Según la figura 21, los participantes expresaron estar de acuerdo con el 20% o muy de acuerdo con el 80% con la afirmación de que estas medidas conducirán a una mejora significativa en la seguridad de la información de la empresa. Esta alta aprobación sugiere una confianza generalizada en la efectividad y la adecuación de las propuestas de mejora para fortalecer la seguridad de la información de la empresa. La unanimidad en estas respuestas también refleja un consenso sobre la importancia de seguir las mejores prácticas establecidas en la norma para mitigar riesgos y proteger los activos de la organización.

14. ¿Están claramente documentados los procedimientos de la gestión de riesgos?

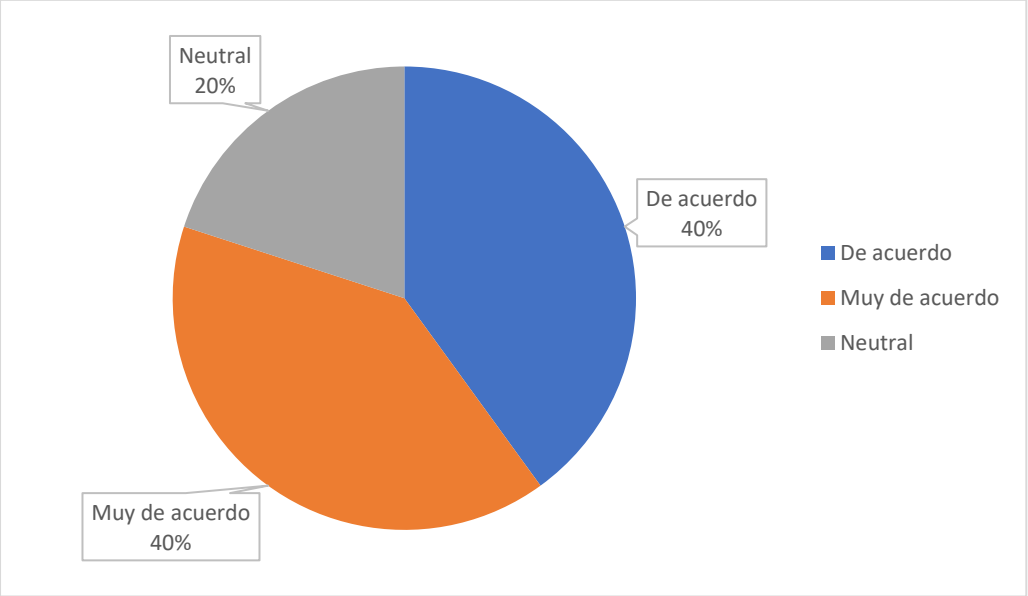


Figura 22 *Resultados pregunta 14 de encuesta a expertos*

Los resultados de la encuesta vistos en la figura 22, muestran una percepción mixta entre los encuestados respecto a la claridad de la documentación de los procedimientos de gestión de riesgos. El 40% de los participantes indicaron estar "De acuerdo" y otro 40% estuvo "Muy de acuerdo" con esta afirmación. Además, el 20% se mostró neutral en su respuesta. Esta distribución sugiere una percepción general positiva hacia la claridad de los procedimientos documentados, con una minoría que no expresó una opinión clara al respecto. Es importante abordar las opiniones neutrales para comprender mejor las necesidades de comunicación y asegurarse de que todos los miembros de la organización estén completamente informados y capacitados sobre los procedimientos de gestión de riesgos. Esto incluye iniciativas para mejorar la accesibilidad, la comprensión y la actualización continua de la documentación, asegurando así una implementación efectiva de los procedimientos de gestión de riesgos en toda la organización.

15. ¿Tiene algún comentario adicional o recomendación sobre la gestión de riesgos que quisiera hacer con base en su experiencia?

- La aplicación de la norma es correcta, y cumple con sus objetivos.

- La valoración de los activos (teléfonos celulares de departamentos y cámaras de seguridad) deberían tener un valor de 3 en el apartado de confidencialidad, ya que la difusión de la información de esos dispositivos puede generar un alto impacto en la reputación de la empresa.
- Todo está bien, solo acotar la importancia de ser proactivos y ver el panorama completo para proteger nuestros activos e información, por ejemplo: la Resiliencia y Recuperación.

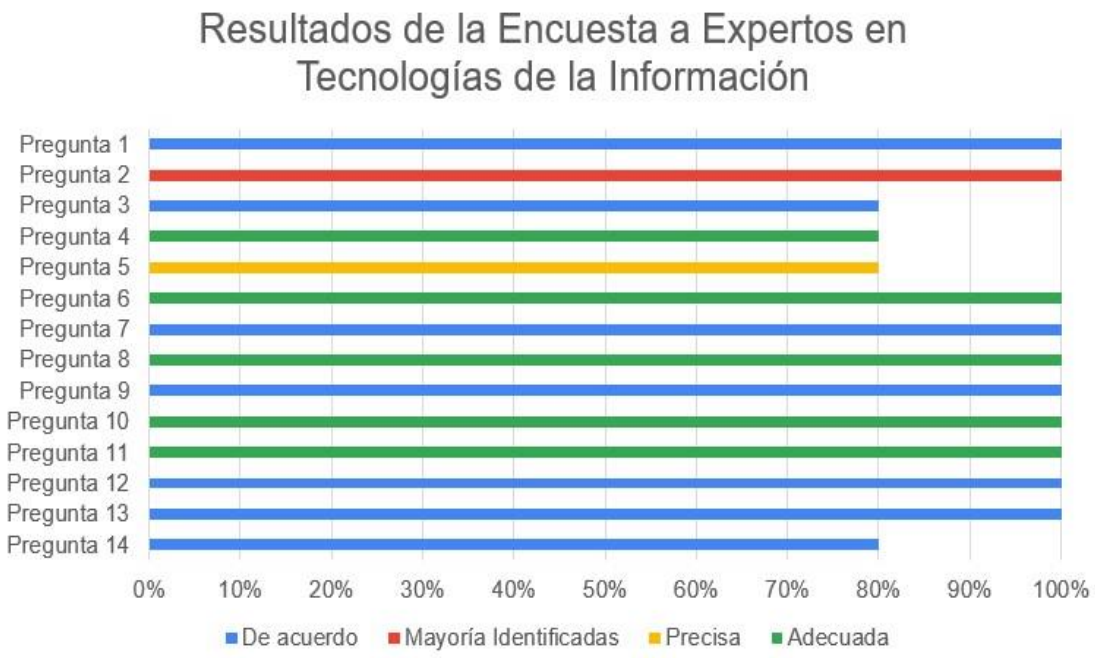


Figura 23 *Resultados finales de la encuesta a expertos*

Luego de aplicar una encuesta a 5 expertos en el área de Tecnologías de la Información con 14 preguntas cerradas y 1 pregunta abierta, las cuales abordaron todas las fases de la gestión de riesgos en seguridad de la información, los resultados muestran que la opinión mayoritaria de los expertos valida que, al seguir los lineamientos de las normas ISO/IEC 27005 y NIST-SP 800-30, se logra un marco sólido y efectivo para la gestión de riesgos. Por lo tanto, la figura 23 evidencia que todos los encuestados validaron el cumplimiento de las normas en al menos un 80% (promedio 94%), por lo que, se puede concluir que la hipótesis planteada sí se cumple, y que la gestión de riesgos llevada a cabo en la empresa es conforme a las normas y estándares internacionales utilizadas, contribuyendo significativamente a la mitigación de incidentes de seguridad.

4. CONCLUSIONES

- En conclusión, la realización de la gestión de riesgos de la seguridad de la información, basándose en la norma ISO/IEC 27005 y la metodología NIST SP 800-30, permitió una identificación precisa de los riesgos y la formulación de propuesta de mejoras. Estas mejoras

están alineadas con los estándares internacionales, fortaleciendo la seguridad de la información en los activos de la empresa.

- La investigación de las normas internacionales proporcionó una base sólida para entender y aplicar políticas, procedimientos y controles de seguridad. Esto facilitó la creación de un marco de gestión de riesgos adaptado a las necesidades específicas de la empresa.
- La identificación de activos y la evaluación de riesgos proporcionaron una visión clara de las vulnerabilidades y amenazas específicas a las que se enfrenta la empresa, permitiendo la priorización de las áreas críticas para la seguridad de la información de la empresa.
- La formulación de propuesta de mejoras, alineadas con las mejores prácticas internacionales, ofrecen a la empresa un plan para fortalecer su seguridad de la información. Entre las propuestas de mejora se incluyen recomendaciones técnicas y organizacionales diseñadas para mitigar los riesgos identificados, se propusieron cambios en las políticas y procedimientos de seguridad, formación y concienciación del personal. Aunque estas propuestas aún no se han implementado y están sujetas a la decisión final de la empresa, su elaboración se fundamentó en un análisis de las necesidades y vulnerabilidades específicas identificadas durante el proceso de evaluación de riesgos.
- El tratamiento de riesgos redujo significativamente el impacto de las amenazas y vulnerabilidades identificadas en los activos. La decisión de reducir los riesgos, en lugar de evitarlos, transferirlos o aceptarlos, refleja un enfoque proactivo y comprometido con la mejora continua de la seguridad de la información. Esta estrategia se fundamentó en la propuesta de controles y medidas de seguridad diseñadas para disminuir tanto la probabilidad de ocurrencia como el impacto potencial de los riesgos identificados.
- La encuesta aplicada a los expertos confirmó que la gestión de riesgos cumple con los aspectos de las normas y estándares internacionales mencionados. De las respuestas obtenidas, la mayoría coincidió en que los aspectos esenciales de ambas normas están presentes y correctamente aplicados en la gestión de riesgos evaluada, permitiendo la mitigación de incidentes de seguridad dentro de la empresa.

5. RECOMENDACIONES

- Recomendar que cuando se haga una próxima gestión de riesgos, verificar que las normas y estándares internacionales utilizados sean las últimas versiones para asegurar que las políticas y procedimientos de seguridad sigan siendo efectivos y relevantes.
- Realizar evaluaciones de riesgos periódicas para identificar y mitigar nuevas amenazas que puedan surgir debido a cambios en el entorno tecnológico y de negocio.
- Fomentar la colaboración entre departamentos para una gestión de riesgos más integral, asegurando que los aspectos de la seguridad de la información sean considerados y abordados en todas las áreas de la empresa.
- Recomendar que la alta dirección de la empresa esté comprometida con la implementación de la propuesta de mejoras y que se asignen los recursos adecuados para llevar a cabo las iniciativas de seguridad de la información.
- Realizar auditorías de seguridad regulares para asegurar que los controles implementados estén funcionando como se espera y para identificar áreas de mejora continua.

- Se recomienda que para lograr evaluar de forma más precisa si la gestión de riesgos cumple o no con los aspectos de las normas y estándares utilizados, se realicen las encuestas a una población más extensa de expertos en el área de TI.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] D. Y. Perwej, S. Q. Abbas, J. P. Dixit, D. N. Akhtar, y A. K. Jaiswal, «A Systematic Literature Review on the Cyber Security», *Int. J. Sci. Res. Manag. IJSRM*, vol. 9, n.º 12, Art. n.º 12, dic. 2021, doi: 10.18535/ijsrm/v9i12.ec04.

[2] A. S. C. Junior y C. H. Arima, «CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW», *Rev. FOCO*, vol. 16, n.º 02, pp. e1188-e1188, feb. 2023, doi: 10.54751/revistafoco.v16n2-215.

[3] D. Carrizo y C. Moller, «Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático», *Ingeniare Rev. Chil. Ing.*, vol. 26, pp. 45-54, nov. 2018, doi: 10.4067/S0718-33052018000500045.

[4] Chacón Prieto, David - Biblioteca Digital FCE, «Análisis de metodologías de la gestión del riesgo aplicables a la norma ISO/IEC 27005: 2018 .» [En línea]. Disponible en: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1645_ChaconPrietoD

[5] DQS, «Normas para la seguridad de la información: una visión general». [En línea]. Disponible en: https://www.dqsglobal.com/es-sv/aprenda/blog/normas-para-la-seguridad-de-la-informacion-una-vision-general

[6] L. G. Álvarez Lozano y M. Andrade, «Políticas de Seguridad de la Información bajo la Norma ISO 27002: 2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián», *Polo Conoc. Rev. Científico - Prof.*, vol. 5, n.º 11, pp. 591-621, 2020.

[7] F. J. Valencia Duque, *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*. Centro Editorial de la Facultad de Administración, 2021. [En línea]. Disponible en: https://repositorio.unal.edu.co/handle/unal/80158

[8] M. N. Z. Morales, «Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte», feb. 2020, [En línea]. Disponible en: https://www.academia.edu/87880396/Modelo_de_gesti%C3%B3n_de_riesgos_de_seguridad_de_la_informaci%C3%B3n_Una_revisi%C3%B3n_del_estado_del_arte

[9] W. A. B. Lourido y M. V. S. Sánchez, «Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó.».

[10] «Nte inen iso iec 27005 - Resumen Riesgos Naturales - INSTITUTO ECUATORIANO DE NORMALIZACIÓN Quito -». [En línea]. Disponible en: https://app.virtualex.ec/documentos/nte_inen_iso_iec_27005.pdf

[11] G. R. D. L. C. Rodríguez, R. A. M. Fernández, y A. C. M. D. L. Santos, «Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática», *Innov. Softw.*, vol. 4, n.º 1, Art. n.º 1, mar. 2023, doi: 10.48168/innosoft.s11.a79.

[12] D. A. K. Mahra, «A SYSTEMATIC LITERATURE REVIEW ON RISK MANAGEMENT FOR INFORMATION TECHNOLOGY», *Int. J. Adv. Sci. Technol.*, vol. 28, n.º 20, Art. n.º 20, nov. 2019.

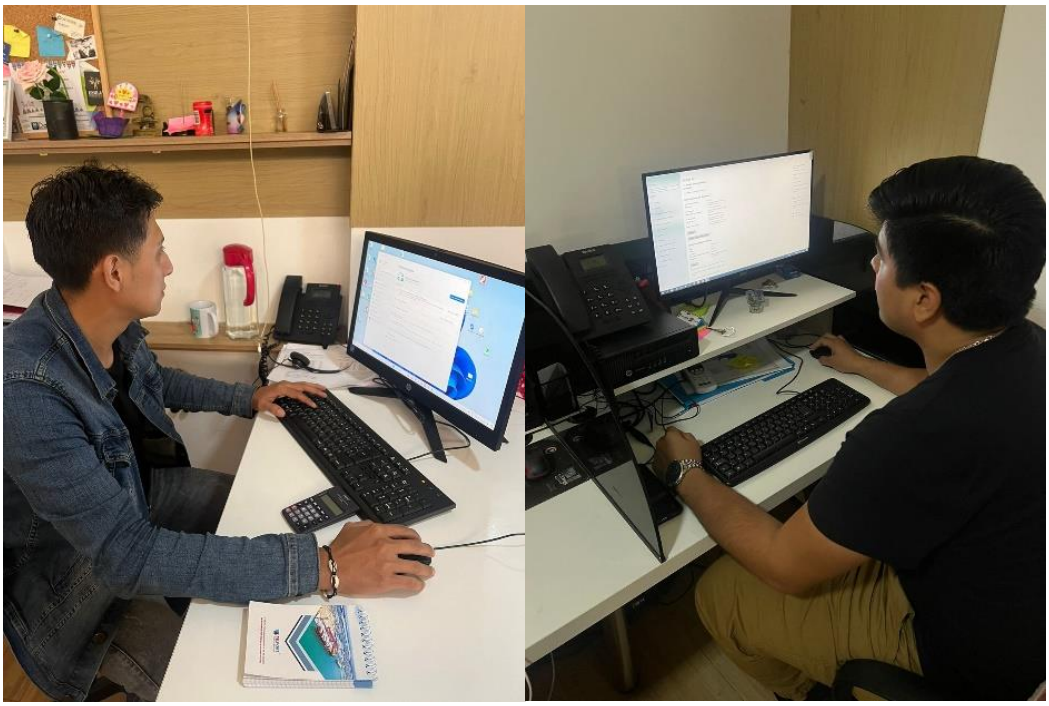
[13] M. Shokry, A. I. Awad, M. K. Abd-Ellah, y A. A. M. Khalaf, «When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method», *Sustainability*, vol. 15, n.º 12, Art. n.º 12, ene. 2023, doi: 10.3390/su15129812.

[14] M. M. M. Macias, R. W. M. Macias, M. L. I. Navarrete, y J. A. I. Navarrete, «Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática», *Rev. Científica Arbitr. Multidiscip. PENTACIENCIAS*, vol. 5, n.º 4, pp. 584-599, jun. 2023, doi: 10.59169/pentaciencias.v5i4.700.

[15] L. C. Hamit, H. M. Sarkan, N. F. M. Azmi, M. N. Mahrin, S. Chuprat, y Y. Yahya, «Adopting ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients Data Theft», *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, n.º 3, Art. n.º 3, jun. 2020, doi: 10.18517/ijaseit.10.3.10172.
[16] E. M. D. Guevara-Vega, J. R. Delgado-Deza, y A. C. Mendoza-de-los-Santos, «Vulnerabilidades y amenazas en los activos de información: una revisión sistemática», *Rev. Científica Sist. E Informática*, vol. 3, n.º 1, Art. n.º 1, ene. 2023, doi: 10.51252/rcsi.v3i1.461.
[17] N. Nikolaou, A. Papadakis, K. Psychogyios, y T. Zahariadis, «Vulnerability Identification and Assessment for Critical Infrastructures in the Energy Sector», *Electronics*, vol. 12, n.º 14, Art. n.º 14, ene. 2023, doi: 10.3390/electronics12143185.
[18] E. Guerra *et al.*, «Development of an information security management system based on analysis methodology and risk identification in university libraries», *Inf. Tecnológica*, vol. 32, n.º 5, pp. 145-156, oct. 2021, doi: 10.4067/S0718-07642021000500145.
[19] N. A. A. Bakar, W. M. W. Ramli, y N. H. Hassan, «The internet of things in healthcare: an overview, challenges and model plan for security risks management process», *Indones. J. Electr. Eng. Comput. Sci.*, vol. 15, n.º 1, Art. n.º 1, jul. 2019, doi: 10.11591/ijeecs.v15.i1.pp414-420.
[20] «Método para Gestionar la Seguridad de activos de Información - ProQuest». Accedido: 26 de julio de 2024. [En línea]. Disponible en: https://www.proquest.com/openview/c9bf3f3b2192c011fc8cb1e991248b56/1?pq-origsite=gscholar&cbl=1006393
[21] E. del C. N. Romero, «IMPACTO DE LOS RIESGOS EN LA GESTIÓN DE PROCESOS DE NEGOCIO», *Encuentro Int. Educ. En Ing.*, sep. 2021, doi: 10.26507/ponencia.1592.
[22] C. Basile, B. De Sutter, D. Canavese, L. Regano, y B. Coppens, «Design, implementation, and automation of a risk management approach for man-at-the-End software protection», *Comput. Secur.*, vol. 132, p. 103321, sep. 2023, doi: 10.1016/j.cose.2023.103321.
[23] A. E. H. Echeverría, «PROPUESTA PARA EL MEJORAMIENTO DE PROCESOS Y GESTIÓN DE RIESGOS TI DEL ÁREA PROGRAMACIÓN Y CONTROL DE LA COMPAÑÍA EMTELCO S.A.S., BASADA EN LAS BUENAS PRÁCTICAS DE ITIL 4 Y COBIT 2019».
[24] I. G. N. Putra Eryawan, G. Sasmita, y A. Cahyawan, «Information Security Risk Strategy at PT. X Using NIST SP 800-30», *J. Ilm. Merpati Menara Penelit. Akad. Teknol. Inf.*, vol. 9, p. 213, may 2021, doi: 10.24843/JIM.2021.v09.i03.p03.
[25] «Vega Briceño - 2021 - Seguridad de la información.pdf». Accedido: 25 de mayo de 2024. [En línea]. Disponible en: https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf
[26] M. J. R. Valiente, J. M. H. C. Sarmiento, y A. C. M. D. L. Santos, «Seguridad de la información en la prevención de perdida de datos: una revisión sistemática», *Innov. Softw.*, vol. 4, n.º 2, Art. n.º 2, sep. 2023, doi: 10.48168/innosoft.s12.a92.
[27] J. F. Vaca Báez, «Sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para el centro médico "Cotacachi"», PUCE Ibarra, 2023. [En línea]. Disponible en: https://repositorio.puce.edu.ec/handle/123456789/43002
[28] J. R. Guzmán Melo y H. S. García Cuta, «Diseño de un Sistema de Gestión de la Seguridad en la Información Para los Procesos Críticos de la Empresa Orange Star S.A.S Bajo la Norma ISO 27001:2013.», sep. 2023, [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/13005
[29] A. P. Putra y B. Soewito, «Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector», *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, n.º 4, 2023, doi: 10.14569/IJACSA.2023.0140468.
[30] Edson Kowask Bezerra Fabiano Alcántara Lima Alexandre Cesar Motta Jacomo Dimmit Boca Piccolin, «Gestión del riesgo de las TI NTC 27005».
[31] R. V. Daniel, «"ANÁLISIS E IMPLEMENTACIÓN DE LA NORMA ISO 27002 PARA EL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL"».

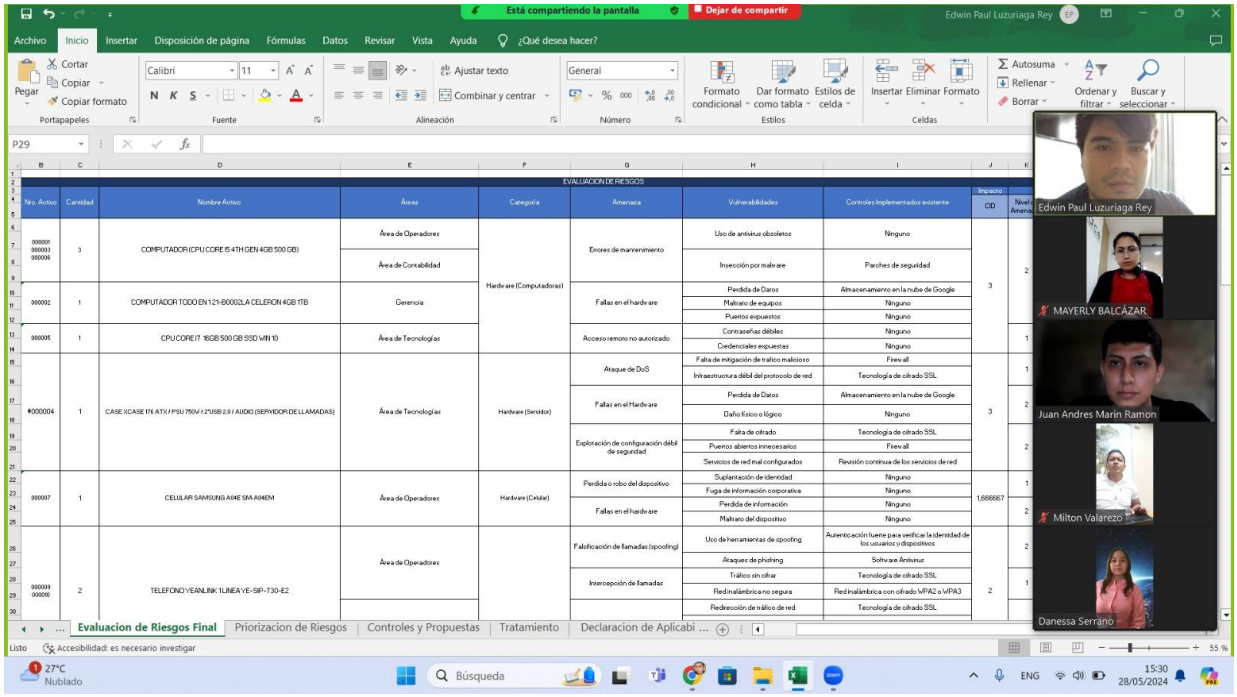
[32] A. D. Khaleefah y H. M. Al-Mashhadi, «Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review», *Iraqi J. Sci.*, pp. 468-486, ene. 2024, doi: 10.24996/ijs.2024.65.1.38.
[33] L. Moreno, «NORMA INTERNACIONAL ISO 31000 Administración/Gestión de riesgos - Lineamientos guía», [En línea]. Disponible en: https://www.academia.edu/41886951/NORMA_INTERNACIONAL_ISO_31000_Administraci%C3%B3n_Gesti%C3%B3n_de_riesgos_Lineamientos_gu%C3%ADa
[34] «Guide for Conducting Risk Assessments NIST SP 800-30», *NIST*, ene. 2020, doi: http://dx.doi.org/10.6028/NIST.SP.800-30r1.
[35] T. Ali, M. Al-Khalidi, y R. Al-Zaidi, «Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review», *J. Comput. Inf. Syst.*, vol. 0, n.º 0, pp. 1-28, 2024, doi: 10.1080/08874417.2024.2329985.
[36] E. L. C. Cedeño y K. E. S. Mena, «El Método Delphi Cualitativo y su Rigor Científico: Una revisión argumentativa», *Soc. Tecnol.*, vol. 5, n.º 3, Art. n.º 3, jul. 2022, doi: 10.51247/st.v5i3.261.
[37] A. Rodríguez-Lifante y M. M. B. Pereira, «El método Delphi en Lingüística Aplicada a la luz de un análisis teórico y crítico», *Rev. Bras. Linguística Apl.*, vol. 21, pp. 271-293, feb. 2021, doi: 10.1590/1984-6398202116351.
[38] M. A. R. Chávez y T. Z. R. Torres, «El método DELPHI como herramienta de investigación. Una revisión: The DELPHI method as a research tool. A review», *LATAM Rev. Latinoam. Cienc. Soc. Humanidades*, vol. 5, n.º 1, Art. n.º 1, mar. 2024, doi: 10.56712/latam.v5i1.1842.
[39] H. Taherdoost, «Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview», *Electronics*, vol. 11, n.º 14, Art. n.º 14, ene. 2022, doi: 10.3390/electronics11142181.
[40] B. M. Dioubate y W. Daud, «A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions», *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 12, may 2022, doi: 10.6007/IJARBSS/v12-i5/12924.
[41] A. Guadarrama, «ISO IEC 27002 2013 Code of Practice for Information Security Controls español», [En línea]. Disponible en: https://www.academia.edu/34675836/ISO_IEC_27002_2013_Code_of_Practice_for_Information_Security_Controls_espa%C3%B1ol

7. ANEXOS

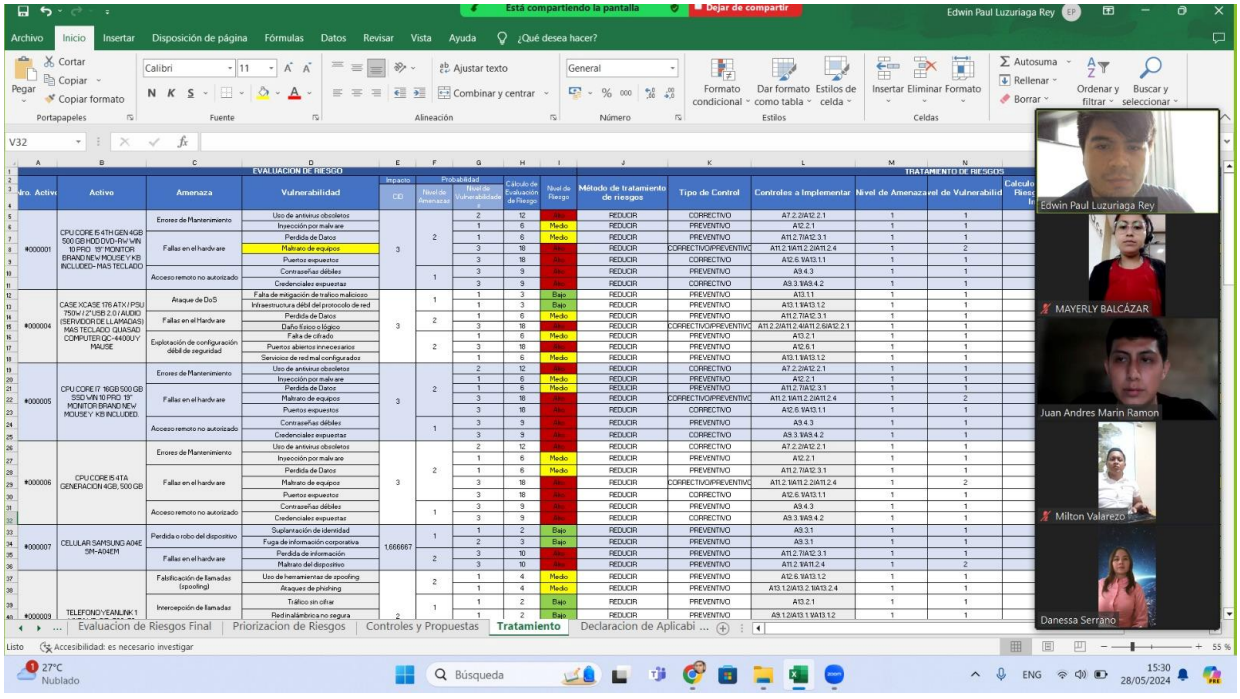


Anexo 1 *Identificación de activos en la empresa*

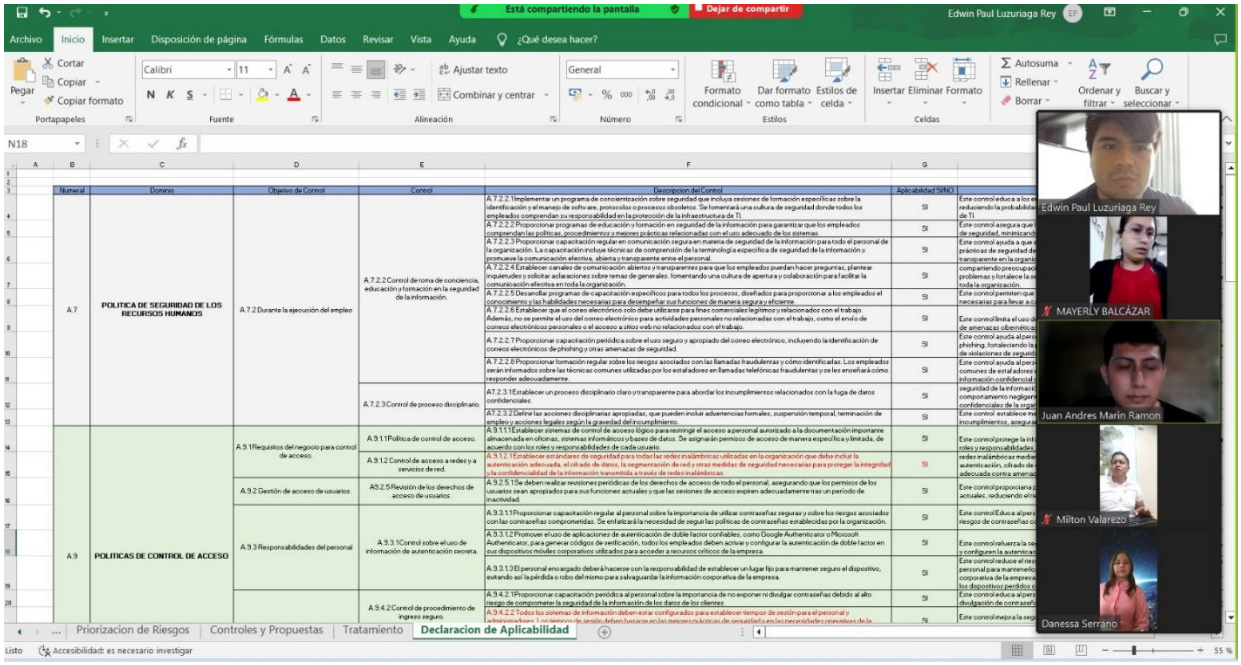
Anexo 2 *Tasación de activos en la empresa*



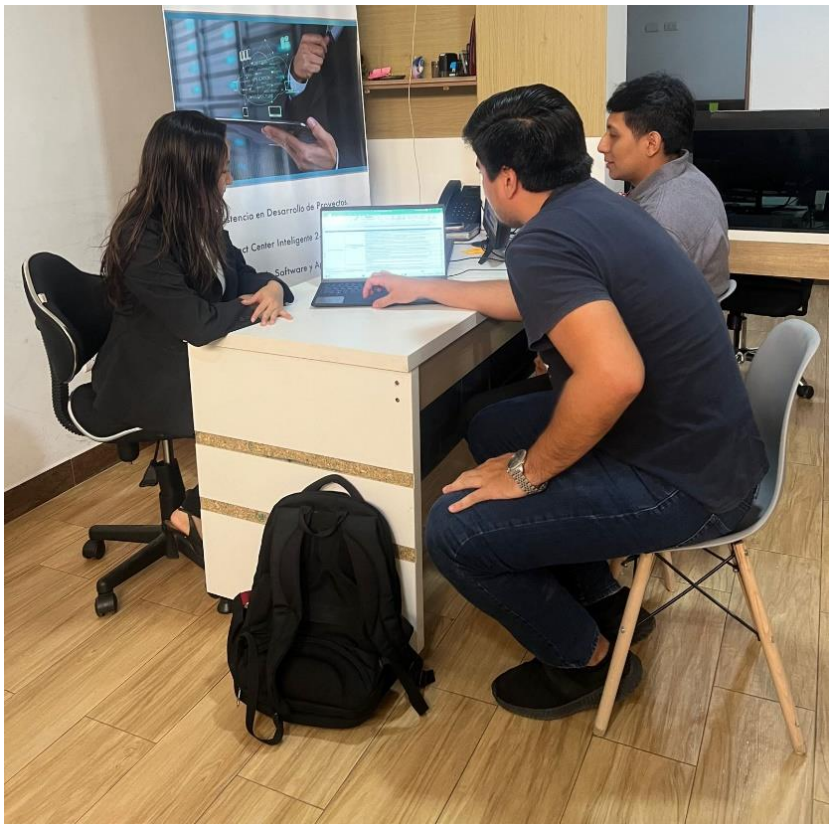
Anexo 3 *Evaluación de riesgos junto al comité de seguridad de la información*



Anexo 4 *Tratamiento de riesgos junto al comité de seguridad de la información*



Anexo 5 *Declaración de aplicabilidad junto al comité de seguridad de la información*



Anexo 6 *Revisión y firma del oficio de entrega de resultados*

Machala, 31 de mayo del 2024

Sr. Edwin Paul Luzuriaga Rey

Sr. Juan Andrés Marín Ramon

Presente:

De mi mayor consideración:

Por medio de la presente, aprovecho la oportunidad de enviarles un cordial saludo.

Nos es grato dirigirnos a ustedes para confirmar la recepción del oficio enviado el 30 de mayo del 2024, referente a la reciente gestión de riesgos realizada en la empresa. Hemos recibido con satisfacción los documentos adjuntos que detallan los procedimientos, acciones y resultados obtenidos durante la ejecución del proyecto.

Los documentos recibidos incluyen:

- Valoración de Activos
- Identificación de Amenazas y Vulnerabilidades
- Evaluación de Riesgos
- Priorización de Riesgos
- Controles y Propuestas de Mejoras
- Tratamiento de Riesgo
- Declaración de Aplicabilidad

Agradecemos su dedicación y transparencia en la presentación de estos resultados, los cuales reflejan el compromiso de su equipo con la seguridad de la información. Nuestro equipo procederá a revisar detenidamente la documentación y nos mantendremos atentos para cualquier consulta o aclaración adicional que sea necesaria.

Reiteramos nuestro agradecimiento por su atención a este asunto y quedamos a su disposición para cualquier interacción futura.

Atentamente,

DANESSA MAGDALENA SERRANO ROBLES

Firmado digitalmente por DANESSA MAGDALENA SERRANO ROBLES
Fecha: 2024.05.31 11:27:16 -05'00'

Eco. Danessa Serrano

Gerente General

Anexo 7 *Oficio de recepción de documentos firmado electrónicamente*

NOMBRE	CORREO	OCUPACIÓN
Ing. Cristhian Rafael Romero León	crrl182@gmail.com	Técnico de seguridad física - División exportadora Palmar.
Ing. Oscar Efrén Cárdenas Villavicencio, Mgs.	oscar90ago@gmail.com	Docente - Facultad de Ingeniería Civil - Universidad Técnica de Machala.
Ing. Lady Tatiana Zambrano Enríquez	leidy.zamb@hotmail.com	Docente de informática - Colegio Bachillerato Particular "Latinoamericano".
Ing. Kevin Shamael Garzón León	kevin_s_l@hotmail.com	Desarrollador de Software - Larvia.
Ing. Salviano Vicente Núñez Apolo	snuneza21@gmail.com	Analista de Sistemas - MachalaDent.

Anexo 8 *Información de expertos en el área de TI encuestados*

NOMBRE	CORREO	OCUPACION
Ing. Fausto Fabian Redrován Castillo, Mgs.	fredrovan@utmachala.edu.ec	Docente - Facultad de Ingeniería Civil - Universidad Técnica de Machala.
Ing. Rodrigo Fernando Morocho Román, Mgs.	fernandiux2000@gmail.com	Docente - Facultad de Ingeniería Civil - Universidad Técnica de Machala.
Ing. Wilmer Braulio Rivas Asanza, Phd.	wrivas@utmachala.edu.ec	Docente - Facultad de Ingeniería Civil - Universidad Técnica de Machala.

Anexo 9 *Información de docentes para encuesta piloto*

ENCUESTA INICIAL PARA PRUEBA PILOTO	CORRECCIONES
No había un contexto introductorio.	Al inicio de la encuesta se escribió el siguiente párrafo para poner en contexto a los expertos sobre en qué deben basarse para realizar la encuesta: "Se solicita a los expertos evaluadores que para dar respuesta a las preguntas se rijan en el

	cumplimiento de las normativas ISO/IEC 27005 y la metodología NIST SP 800-30.”
1. ¿Considera usted que se han clasificado adecuadamente los activos de la empresa?	
2. ¿Se han identificado todas las posibles amenazas de seguridad de la información a los activos de la empresa?	2. ¿Se han identificado las posibles amenazas de seguridad de la información a los activos de la empresa?
3. ¿Se han considerado todas las vulnerabilidades involucradas para la seguridad de la información?	3. ¿Se han considerado las vulnerabilidades involucradas para la seguridad de la información?
4. ¿Cree que se han considerado adecuadamente los impactos potenciales de los riesgos?	
5. ¿Cómo calificaría la precisión para evaluar el análisis cuantitativo de los riesgos?	
6. ¿Cree que se ha utilizado un criterio adecuado para la priorización de riesgos?	
7. ¿Considera que se ha dado suficiente importancia a los riesgos de alto impacto?	
8. ¿Cómo evalúa la adecuación de los controles propuestos, basados en la norma ISO/IEC 27002:2013, para mitigar los riesgos?	8. ¿Cómo evalúa la adecuación de los controles propuestos, basados en la norma ISO/IEC 27002:2013, para reducir los riesgos?
9. ¿Está de acuerdo con la factibilidad de implementar los controles sugeridos?	
10. ¿Considera que las estrategias de tratamiento de riesgos (evitar, transferir, mitigar, aceptar) son adecuadas?	10. ¿Considera que las estrategias de tratamiento de riesgos (evitar, transferir, reducir, aceptar) son adecuadas?
11. ¿En qué medida considera que la gestión de riesgos cumple con los principios de la norma ISO/IEC 27005?	
12. ¿Considera que la comunicación de resultados ha sido clara y comprensible para la organización?	
13. ¿Cree que las medidas propuestas, basadas en la norma ISO/IEC 27002:2013, mejorarán significativamente la resiliencia de la empresa?	13. ¿Cree que las medidas propuestas, basadas en la norma ISO/IEC 27002:2013, mejorarán significativamente la seguridad de la información de la empresa?
14. ¿Están claramente documentados los procedimientos de la gestión de riesgos?	
15. ¿Tiene algún comentario adicional o recomendación sobre la gestión de riesgos que quisiera hacer con base en su experiencia?	

Anexo 10 *Encuesta Inicial y correcciones basadas en la prueba piloto*

Se solicita a los expertos evaluadores que para dar respuesta a las preguntas se rijan en el cumplimiento de las normativas ISO/IEC 27005 y la metodología NIST SP 800-30.
1. ¿Considera usted que se han clasificado adecuadamente los activos de la empresa?
2. ¿Se han identificado las posibles amenazas de seguridad de la información a los activos de la empresa?
3. ¿Se han considerado las posibles vulnerabilidades involucradas para la seguridad de la información?
4. ¿Cree que se han considerado adecuadamente los impactos potenciales de los riesgos?
5. ¿Cómo calificaría la precisión para evaluar el análisis cuantitativo de los riesgos?
6. ¿Cree que se ha utilizado un criterio adecuado para la priorización de riesgos?
7. ¿Considera que se ha dado suficiente importancia a los riesgos de alto impacto?
8. ¿Cómo evalúa la adecuación de los controles propuestos, basados en la norma ISO/IEC 27002:2013, para reducir los riesgos?
9. ¿Está de acuerdo con la factibilidad de implementar los controles sugeridos?
10. ¿Considera que las estrategias de tratamiento de riesgos (evitar, transferir, reducir, aceptar) son adecuadas?
11. ¿En qué medida considera que la gestión de riesgos cumple con los principios de la norma ISO/IEC 27005?
12. ¿Considera que la comunicación de resultados ha sido clara y comprensible para la organización?
13. ¿Cree que las medidas propuestas, basadas en la norma ISO/IEC 27002:2013, mejorarán significativamente la seguridad de la información de la empresa?
14. ¿Están claramente documentados los procedimientos de la gestión de riesgos?
15. ¿Tiene algún comentario adicional o recomendación sobre la gestión de riesgos que quisiera hacer con base en su experiencia?

Anexo 11 *Encuesta final aplicada a los expertos seleccionados*