

UNIVERSIDAD CATÓLICA DE CUENCA



Maestría en Ciberseguridad

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

Tema:

Modelo de un Sistema de Gestión de Seguridad de la Información (SGSI) para redes móviles en empresa pública de Telecomunicaciones en el Ecuador.

Autor: Ing. Héctor Javier Erazo Chulde

Asesores: Ing. Daniel Andrade Pesantez

Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Modelo de un Sistema de Gestión de Seguridad de la Información (SGSI) para redes móviles en empresa pública de Telecomunicaciones en el Ecuador”, de autoría del Señor Ingeniero en Electrónica y Telecomunicaciones HECTOR JAVIER ERAZO CHULDE, CC: 1714649058, ecuatoriano, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.

Ing. Daniel Andrade Pesantez
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Modelo de un Sistema de Gestión de Seguridad de la Información (SGSI) para redes móviles en empresa pública de Telecomunicaciones en el Ecuador”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.

Ing. Héctor Javier Erazo Chulde

CC: 1714649058

AGRADECIMIENTO

En primer lugar, quiero expresar mi más sincero agradecimiento a mi familia, mi esposa Paola, mis hijas Valentina, Martina y Romina, han sido mi fuente de inspiración, siempre creyeron en mí y me brindaron su apoyo incondicional a lo largo de esta etapa.

Agradezco profundamente al Ing. Daniel Andrade, mi tutor del proyecto de investigación, y al Ing. Juan Carlos Ortega por su guía, paciencia, dedicación y profesionalismo. Sus conocimientos y su enfoque me inspiraron a profundizar la investigación en el campo de los Sistemas de Gestión de Seguridad de Información. Asimismo, quiero agradecer a todos los profesores del programa de Maestría en Ciberseguridad de la Universidad Católica de Cuenca, quienes contribuyeron a mi formación académica.

Finalmente, quiero expresar mi gratitud a todos mis compañeros de estudio, quienes compartieron conmigo este camino y me brindaron su apoyo y amistad.

DEDICATORIA

A Dios: Creador del Universo, dador de salud y vida, mi fuente de sabiduría y conocimiento. Gracias por iluminar mi camino y fortalecer mi espíritu en cada paso de esta investigación.

A mi esposa Paola: Por su amor y entrega constante, por creer en mí y brindarme su apoyo incondicional en todo momento.

A mis padres, Luis y Luz: Por su cariño, paciencia y apoyo; muchos de mis logros se los debo a ustedes.

A mis hijas, Valentina, Martina y Romina: Con todo mi amor, dedico este trabajo a ustedes, mi mayor inspiración. Gracias por llenar mis días de alegría y por ser mi motor para seguir adelante.

A mis profesores: Por compartir sus conocimientos y guiarme en este apasionante mundo de la ciberseguridad.

RESUMEN

Palabras claves: Seguridad información, SGSI, telecomunicaciones, redes, móviles.

El presente proyecto tiene como objetivo valorar los riesgos relacionados a la seguridad de la información y el presente caso de estudio está delimitado a las redes móviles de la empresa pública de telecomunicaciones en el Ecuador, con el objetivo de desarrollar una propuesta de solución para minimizar el impacto de los ataques maliciosos.

Mediante la propuesta de un modelo de SGSI se va a identificar las vulnerabilidades y amenazas en las redes móviles de la empresa pública de telecomunicaciones, tomando en cuenta la normativa de seguridad de la información ISO/IEC 27001:2022 (buenas prácticas en relación a la gestión del SGSI), ISO/IEC 27002:2022 (establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización), ISO/IEC 27005:2018 (proporciona directrices para la gestión de riesgos de la seguridad de la información (SGSI) en las diferentes organizaciones), la ISO 27011:2022 (normativa para la gestión de seguridad en compañías de telecomunicaciones), para mitigar los riesgos a los que la empresa pública está expuesta y minimizar el impacto a la disponibilidad, confidencialidad e integridad de la información.

En el presente proyecto se ha usado el método deductivo, mediante investigación exploratoria de diferentes artículos de investigación y la aplicación del EGSI establecido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), se ha logrado establecer controles y medidas de seguridad para proteger la información confidencial y sensible de la empresa, para reducir el riesgo de filtraciones, accesos no autorizados, sabotajes y otras amenazas a la seguridad de la información.

ABSTRACT

Keywords: Information security, SGSI, telecommunications, network, mobile

The objective of this project is to assess the risks related to information security and this case study is limited to the mobile networks of the public telecommunications company in Ecuador. With the aim of developing a solution proposal to minimize the impact of malicious attacks.

Through the proposal of an ISMS model, the vulnerabilities and threats in the mobile networks of the public telecommunications company will be identified, taking into account the information security regulations ISO/IEC 27001:2022 (good practices in relation to the management of the ISMS), ISO/IEC 27002:2022 (establishes general guidelines and principles to initiate, implement, maintain and improve information security management in an organization) and ISO 27011:2022 (regulations for security management in telecommunications companies), to mitigate the risks to which the public company is exposed and minimize the impact on the availability, confidentiality and integrity of the information.

For this project, the deductive method has been used, through exploratory research of different research articles and the application of the Government Information Security Scheme - EGSI established by MINTEL, it has been possible to establish controls and security measures to protect confidential information. and sensitive of the company, to reduce the risk of leaks, unauthorized access, sabotage and other threats to information security.

ÍNDICE DE CONTENIDO

1.	INTRODUCCIÓN	13
1.1.	Situación problemática.....	13
1.2.	Justificación del Proyecto	14
1.3.	Objetivos del Proyecto	15
1.3.1.	Objetivo General	15
1.3.2.	Objetivos Específicos.....	15
1.4.	Fundamentación teórica	15
1.5.	Ataque informático.....	16
1.6.	Malware.....	16
1.6.1.	Virus	16
1.6.2.	Gusanos.....	16
1.6.3.	Troyanos	16
1.6.4.	Spyware.....	17
1.6.5.	Ramsonware	17
1.6.6.	Adware	17
1.6.7.	Botnets.....	17
1.7.	Normativas de ciberseguridad	17
1.8.	NIST SP 800.....	18
1.9.	COBIT	18
1.10.	ISO/IEC 27001	18
1.10.1.	Principios	20
1.10.2.	Confidencialidad.....	20
1.10.3.	Disponibilidad.....	21
1.10.4.	Integridad	21
1.11.	ISO 27002.....	21
1.12.	ISO 27005.....	21
1.13.	ISO 27011.....	21
1.14.	SGSI.....	22
1.15.	Riesgo.....	23
1.15.1.	Gestión de Riesgos	23
1.15.2.	Amenazas	24
1.15.3.	Activo vulnerable.....	24

1.15.4.	Vulnerabilidad	24
1.16.	Conceptos Básicos de Redes Móviles	24
1.16.1.	Retos y Amenazas en Redes Móviles	26
1.17.	Estado del arte	26
2.	DIAGNÓSTICO SITUACIONAL	28
2.1.	Diagnóstico de la situación empresarial.....	28
2.2.	Metodología	28
2.2.1.	Tratamiento de riesgos.....	29
2.2.2.	Variables Dependientes	31
2.2.3.	Variables Independientes.....	31
2.3.	Análisis situacional	32
2.3.1.	Análisis Situacional de la Ciberseguridad en Redes Móviles de Empresas de Telecomunicaciones	32
2.4.	Panorama Actual de Ciberseguridad en Empresas de Telecomunicaciones en Ecuador	33
2.5.	Situación Actual de la Ciberseguridad en empresas públicas en Ecuador	34
3.	DESARROLLO	36
3.1.	Análisis de ciberseguridad en redes móviles	36
3.1.1.	Filtración de información	36
3.1.2.	Los dispositivos móviles.....	36
3.1.3.	Los recursos informáticos tradicionales.....	37
3.1.4.	Función versátil de los dispositivos móviles	37
3.1.5.	Robo de información transfronterizo.....	37
3.1.6.	Eliminación de datos	37
3.2.	Seguridad en redes móviles según el marco ISO/IEC 27001	38
3.2.1.	Gestión de la Seguridad de la Información	38
3.2.2.	Seguridad de Recursos Humanos.....	38
3.2.3.	Seguridad Física y Ambiental	39
3.2.4.	Gestión de Comunicaciones.....	39
3.2.5.	Monitoreo de Acceso para Dispositivos Móviles	40
3.3.	Enfoque para la gestión de seguridad en empresas públicas	41
3.4.	Modelo de gestión de riesgos	41
3.5.	Análisis de riesgos Livermore LRAM.....	41
3.5.1.	Características principales del LRAM	42

3.5.2.	Procedimiento del LRAM	42
3.5.3.	Beneficios del LRAM.....	42
3.6.	Métodos cualitativos vs. cuantitativos para la gestión de riesgos	42
3.6.1.	Métodos Cualitativos	44
3.6.2.	Enfoques tradicionales de gestión de riesgos.....	44
3.6.3.	Criterios de evaluación del riesgo.....	45
3.7.	Evaluación de Riesgos de Seguridad de la Información	46
3.7.1.	Identificación de Riesgos.....	47
3.7.2.	Verificación de la Identificación	47
3.7.3.	Identificación de Vulnerabilidades.....	47
3.7.4.	Análisis de Riesgos	47
3.7.5.	Tratamiento del Riesgos.....	48
3.8.	Análisis de Riesgos de Livermore (LRAM) para Redes Móviles de una Empresa Pública de Telecomunicaciones	49
3.9.	Propuesta de mejora de SGSI	50
3.9.1.	Valoración de los activos.....	51
3.9.2.	Identificación de Amenazas	52
3.9.3.	Identificación de Vulnerabilidades.....	53
3.9.4.	Identificación de existencia de controles.....	54
3.9.5.	Análisis del riesgo.....	55
3.9.6.	Valoración de los riesgos.....	56
4.	RESULTADOS	64
5.	CONCLUSIONES	66
6.	RECOMENDACIONES.....	67
7.	BIBLIOGRAFÍA.....	69

ÍNDICE DE FIGURAS

Figura 1	Familia ISO/IEC 27000	19
Figura 2	Principios de Seguridad de Información	20
Figura 3	Modelo PDCA	22
Figura 4	Estructura PDCA-ISO27001.....	23
Figura 5	Evolución de Redes Inalámbricas	25
Figura 6	Tratamiento del Riesgo.....	30

ÍNDICE DE TABLAS

Tabla 1	Comparación de Riesgos de Seguridad de Información	20
Tabla 2	Métricas de Riesgo Cualitativas	44
Tabla 3	Valor del Riesgo.....	48
Tabla 4	Prioridad del Riesgo.....	49
Tabla 5	Identificación de Activos.....	50
Tabla 6	Evaluación de Impacto por Pérdida de Confidencialidad	51
Tabla 7	Evaluación de Impacto por Pérdida de Integridad.	51
Tabla 8	Evaluación de Impacto por Pérdida de Disponibilidad.....	51
Tabla 9	Evaluación de los Activos	52
Tabla 10	Identificación de Amenazas	52
Tabla 11	Identificación de Vulnerabilidades	53
Tabla 12	Identificación de Controles.....	54
Tabla 13	Criterios de Probabilidad de Ocurrencia de Amenazas.....	56
Tabla 14	Criterio de Probabilidad de Ocurrencia de Vulnerabilidades.....	57
Tabla 15	Nivel de Riesgo	57
Tabla 16	Evaluación de Riesgos.....	58

1. INTRODUCCIÓN

1.1.Situación problemática

Hoy en día, dedicamos una considerable cantidad de tiempo a navegar y explorar en internet, ya sea para fines educativos, laborales o simplemente para entretenernos. Durante estos momentos, corremos el riesgo de que nuestra información sea objeto de robo (Vilchez Jose, 2022).

Hoy en día se produce una gran cantidad de información, que conlleva a que empresas e instituciones utilicen sistemas y herramientas informáticas. Sin embargo, a menudo no se concede la debida importancia a la seguridad y auditoría informática, considerándolas como un gasto en lugar de una inversión. La ISO/IEC 27001 define los requisitos que el SGSI que debe respetar para garantizar el cuidado de los activos de información (Coaguila Maribel, 2020).

Los ataques maliciosos como el phishing (donde el ciberdelincuente remite un email fingiendo ser una entidad legítima con el propósito de acceder a información privada) y el ransomware (tipo de programa malicioso, cuyo objetivo es negar el acceso a los datos), para los siguientes propósitos el fraude y la apropiación indebida de información, han causado importantes pérdidas financieras en varias compañías; donde el atacante cifra el mensaje y exige un rescate para liberarlo, en ocasiones recurren al chantaje y amenazan con revelar los datos de la organización, si la empresa no paga el dinero requerido (Gómez Vieites, 2019).

Las compañías dedicadas a las telecomunicaciones, experimentan pérdidas financieras debido a diversos factores, tanto internos como externos, como la fuga de datos, ya que los riesgos no se gestionan correctamente, estos riesgos son de origen conocido o desconocido. La combinación del tratamiento de los riesgos y la ciberseguridad es importante para que las compañías logren alcanzar sus metas (Huaura Miguel, 2019).

Dado la gran cantidad de ventajas que ofrecen las tecnologías informáticas, es crucial reconocer que también conllevan riesgos significativos; por ende, es imperativo salvaguardar la información frente a las amenazas cibernéticas. Se busca promover la confianza en el uso de internet, el cumplimiento de las regulaciones y ejercer derechos a la protección de los datos (Michelena Andrés, 2019).

1.2. Justificación del Proyecto

El auge de los negocios digitales ha sido impulsado por el desarrollo tecnológico y la evolución simultánea de las telecomunicaciones. No obstante, el riesgo de ataques cibernéticos también ha incrementado (Hidalgo Geovanna, 2021).

La importancia de protegerse contra los ciberataques está relacionada al crecimiento de la digitalización de la información; con el aumento del volumen de información se incrementa la necesidad de protección de los datos. En consecuencia, la ciberseguridad se ha establecido como una inversión esencial tanto para entidades gubernamentales como para empresas (Fuentes Alejandro, 2023).

El SGSI funciona como un marco integral para proteger la información y minimizar los riesgos a los que puede estar expuesto. Este proceso de gestión permite emplear estrategias y operaciones para asegurar y segmentar la información que se maneja en diferentes entidades, ya sean de carácter público o privado (Falcón Elida, 2022).

Es esencial establecer un enfoque sistemático de evaluación de riesgos dentro de un SGSI, esto nos permite descubrir tanto las vulnerabilidades como las fortalezas presentes en una organización respecto a los activos informáticos, para identificar y analizar los procedimientos más críticos de la compañía, que facilita la determinación del nivel de protección adecuado y la evaluación de las amenazas frente a los riesgos (Suéscum Even, 2021).

La gestión de información confidencial y reservada en las entidades gubernamentales de Ecuador obliga a poner en marcha controles de seguridad; para este fin, se emplea el SGSI conforme a las directrices de la normativa ISO 27001 (Falcón Helida, 2022).

El proyecto de investigación presenta un modelo de SGSI para incrementar la seguridad de información de la empresa pública, proporcionando así una mejora significativa en la confidencialidad, disponibilidad e integridad de la información.

1.3.Objetivos del Proyecto

1.3.1. Objetivo General

Mitigar los riesgos de la seguridad de información de las redes móviles en una empresa pública de telecomunicaciones a través de un modelo de SGSI para evitar ataques maliciosos.

1.3.2. Objetivos Específicos

- Identificar las vulnerabilidades, amenazas y riesgos asociados a seguridad de la empresa que afectan la integridad, disponibilidad y confidencialidad de la información.
- Elaborar un modelo de Sistema de Gestión de Seguridad de Información, para desarrollar políticas de seguridad, considerando las mejores prácticas y normativas internacionales (ISO/IEC 27001, ISO 27002 y la ISO/IEC 27011).

1.4.Fundamentación teórica

La ciberseguridad es una serie de herramientas que protegen los datos de intrusiones no legítimas, modificaciones no deseadas y fallos en los sistemas y redes, manteniendo la confianza en los servicios que estos ofrecen (Garro Eduardo, 2022).

La seguridad de información se centra en salvaguardar los datos de la organización, asegurando que esta se mantenga protegida, precisa y accesible para los usuarios autorizados. Para lograrlo, se ejecuta un sistema de gestión que incluye medidas de protección para cada amenaza existente, para minimizar el impacto de las incidencias y proteger la viabilidad del negocio (GUÍA PARA LA IMPLEMENTACIÓN DE EGSI - MINTEL, 2024).

En el contexto actual, la ciberseguridad para las empresas juega un papel importante, donde la digitalización y la interconexión de redes de datos se han vuelto fundamentales, fomentando el bienestar social y la prosperidad económica.

1.5. Ataque informático

Los ciberataques, también conocidos como ataques informáticos, son acciones que buscan vulnerar los sistemas de información. Estos ataques aprovechan las fallas, debilidades o vulnerabilidades del hardware, software o incluso de las personas dentro de la organización. Su objetivo final es obtener un beneficio económico, causando daños a la ciberseguridad de la organización (Andrade Diego, 2021).

1.6. Malware

El malware, es un software malicioso, y se describe como cualquier tipo de aplicación creada para tomar el control de un sistema de información y ejecutar acciones no autorizadas.

1.6.1. Virus

Es un programa malicioso que se esconde dentro de archivos, como documentos o programas, se propaga cuando se abra o ejecute el programa. Una vez activado, el virus se replica y se propaga a otros archivos de tu sistema. Este programa dañino puede afectar archivos y programas importantes, incluso dañar o destruir tus datos valiosos (Arango Oscar, 2023).

1.6.2. Gusanos

Los gusanos informáticos son programas malintencionados que se reproducen por sí mismos y se replican a través de infraestructuras de red. A medida que se replican, los gusanos ocupan recursos de red y degradan el desempeño del sistema e incluso pueden causar fallas. Además, algunos gusanos pueden robar datos confidenciales, contraseñas e información financiera.

1.6.3. Troyanos

Es un software malicioso que se hace pasar por una aplicación legítima. Una vez que el usuario instala o ejecuta el troyano, este abre una puerta trasera en el sistema, donde los piratas informáticos asumen el control y manipulan la computadora (Arango Oscar, 2023).

1.6.4. Spyware

El spyware es un software malicioso que se infiltra secretamente en la herramienta computacional del cliente sin consentimiento y recopila información sobre sus actividades, incluyendo sus hábitos de navegación, sus datos personales y sus contraseñas; puede enviar esta información confidencial a terceros, como cibercriminales o empresas sin escrúpulos, podrían espiar su actividad y transmitir estos datos a un tercero (Guaña-Moya et al., 2022).

1.6.5. Ramsonware

El ransomware es un malware malicioso que encripta los archivos importantes, como documentos, fotos y datos financieros, y luego exige un rescate para descifrarlos y devolverle el acceso y podría ocasionar la pérdida de los archivos (Arango Oscar, 2023).

1.6.6. Adware

El adware es un programa publicitario que se instala y opera aprobación del cliente, mostrando anuncios emergentes o redirigiendo el navegador a páginas web publicitarias. La publicidad suele estar personalizada en función de los intereses del usuario, obtenidos a partir de su historial de navegación o búsquedas en línea (Guaña-Moya et al., 2022).

1.6.7. Botnets

Una botnet se relaciona como un ejército digital de computadoras zombies controladas por un pirata informático, donde el atacante malicioso infecta dispositivos con malware, convirtiéndolos en marionetas bajo su mando. La botnet puede ser utilizada para lanzar ataques inundando sitios web con tráfico falso y haciéndolos inaccesibles, o para enviar spam masivo a direcciones de correo electrónico desprevenidas (Arango Oscar, 2023).

1.7. Normativas de ciberseguridad

Existen diversas normas de ciberseguridad que establecen las pautas y requisitos para salvaguardar la información confidencial. Entre las más importantes se encuentran:

NIST SP 800: Seguridad en sistemas de información

COBIT: Objetivos de control para la información y las tecnologías relacionadas

ISO/IEC 27001: Sistema de gestión de seguridad de la información (SGSI)

1.8.NIST SP 800

La NIST SP 800 (Instituto Nacional de Estándares y Tecnología de los Estados Unidos) es un manual que describe los pasos técnicos básicos para realizar evaluaciones de ciberseguridad, estas publicaciones contienen directrices para ayudar a las empresas a proteger sus datos contra amenazas cibernéticas. Proporciona a las organizaciones métodos, técnicas y exámenes que pueden usarse como parte de una evaluación. También ofrece orientación a los evaluadores sobre cómo realizar estas evaluaciones, y cómo pueden afectar a los sistemas y redes de comunicaciones (Bonilla Jefersson, 2021).

1.9.COBIT

Las siglas de COBIT significan Objetivos de Control para la Información y Tecnologías Relacionadas (en inglés, Control Objectives for Information and Related Technology). Es un conjunto de normas que ayudan a las empresas a mejorar la gestión informática, permite a la Alta Gerencia de la empresa comprender las exigencias del monitoreo de la información. El objetivo es proporcionar herramientas para valorar los riesgos asociados a la gestión de la información y una mejora continua de los procesos de seguridad informática (Freire Jonatan, 2024).

1.10. ISO/IEC 27001

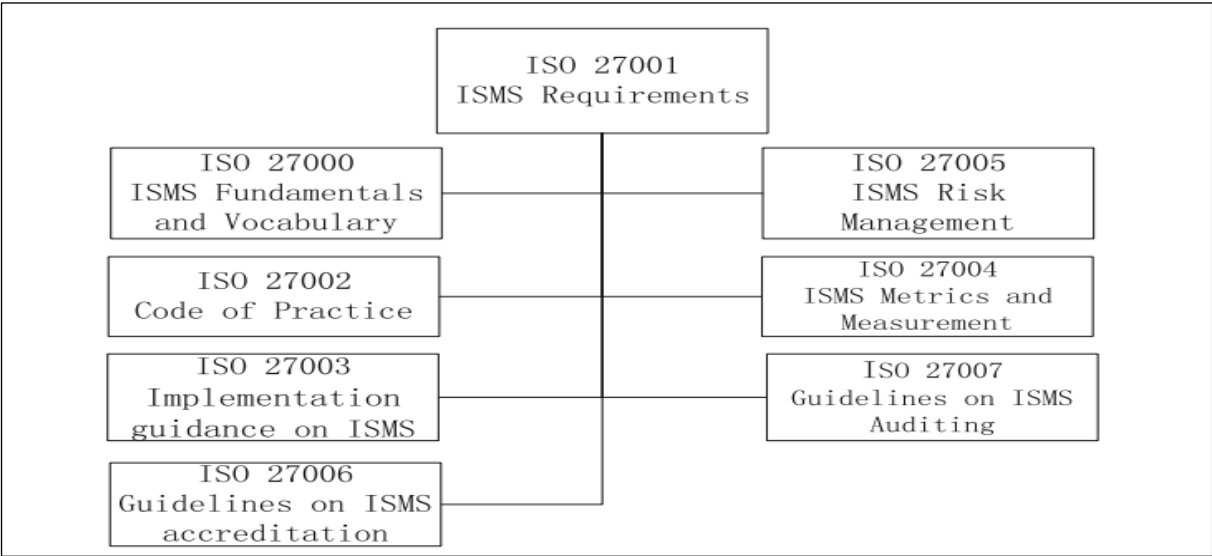
ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) se erigen como las entidades líderes en la elaboración de estándares a nivel global. La Norma ISO/IEC 27001, está diseñada para que sea utilizada por cualquier entidad (empresas privadas, entidades públicas, organizaciones sin fines de lucro). La norma ISO 27001 determina

los criterios para el SGSI, siendo una normativa reconocida a nivel internacional, para garantizar la ciberseguridad de la organización (Mora Jaime, 2021).

La normativa ISO 27001 permite valorar el desempeño y efectividad del SGSI de una organización. Las auditorías, herramienta fundamental en este proceso asegura que la evaluación se centre en el cumplimiento de estos y de los requerimientos específicos de ciberseguridad definidos por la organización (NORMA ISO 27001, 2020).

La norma ISO 27001 del 2013 actualizada a la versión 2022 brinda una guía completa sobre los aspectos esenciales hacia los estándares más recientes en ciberseguridad. Las modificaciones en los requisitos, la implementación de una herramienta de diagnóstico posterior a la Declaración de Aplicabilidad y la realización de una auditoría interna han resaltado la relevancia de adoptar las últimas actualizaciones (Galarza Johanna, 2024). En la figura 1 se muestra la familia ISO/IEC 27000, que incluye múltiples normas para la creación de un SGSI.

Figura 1
Familia ISO/IEC 27000



Nota. El gráfico representa la familia ISO 27001 (Zhu & Zhu, 2019)

Existen diversas metodologías reconocidas para la gestión de riesgos, otros enfoques comunes de gestión de riesgos de seguridad de la información, como NIST SP 800-30, Octave y el propio ISO 27005.

Tabla 1
Comparación de Riesgos de Seguridad de Información

Framework	Description	Target organization	Target level organization
ISO27005	Complete process in generic manner	Government large companies SME	Management Operational
OCTAVE	Self directed approach	SME	Management Operational
NIST SP 800-53	Very detailed guidance and identifications	Government large companies SME	Management Operational

Nota. Riesgos en ISO27005, OCTAVE, NIST SP 800-53

1.10.1. Principios

El SGSI es un grupo de medidas y controles que garantizan que la información se conserve íntegra, confidencial y disponible, protegiéndola de amenazas y riesgos (Guía para la implementación de EGSI, MINTEL. 2024).

Figura 2
Principios de Seguridad de Información



Nota. Adaptado de EGSI (p.18), por MINTEL, 2024.

1.10.2. Confidencialidad

La confidencialidad permite que la información solo sea accesible para usuarios específicos, previniendo accesos no autorizados y protegiendo la privacidad (Lina Ibarbo, 2019).

1.10.3. Disponibilidad

La disponibilidad garantiza el acceso continuo a la información para los usuarios autorizados, en el momento y lugar que lo necesiten (Chapoñan Wilmer, 2023).

1.10.4. Integridad

Es la propiedad de los datos respecto a ser precisos, completos y coherentes, la integridad permite que la información no sea afectada ni manipulada durante su envío o recepción, manteniendo su veracidad y confiabilidad (Chapoñan Wilmer, 2023).

1.11. ISO 27002

A partir del 1 de julio de 2007, el estándar ISO 17799:2005 cambió a ISO 27002, conservando el año 2005 como referencia. Esta guía no es un estándar certificable, sino que sugiere buenas prácticas para la gestión de ciberseguridad. (Inampues William, 2019).

1.12. ISO 27005

La ISO 27005 ofrece una directriz específica para la administración de los riesgos en ciberseguridad. En este sentido, el plan de acción permite mitigar los riesgos, como aquellos derivados de software vulnerable, sistemas operativos obsoletos o tecnologías obsoletas. La gestión de riesgos, en general, comprende la determinación, valoración y procesamiento de dichos riesgos (Gamboa et al., 2022).

1.13. ISO 27011

Es un manual para la ejecución y tratamiento de la ciberseguridad en las empresas de telecomunicaciones, siguiendo los lineamientos de ISO/IEC 27002:2005 y adaptado a las particularidades del sector (Bernal Harol, 2022).

1.14. SGSI

Un SGSI comprende una serie de procedimientos que una organización gestiona de manera conjunta, cuyo objetivo es salvaguardar sus activos claves (Fuentes Alejandro, 2023).

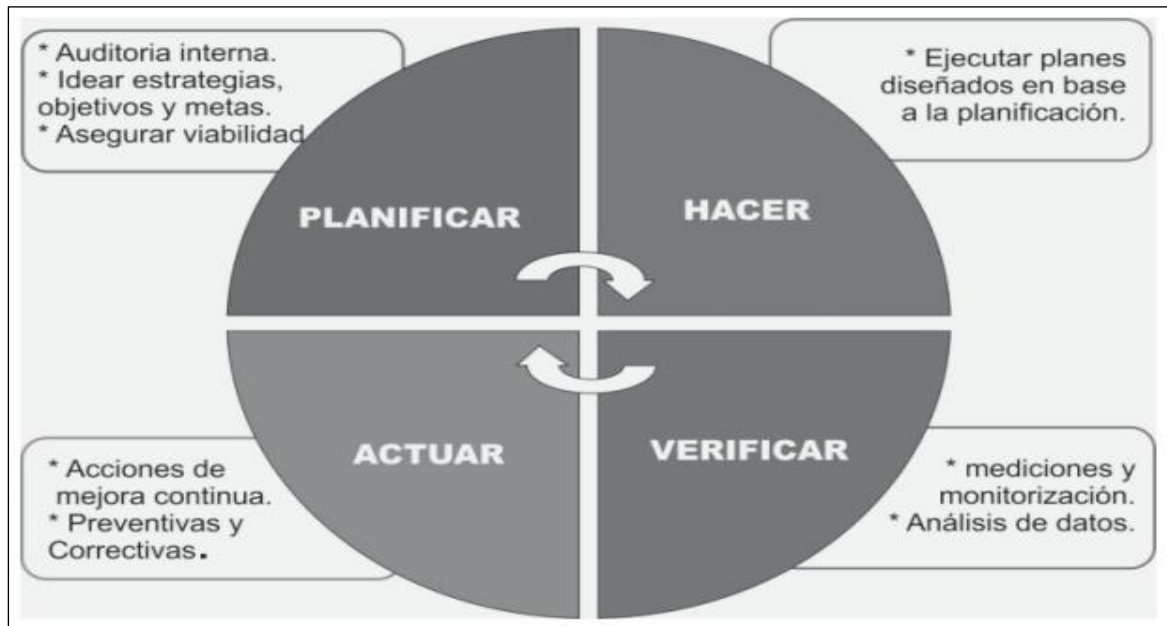
La perspectiva principal de un SGSI es la gestión proactiva de riesgos de la empresa, siguiendo el ciclo de Deming, cuyo objetivo es planificar, implementar, comprobar y mejorar continuamente las medidas de seguridad (Mera Fabricio, 2020).

- Plan (Planificar): Se identifican debilidades.
- Do (Hacer): Se ejecutan los procesos de la empresa.
- Check (Verificar): Se verifica los resultados obtenidos.
- Act (Actuar): Se busca una mejora continua, con la ayuda de lecciones aprendidas.

Para lograr una gestión eficaz, se recomienda implementar la metodología de mejora continua, también conocido como círculo PDCA.

Figura 3

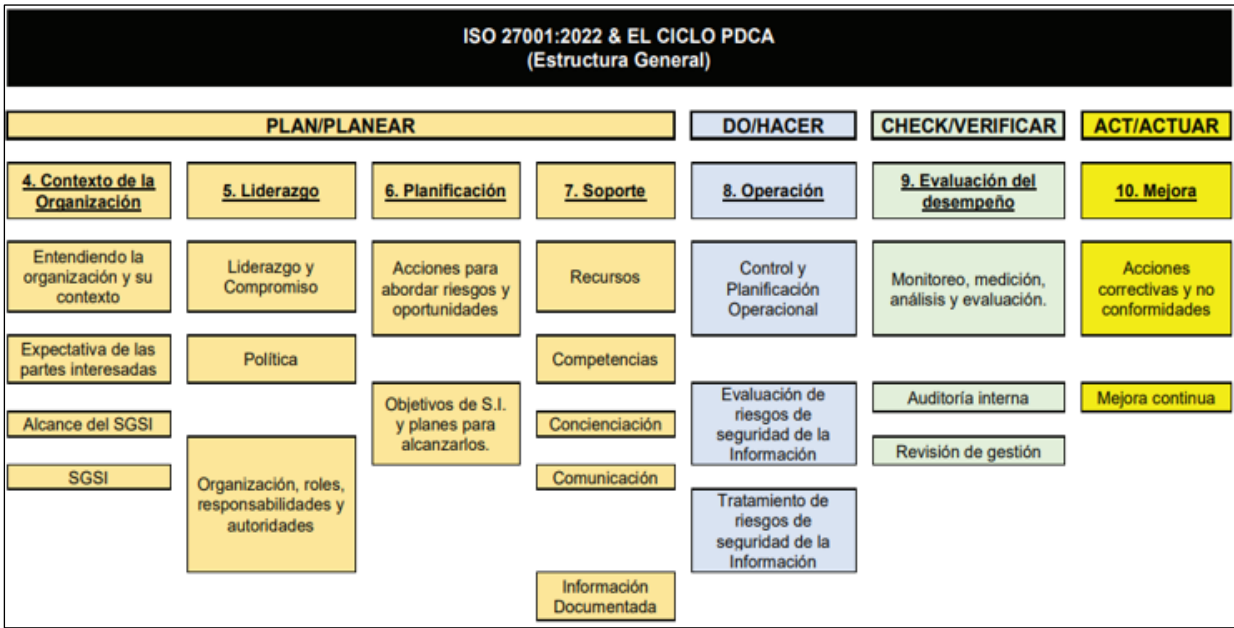
Modelo PDCA



Nota. Adaptado a Ciclo de Deming (p.5), por Montesinos Salvador, 2020.

A continuación, la relación que existe entre la ISO 27001:2013 y el modelo PDCA:

Figura 4
Estructura PDCA-ISO27001



Nota. Adaptado a Guía para implementación del EGSI (p.19), MINTEL, 2024.

1.15. Riesgo

Es la posibilidad que un actor malicioso explote la debilidad de un activo específico, resultando en un impacto negativo en el sistema (Roldán Álvarez & Vargas Montoya, 2021).

1.15.1. Gestión de Riesgos

Consiste en un procedimiento organizado que permite evaluar la gravedad de los peligros que enfrenta una entidad, con el objetivo de tomar decisiones acertadas frente a posibles contingencias. (Sánchez et al., 2020).

Gestionar los riesgos relacionados con las amenazas humanas o tecnológicas que puedan afectar a cualquier tipo de activo de información. La clave está en comprender y dominar los

peligros que amenazan a la información, que se sustentan en la política de seguridad de la entidad, y tomar las medidas adecuadas para afrontarlos (Andrade Diego, 2021).

1.15.2. Amenazas

Las amenazas cibernéticas son los potenciales intentos maliciosos o de Intrusión en sistemas informáticos, pararobar, modificar, dañar o interrumpir los datos. Estos ataques son llevados a cabo por delincuentes cibernéticos, quienes pueden ser individuos o grupos, y sus motivaciones abarcan desde actividades financieras ilegales, espionaje, interrupción de servicios, hasta conflictos cibernéticos. Hay tres tipos de amenazas: deliberadas (intencionales), accidentales e involuntarias (naturales) (Guamán José, 2023).

1.15.3. Activo vulnerable

Un activo (información, sistema, etc.) debe estar expuesto a la amenaza para que exista riesgo. La exposición puede deberse a errores de configuración, fallos de software o políticas de seguridad débiles que permitan a un atacante acceder a la información.

1.15.4. Vulnerabilidad

La vulnerabilidad es la debilidad que permite a la amenaza explotar el activo expuesto. Se relaciona con la facilidad con la que un atacante puede aprovechar la situación y violentar los controles existentes para acceder a información de la institución (Baghdadi et al., 2020).

1.16. Conceptos Básicos de Redes Móviles

Desde la antigüedad, la comunicación ha sido la necesidad fundamental para el ser humano, en la búsqueda por conectar con sus semejantes, para compartir ideas y experiencias. En este sentido, la comunicación ha sido un componente indispensable en la vida humana, permite establecer vínculos, transmitir información, colaborar y construir sociedades. A través del tiempo, el ingenio humano ha dado lugar a una amplia gama de mecanismos de comunicación, desde las señales de humo y los tambores hasta los sofisticados sistemas de telecomunicaciones actuales. Cada uno de estos avances ha respondido a la necesidad de superar las limitaciones de distancia y tiempo. Gracias al desarrollo tecnológico, nuevas herramientas y dispositivos han revolucionado

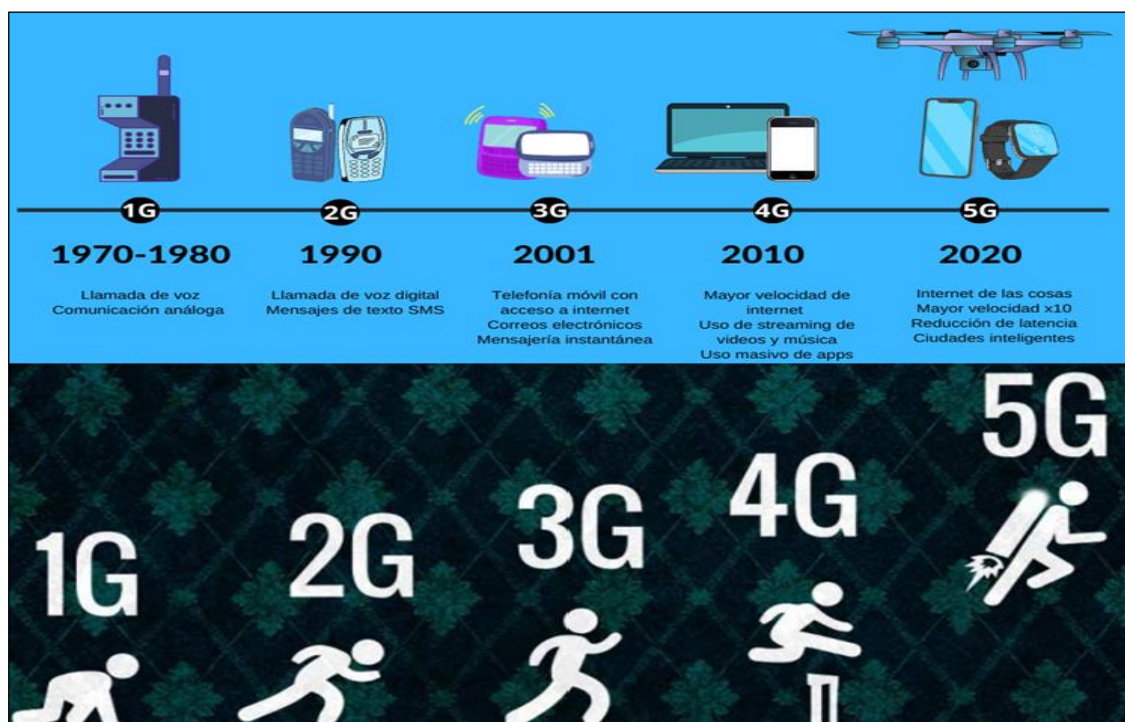
la forma de comunicación. Desde la imprenta hasta internet, pasando por el teléfono y la televisión, cada invento ha ampliado nuestras posibilidades de interacción y ha transformado la manera en que percibimos el mundo (Anchundia Morales et al., 2020).

La tecnología de telefonía móvil ha experimentado una evolución constante a lo largo del tiempo, dividiéndose en distintas generaciones según su nivel de sofisticación técnica. Cada generación se caracteriza por mejoras en la capacidad de telecomunicaciones entre las compañías telefónicas y los clientes, así como en la cantidad de información que pueden transmitir (Conde Lorena, 2020).

Las redes de comunicación móvil se caracterizan por su capacidad y desarrollo; a diferencia de las redes fijas, donde los dispositivos están conectados a un punto físico específico, las redes móviles permiten que los usuarios se desplacen sin perder su conexión. Esto se logra gracias a una infraestructura compuesta por diferentes elementos, como torres de telefonía celular, antenas y dispositivos móviles.

Figura 5

Evolución de Redes Inalámbricas



Nota. Referencia *Historia del internet móvil*, Duarte David, 2024.

1.16.1. Retos y Amenazas en Redes Móviles

Tras décadas de vertiginoso desarrollo, la tecnología de comunicaciones móviles se ha impregnado en numerosos aspectos de nuestra vida cotidiana. La tecnología móvil ha experimentado una constante evolución, adaptándose a las necesidades de los usuarios con el desarrollo de nuevas aplicaciones. Las redes móviles fueron esenciales durante la pandemia, para mantener a las familias unidas a pesar de la distancia y a las empresas funcionando en el mundo digital (Conde-Zhingre et al., 2019).

1.17. Estado del arte

El estado del arte del presente proyecto incluye experiencias muy similares en relación con investigaciones para establecer un modelo de SGSI en empresas de Telecomunicaciones, las cuales contribuyen significativamente al análisis y desarrollo de este proyecto y del modelo propuesto. En el contexto actual, la ciberseguridad juega un papel importante en la digitalización y la interconexión de redes de datos en nuestra sociedad.

A continuación, se presentan diferentes tipos de investigaciones desarrollados en el ámbito internacional y nacional, relacionadas con la ciberseguridad para empresas de telecomunicaciones:

La información confidencial y reservada en las entidades gubernamentales de Ecuador requiere la ejecución de medidas de seguridad para un control más efectivo. Para este fin, se emplea el SGSI conforme a las directrices de la normativa ISO 27001 (Falcón Helida, 2022).

La investigación realizada por Lina Ibarbo (2019) refiere al estado de la norma técnica de seguridad ISO27002 como soporte para la norma ISO27001 en empresas de telecomunicaciones, la autora considera importante adoptar un enfoque centrado en la norma ISO 27002 debido a sus prácticas recomendadas y su relación con la normativa.

En proyecto presentado por Mónica Zorro (2022), sobre la propuesta de normativa de calidad, presenta los estudios y enfatiza la relevancia de la ciberseguridad en las empresas de telecomunicaciones.

El modelo de ciberseguridad basado en la NIST y COBIT 2019, para el sector de las telecomunicaciones, desarrollado para el departamento de transmisiones para la CNT EP, presenta una propuesta de solución de ciberseguridad enmarcado en la norma NIST v1.1 (Tipán Darío, 2023).

La investigación desarrollada por Daniela Buitrago y Edward Alvarado aborda la crucial temática de la ejecución de un SGSI en el departamento de operación y mantenimiento de una compañía de telecomunicaciones. El estudio destaca la naturaleza sensible de los datos manejados por estas empresas y la importancia de disponer de procedimientos robustos para protegerla (Buitrago Daniela, 2018).

Del análisis realizado a los trabajos citados, se concluye que el presente proyecto modelo de SGSI permitirá fortalecer la ciberseguridad en las redes inalámbricas de la entidad pública de telecomunicaciones en el Ecuador.

La ciberseguridad es un punto crítico en el campo de las telecomunicaciones debido a los datos sensibles que manejan estas compañías; con el incremento de las amenazas cibernéticas, las organizaciones deben implementar sistemas robustos para preservar sus activos. La investigación de Luis Fernando Molina Batallas se centra en diseñar un SGSI para la CNT EP, específicamente para la sucursal Doral.

2. DIAGNÓSTICO SITUACIONAL

2.1.Diagnóstico de la situación empresarial

El objetivo de esta investigación es evaluar el contexto actual de las empresas públicas de telecomunicaciones en Ecuador, enfocándose a la ciberseguridad de sus redes móviles. Este análisis permitirá desarrollar un modelo de SGSI adaptado a las exigencias de la organización.

La situación empresarial de las entidades públicas de telecomunicaciones en Ecuador presenta diversos desafíos en cuanto a seguridad de información; donde las amenazas, vulnerabilidades y debilidades pueden generar riesgos a la ciberseguridad de la empresa, lo que podría generar impactos negativos considerables.

En este contexto, la propuesta de un modelo de SGSI personalizado para las exigencias de la empresa, sirve como instrumento para determinar, evaluar, y prevenir los riesgos de ciberseguridad, y garantizar la confianza de los clientes.

2.2.Metodología

Se ha empleado el método deductivo, con la ayuda de la investigación exploratoria, mediante la búsqueda de información, identificando las diferentes fuentes bibliográficas para la localización de estudios bibliográficos primarios de la ciberseguridad para redes móviles en empresas de telecomunicaciones, análisis de artículos investigativos y la ejecución de la propuesta en base a la normativa ISO/IEC 27001. Asimismo, se toma en cuenta las restricciones y criterios de inclusión, exclusión y la síntesis de datos.

Tras definir las fuentes de información, se detalló el proceso y los criterios empleados para seleccionar los estudios acordes al tema de estudio. Inicialmente, se combinaron las palabras clave seleccionadas utilizando conectores AND y OR para construir la cadena de búsqueda en las aplicaciones Scopus y Web of Science.

El procedimiento de selección de estudios, inició con la adaptación al motor de búsqueda de cada fuente y la ejecución de la consulta, restringiendo únicamente a la búsqueda de trabajos publicados en los últimos 5 años (2019 - 2024).

Se adoptó el Esquema Gubernamental de Seguridad de Información (EGSI) establecido por el MINTEL, reconocido por su enfoque en el tratamiento de riesgos en cuanto a la ciberseguridad.

2.2.1. Tratamiento de riesgos

El abordaje del tratamiento de riesgos se fundamenta en una adecuada elección de controles apropiados para mitigar o aceptar los riesgos, y la elaboración de un plan detallado para su gestión. Existen cuatro opciones disponibles para el tratamiento del riesgo:

Prevención del riesgo: Si los riesgos identificados sobrepasan el umbral de tolerancia de la organización, o si los costos para ejecutar el tratamiento de riesgos son mayores a las ventajas esperadas.

Modificación del riesgo: La selección de controles debe ser rigurosa y basado en el tratamiento de riesgos. Esta elección debe considerar factores como el costo y el tiempo de ejecución, así como aspectos técnicos, sociales y ambientales.

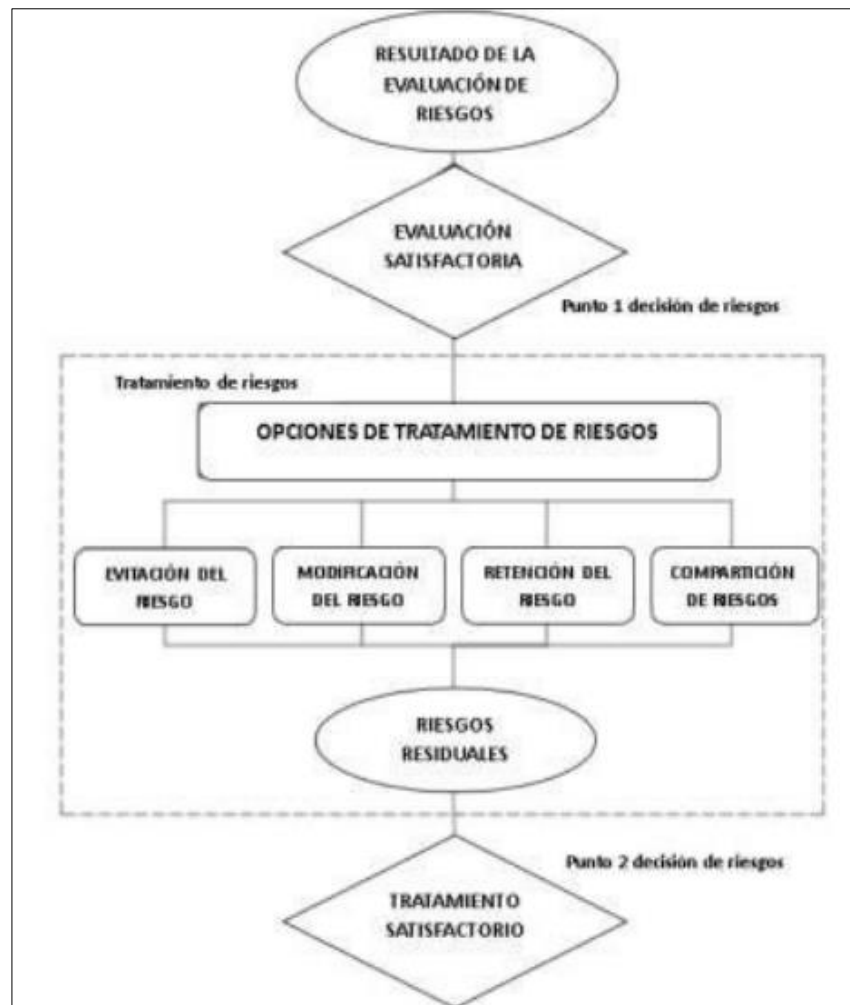
Aceptación del riesgo: Salvaguardar un riesgo sin tomar acciones, dentro de los límites de aceptación, donde no sea necesario la ejecución de controles adicionales.

Compartición del riesgo: La opción de compartir el riesgo para gestionarlo de manera efectiva; y transferir ciertos riesgos a entidades externas (EGSI, MINTEL. 2024).

En la Figura 6 se visualiza el tratamiento de riesgo en el procedimiento de gestión en ciberseguridad:

Figura 6

Tratamiento del Riesgo



Nota. Tomado de *Guía para implementación del EGSi* (p.37), MINTEL, 2024.

Además, para complementar este análisis, se empleará también el Método de Análisis de Riesgos de Livermore (LRAM); que, basada en un enfoque cuantitativo, permite evaluar los riesgos y desarrollar estrategias de mitigación, considerando las actividades:

- Identificar las vulnerabilidades y amenazas asociadas a seguridad informática.
- Evaluar los riesgos potenciales que afectan la disponibilidad, confidencialidad e integridad de la información.

- Basado en los resultados obtenidos, un modelo de SGSI para desarrollar la propuesta de SGSI para el departamento de comunicaciones en la empresa pública de telecomunicaciones, considerando las mejores prácticas y normativas internacionales (ISO 27001, 27002, 27005 y la ISO 27011)

Hoy en día las empresas, sin importar la actividad que desarrollan, tienen activos de información vitales para sus operaciones, los continuos avances tecnológicos no solo se manifiestan en la infraestructura empresarial, sino también en la creciente sofisticación de los ataques cibernéticos, estos ataques buscan obtener beneficios económicos (López Fernando, 2022).

Con el crecimiento de la digitalización y la transferencia de datos, aumenta también el peligro de pérdida y uso indebido de dicha información. Por esta razón, tanto las personas como entidades desarrollan y ejecutan medidas para reforzar la seguridad en este ámbito, conocido como ciberseguridad (Fuentes Alejandro, 2023).

El término "vulnerabilidad" se refiere a una falla en un sistema que posibilita que un ciberatacante comprometa la seguridad de los datos (Arévalo Felipe, 2020).

La metodología de "Análisis de Riesgos de Livermore" (LRAM) utiliza resultados numéricos para analizar la posibilidad de ocurrencia de riesgos y la afectación a los objetivos de la organización (Baghdadi et al., 2020).

2.2.2. Variables Dependientes

La variable dependiente está relacionada con la ciberseguridad para redes móviles en la empresa pública de telecomunicaciones.

2.2.3. Variables Independientes

En el contexto de la ciberseguridad, se considera las siguientes variables independientes:

Las vulnerabilidades refieren a las debilidades en una red de información, que podría ser explotada por un ciberdelincuente para afectar la seguridad del sistema.

Las amenazas son cualquier eventos o acciones potenciales que puede afectar la vulnerabilidad en una red de información, para comprometer su seguridad.

Los riesgos son las posibles pérdidas o daños que pueden ocurrir como resultado de amenazas que explotan vulnerabilidades en un sistema de información.

2.3.Análisis situacional

La ciberseguridad de empresas públicas se encuentra amenazada por ciberataques, lo que las convierte en objetivos de alto riesgo. El incremento de los ciberataques obliga a las instituciones públicas a crear estrategias para fortalecer su seguridad tecnológica. Sin embargo, mediante la implementación de controles de identidad robustos, es posible reducir significativamente el impacto de estos ataques maliciosos (Moran Nicole, 2021).

Las compañías dedicadas a las telecomunicaciones, experimentan pérdidas financieras debido a diversos factores, tanto internos como externos, como la pérdida de datos, ya que los riesgos no se manejan adecuadamente, estos riesgos son de origen conocido o desconocido. La combinación de ciberseguridad y evaluación de los riesgos es fundamental para que las empresas logren alcanzar sus metas (Huaura_mm, 2019).

Dado la gran cantidad de ventajas que brindan las tecnologías informáticas, es crucial reconocer que también conllevan riesgos significativos; por ende, es imperativo salvaguardar la información frente a las amenazas cibernéticas. Se busca promover la confianza en el uso de Internet, proporcionar instrumentos que faciliten la observancia de la normativa y el ejercicio de derechos relacionados con el resguardo de información personal y el uso adecuado de las TICs (Michelena Andrés, 2019).

2.3.1. Análisis Situacional de la Ciberseguridad en Redes Móviles de Empresas de Telecomunicaciones

Las compañías de telecomunicaciones se encuentran en un entorno dinámico y complejo, donde la ciberseguridad ha cambiado a un aspecto crítico para su éxito. Las redes móviles, en particular, son cada vez más utilizadas para transmitir datos de suma importancia, como información personal, comercial y económica, que se perfila como un anhelo irresistible para los atacantes.

Las redes móviles enfrentan amenazas y vulnerabilidades, incluyendo lo siguiente:

Ataques cibernéticos: Afecta la disponibilidad, integridad y confidencialidad de la ciberseguridad en redes móviles.

Fuga de datos: Puede suceder por errores humanos, fallas en los sistemas, y que puede generar consecuencias para los clientes.

Interferencia en las comunicaciones: La interferencia en las comunicaciones móviles puede afectar la calidad del servicio y generar pérdidas económicas para la empresa.

Espionaje industrial: Las empresas de telecomunicaciones pueden ser objeto de espionaje industrial para obtener información confidencial sobre sus productos, servicios o estrategias.

2.4.Panorama Actual de Ciberseguridad en Empresas de Telecomunicaciones en Ecuador

La gestión de datos confidencial y reservada en las entidades gubernamentales de Ecuador requiere la ejecución de metodologías de seguridad para un control más efectivo. Para este fin, se emplea el SGSI conforme a las directrices de la normativa ISO 27001 (Falcón Helida, 2022).

Varias compañías en Ecuador han sufrido perjuicios por ataques cibernéticos, tal como ocurrió con una empresa pública de telecomunicaciones, donde se sospecha que un empleado abrió un correo electrónico que contenía un ransomware, finalmente los datos de los clientes masivos y corporativos se encontraban debidamente resguardados (Pérez Fernando, 2023).

Mediante Registro Oficial Suplemento No. 459 del 26 de mayo de 2021, es publicada la Ley Orgánica de Protección de Datos Personales que tiene por objeto garantizar el derecho a la protección de datos incluye el acceso a la información y datos (MINTEL, 2021).

El MINTEL, mediante Acuerdo Ministerial Nro. MINTEL-2024-0003 del 1 de marzo de 2024, expide el EGSI como aporte a la ciberseguridad en el Sector Público (MINTEL, 2024).

Un ataque cibernético contra la empresa pública de telecomunicaciones en Ecuador, podría paralizar las operaciones críticas, ocasionar afectación de los servicios y comprometer la confianza del cliente en cuanto a la protección de información manejada por la empresa.

2.5.Situación Actual de la Ciberseguridad en empresas públicas en Ecuador

En la era digital actual, Ecuador ha enfrentado un auge en cuanto al empleo de la tecnología de la información, tanto dentro como fuera de las instituciones públicas. Sin embargo, este avance obliga a mejorar la ciberseguridad, convirtiéndola en una inversión crucial para proteger la información. Salvaguardar la información en instituciones gubernamentales como el Registro Civil, la Contraloría General del Estado, el MINTEL y el Consejo Nacional Electoral, entre otras, ha sido un tema de especial atención (Moran Nicole, 2021).

Durante el año 2019, varios sitios web de entidades tanto gubernamentales como privadas en Ecuador fueron blanco de ataques cibernéticos. Entre las instituciones que sufrieron intentos de ataques en las entidades como: Cancillería, Banco Central, Presidencia de la República, ministerio del Interior, Servicio de Rentas Internas, CNT, varios GAD, Consejo de la Judicatura, ministerio de Telecomunicaciones y de la Sociedad de la Información, ministerio de Turismo, ministerio de Ambiente y algunas universidades, debido a conflictos diplomáticos entorno a Julián Assange, Estos ataques cibernéticos demostraron que Ecuador no estaba lo suficientemente preparado para enfrentar este tipo de amenazas (MINTEL, 2019).

A pesar que los ataques recibidos no tuvieron mayor impacto, la desatención de las empresas en invertir en ciberseguridad las dejó expuestas a futuros ataques, lo que ocasionó la vulneración de sitios web, bases de datos y otros incidentes. El principal obstáculo en empresas públicas en Ecuador para invertir en ciberseguridad, es la limitación del presupuesto destinado a este fin.

Si bien Ecuador no contaba con procedimientos formales de seguridad informática establecidos, ha realizado avances significativos en la lucha contra los ciberataques gracias a la colaboración con organismos como EcuCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador). Esta agrupación, bajo la supervisión de ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), cuyo objetivo es responder a los requerimientos de seguridad en todo el país. Además, Ecuador forma parte de CSIRT Américas (Red de los Equipos de Respuesta ante Incidentes Cibernéticos), lo que le proporciona una red de intercambio, colaboración y participación en proyectos de defensa

gubernamentales ofrecidos por esta institución. Esto facilita el desarrollo de mejores estrategias nacionales de ciberseguridad (Moran Nicole, 2021).

3. DESARROLLO

3.1. Análisis de ciberseguridad en redes móviles

En la actualidad, los dispositivos móviles son esenciales en cualquier organización, y por eso, su gestión de seguridad se vuelve fundamental. Sin embargo, es crucial reconocer los problemas y riesgos asociados a esta tarea. La rápida evolución de la tecnología móvil genera nuevos desafíos, desde la falta de controles hasta la necesidad de consideraciones específicas para estos dispositivos (Zhu & Zhu, 2019).

3.1.1. Filtración de información

Una organización puede tener un su sistema de seguridad de información, firewalls o IDS/IPS; sin embargo, persiste el alto riesgo a la ciberseguridad por el uso de dispositivos móviles. Por ejemplo, un usuario puede fotografiar la pantalla con su smartphone mientras maneja información importante, y si el teléfono está conectado a internet, ese contenido ya está circulando. Filtrar información con dispositivos móviles es muy sencillo; está claro que prohibir su uso a los empleados no es la solución. Además, la escasa conciencia sobre seguridad de los usuarios convierte a los dispositivos móviles en presas fáciles para accesos no autorizados, poniendo en riesgo información confidencial y la seguridad de la organización. Si un malware infecta al dispositivo, el riesgo de ciberseguridad aumenta significativamente (Zhu & Zhu, 2019).

3.1.2. Los dispositivos móviles

Los smartphones, PDAs y similares ahora cuentan con procesadores rápidos y sistemas operativos integrados (SO) potentes, permitiendo el desarrollo y uso de numerosas aplicaciones específicas. De hecho, estos dispositivos son computadoras poderosas en miniatura. Sin embargo, estos dispositivos incluyen diversas formas de comunicación, como Bluetooth y protocolos TCP/IP. Estas características crean vulnerabilidades que los atacantes pueden aprovechar, debido a su capacidad y conectividad, los terminales móviles se han transformado en objetivos codiciados, con el aumento constante de malware diseñado para robar información valiosa.

3.1.3. Los recursos informáticos tradicionales

Una computadora de escritorio o un servidor dentro de un inmueble, tiene su perímetro de seguridad claro y manejable, ya que se encuentra en un entorno físico controlado. Sin embargo; con los dispositivos móviles, la situación es completamente distinta, su naturaleza portátil desvanece las fronteras de seguridad, ya que el dispositivo puede encontrarse en cualquier lugar en un momento dado. Por ello, la gestión de ciberseguridad se vuelve más complicada con el uso de estos dispositivos (Zhu & Zhu, 2019).

3.1.4. Función versátil de los dispositivos móviles

Las unidades USB ahora pueden almacenar mucha más información, por lo que es bastante fácil convertir una unidad USB en un disco de arranque, que puede eludir el software de protección de una PC. Un teléfono inteligente puede tener 128 GB de espacio de almacenamiento y funciones versátiles como grabación, fotografía, GPS, etc. Por lo tanto, los dispositivos móviles pueden desempeñar más funciones, como almacenar datos, arrancar sistemas, reproducir mp3, etc. Es conveniente para las personas usar dispositivos móviles, pero también conlleva un alto riesgo al utilizar estas funciones versátiles.

3.1.5. Robo de información transfronterizo

Los dispositivos móviles pueden estar en cualquier lugar, ya que su movilidad inherente ha impedido confiar para una protección adecuada. La revolución de las redes de telecomunicaciones en la nube y la multitud de servicios de aplicaciones alojadas que no están geográficamente fijos ha facilitado el cruce de datos a través de fronteras nacionales. Con el uso creciente de la red móvil, las aplicaciones y los datos almacenados en dispositivos móviles, tanto a nivel local como global, pueden poner en riesgo infraestructuras críticas. Además, los datos que viajan en dispositivos móviles están sujetos a leyes y regulaciones que varían de una jurisdicción a otra (Zhu & Zhu, 2019).

3.1.6. Eliminación de datos

Un conjunto de datos puede almacenarse en dispositivos móviles, y su crecimiento ha sido de manera exponencial. Los procedimientos inadecuados de eliminación de dispositivos pueden conllevar el riesgo de que se retenga información sensible en el dispositivo y se acceda a ella de

forma no autorizada. Los activos informáticos de la organización deben estar sujetos a metodologías para el control de activos en la compañía, que incluyan la eliminación segura de aquellos que contengan datos sensibles. Sin embargo, la ejecución de estos procedimientos puede ser una zona gris cuando se trata de dispositivos personales en el lugar de trabajo. Esto requiere políticas organizacionales claras para salvaguardar la información sensible, confidencial y de alto valor.

3.2.Seguridad en redes móviles según el marco ISO/IEC 27001

Como dice el estándar ISO/IEC 27001, el objetivo de la política de ciberseguridad es establecer la gestión para la seguridad de la información. Para los dispositivos móviles es importante presentar los siguientes aspectos: visión, objetivo, estrategia, alcance, organización, responsabilidades, activos, etc. (Zhu & Zhu, 2019).

3.2.1. Gestión de la Seguridad de la Información

La ciberseguridad se gestionará internamente en la empresa; la gerencia aprobará los procedimientos de seguridad, asignará roles y revisará la ejecución en la empresa; para lo cual, se debe identificar y actualizar periódicamente los activos de información relacionados con los dispositivos móviles.

3.2.2. Seguridad de Recursos Humanos

Como los dispositivos móviles son utilizados por personas, la seguridad de Recursos Humanos es crucial, deben comprender sus responsabilidades para reducir los riesgos. Para lograr esto, se debe establecer un sistema de seguridad con diferentes niveles de responsabilidad, donde el nivel superior monitoriza y audita las actividades de la empresa, el nivel medio gestiona las actividades rutinarias y nivel básico corresponde a clientes con dispositivos móviles, que deben operar estos equipos según las políticas establecidas y sujetos a la supervisión de los niveles superiores.

3.2.3. Seguridad Física y Ambiental

Si bien los dispositivos móviles no tienen un límite físico definido, la seguridad sigue siendo importante para prevenir los robos y filtraciones a la información relacionadas con estos dispositivos.

Protección de los dispositivos: Los lugares donde se guardan los dispositivos móviles estarán protegidos con controles de acceso adecuados. Se implementarán medidas para resguardar físicamente los dispositivos del acceso no autorizado, daños e interferencias. Las áreas seguras estarán restringidas mediante controles para asegurar que el personal con credenciales adecuadas pueda ingresar.

Seguridad fuera de la oficina: Aplican medidas de ciberseguridad a los dispositivos que se encuentren fuera de la empresa. Todos los equipos con almacenamiento de datos deberán revisarse para verificar que cualquier información confidencial y garantizar la eliminación o sobrescritura segura del software con licencia previo a la disposición final de cualquier dispositivo y prevenir posibles filtraciones de datos (Zhu & Zhu, 2019).

3.2.4. Gestión de Comunicaciones

Los dispositivos móviles necesitan una mejor gestión tecnológica y de operación y mantenimiento más compleja que los equipos tradicionales. Por ello, se debe establecer las siguientes responsabilidades:

Protección contra virus y malware: Se deben implementar medidas para identificar virus y software malintencionado de dispositivos móviles, para preservar la integridad de las aplicaciones y la información almacenada.

Intercambio de datos sensibles: El intercambio de información con otras organizaciones debe realizarse siguiendo las políticas establecidas.

Seguridad de dispositivos con datos sensibles: Los dispositivos móviles que contienen información confidencial deben contar con políticas adecuadas para salvaguardar el acceso y evitar el uso inapropiado.

3.2.5. Monitoreo de Acceso para Dispositivos Móviles

El acceso a organizaciones que utilizan dispositivos móviles tiene dos vertientes:

Acceso a información interna: Controlar quién puede acceder a las redes informáticas de la empresa desde dispositivos móviles.

Acceso a información externa: Controlar el acceso a fuentes de información externas desde dispositivos móviles.

Ambos aspectos del control de acceso deben basarse en las necesidades de la empresa y los requerimientos de seguridad. Se debe establecer procedimientos para que los dispositivos móviles cuenten con permisos de acceso adecuados, para la transmisión de la información interna como externa.

Las normas ISO/IEC 27001 para ciberseguridad con dispositivos móviles enfrentan nuevos desafíos constantemente debido al rápido desarrollo de las redes móviles. El uso y administración de los activos de datos móviles deben cumplir con la legislación de seguridad para evitar violaciones (Zhu & Zhu, 2019).

Los siguientes controles sirven como una buena referencia para ciberseguridad bajo el marco ISO/IEC 27001:

- Mantener actualizada la protección antivirus y parches de seguridad para sistemas operativos.
- Proteger con contraseña todos los dispositivos, como unidades extraíbles y discos compactos (CD).
- No almacenar información confidencial sin cifrar en dispositivos móviles.
- Incorporar una función de tiempo de espera que requiera una nueva autenticación después de 30 minutos de inactividad.
- Realizar copias de seguridad de información.
- Incluir mecanismos de control de acceso mediante autorización de hardware y otras basados en aplicaciones.
- No mantener los dispositivos móviles en línea cuando no estén en uso. Apagarlos o desconectarlos físicamente de la conexión a internet.

- Reportar inmediatamente a la administración la pérdida o extravío de dispositivos emitidos por el gobierno.

3.3.Enfoque para la gestión de seguridad en empresas públicas

El análisis de la literatura coincide en que la consideración de los empleados y su sensibilización sobre los peligros del ciberespacio son factores clave para el desarrollo sostenible de un SGSI. En este contexto, a diferencia de muchos otros proyectos o estándares tradicionales, es de suma importancia en el procedimiento del SGSI. La organización debe determinar con qué roles se llevará a cabo el próximo proyecto del SGSI; es esencial establecer un equipo central e integrar roles o conocimientos adicionales del proyecto (Moses & Sandkuhl, 2023).

Otro aspecto importante es aplicar el Ciclo de Deming, inherente a todo sistema de gestión, y se prioriza la planificación; en este contexto, el siguiente paso del modelo de procedimiento se centra en la obtención de la documentación adecuada para el SGSI. Esta documentación, pensada para apoyar a la organización en la operación del SGSI, cumplir con los requisitos de estructura, claridad, completitud, comprensión, corrección, trazabilidad, objetividad, integridad y autenticidad del SGSI.

La implementación del procedimiento de mantenimiento (control y ejecución de tareas de parches y actualizaciones), procesos de cambio (incorporación, alta y baja) y procesos de incidentes permite mejorar de mejor manera la ciberseguridad (Moses & Sandkuhl, 2023).

3.4. Modelo de gestión de riesgos

El auge de las redes y el teletrabajo exigen una evaluación más profunda de la seguridad de información. Para lograr esto, es indispensable disponer de sistemas apropiados de gestión de riesgos. Las empresas buscan mitigar los riesgos potenciales dentro de sus estructuras mediante controles adecuados de los riesgos (Sánchez et al., 2020).

3.5.Análisis de riesgos Livermore LRAM

El Análisis de Riesgos de Livermore (LRAM) permite analizar los riesgos de ciberseguridad, se desarrolló en el Laboratorio Nacional Lawrence Livermore (LLNL) de la Universidad de California de los Estados Unidos y ha sido ampliamente adoptada por

organizaciones de diversos sectores, incluyendo el gobierno, la industria y la academia (Sánchez et al., 2020).

3.5.1. Características principales del LRAM

El Análisis de Riesgos de Livermore, combina técnicas cuantitativas y cualitativas para evaluar los riesgos, esto permite obtener una visión concreta de la situación. También tiene una estructura modular, se divide en módulos que facilitan su comprensión y aplicación, se enfoca en la identificación y tratamiento de los activos, amenazas, vulnerabilidades y riesgos. Finalmente, LRAM se acopla a las necesidades de la empresa, se analiza los riesgos desde los más simples hasta los más complejos.

3.5.2. Procedimiento del LRAM

El primer paso del LRAM es identificar todos los activos informáticos; como sistemas, dispositivos y aplicaciones, se analiza las amenazas y vulnerabilidades que afectan a los activos, para continuar con la evaluación de los riesgos, se revisa la probabilidad que se produzca un incidente y se analiza el impacto del mismo. En cuanto a la priorización de los riesgos se desarrolla estrategias de mitigación.

3.5.3. Beneficios del LRAM

LRAM proporciona a las organizaciones una herramienta para tratar los riesgos y permite tomar de mejor manera las decisiones en cuanto a ciberseguridad.

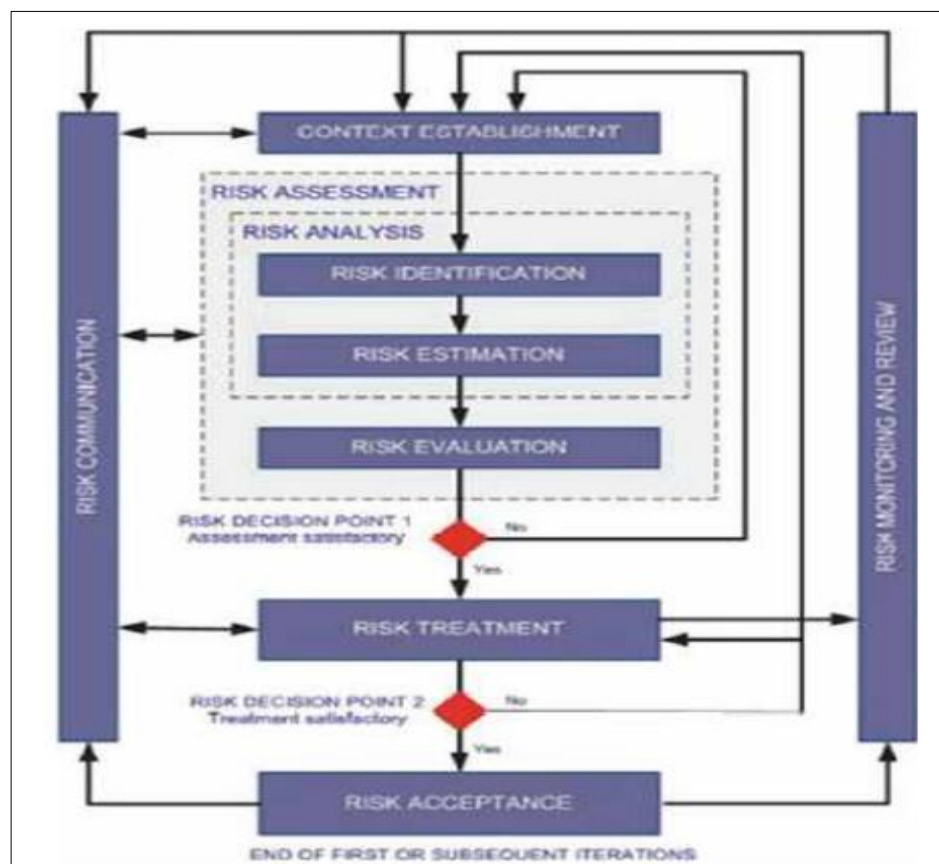
3.6. Métodos cualitativos vs. cuantitativos para la gestión de riesgos

La gestión de riesgos puede apoyarse en métodos cuantitativos o cualitativos, dependiendo del análisis previo realizado. Sin embargo, las organizaciones públicas necesitan enfoques más simples, genéricos y colaborativos. Habitualmente, la gestión de riesgos se basa en metodologías cuantitativas usadas por entidades financieras y aseguradoras. Ejemplos de métodos cuantitativos son la Expectativa Anual de Pérdida (ALE) y la Metodología Livermore de Análisis de Riesgos (LRAM). Estos métodos emplean resultados numéricos para expresar el evento de cada factor de riesgo y su afectación a los objetivos de la empresa (Baghdadi et al., 2020).

Las etapas clave de la gestión de riesgos, está definido por el alcance, así como la organización adecuadamente de las actividades. Los responsables realizan una medición o descripción cualitativa del riesgo para priorizarlo en función de la gravedad. Al momento de reducir, mantener, evitar o transferir el riesgo se debe establecer los planes correspondientes. En base a la evaluación del riesgo y a los costos y beneficios esperados, se seleccionan e implementan las opciones de gestión del riesgo. Se considera la decisión formal para aceptar el riesgo y su responsabilidad, para continuar con el intercambio o la puesta en común con los delegados de la Alta Gerencia para llegar a un acuerdo sobre cómo llevar a cabo la gestión del riesgo. El riesgo no es estático, ya que las amenazas y vulnerabilidades pueden cambiar repentinamente. Por tanto, se debe monitorear las amenazas o vulnerabilidades, para detectar posibles cambios (Baghdadi et al., 2020).

Figura 5

Procedimiento de la gestión de riesgos



Nota. Seguridad de la información según ISO 27005

Por tanto, las infraestructuras de grandes sistemas de información con amplios recursos humanos y financieros se benefician de métodos cuantitativos. La objetividad de estos métodos se basa en fórmulas matemáticas fácilmente verificables. Sin embargo, dependen de estimaciones de posibles daños a los activos o pérdidas en los sistemas de información.

3.6.1. Métodos Cualitativos

Estos métodos dependen de la estimación de posibles daños a los activos o pérdidas en los sistemas de información. Los métodos cuantitativos requieren más costos, mayor experiencia y herramientas más avanzadas en comparación con los métodos cualitativos utilizados en la gestión de riesgos. Sin embargo, para el tipo cualitativo es necesaria evaluar los efectos identificados de los riesgos potenciales sobre los activos informáticos y establecer prioridades al momento de tomar decisiones para dar soluciones. Cualquier conocimiento disponible en una organización puede adaptar los métodos cualitativos para facilitar su uso. Además, requieren menos tiempo, dinero y esfuerzo, ya que los riesgos se pueden expresar mediante variables descriptivas en lugar de valores monetarios exactos. Se basan en el juicio, la intuición y la experiencia de un individuo para gestionar el riesgo (Baghdadi et al., 2020).

Tabla 2

Métricas de Riesgo Cualitativas

Consequences	Likelihood		
	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

H: Riesgo alto
M: Riesgo medio
L: Riesgo bajo

Nota. Se muestra un ejemplo de métricas de riesgo cualitativas.

3.6.2. Enfoques tradicionales de gestión de riesgos

Diversos informes, encuestas y publicaciones señalan que los métodos actuales del tratamiento de riesgos no se utilizan ampliamente en las empresas, a pesar de la existencia de cada vez más estándares y soluciones comerciales. Esto se debe a la falta de conocimiento sobre su

importancia, costo elevado de implementación, necesidad de contar con personal especializado, proceso largo y complejo.

Los métodos tradicionales presentan otros inconvenientes que hacen que las organizaciones confíen menos en ellos, tales como generan informes voluminosos y confusos, tienen un alcance tecnológico limitado y existe una gran cantidad de métodos disponibles (más de 200 en la actualidad) dificultando la elección.

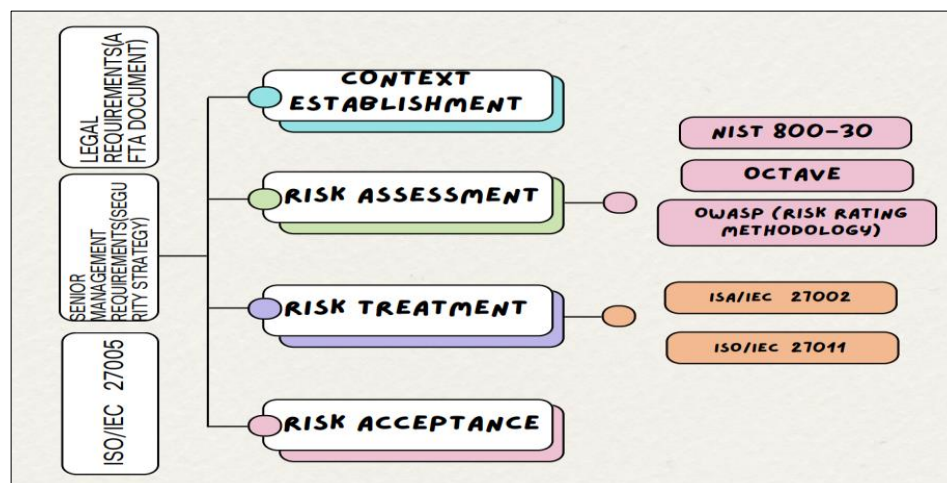
No hay marcos de referencia o herramientas comparativas acordadas para valorar los riesgos de ciberseguridad. Un error común es considerar la seguridad de la información como un asunto puramente técnico, los métodos tradicionales se centran principalmente en la tecnología y solo abordan los riesgos desde una perspectiva técnica, ignoran en gran medida los factores humanos, organizativos y estratégicos (Baghdadi et al., 2020).

3.6.3. Criterios de evaluación del riesgo

La evaluación del riesgo se centra en el impacto que las pérdidas de CIA tienen en el negocio. En los criterios de impacto se analiza de tres maneras: pérdida de valor financiero, interrupción del servicio y daño a la imagen de la empresa. Para la aceptación del riesgo se debe comparar el impacto en el incidente de seguridad en relación al costo que implica prevenirlo.

Figura 6

Tratamiento del riesgo



Nota. Tratamiento del riesgo en ciberseguridad

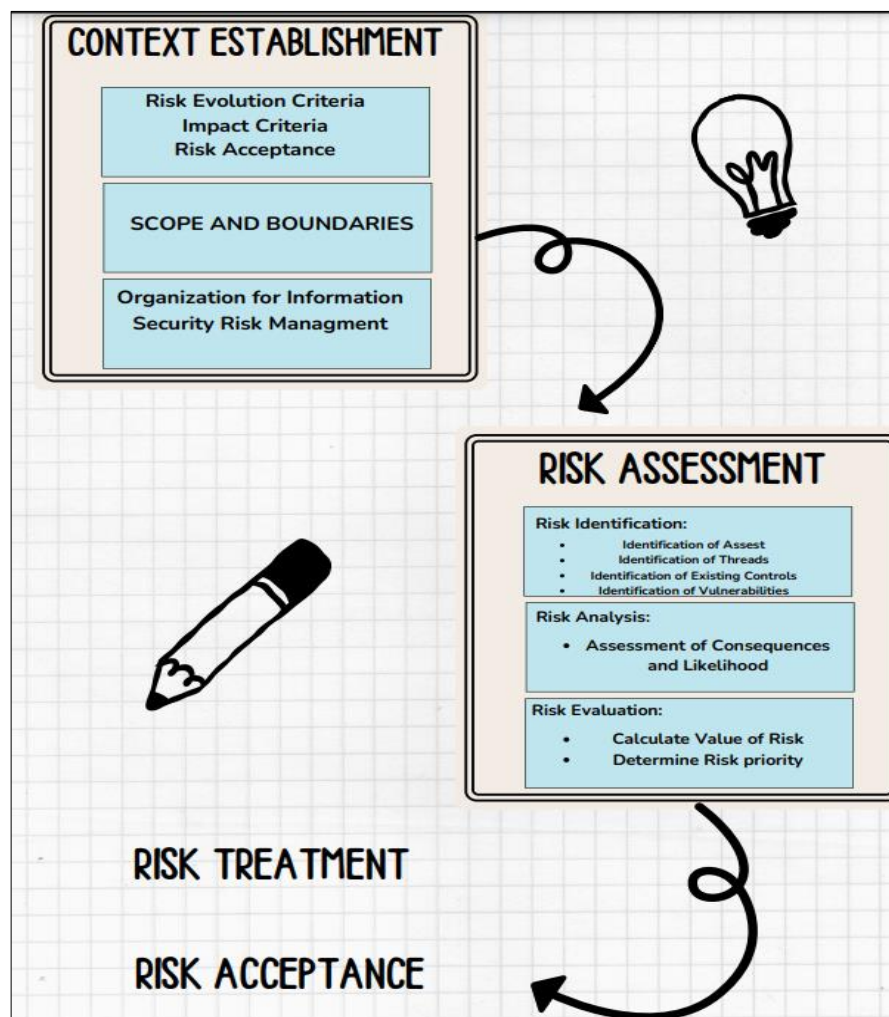
El alcance se centró en el departamento de TI debido a su responsabilidad de los datos de la organización, este departamento es encargado del procedimiento de gestión de riesgos (Baghdadi et al., 2020).

3.7.Evaluación de Riesgos de Seguridad de la Información

El departamento de TI es el responsable del proceso de identificación y gestión de los riesgos.

Figura 7

Planificación de gestión de riesgos



Nota. Planificación del proceso de gestión de riesgos de seguridad de la información.

3.7.1. Identificación de Riesgos

La identificación de riesgos es un proceso fundamental en el SGSI. Para lo cual, se identifican los activos informáticos, y se consideran cuatro tipos de activos como el de información, de dispositivos de infraestructura, de portadores de información y activos intangibles. Se identifican las amenazas que pueden afectar a cada activo, así como el origen de dichas amenazas, para finalmente identificar los controles de seguridad para garantizar su correcto funcionamiento y evitar trabajos o costos innecesarios.

3.7.2. Verificación de la Identificación

Se identifican los controles de protección para asegurar su correcto funcionamiento y evitar trabajos o costos innecesarios. La identificación de vulnerabilidades se verifica mediante entrevistas al personal relevante del departamento de TI y revisiones presenciales para los controles físicos (por ejemplo, verificar la seguridad perimetral o el acceso a áreas restringidas).

3.7.3. Identificación de Vulnerabilidades

Identificadas las amenazas y los controles para cada activo, se procede a identificar las debilidades o fallas que podrían presentarse en ellos (vulnerabilidades). Para identificar las vulnerabilidades se utilizan diferentes métodos, como entrevistas con personal clave del departamento de TI, observaciones directas de los procesos y controles, herramientas técnicas especializadas en la detección de vulnerabilidades, como Nessus, las vulnerabilidades pueden surgir por la falta de controles adecuados. Las vulnerabilidades de organización están relacionadas con deficiencias en los procesos, políticas o la estructura organizacional y las de recursos humanos derivadas de la falta de conocimiento, habilidades o comportamiento inadecuado del personal (Baghdadi et al., 2020).

3.7.4. Análisis de Riesgos

Se asigna valor a los activos en función de los resultados de un posible incidente; este escenario se define como una amenaza que aprovecha una vulnerabilidad en un incidente de seguridad de la información. Para determinar la afectación de estos posibles escenarios, se

consideran los criterios establecidos durante la actividad de definición. El valor de cada activo se determina analizando el impacto que tendría la pérdida de los datos.

3.7.5. Tratamiento del Riesgos

Al respecto, se considera cuatro opciones principales para evaluar los riesgos identificados:

Reducción: Se deben implementar controles apropiados para cumplir con los parámetros establecidos en la valoración de los riesgos, se debe considerar una tolerancia al riesgo definida por la entidad, las regulaciones legales aplicables, así como el costo, tiempo y aspectos técnicos, ambientales y sociales.

Aceptación: Se debe considerar que el nivel del riesgo se encuentre dentro de los parámetros de tolerancia al riesgo establecidos por la entidad.

Prevención: Para el caso donde el riesgo se considera demasiado alto; o su vez, los costos asociados a la implementación que superen los beneficios potenciales para la empresa, se puede optar por evitar el riesgo.

Transferencia: Que consiste en transferir el riesgo a una tercera parte. (Baghdadi et al., 2020).

Tabla 3

Valor del Riesgo

Incidente de probabilidad	Muy Alto (4)	Alto (3)	Medio (2)	Bajo (1)
1	4	3	2	1
2	8	6	4	2
3	12	9	6	3
4	16	12	8	4
5	20	15	10	5
6	24	18	12	6

Nota. Tabulación del valor del riesgo

Tabla 4

Prioridad del Riesgo

Risk score	Priority
1 -5	Low
6-10	Medium
11-17	High
18-24	Very High

Nota. Priorización del riesgo

3.8.Análisis de Riesgos de Livermore (LRAM) para Redes Móviles de una Empresa Pública de Telecomunicaciones

El Análisis de Riesgos de Livermore (LRAM) es una metodología integral que permite analizar los riesgos en sistemas críticos, como es el caso de redes móviles de una empresa pública de telecomunicaciones. LRAM facilita un marco robusto para identificar, analizar, priorizar y mitigar los riesgos, facilitando a la empresa para tomar decisiones y proteger su infraestructura, operaciones y servicios. En el contexto de las redes móviles, LRAM puede ser usado para evaluar diferente tipo de riesgos, incluyendo:

Ciberataques: Intrusiones no autorizadas a la red que pueden comprometer datos confidenciales o interrumpir operaciones críticas.

Fallos de infraestructura: Interrupciones del servicio causadas por fallas en equipos, software o instalaciones.

Errores humanos: Actos negligentes o intencionales que pueden provocar interrupciones del servicio o pérdidas financieras.

Regulaciones cambiantes: Modificaciones en las leyes o regulaciones.

Desastres naturales: Eventos que pueden ocasionar daños en la infraestructura de la red.

3.9.Propuesta de mejora de SGSI

El manejo de riesgos en ciberseguridad permite profundizar, así como detallar cada iteración de evaluación, logrando un equilibrio entre la eficiencia (optimización del proceso de identificación de controles) y la efectividad; es decir, la garantía de evaluar correctamente los riesgos de alto impacto (EGSI, MINTEL 2024).

Tabla 5
Identificación de Activos

IDENTIFICACIÓN DE ACTIVOS						
Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Propietario del Activo
A1	Gerencia de Ciberseguridad y Control	Infraestructura	Hardware	Firewall	Sistema de defensa el tráfico de entrada o salida	Responsable de Ciberseguridad
A2	Gerencia Nacional Técnica	Infraestructura	Hardware	Datacenter	Equipo de networking	Responsable de Data Center
A3	Gerencia de Tecnologías de Información	Infraestructura	Software	Portales Institucionales	En este portal se recopila información de clientes	Responsable Tecnologías de Información
A4	Gerencia Nacional Técnica	Infraestructura	Hardware	Aplicaciones móviles	Aplicaciones móviles para red inalámbrica	Responsable de Acceso Inalámbrico
A5	Gerencia de Tecnologías de Información	Infraestructura	Software	Desarrollo de aplicaciones	Desarrollo y mantenimiento de software	Responsable Tecnologías de Información

Nota. Elaboración del autor

3.9.1. Valoración de los activos

En la ponderación de los activos participan los diferentes departamentos involucrados de la empresa, para establecer cualitativamente la criticidad de los distintos activos.

Tabla 6

Evaluación de Impacto por Pérdida de Confidencialidad

CONFIDENCIALIDAD	Criterio
Alto (3)	La difusión no autorizada de la información tiene un efecto crítico para la institución
Medio (2)	La difusión no autorizada de la información tiene un efecto limitado para la institución
Bajo (1)	La difusión de la información no tiene ningún efecto para la institución

Nota. EGSI, MINTEL, 2024.

Tabla 7

Evaluación de Impacto por Pérdida de Integridad.

INTEGRIDAD	Criterio
Alto (3)	La eliminación o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La eliminación o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La eliminación o modificación de la información tiene un efecto leve para la institución

Nota. EGSI, MINTEL, 2024.

Tabla 8

Evaluación de Impacto por Pérdida de Disponibilidad

INTEGRIDAD	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	Interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Nota. EGSI, MINTEL, 2024.

Para el presente proyecto relacionado a la propuesta del SGSI para redes móviles en empresa pública de telecomunicaciones en Ecuador, se presenta la evaluación del modelo en relación al CID, principios fundamentales de la ciberseguridad.

Tabla 9

Evaluación de los Activos

EVALUACIÓN DE LOS ACTIVOS DE INFORMACIÓN							
Nro. Activo	Nombre de Activo	Tipo de soporte	Propietario del Activo	Valoración de Impacto (pérdida)			
				C	I	D	VA
A1	Firewall	Virtual	Responsable de Ciberseguridad	3	3	3	3
A2	Datacenter	Virtual	Responsable de Data Center	1	1	3	1,67
A3	Portales Institucionales	Virtual	Responsable Tecnologías de Información	2	3	1	2
A4	Aplicaciones móviles	Virtual	Responsable de Acceso Inalámbrico	2	2	3	2,33
A5	Desarrollo de aplicaciones	Virtual	Responsable Tecnologías de Información	2	2	2	2

Nota. Elaboración del autor

La evaluación del impacto (VA), es la suma de los valores correspondiente a CID.

3.9.2. Identificación de Amenazas

Es necesario ubicar las amenazas y sus fuentes; que tiende a perjudicar activos, y, en consecuencia, afectar a la empresa.

Tabla 10

Identificación de Amenazas

IDENTIFICACIÓN DE AMENAZAS		
Nro. Activo	Nombre Activo	Amenaza
A1	Firewall	Arriesgar información confidencial Ataques cibernéticos Fuga de información.

A2	Datacenter	Afectación a la integridad, disponibilidad y confiabilidad (CID) de los datos Ataque de un ramsonware Ataque denegación de servicio
A3	Portales Institucionales	Ataques a la página web Suspensión del servicio Acceso de ciberdelincuentes a información restringida
A4	Aplicaciones móviles	Inyección de código malicioso Acceso a datos sensibles de la empresa
A5	Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente Aprovechamiento de fallas en el código

Nota. Elaboración del autor

3.9.3. Identificación de Vulnerabilidades

Una vulnerabilidad por sí sola no causa daño, ya que necesita de una amenaza que pueda ejecutarla. Una vulnerabilidad sin una amenaza puede no necesitar la implementación de una comprobación inmediata, pero debe ser identificada y vigilada para detectar cualquier cambio.

Tabla 11

Identificación de Vulnerabilidades

Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad
A1	Firewall	Arriesgar información confidencial	Manejo deficiente de claves de acceso
		Ataques cibernéticos	Actualización de certificados
		Fuga de información.	Configuración de equipos sin revisión
A2	Datacenter	Afectación a la CID de los datos	Plataforma desactualizada
		Ataque de un ramsonware	Sistemas desactualizados

A3	Portales Institucionales	Ataque de denegación de servicio distribuido	Ausencia de políticas para filtrar tráfico malicioso
		Ataques a la página web	Falta de monitoreo de red
		Suspensión del servicio	Actualización de parches del software
A4	Aplicaciones móviles	Acceso de ciberdelincuentes a información restringida	Compartir credenciales de acceso
		Inyección de código malicioso	Falta de actualización de software y parches de seguridad
		Acceso a datos sensibles de la empresa	Uso de contraseñas débiles
A5	Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente	Falta de recursos humanos especializados en desarrollo de software
		Aprovechamiento de fallas en el código	Errores de inyección de código

Nota. Elaboración del autor

3.9.4. Identificación de existencia de controles

Es fundamental localizar los controles ya implementados para evitar la redundancia y optimizar el uso de recursos. La evaluación de su efectividad mediante reportes del SGSI permite reducir el tiempo invertido en esta acción.

Tabla 12

Identificación de Controles

IDENTIFICACIÓN DE CONTROLES EXISTENTES				Impacto	
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Controles existentes
A1	Firewall	Arriesgar información confidencial	Manejo deficiente de claves de acceso	3	Monitoreo continuo
		Ataques cibernéticos	Actualización de certificados	3	Monitoreo continuo
		Fuga de información.	Configuración de equipos sin revisión	3	Monitoreo continuo

A2	Datacenter	Afectación a la CID de los datos	Plataforma desactualizada	2	Monitoreo continuo
		Ataque de un ransomware	Sistemas desactualizados	2	Monitoreo continuo
		Ataque de denegación de servicio distribuido	Ausencia de políticas para filtrar tráfico malicioso	2	Monitoreo continuo
A3	Portales Institucionales	Ataques a la página web	Falta de monitoreo de red	2	Monitoreo continuo
		Suspensión del servicio	Actualización de parches del software	2	Monitoreo continuo
		Acceso de ciberdelincuentes a información restringida	Compartir credenciales de acceso	2	Monitoreo continuo
A4	Aplicaciones móviles	Inyección de código malicioso	Falta de actualización de software y parches de seguridad	2,33	Monitoreo continuo
		Acceso a datos sensibles de la empresa	Uso de contraseñas débiles	2,33	Monitoreo continuo
A5	Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente	Falta de recursos humanos especializados en desarrollo de software	2	Monitoreo continuo
		Aprovechamiento de fallas en el código	Errores de inyección de código	2	Monitoreo continuo

Nota. Elaboración del autor

3.9.5. Análisis del riesgo

El análisis de riesgos se adapta a las características específicas de cada organización, considerando la importancia de sus activos, las vulnerabilidades conocidas y los incidentes previos.

3.9.6. Valoración de los riesgos

El nivel de riesgo se obtiene multiplicando la probabilidad de amenaza por la probabilidad de vulnerabilidades y el valor del impacto del activo de la información (CID).

Tabla 13
Criterios de Probabilidad de Ocurrencia de Amenazas

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y < 50%)	En rara ocasión	El atacante no se beneficia del ataque

Nota. EGSI, MINTEL, 2024.

Tabla 14

Criterio de Probabilidad de Ocurrencia de Vulnerabilidades

Nivel de vulnerabilidad	Criterio
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable
Bajo (1)	La medida de seguridad es adecuada

Nota. EGSI, MINTEL, 2024.

Tabla 15

Nivel de Riesgo

Valoración	Nivel de Riesgo	Acciones
1 - 3	El riesgo es BAJO	Retención y monitoreo del activo
4 - 8	El riesgo es MEDIO	Requiere atención mediante la aplicación de controles que permita disminuir el riesgo, durante un tiempo determinado de acuerdo a la importancia del activo
9 - 27	El riesgo es ALTO	Requiere atención inmediata, para

Nota. EGSI, MINTEL, 2024.

Para determinar el riesgo se considera el producto del factor Vulnerabilidad Amenaza (CID) por el factor nivel amenaza y factora nivel vulnerabilidad. Con base a lo expuesto, se procede a evaluar los riesgos:

Tabla 16

Evaluación de Riesgos

					Valoración de los riesgos				
Análisis de Riesgos				Im	Probabilidad		Cálcul	o de	Nivel
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Firewall	Arriesgar información confidencial	Manejo deficiente de claves de acceso	3	2	2	Monitoreo continuo	12	ALTO
		Ataques cibernéticos	Actualización de certificados	3	2	1	Monitoreo continuo	6	MEDIO
		Fuga de información	Configuración de equipos sin revisión	3	2	1	Monitoreo continuo	6	MEDIO
A2	Datacenter	Afectación a la CID de los datos	Plataforma desactualizada	2	2	1	Monitoreo continuo	4	MEDIO
		Ataque de un ramsonware	Sistemas desactualizados	2	2	2	Monitoreo continuo	8	ALTO
		Ataque de denegación de servicio	Ausencia de políticas para filtrar tráfico malicioso	2	2	1	Monitoreo continuo	4	MEDIO
A3	Portales Institucionales	Ataques a la página web	Falta de monitoreo de red	2	2	2	Monitoreo continuo	8	ALTO
		Suspensión del servicio	Actualización de parches del software	2	2	1	Monitoreo continuo	4	MEDIO
		Acceso de ciberdelincuentes a información restringida	Compartir credenciales de acceso	2	2	1	Monitoreo continuo	4	MEDIO

A4	Aplicaciones móviles	Inyección de código malicioso	Falta de actualización de software y parches de seguridad	2,33	2	1	Monitoreo continuo	4,66	MEDIO
		Acceso a datos sensibles de la empresa	Uso de contraseñas débiles	2,33	2	1	Monitoreo continuo	4,66	MEDIO
A5	Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente	Falta de recursos humanos especializados en desarrollo de software	2	1	1	Monitoreo continuo	2	BAJO
		Aprovechamiento de fallas en el código	Errores de inyección de código	2	2	1	Monitoreo continuo	4	MEDIO

Nota. Elaboración del autor

El detalle del tratamiento de los riesgos se presenta a continuación:

		Análisis de Riesgos						Control de Riesgos						Riesgo residual	
		Impacto	Probabili dad		Contr oles imple ment ados exis tentes	Cálcu lo de Evalu ación Riesg o	Nivel de Riesgo	Métod o de tratami ento de Riesgos	Tipo de contr ol	Controles a Implementar	Nivel de amen aza	Nive l de vuln era bilidad ad	Cálculo de Evaluaci ón Riesgo con el control impleme ntado		Nivel de Riesgo con el control Implem enta do
Activo	Amenaza		CID	Niv el de ame naz a											
Firewall	Arriesgar información confidencial	3	2	2	Moni toreo conti nuo	12	ALTO	Modifi car / Preven ción	Contr ol corre ctivo	Proteger la información confidencial mediante la identificación, clasificación y manejo adecuado de la misma.	1	1	2	BAJO	Aceptable
	Ataques cibernéticos	3	2	1	Moni toreo conti nuo	6	MEDI O	Modifi car / Preven ción	Contr ol corre ctivo	Implementar un programa de concienciación sobre seguridad cibernética	1	1	2	BAJO	Aceptable
	Fuga de información	3	2	1	Moni toreo conti nuo	6	MEDI O	Modifi car / Preven ción	Contr ol corre ctivo	Implementar un programa de gestión de derechos de acceso	1	1	2	BAJO	Aceptable

	Afectación a la CID de los datos	2	2	1	Monitoreo continuo	4	MEDIO	Modificar / Prevención	Control correctivo	Garantizar continuidad de servicios y la recuperación de datos, cuando se interrumpa el servicio.	1	1	2	BAJO	Aceptable
Datacenter	Ataque de un ransomware	2	2	2	Monitoreo continuo	8	ALTO	Modificar / Prevención	Control correctivo	Implementar un programa de copias de seguridad y recuperación de información.	1	1	2	BAJO	Aceptable
	Ataque de denegación de servicio distribuido	2	2	1	Monitoreo continuo	4	MEDIO	Modificar / Prevención	Control correctivo	Implementar una solución de mitigación de DDoS, que pueda detectar, filtrar y mitigar el tráfico malicioso	1	1	2	BAJO	Aceptable
Portales Institucionales	Ataques a la página web	2	2	2	Monitoreo continuo	8	ALTO	Modificar / Prevención	Control correctivo	Implementar un Web Application Firewall	1	1	2	BAJO	Aceptable

	Suspensión del servicio	2	2	1	Monitoreo continuo	4	MEDIO	Modificar / Prevención	Control correctivo	Implementar un plan de continuidad del servicio Minimizar el riesgo de acceso no autorizado a datos	1	1	2	BAJO	Aceptable
	Acceso de ciberdelincuentes a información restringida	2	2	1	Monitoreo continuo	4	MEDIO	Prevención	Control preventivo	confidenciales, mediante asignación de permisos de acceso en función de sus roles y responsabilidades	1	1	2	BAJO	Aceptable
	Inyección de código malicioso	2,33	2	1	Monitoreo continuo	4,66	MEDIO	Modificar / Prevención	Control correctivo	Implementar validación de entrada y salida de datos, contra ataques de inyección de código malicioso	1	1	2	BAJO	Aceptable
Aplicaciones móviles	Acceso a datos sensibles de la empresa	2,33	2	1	Monitoreo continuo	4,66	MEDIO	Modificar / Prevención	Control correctivo	Implementar la gestión de derechos de información	1	1	2	BAJO	Aceptable

Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente	2	1	1	Monitoreo continuo	2	BAJO	Prevención	Control preventivo	Implementar un plan de backups para recuperar datos, y garantizar la continuidad de servicios y atención al cliente	1	1	2	BAJO	Aceptable
	Aprovechamiento de fallas en el código	2	2	1	Monitoreo continuo	4	MEDIO	Modificar / Prevención	Control correctivo	Implementar un programa de desarrollo seguro (DevSecOps)	1	1	2	BAJO	Aceptable

4. RESULTADOS

A continuación, se presenta los resultados más importantes por orden de prioridad:

Activo	Amenaza	Controles a Implementar	Riesgo residual
Firewall	Arriesgar información confidencial	Proteger la información confidencial mediante la identificación, clasificación y manejo adecuado de la misma.	Aceptable
	Ataques cibernéticos	Ejecutar charlas de concientización sobre seguridad cibernética	Aceptable
	Fuga de información	Implementar un programa de gestión de derechos de acceso	Aceptable

Activo	Amenaza	Controles a Implementar	Riesgo residual
Datacenter	Afectación a la CID de los datos	Garantizar continuidad de operaciones y la recuperación de los activos, cuando se interrumpa el servicio.	Aceptable
	Ataque de un ramsonware	Implementar un programa de backups, copias de seguridad y software para recuperar datos.	Aceptable
	Ataque de denegación de servicio distribuido	Implementar una solución de mitigación de DDoS, que pueda detectar, filtrar y mitigar el tráfico malicioso	Aceptable

Activo	Amenaza	Controles a Implementar	Riesgo residual
Portales Institucionales	Ataques a la página web	Implementar un Web Application Firewall	Aceptable
	Suspensión del servicio	Implementar un plan de continuidad del servicio	Aceptable
	Acceso de ciberdelincuentes a información restringida	Minimizar el riesgo de acceso no autorizado a datos confidenciales, mediante asignación de permisos de acceso en función de sus roles y responsabilidades	Aceptable

Activo	Amenaza	Controles a Implementar	Riesgo residual
Aplicaciones móviles	Inyección de código malicioso	Implementar validación de entrada y salida de datos, contra ataques de inyección de código malicioso	Aceptable
	Acceso a datos sensibles de la empresa	Implementar la gestión de derechos de información	Aceptable

Activo	Amenaza	Controles a Implementar	Riesgo residual
Desarrollo de aplicaciones	Interrupción del servicio y cese de la atención al cliente	Implementar un plan que permita garantizar la continuidad de servicios y atención al cliente	Aceptable
	Aprovechamiento de fallas en el código	Implementar un programa de desarrollo seguro (DevSecOps)	Aceptable

El modelo de ciberseguridad propuesto permitirá proteger la información contra ataques cibernéticos mediante la identificación de anomalías en los datos y patrones de uso. A diferencia de los métodos tradicionales de exploración, este enfoque se basa en el análisis de datos. El sistema de seguridad de información permitirá reconocer los ataques, para que las organizaciones puedan adoptar medidas proactivas para reducir los riesgos y proteger sus activos.

Para reducir aún más las vulnerabilidades, se recomienda establecer políticas de defensa sólidas en los diferentes departamentos de la organización, robustecer el equipo de ciberseguridad del departamento de TI. Esta área especializada debería contar con los recursos y la experiencia para ejecutar y gestionar eficazmente el procedimiento de defensa, así como para mantenerse a la vanguardia de las últimas amenazas y vulnerabilidades.

La gestión de recursos en el contexto del estándar ISO 27001, para el control y correcto funcionamiento del SGSI. Estos recursos incluyen personal, infraestructura, tecnología y presupuesto, todos ellos esenciales para materializar los objetivos de seguridad de los datos en la entidad, esta gestión ha cobrado gran relevancia para las empresas, convirtiéndose en un pilar fundamental para la mejora del nivel de gestión estratégica.

El SGSI basado en los estándares ISO 27001, permite evaluar a la empresa para proteger sus activos de información de manera eficaz, garantizando que la organización cuenta con las medidas de seguridad adecuadas para afrontar los riesgos y amenazas del entorno actual. Una vez identificados los parámetros críticos y las vulnerabilidades en la red, se implementan medidas de protección adecuadas. Estas medidas pueden incluir la instalación de firewalls, Sistemas de Detección de Intrusiones (IDS).

El control del tráfico de las redes móviles tiene como objetivo principal optimizar el rendimiento, la seguridad y la experiencia del usuario, asegurando un funcionamiento óptimo y confiable de la red de telecomunicaciones. La incorporación de indicadores clave de desempeño (KPI) permitirá medir la eficacia de un programa de seguridad de la información en una entidad; así también, evaluar el rendimiento de la red móvil, como la tasa de alteración de paquetes, la pérdida de paquetes y el tiempo de inactividad. Los KPIs proporcionarán información útil que pueda utilizarse para tomar medidas concretas y mejorar las políticas de seguridad en la empresa.

5. CONCLUSIONES

El proyecto de investigación se enfocó en el diseño de un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para redes móviles en empresas públicas de telecomunicaciones en Ecuador, la investigación surgió como respuesta a la imperiosa necesidad de robustecer la protección de la información de las redes móviles en el sector de las Telecomunicaciones en el Ecuador.

La gestión de riesgos es un proceso fundamental para identificar, evaluar y mitigar los riesgos potenciales que puedan afectar la seguridad de la información en una empresa; por lo tanto, la información confidencial de los clientes, la disponibilidad de los servicios y la integridad de las redes móviles son activos críticos que deben ser protegidos de manera efectiva para garantizar la continuidad del negocio, la reputación de la organización y el cumplimiento de las regulaciones en el Ecuador.

El presente proyecto de tesis contribuye al fortalecimiento de la seguridad de la información en el sector de las telecomunicaciones en Ecuador, sentando un precedente para la

implementación de SGSI en otras empresas públicas, el SGSI propuesto permitirá generar beneficios tangibles para la empresa pública de telecomunicaciones, incluyendo una reducción de incidentes de seguridad y un aumento en la confianza de los clientes.

6. RECOMENDACIONES

A partir de las conclusiones obtenidas, se recomiendan las siguientes acciones:

Para una toma de decisiones oportuna y efectiva ante cualquier eventualidad relacionada con la gestión de riesgos en el tratamiento de información, es fundamental que el responsable del departamento de seguridad informática cuente con el respaldo de la alta gerencia, se implemente el sistema de gestión de riesgos e incluya a los líderes de los diferentes departamentos en su proceso de ejecución.

Es fundamental promover una cultura de seguridad de la información en las empresas públicas de telecomunicaciones, sensibilizando al personal sobre la importancia de proteger la información y los activos de la organización.

Para optimizar la gestión de riesgos en las empresas públicas de telecomunicaciones, se recomienda evaluar la implementación de herramientas que faciliten la administración y centralización de este proceso. Asimismo, la inversión en recursos humanos, tecnológicos y financieros es fundamental para garantizar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).

Se recomienda a las empresas públicas de telecomunicaciones en Ecuador adoptar el Modelo de SGSI propuesto en esta investigación, adaptándolo a las características y necesidades específicas de cada organización.

Es fundamental realizar revisiones y actualizaciones constantes del SGSI para responder de manera efectiva a los nuevos riesgos y amenazas que surjan en el entorno tecnológico de la empresa.

Se recomienda fomentar la colaboración entre las empresas públicas de telecomunicaciones, las entidades gubernamentales y el sector privado para compartir buenas prácticas en cuanto a seguridad de información.

7. BIBLIOGRAFÍA

- Andrade, D. (2021). *Análisis de los conceptos, elementos, técnicas de la gestión de riesgos orientado a las PYMES del sector de las telecomunicaciones.*
- Arango, O. (2023). *El ABC de la seguridad informática, guía práctica para entender la seguridad digital.*
- Baghdadi, Y. (2020). *ICT for an Inclusive World Industry 4.0—Towards the Smart Enterprise.*
- Bonilla, J. (2021). *Análisis de seguridad de la información aplicando la Metodología NIST SP 800-30 y NIST 800-115 para la empresa Textiles Jhonathex.*
- Chapoñan, W. (2023). *Ciberseguridad y su incidencia en la seguridad de la información digital de una universidad pública, 2023.*
- Duarte, D. (2020). *De 1G a 5G: Un Recorrido por la historia del internet móvil.*
- Falcón, E. (2022). *Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, para el Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil.*
- Freire, J. (2024). *Aplicación del método COBIT y el control de seguridad de la información en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda.*
- Galarza J (2024). *Plan de migración de la Norma Internacional ISO 27001:2013 a la versión 27001:2022.*
- Gamboa, E. (2022). *Enfoque de la Norma ISO/IEC 27005 para la Gestión de riesgos de seguridad operacional en la Clínica SERVIMEDIC, Bagua Grande.*
- Guaña, J. (2022). *Ataques informáticos más comunes en el mundo digitalizado.*
- Hidalgo, G. (2021). *Estudio de un modelo de seguridad de red y propuesta de mejoramiento del sistema de seguridad perimetral caso de estudio empresa AKEA S.A.*
- Huaura, M. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.*

- López, F. (2022). *Diseño del sistema de gestión de seguridad de la información – SGSI – para los procesos críticos de ofimarcas tomando como guía la norma ISO 27001:2013.*
- Mera, F. (2020). *Propuesta de gestión de la seguridad de la información basado en la norma iso 27001. caso de estudio: empresa ALTAC.*
- Montesinos, S. (2020). *Mejora Continua en una empresa en México: estudio desde el ciclo Deming.*
- Morán, N. (2021). *Estado de la ciberseguridad en las empresas del sector público del Ecuador. Una revisión sistemática.*
- Moses, F. (2023). *Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach.*
- Sánchez, L. (2020). *Gestión de la seguridad y análisis de riesgos.*
- Suércum, E. (2021). *Aplicar un esquema de seguridad de la información utilizando la norma ISO 27001 en el área de posventa en una empresa de telecomunicaciones.*
- Vilchez, J. (2020). *Ciberseguridad y robo de información: Una revisión sistemática de la literatura.*
- Zhu X, (2019). *Extension of ISO/IEC27001 to Mobile Devices Security Management.*