UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR
FACULTAD DE COMUNICACIÓN Y TICS
CARRERA: Desarrollo de Software

DISEÑO DE UNA METODOLOGÍA BASADA EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN PARA POSTERIOR IMPLEMENTACIÓN EN UNA EMPRESA PRIVADA.

Trabajo de Integración Curricular para la obtención
del Título de Ingeniero en Desarrollo de Software

Autores:
Alvarado Males Henrry David
Santillán Jumbo Anthony Sebastián

Tutor (a):
Mgtr. Flavio López

Quito, Ecuador
Febrero de 2024

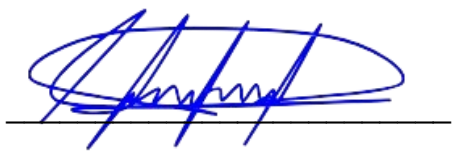
DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

1. Nosotros, **Henrry David Alvarado Males** y **Anthony Sebastián Santillán Jumbo,** declaramos en forma libre y voluntaria, que los criterios emitidos en el presente Trabajo de Integración Curricular, titulado: **"Diseño de una metodología basada en el Esquema Gubernamental de Seguridad de la Información para posterior implementación en una empresa privada",** previo a la obtención del título profesional de **Ingeniero en Desarrollo de Software**, así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de nosotros, como autores.

2. Declaramos, igualmente, tener pleno conocimiento de la obligación que tiene la Universidad Iberoamericana del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital una copia del referido Trabajo de Integración Curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública, respetando los derechos de autor.

3. Autorizamos, finalmente, a la Universidad Iberoamericana del Ecuador a difundir a través del sitio web de la Biblioteca de la UNIB.E (Repositorio Digital Institucional), el referido Trabajo de Integración Curricular, respetando las políticas de propiedad intelectual de la Universidad Iberoamericana del Ecuador.

Quito, DM., a los 21 días del mes de febrero de 2024.



Henrry David Alvarado Males

1727113159

Anthony Sebastián Santillán Jumbo

1754052718

AUTORIZACIÓN DE PRESENTACIÓN FINAL DE LA PROPUESTA DE INVESTIGACIÓN POR PARTE DEL TUTOR

PhD Alicia Elizundia
Decana de la Facultad Comunicación y Tecnologías.
Presente. -

Yo, **FLAVIO EDUARDO LÓPEZ VASCO, MAGISTER,** Tutor de la Propuesta de Investigación realizada por el estudiante **HENRRY DAVID ALVARADO MALES** Y **ANTHONY SEBASTIÁN SANTILLÁN JUMBO** de la carrera de **DESARROLLO DE SOFTWARE** informo haber revisado el presente documento titulado **DISEÑO DE UNA METODOLOGÍA BASADA EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN PARA POSTERIOR IMPLEMENTACIÓN EN UNA EMPRESA PRIVADA**, el mismo que se encuentra elaborado conforme a lo establecido en el Reglamento de Titulación y el Manual de Estilo de la Universidad Iberoamericana del Ecuador, UNIB.E de Quito, por lo tanto, autorizo la entrega de la Propuesta de Investigación a la Unidad de Titulación para la presentación final ante el tribunal evaluador.

Atentamente,
Flavio Eduardo López Vasco

Tutor

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Comunicación y Tecnologías

Carrera: Ingeniería de Software

Modalidad: Presencial

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los catorce días del mes de marzo del 2024 (14-03-2024) a las nueve horas con treinta minutos (09:30), ante el Tribunal de Presentación Oral, se presentó el señor: **ALVARADO MALES HENRRY DAVID**, titular de la cédula de ciudadanía No. **1727113159** a rendir la evaluación oral del Trabajo de Integración Curricular: " **Diseño de una metodología basada en el esquema gubernamental de seguridad de la información para posterior implementación de una empresa privada**", previo a la obtención del Título de Ingeniro de Software. Luego de la exposición, el referido estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	7.9 /10
Evaluación Oral del Trabajo de Integración Curricular	9.3 /10
Calificación Final del Trabajo de Integración Curricular	8.6 /10

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los catorce días del mes de marzo del 2024 (14-03-2024).

PhD. Jesús Gomez
VICERRECTOR

UNIVERSIDAD IBEROAMERICANA DEL ECUADOR
UNIB.E
DIRECCIÓN ACADÉMICA

PhD. Luisa Taborda
DIRECTOR ACADEMICO

Mgst. Flavio Lopez
TUTOR

UNIVERSIDAD IBEROAMERICANA DEL ECUADOR
UNIB.E
SECRETARIA DE ADMINISTRACIÓN Y REGISTRO

Mgst. Juan Pabon
LECTOR

UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Comunicación y Tecnologías

Carrera: Ingeniería de Software

Modalidad: Presencial

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los catorce días del mes de marzo del 2024 (14-03-2024) a las nueve horas con treinta minutos (09:30), ante el Tribunal de Presentación Oral, se presentó el señor: **SANTILLAN JUMBO ANTHONY SEBASTIAN**, titular de la cédula de ciudadanía No. **1754052718** a rendir la evaluación oral del Trabajo de Integración Curricular: " **Diseño de una metodología basada en el esquema gubernamental de seguridad de la información para posterior implementación de una empresa privada**", previo a la obtención del Título de Ingeniro de Software. Luego de la exposición, el referido estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	7.9 /10
Evaluación Oral del Trabajo de Integración Curricular	9.6 /10
Calificación Final del Trabajo de Integración Curricular	8.8 /10

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los catorce días del mes de marzo del 2024 (14-03-2024).

UNIB.E DIRECCIÓN ACADEMICA

PhD. Jesús Gómez
VICERRECTOR

PhD. Luisa Taborda
DIRECTOR ACADEMICO

UNIB.E SECRETARÍA DE ADMINISTRACIÓN Y REGISTRO

Mgst. Flavio Lopez
TUTOR

Mgst. Juan Pabon
LECTOR

Campus Colón : 9 de Octubre N25-12 y Av. Colón, Quito 170522.
Campus Norte : José Queri y Av. Eloy Alfaro, Quito 170513
www.unibe.edu.ec

ÍNDICE GENERAL

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

Henrry David Alvarado Males y Anthony Sebastián Santillán Jumbo. Diseño de una metodología basada en el Esquema Gubernamental de Seguridad de la Información para posterior implementación en una empresa privada. Carera Ingeniería de desarrollo de software. Universidad Iberoamericana del Ecuador. Quito Ecuador. 2024. (**98**) pp.

RESUMEN

Este estudio propone el diseño de una metodología para la implementación efectiva del Esquema Gubernamental de Seguridad de la Información, EGSI, en una empresa privada. El objetivo central es establecer un marco sólido que garantice la integridad, confidencialidad y disponibilidad de la información, adaptando las mejores prácticas gubernamentales a las necesidades específicas del entorno empresarial. La metodología abarca un análisis exhaustivo del entorno y activos de información de la empresa, seguido por la adaptación de los principios del EGSI para diseñar políticas y controles específicos orientados a los riesgos de información en el sector privado. Se subraya la importancia de la concienciación y capacitación del personal, considerándolos elementos esenciales en la implementación exitosa. Además, se proponen mecanismos de monitoreo continuo y evaluación para asegurar la eficacia a lo largo del tiempo. La aplicación de esta metodología pretende proporcionar a la empresa una estructura de seguridad de la información robusta, fortaleciendo su resiliencia ante amenazas tanto internas como externas. La adaptación del EGSI para el ámbito privado representa una innovación estratégica, aprovechando las mejores prácticas ya establecidas en el sector público y adaptándolas de manera inteligente para abordar los desafíos particulares del sector empresarial.

Palabras clave: Seguridad, Metodología, Amenazas, Estrategias, Integridad

ABSTRACT

This study proposes the design of a methodology for the effective implementation of the Government Information Security Scheme in a private company. The central objective is to establish a solid framework that guarantees the integrity, confidentiality and availability of information, adapting the best governmental practices to the specific needs of the business environment. The methodology encompasses a thorough analysis of the company's information environment and assets, followed by the adaptation of the principles of the Governmental Scheme to design specific policies and controls oriented to the risks of the private sector. The importance of staff awareness and training is emphasized as essential elements in successful implementation. In addition, continuous monitoring and evaluation mechanisms are proposed to ensure effectiveness over time. The application of this methodology aims to provide the company with a robust information security structure, strengthening its resilience to both internal and external threats. The adaptation of the Government Information Security Scheme for the private sector represents a strategic innovation, taking advantage of best practices already established in the public sector and adapting them intelligently to address the particular challenges of the business sector.

Keywords: Security, Methodology, Threats, Strategies, Integrity

INTRODUCCIÓN

En un mundo cada vez más interconectado y dependiente de la tecnología, la seguridad de la información se ha convertido en un pilar fundamental para la supervivencia y prosperidad de las organizaciones. La creciente sofisticación de las amenazas cibernéticas y la constante evolución de los entornos empresariales exigen enfoques innovadores y sólidos para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

En este contexto, la presente tesis se sumerge en el desafiante terreno de la seguridad de la información en el ámbito empresarial, proponiendo una metodología diseñada para la implementación del Esquema Gubernamental de Seguridad de la Información. Esta iniciativa no solo busca establecer un marco robusto para la protección de los activos de información, sino que también pretende adaptar las mejores prácticas gubernamentales a la realidad y dinámicas propias de una empresa privada.

La adopción del Esquema Gubernamental de Seguridad de la Información en entidades gubernamentales ha demostrado ser exitosa en la gestión de riesgos y la promoción de una cultura de seguridad. Sin embargo, trasladar este enfoque al sector privado implica enfrentarse a desafíos particulares, como la variabilidad en la naturaleza de los datos manejados, los modelos de negocio específicos y las diferentes amenazas a las que se enfrentan.

El Esquema Gubernamental de Seguridad de la Información implica la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001. Esto implica identificar los activos de información críticos, evaluar y gestionar los riesgos, implementar controles de seguridad adecuados, capacitar al personal, gestionar incidentes y realizar auditorías periódicas.

La ISO/IEC 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) en una organización. La implementación de esta norma ayuda a las empresas a proteger la confidencialidad, integridad y disponibilidad de la información que manejan, asegurando su correcto

manejo y reduciendo los riesgos de seguridad. (Mes De La Concientización De La Ciberseguridad, 2022)

La norma ISO 27001 también permite regular, gestionar y mitigar al máximo los riesgos a los que se encuentran expuestos los activos de una empresa; tales como pérdida de información, disponibilidad de servicios entre otros.

De acuerdo con el documento "Análisis del reporte de avances de la implementación Esquema Gubernamental de Seguridad de la Información (EGSI Versión 2.0)" (Ver anexos 1 y 2), se presentan diversos puntos sobre la implementación, seguimiento y control de la EGSI. Este proceso se divide en dos etapas, las cuales se detallan en el anexo número 1 del documento. El objetivo de la EGSI es vigilar la correcta gestión de la seguridad de la información en las instituciones gubernamentales y promover la responsabilidad y el cuidado de los recursos tecnológicos. La implementación de la EGSI puede ser monitoreada mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas similares.

Si una empresa no ha aplicado la norma de seguridad ISO 27001, puede enfrentar diversos riesgos y problemas de seguridad de la información. Algunos de los posibles impactos negativos que puede sufrir una empresa son: vulnerabilidades de seguridad, pérdida de confianza del cliente, multas y sanciones, pérdida financiera y pérdida de productividad. Por lo tanto, es importante que las empresas implementen la norma de seguridad ISO 27001 para minimizar los riesgos de seguridad y mejorar la confianza de los clientes. (López, 2022)

En última instancia, la aplicación exitosa de esta metodología no solo fortalecerá la postura de seguridad de la empresa en cuestión, sino que también contribuirá al crecimiento de un cuerpo de conocimientos que pueda beneficiar a otras organizaciones enfrentadas a desafíos similares en la preservación de la integridad y confiabilidad de su información. A continuación, se muestra la descripción general de cada uno de los capítulos que conforman el trabajo.

El primer capítulo tiene los siguientes contenidos: planteamiento del problema, objetivos de la investigación, justificación e impacto de la investigación y alcance de la investigación.

En el segundo capítulo se exponen los antecedentes de la investigación en las cuales se presentan documentos relacionados con el problema de la presente investigación. También se presentan las bases teóricas, las cuales permiten conocer los conceptos de temas relacionados con la seguridad de la información y finalmente los fundamentos legales, donde se detallan las leyes o reglamentos que serán tomados en cuenta en el diseño de la metodología.

En el tercer capítulo se especifica la metodología, tipo, nivel y diseño de la investigación, en el contexto en el que se describe la población que se utilizó, así como la técnica de recolección de datos y el instrumento empleado en la misma.

En el cuarto capítulo se presenta la propuesta de la metodología, en el cual se detalla cómo está estructurada, el análisis y diseño del mismo. Culminando, con el detalle de los resultados obtenidos del plan piloto aplicado a la empresa Toc Systems

En el quinto capítulo se indica las conclusiones y recomendaciones que surgieron a lo largo del presente trabajo de investigación y durante el diseño de la metodología que servirán como referencia para futuros proyectos que abarquen temáticas similares.

CAPÍTULO I

EL PROBLEMA

El presente capítulo tiene la finalidad de desarrollar los siguientes apartados: planteamiento del problema, interrogante de la investigación, los objetivos, la justificación e impacto de la investigación y el alcance de la investigación.

Planteamiento del problema

En la era digital, donde la información se erige como uno de los activos más valiosos para las empresas, la seguridad de la información se convierte en un requisito indispensable. Sin embargo, a pesar de los avances en las estrategias de seguridad, muchas empresas privadas enfrentan desafíos significativos al intentar establecer y mantener un entorno seguro para sus datos críticos.

El panorama actual de amenazas cibernéticas, caracterizado por su complejidad y constante evolución, plantea un riesgo latente para la integridad, confidencialidad y disponibilidad de la información empresarial. La magnitud de estas amenazas se ve agravada por la falta de un marco de seguridad de la información estandarizado y adaptado a las particularidades del sector privado.

La creciente complejidad del panorama de amenazas cibernéticas ha llevado a un aumento alarmante en la vulnerabilidad de las empresas frente a ataques sofisticados. Como ilustración de esta realidad, Felipe Gómez, director regional de Fluid Attacks, dice que en el 2022 Ecuador tuvo 84 intentos de infección por virus cada minuto. Es el cuarto país en el ranking de un estudio, donde Brasil ocupa el primero, le sigue México y Perú.

La carencia de un marco de seguridad de la información adaptado específicamente a las particularidades del sector privado constituye un desafío sustancial. En este escenario, surge la pregunta esencial: ¿Cómo puede una metodología basada en el Esquema Gubernamental de Seguridad de la Información de Ecuador facilitar una efectiva gestión del riesgo en las empresas privadas y proporcionar beneficios significativos?

La importancia de esta investigación se destaca aún más al considerar las experiencias y lecciones aprendidas en otros sectores. Experiencias previas en la implementación del EGSI en entidades gubernamentales han demostrado su eficacia en la gestión de riesgos y protección de activos críticos de información. Sin embargo, la aplicación directa de estas prácticas al sector privado requiere un análisis cuidadoso de las diferencias contextuales y operativas.

Objetivo general

Diseñar una metodología basada en el Esquema Gubernamental de Seguridad de la Información para su posterior implementación en empresas privadas.

Objetivos específicos

- Realizar un análisis bibliográfico sobre el contenido del Esquema Gubernamental de Seguridad de la Información (EGSI) vigente en Ecuador.
- Analizar las prácticas exitosas de implementación del Esquema Gubernamental de Seguridad de la Información en Ecuador y otras jurisdicciones, identificando aspectos transferibles al ámbito empresarial.
- Evaluar las necesidades de seguridad de la información en empresas privadas, considerando la naturaleza de los datos, modelos de negocio y amenazas cibernéticas, desde la adaptación de la metodología basada en el EGSI
- Desarrollar un marco metodológico detallado que incorpore principios del Esquema Gubernamental de Seguridad de la Información, ajustados a las características de las empresas privadas.

Justificación e impacto de la investigación

El Esquema Gubernamental de Seguridad de la Información (EGSI) es una iniciativa desarrollada por el Gobierno del Ecuador con el objetivo de establecer políticas, estándares y lineamientos para garantizar la seguridad de la información en las entidades públicas o privadas. Su propósito es proteger la confidencialidad, integridad y disponibilidad de los datos manejados por las organizaciones, así como promover buenas prácticas en materia de seguridad de la información. (EGSI, 2020)

Dentro del Esquema Gubernamental de Seguridad de la Información se contempla la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual es un marco de trabajo que permite a las organizaciones establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la seguridad de la información. El SGSI se basa en la norma internacional ISO/IEC 27001, proporcionando los requisitos y directrices para establecer un sistema de gestión de seguridad de la información efectivo, asegurando la confidencialidad, integridad y disponibilidad de la información, así como gestionar los riesgos de seguridad de manera sistemática. (SGSI, 2023)

La presente investigación pretende prevenir los problemas que puedan darse en las empresas privadas, ayudando así a reducir los riesgos existentes y a proponer una serie de controles para resguardar los activos de información y asegurar la información que las empresas considera importante, reduciendo las vulnerabilidades y amenazas que acechan a los activos de información los cuales apoyan al cumplimiento de los objetivos del negocio.

Dentro de las empresas es muy importante adoptar una metodología en base al Esquema Gubernamental de Seguridad de la Información que proporcione un marco estructurado y basado en mejores prácticas para la gestión y protección de la información, con la finalidad de dar cumplimiento al EGSI ecuatoriano este trabajo propone el diseño de una metodología de gestión de riesgos, misma que al implementarse permite la adecuada administración de los mismos.

La relevancia social de esta investigación se manifiesta en su contribución a la seguridad de la información en el ámbito empresarial, impactando directamente en la

protección de los datos sensibles de las empresas privadas. Al diseñar una metodología basada en el EGSI, se busca no solo cumplir con los estándares nacionales, sino también elevar los niveles de conciencia y preparación ante las crecientes amenazas cibernéticas. La implementación exitosa de esta metodología en empresas privadas no solo resguardará la información crítica para el funcionamiento de las organizaciones, sino que también contribuirá a la creación de un entorno empresarial más seguro, fortaleciendo la confianza de los stakeholders y promoviendo una cultura de seguridad informática.

Por otro lado, este proyecto tendrá un aporte académico, ya que esta investigación contribuye al cuerpo de conocimientos en el campo de la seguridad de la información y la gestión de riesgos. Al proponer una metodología específica basada en el EGSI, se añade una perspectiva única a la literatura existente, ofreciendo un enfoque práctico y adaptado al entorno empresarial. Además, al integrar los principios del SGSI basado en la norma ISO/IEC 27001, se establece un puente entre las mejores prácticas internacionales y la realidad empresarial local, enriqueciendo el entendimiento y la aplicabilidad de estos estándares en un contexto específico.

Así mismo, en el ámbito metodológico, esta investigación propone una metodología específica para la gestión de riesgos en empresas privadas, consolidando las mejores prácticas del EGSI y del SGSI. Este enfoque metodológico no solo proporciona un marco estructurado para la implementación práctica en el entorno empresarial, sino que también sirve como modelo para futuras investigaciones y aplicaciones en el ámbito de la seguridad de la información. Al abordar la gestión de riesgos de manera sistemática, se establece un precedente metodológico que puede ser adoptado y replicado en diversas organizaciones, contribuyendo a la evolución y mejora continua de las prácticas de seguridad de la información a nivel empresarial.

Alcance de la investigación

El presente trabajo tiene como objetivo principal la propuesta de una metodología de gestión de riesgos de la información adaptada a las especificaciones del EGSI ecuatoriano, con la finalidad de su eventual implementación en el entorno de una empresa privada. Para ello, se llevará a cabo un análisis exhaustivo y un diseño detallado de ciertos aspectos clave del EGSI, concentrándose en aquellos principios y lineamientos que se consideren más pertinentes y desafiantes para la implementación en el entorno empresarial.

La metodología de gestión de riesgos de la información se propone llevar a cabo un plan piloto dentro de la empresa TOC Systems, donde se aplicará y evaluará la metodología diseñada. Es importante resaltar que el EGSI, en el cual se basa esta metodología, está directamente vinculado con la norma ISO 27001:2013, estableciendo así un marco sólido y reconocido internacionalmente para la gestión de la seguridad de la información. Este enfoque metodológico busca contribuir al fortalecimiento de los mecanismos de seguridad de la información en entornos empresariales.

La investigación tiene como población objetivo a los encargados de la seguridad de la información en la empresa. Su propósito se limita a evaluar únicamente el conocimiento, cumplimiento e implementación del EGSI en la empresa. El proyecto antes descrito será desarrollado durante el período académico octubre-febrero del 2023.

CAPÍTULO II

MARCO TEÓRICO

Según Rodríguez, G. (2019) El marco teórico se conforma a partir de una revisión exhaustiva de la literatura existente, donde se recopilan y sintetizan las ideas, posturas de distintos autores, conceptos y definiciones relevantes que fundamentan y orientan la investigación que se llevará a cabo" (pág. 72). Esto sirve como referencia para el desarrollo del presente capítulo el cual se estructura por antecedentes de la investigación, bases teóricas y referentes legales como se desarrolla a continuación.

Estudio del arte

El estudio del arte realizado para el diseño de la metodología de seguridad de la información se llevó a cabo con un enfoque minucioso y detallado, con especial atención en las prácticas de protección de datos en el contexto de las empresas de software. La revisión exhaustiva abordó diversos aspectos fundamentales, comenzando con una comprensión profunda de los conceptos esenciales de seguridad de la información, como la confidencialidad, integridad, disponibilidad y autenticación.

Uno de los pilares fundamentales del estudio fue el análisis detallado del EGSI y su vinculación con la normativa ISO 27001:2013. Se profundizó en la estructura, objetivos y principios del EGSI, y se identificó cómo se basa en la norma ISO 27001:2013, la cual establece un marco de referencia ampliamente reconocido para la gestión de la seguridad de la información.

La investigación también involucró un análisis exhaustivo de metodologías y buenas prácticas en seguridad de la información, donde se identificaron las mejores prácticas en el diseño y aplicación de controles de seguridad, así como en la gestión de riesgos y vulnerabilidades en el entorno de empresas de software.

Además de revisar la teoría y los enfoques conceptuales, se indagó sobre casos de éxito y experiencias de otras empresas de software que han implementado metodologías de seguridad efectivas. Se extrajeron lecciones valiosas de estos casos, lo que permitió identificar enfoques exitosos y prácticas recomendadas que podrían ser aplicables y adaptadas al contexto específico de las empresas privadas.

Finalmente, el estudio del arte proporcionó una base sólida y completa de conocimientos, integrando el enfoque del EGSI basado en la norma ISO 27001:2013, junto con las mejores prácticas y experiencias exitosas en la industria de empresas de software. Esta revisión en profundidad, sentó las bases para el diseño de una metodología de seguridad de la información altamente efectiva y adaptada específicamente a las necesidades y características de las empresas privadas.

Antecedentes de la investigación

Para comprender los antecedentes de la investigación se tomará en cuenta lo que menciona García (2021) en torno a ellos:

> (…) Los antecedentes de investigación se refieren a los estudios previamente realizados que se encuentran dentro de la misma línea investigativa o en un nivel investigativo similar. Según García (2021), estos estudios se ubican en la intersección entre la línea de investigación y el nivel investigativo, lo que representa el punto donde se desarrolla el estudio" (pág. 45).

En consecuencia, a continuación, se desarrollan estudios previos los cuales han resultado ser de gran relevancia.

Como primer estudio se tomó como referencia al trabajo de Martínez y Gómez (2023), titulado "Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 en una empresa del sector financiero utilizando herramientas de ciberseguridad avanzadas". Este estudio se centra en minimizar los riesgos de seguridad de la información mediante el análisis detallado para la implementación de la norma ISO 27001, combinando herramientas avanzadas de ciberseguridad. El objetivo es fortalecer el sistema de gestión de control para el área de tecnología de información, empleando un enfoque cualitativo que involucra métodos como la observación y la entrevista, similar al enfoque utilizado en el estudio previamente mencionado.

Partiendo del trabajo de titulación, se pueden identificar riesgos que podrían afectar a 18 procesos críticos de la empresa, lo que se relaciona con el proyecto que busca desarrollar una metodología basada en el EGSI, donde la implementación se orienta como un SGSI con la norma ISO 27001:2013.

Como segundo estudio se seleccionó la tesis elaborada por López (2020), en la ciudad de Ambato titulado, “Implementación de una Metodología para Gestión de

Riesgos de Información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre", estableciendo como objetivo Implementar una metodología de gestión de riesgos de información basada en ISO 27001 y 27002 para reducir los niveles de vulnerabilidad en los activos de información del ITS Sucre. En cuanto a la metodología de la investigación se observó que se utilizó un cuestionario estructurado en tres partes denominados logros: a) marco de seguridad, b) implementación del plan de seguridad y c) monitoreo y mejoramiento continuo. La exploración de estos tres logros contemplo porcentajes diferenciados, en el primero se asumió el 30%, en segundo el 40% y finalmente en el tercero el 30%, haciendo un total del 100%. Los resultados obtenidos muestran: que el Marco de Seguridad obtuvo un 19,2% sobre 30%; la Implementación del Plan de Seguridad mantuvo valores de 8,2% sobre el 40%, y 11,3% sobre 30% en los Procesos de Monitoreo y Mejora Continua; totalizando un valor de 38%, lo cual refleja una subida en el valor ponderado de la seguridad de la información del 25% respecto al resultado obtenido en el diagnóstico inicial.

Tomando en cuenta la tesis mencionada anteriormente, se destaca la importancia de desarrollo de una Metodología de Gestión de Riesgos de Seguridad de la Información, de acuerdo con las normas internacionales ISO/IEC 27001 y 27002; y su alineación con el Proceso de Gestión de Riesgos de Seguridad de la Información especificado en la norma ISO/IEC 27005. Además, se relaciona con el producto de este proyecto de investigación, en el cual es el diseño de una metodología basada en EGSI, y sirve como precedente guía para el correcto diseño.

Bases teóricas

Según Hernández (2020) las bases teóricas "constituyen un desarrollo detallado de los conceptos fundamentales y las proposiciones que respaldan el enfoque adoptado para explicar o fundamentar el problema de investigación" (pág. 82). Lo que da una clara percepción de la importancia de este apartado en el desarrollo del presente proyecto de investigación, debido a que sustentan el tema de estudio desde el punto de vista científico.

Seguridad de la información

La seguridad de la información es una práctica que consiste en identificar y proteger la información confidencial, y garantizar que los datos sean seguros a lo largo de su ciclo de vida. Esta es una parte importante para que las empresas realicen sus operaciones, porque los datos administrados son muy importantes para las actividades que desarrollaron. De la manera mayoritaria, los sistemas organizacionales se basan en una nueva tecnología, la seguridad no puede confundirse con la información y la seguridad informática, a pesar de que están estrechamente relacionados, no el mismo concepto. (*S*eguridad De La Información, 2020)

Seguridad de la información vs. Seguridad informática

Mientras la seguridad informática implica la protección de la infraestructura que soporta el negocio; la seguridad de la información es la protección de la información de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar las oportunidades. (Norma ISO/IEC, 2021)

Identificación de los activos del sistema

Los activos son aquellos elementos relacionados con el entorno, como son el personal, los edificios, las instalaciones, los equipos, o los suministros; los relacionados con los sistemas de TIC (Tecnologías de la información y la Comunicación), como los equipos de hardware, el software, los componentes de comunicaciones de datos; los relacionados con la información, los relacionados con las funcionalidades de la organización, como la capacidad de proporcionar un servicio, crear un producto. (Martínez, 2021)

Importancia de la seguridad de la información para las organizaciones

La Seguridad de la Información se refiere a la protección de los datos que personas y empresas manejan diariamente y a la práctica que asegura que la información sensible sólo puede ser accedida por sus dueños; es un gran aliado para las empresas, ya que se encarga de evitar que cualquier persona distribuya indebidamente datos sobre ventas, márgenes de ganancia, competencia, entre otros; también es importante para los usuarios de dispositivos tecnológicos y que tienen

acceso a la internet, para que nadie que pueda tener acceso a fotos, vídeos, información personal. (Grupo STT, 2021)

La seguridad de la información se engrana a partir de 3 elementos esenciales: Las personas, la tecnología y los procesos. (Ver Figura 1)

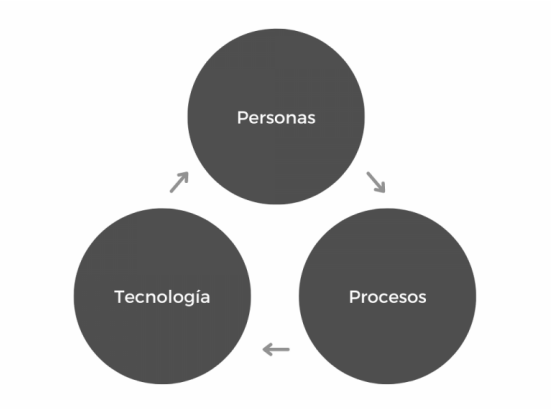


Figura 1: *Elementos esenciales de la seguridad de la información*

Fuente: *Elaboración Propia*

- Las personas: son todos y cada uno de los miembros de la organización; desde la alta gerencia hasta los cargos operativos y de apoyo. Las personas suelen ser el eslabón más débil en la cadena de riesgos e incidentes.
- La tecnología: comprende las diferentes herramientas y programas que contribuyen a minimizar los riesgos como son los antivirus.
- Los procesos: son todos los mecanismos, sistemas y estrategias encaminadas a preservar la seguridad de la información lo cual contempla la normatividad vigente como la ISO/IEC.

Definición de un sistema de gestión de la seguridad de la información (SGSI)

Un SGSI consiste en políticas, procedimientos y directrices junto a recursos y actividades asociados administrados colectivamente por una organización para proteger sus activos de información esenciales. De acuerdo al estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio. (SGSI, 2023)

Beneficios de un SGSI

Los principales beneficios que obtiene una empresa al implantar un sistema SGSI para la seguridad de sus datos son:

- Reducción de riesgos: Se identifican encuestas y amenazas para reducir significativamente el número de amenazas mediante el monitoreo de controles, protocolos, políticas y procesos: Si se produce un incidente relacionado con los datos, el negocio se preparará de inmediato para minimizar su impacto.
- Reducción de costos. El uso razonable de los recursos ahorra seguridad.
- Integración de la seguridad en el negocio: Este sistema requiere un cambio en la participación y mentalidad de todas las empresas y se convierte en uno de los componentes más importantes en cualquier proceso o actividades comerciales.
- Cumplimiento de la normativa vigente en seguridad. Las leyes nacionales e internacionales para el tratamiento y protección de datos estarán cubiertas garantizando que se cumplen en todos los niveles o áreas de la empresa.
- Incremento de la competitividad: Con este sistema, puede usar autenticación de la seguridad ISO autorizada, que es un factor diferenciador en la competencia. (AMBIT - BST, 2021)

Amenazas y vulnerabilidades en la seguridad de la información

La seguridad de la información enfrenta diversas amenazas y vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. Algunas de las principales amenazas y vulnerabilidades en este ámbito incluyen:

- **Ciberataques:** Los ciberataques son una de las mayores amenazas para la seguridad de la información. Esto incluye ataques como el malware, ransomware, phishing, ataques de denegación de servicio, entre otros. Los atacantes buscan acceder, dañar o robar información sensible. (Smith, 2021)
- **Ingeniería social**: La ingeniería social se refiere a técnicas mediante las cuales los atacantes manipulan a las personas para obtener acceso a información confidencial. Esto puede incluir el engaño a través de correos electrónicos, llamadas telefónicas o mensajes falsos, con el fin de obtener contraseñas, datos personales o información confidencial. (Johnson & Patel ,2020)

- **Fallos en la seguridad física:** La seguridad física inadecuada de los equipos y los centros de datos puede permitir el acceso no autorizado a la información. Esto incluye el acceso físico a servidores, dispositivos de almacenamiento o redes sin las debidas medidas de protección. (Wang & Li 2021)
- **Brechas en la seguridad de la red**: Las redes y los sistemas de comunicación pueden estar expuestos a vulnerabilidades que permiten a los atacantes interceptar o manipular la información transmitida. Esto puede ocurrir si las conexiones no están debidamente protegidas o si se utilizan protocolos débiles. (Chen & Kim, 2020)
- **Mal uso interno:** Las amenazas a la seguridad de la información también pueden originarse dentro de la organización. El acceso no autorizado o el mal uso de los privilegios de los empleados pueden comprometer la seguridad de la información y poner en riesgo los datos sensibles. (Kumar, 2021)
- **Robo o pérdida de dispositivos:** El robo o la pérdida de dispositivos móviles, como laptops, smartphones o unidades de almacenamiento, pueden exponer información confidencial si no se toman las medidas adecuadas de cifrado o protección de datos. (García, 2020)
- **Falta de conciencia y capacitación:** La falta de conciencia y capacitación en seguridad de la información puede ser una vulnerabilidad significativa. Los empleados pueden no estar al tanto de las mejores prácticas de seguridad, como el uso de contraseñas seguras, la protección contra el phishing o la actualización regular de software, lo que puede dejar abiertas puertas para posibles ataques. (Johnson, 2020)

Esquema gubernamental de seguridad de la información

Descripción

El Esquema Gubernamental de Seguridad de la Información (EGSI) es un marco de referencia que el gobierno utiliza para establecer políticas, procedimientos y estándares de seguridad de la información en sus instituciones y organismos públicos. El objetivo principal del EGSI es proteger la confidencialidad, integridad y disponibilidad de la información manejada por el gobierno del Ecuador, así como los sistemas y recursos asociados. (EGSI, 2023)

Objetivos

1. **Eficiencia y eficacia administrativa:** El esquema gubernamental busca mejorar la eficiencia y eficacia en la administración del gobierno del Ecuador, optimizando los procesos y recursos para brindar servicios públicos de calidad de manera oportuna y efectiva. (EGSI, 2023)
2. **Transparencia y rendición de cuentas:** Se busca promover la transparencia en la gestión gubernamental y fortalecer la rendición de cuentas. Esto implica proporcionar acceso a la información pública, permitir la participación ciudadana y garantizar que los funcionarios públicos rindan cuentas por sus acciones. (EGSI, 2023)
3. **Desarrollo económico y social:** El esquema gubernamental tiene como objetivo promover el desarrollo económico y social del país. Esto implica implementar políticas y programas que fomenten la inversión, generen empleo, impulsen el crecimiento económico sostenible y mejoren las condiciones de vida de la población. (EGSI, 2023)
4. **Justicia social e inclusión:** El gobierno del Ecuador busca garantizar la igualdad de oportunidades y la justicia social, promoviendo la inclusión de los grupos vulnerables y reduciendo las brechas sociales. Se busca brindar acceso equitativo a los servicios básicos, como salud, educación, vivienda y empleo. (EGSI, 2023)
5. **Seguridad ciudadana:** El esquema gubernamental busca garantizar la seguridad ciudadana, promoviendo la prevención del delito, la protección de los derechos humanos y el fortalecimiento de las instituciones encargadas de la seguridad pública. (EGSI, 2023)
6. **Protección del medio ambiente:** El gobierno del Ecuador busca promover el desarrollo sostenible y la protección del medio ambiente. Esto implica implementar políticas y acciones para la conservación de los recursos naturales, la mitigación del cambio climático y la promoción de prácticas de desarrollo sustentable. (EGSI, 2023)

Beneficios de un esquema gubernamental del Ecuador

La implementación de un esquema gubernamental eficiente y efectivo en Ecuador puede proporcionar varios beneficios para el país. A continuación, se presenta algunos de los beneficios del Esquema Gubernamental de Seguridad de la Información (EGSI):

- “Identificación, gestión y tratamiento de riesgos altos para la compañía: el EGSI permite identificar los riesgos de seguridad de la información y establecer medidas para su gestión y tratamiento” (EGSI | Cascante, 2020)
- “Implantación de controles de seguridad: el EGSI establece controles de seguridad para proteger la información de la empresa” (Esquema De Seguridad De La Información De Ecuador | GSS, 2022)
- “Establecimiento de un marco de gestión eficaz: el EGSI establece un marco de gestión eficaz para la seguridad de la información” (Esquema De Seguridad De La Información De Ecuador | GSS, 2022)
- “Protección de la información de la empresa: el EGSI protege la información de la empresa de posibles amenazas y riesgos” (Esquema De Seguridad De La Información De Ecuador | GSS, 2022)
- “Cumplimiento de normas técnicas y estándares internacionales: el EGSI cumple con las normas técnicas y estándares internacionales para la seguridad de la información” (Esquema De Seguridad De La Información De Ecuador | GSS, 2022
- “Reducción de los riesgos de seguridad de la información: el EGSI reduce los riesgos de seguridad de la información de la empresa” (Esquema De Seguridad De La Información De Ecuador | GSS, 2022)
- “Mejora de la confidencialidad, integridad y disponibilidad de la información: el EGSI mejora la confidencialidad, integridad y disponibilidad de la información de la empresa” (EGSI | Cascante, 2020)
- “Aseguramiento de la continuidad del negocio: el EGSI asegura la continuidad del negocio de la empresa ante posibles incidentes de seguridad de la información” (EGSI del Ecuador | GSS, 2022)

- “Fortalecimiento de la seguridad de la información en el sector público: el EGSI fortalece la seguridad de la información en el sector público” (EGSI | Cascante, 2020)
- “Mejora de la eficiencia y eficacia en la gestión de la información: el EGSI mejora la eficiencia y eficacia en la gestión de la información de la empresa” (Cuervo, 2021)

Componentes y requisitos del EGSI

El Esquema Gubernamental de Seguridad de la Información (EGSI) en Ecuador es un marco normativo que establece los lineamientos, políticas y procedimientos para garantizar la seguridad de la información en las entidades gubernamentales. Algunos de los componentes y requisitos clave del EGSI en Ecuador se muestran en la Figura 2. (EGSI | Cascante,2020)

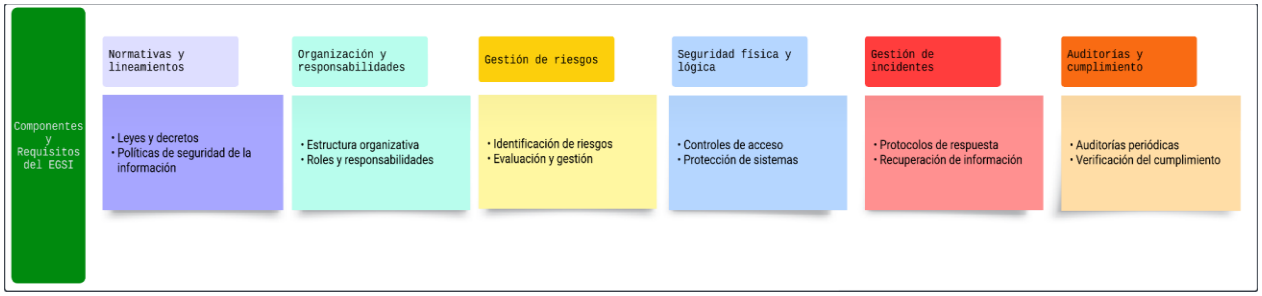


Figura 2: *Listado de Componente y Requisitos*

Fuente: *Elaboración Propia*

Aplicación del EGSI en organizaciones públicas o privadas

El EGSI tiene aplicabilidad tanto en organizaciones públicas como en organizaciones privadas, aunque pueden existir variaciones en los requisitos específicos dependiendo del sector y las regulaciones correspondientes. A continuación, se detallan las formas en que el EGSI se implementa en cada tipo de organización:

1. Políticas y seguridad de la información:

- Políticas y normativas: Las instituciones gubernamentales tienen la obligación de desarrollar políticas y normativas que supervisen y controlen la seguridad de la información, siguiendo las directrices establecidas por el EGSI. Estas políticas pueden abarcar diversos aspectos, como la categorización de la información, el control de acceso y seguridad, la gestión de riesgos y la salvaguardia de datos personales. (Martínez, 2021)
- Cumplimiento normativo: Es responsabilidad de las entidades del sector público asegurar el cumplimiento de las leyes y regulaciones específicas relacionadas con la seguridad de la información y la privacidad. Esto implica la implementación de controles y medidas de seguridad adecuadas para salvaguardar la información confidencial y garantizar la confidencialidad, integridad y disponibilidad de los datos. (López, 2020)
- Auditorías y cumplimiento: Las instituciones gubernamentales son objeto de auditorías y evaluaciones regulares para verificar el cumplimiento de las políticas y los controles de seguridad de la información. Estas auditorías pueden ser realizadas tanto por equipos de auditoría interna como por entidades externas independientes. (Pérez, 2020)

2. Aplicación en organizaciones privadas:

- Adaptación al marco normativo: Las empresas privadas tienen la opción de adoptar y adaptar el EGSI en función de las regulaciones y leyes aplicables a su sector. Esto implica la implementación de políticas y controles de seguridad de la información que estén alineados con las mejores prácticas y estándares reconocidos. (Gómez, 2021)
- Gestión de riesgos: Las empresas privadas tienen la responsabilidad de llevar a cabo evaluaciones de riesgos para identificar y evaluar los posibles riesgos de seguridad de la información a los que se enfrentan. Con base en dicha evaluación, deben implementar controles y medidas de seguridad adecuadas para mitigar los riesgos identificados. (Díaz, 2020)
- Protección de datos personales: En varias jurisdicciones, las empresas privadas también están sometidas a regulaciones de protección de datos personales. Por consiguiente, es necesario que establezcan medidas de

seguridad adecuadas para salvaguardar la confidencialidad y privacidad de la información personal que gestionan. (Sánchez, 2019)

ISO/IEC 27001

El estándar internacional ISO/IEC 27001, aprobado y publicado conjuntamente por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) en octubre de 2005, establece los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) siguiendo el ciclo PDCA (Ver anexo 3) (Planificar, Hacer, Verificar, Actuar). (ISO/IEC 27001, 2023)

ISO 27001 es una norma que asegura la confidencialidad, integridad y disponibilidad de los datos, la información y los sistemas que los procesan. Su aplicación permite a las organizaciones evaluar y gestionar los riesgos, implementando los controles necesarios para mitigarlos o eliminarlos, lo que mejora su competitividad y su imagen. La norma ISO 27001:2013 se complementa con las buenas prácticas y controles establecidos en la norma ISO 27002. (ISO 27001 - Software ISO 27001 De Sistemas De Gestión, 2022)

Objetivos de la seguridad

Entre los objetivos de la seguridad se tiene:

- **Disponibilidad y accesibilidad de los sistemas y datos**: “Solo para uso autorizado, es un requisito necesario que garantiza que el sistema trabaja puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado.” (Martínez, 2021)
- **Integridad**: “Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados mientras se almacena, procesan o transmiten así evitando la pérdida de consistencia.” (Martínez, 2021)
- **Confidencialidad de datos**: “Es el requisito que intenta que la información privada o secreta no se rebele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito.” (Martínez, 2021)

Elementos de gestión de la seguridad de los sistemas de información

Los elementos involucrados en la seguridad de los sistemas de información lo podemos ver en la Tabla 1.

Tabla 1: *Elementos de gestión*

Elementos	Descripción
Identificación de todos los activos	Proceso de identificar y listar todos los activos de información de una organización, incluyendo sistemas, datos, infraestructuras y recursos
Identificación de amenazas a los activos	Identificación y documentación de las posibles fuentes de riesgo o amenazas que podrían comprometer la seguridad de los activos de información.
Identificación de vulnerabilidades	Identificación de debilidades o fallos en los activos de información que podrían ser explotados por amenazas, poniendo en riesgo su seguridad.
Identificación de impactos	Evaluación de los posibles efectos negativos que podrían surgir si una amenaza explota una vulnerabilidad en un activo de información.
Identificación de riesgos	Proceso de combinar la información sobre amenazas, vulnerabilidades e impactos para evaluar y priorizar los riesgos a los activos de información.
Aplicación de controles	Implementación de medidas y controles de seguridad para mitigar o eliminar los riesgos identificados y proteger los activos de información.

Fuente: *Elaboración Propia*

Aplicación de controles y su descripción

Para tratar los riesgos de seguridad de la información, existe un grupo de controles que en base a los resultados del análisis de riesgos deben ser implementados en función de su aplicabilidad para la organización, dichos controles se encuentran descritos en el Edición Especial Nº 228 – Registro Oficial, sin embargo, el detalle de cada uno de estos se profundiza en la ISO/IEC 27001: 2013. (Gobierno Electrónico, 2020)

A continuación, la descripción de cada uno de los 14 dominios de control.

1. **Política de seguridad de la información**

El objetivo de este dominio es tener un instrumento que denote la intención de la alta gerencia de la organización sobre la seguridad de la información bajo consideraciones legales, comerciales y de cumplimiento regulatorio, por eso, una política de seguridad de la información debe definirse, aprobada por la gerencia general y difundida en la organización, así que todos los funcionarios y terceros relacionados deben conocer y aceptar su cumplimiento. (Gobierno Electrónico, 2020)

2. **Organización de la seguridad de la información**

Este dominio tiene como foco una organización formal de la función de seguridad de la información como un proceso de la organización, es así que, como todo proceso, requiere actores (tanto internos como terceras partes), directrices, asignaciones, compromisos y responsabilidades soportadas por la alta gerencia, además, señala que al ser complementaria a los otros procesos, la seguridad de la información requiere también la participación de los diferentes representantes de los procesos de la organización. (Gobierno Electrónico, 2020)

3. **Seguridad de los recursos humanos**

Este dominio es el nexo entre la seguridad de la información y la administración del activo de información más importante, las personas, es por esto que dentro de este se abarcan controles relacionados a la selección de personal, vinculación, asignación de recursos para el funcionario, esquema de sanciones y desvinculaciones.

Los controles que forman parte de este control se orientan a que las personas conozcan sus roles y responsabilidades en seguridad de la información, las misma que deben estar claramente definidas y documentadas. (Gobierno Electrónico, 2020)

4. **Gestión de activos de información**

Este dominio tiene como objetivo la identificación de los activos de Información de la organización (de los procesos que forman parte del alcance del Sistema de Gestión de Seguridad de la Información), siendo necesario indicar que un

activo de información es todo lo que procesa, genera o almacena información relacionada a los distintos procesos de negocio, es así que, estos activos pudieran ser hardware, software, documentos físicos, documentos electrónicos o personas.

Cada activo de información debe tener un propietario o responsable designado por la organización, cuya responsabilidad es clasificar el activo según su valor, la dependencia del negocio hacia este, requisitos legales, etc., para determinar su criticidad, sensibilidad y etiquetado para aplicar reglas para su uso aceptable (controles). (Gobierno Electrónico, 2020)

5. **Control de acceso**

   El objetivo general de este dominio es regular y restringir la interacción entre sujetos y objetos a nivel lógico a través de la adecuada gestión de usuarios, contraseñas y perfiles de acceso tanto a aplicaciones, redes y sistemas operativos, el bloqueo de equipos, caducidad de sesiones y teletrabajo. (Gobierno Electrónico, 2020)

6. **Criptografía**

   Se usa para proteger la confidencialidad e integridad de los datos usando técnicas de cifrado. El objetivo principal de este control es garantizar que la información sensible o confidencial solo sea accesible y comprensible para las partes autorizadas. (Gobierno Electrónico, 2020)

7. **Seguridad física y del entorno**

   El objetivo de este dominio es prevenir el acceso físico no autorizado, así como, evitar daños e interferencias en las instalaciones y actos de información. Dentro de este dominio se consideran controles de seguridad física como puerta, archivadores, lectores biométricos, cámaras de seguridad, etc.

   Este dominio considera reguladores de voltaje, detectores y extintores de incendios, controles contra inundaciones, cableado seguro, transporte de equipos fuera de las instalaciones, etc. Además, con respecto a los controles

existentes, obliga a que estos sean monitoreados, revisados y que exista soporte. (Gobierno Electrónico, 2020)

8. **Seguridad de las operaciones.**

   Asegurar que los sistemas de información y los datos estén protegidos y disponibles de manera confiable. Este control abarca una serie de prácticas y medidas que ayudan a minimizar los riesgos y mantener la integridad de los sistemas en el día a día de la organización. Al establecer procesos adecuados para la gestión de incidentes, control de cambios, gestión de configuraciones y continuidad del negocio, se puede responder de manera efectiva a los desafíos de seguridad y garantizar que las operaciones se realicen sin interrupciones y con un alto nivel de seguridad. (Gobierno Electrónico, 2020)

9. **Seguridad en las telecomunicaciones.**

   Es una medida esencial en la protección de la información que se transmite a través de redes de comunicación. Este control se enfoca en garantizar la confidencialidad, integridad y disponibilidad de los datos durante su transmisión y recepción. Además, se establecen políticas y procedimientos para el uso seguro de los medios de comunicación, como redes cableadas, inalámbricas y satelitales. El control de seguridad de las telecomunicaciones asegura que la información confidencial no sea interceptada o alterada durante su transferencia y contribuye a mantener la integridad de las comunicaciones en el entorno digital actual. (Gobierno Electrónico, 2020)

10. **Adquisición, desarrollo y mantenimiento de sistemas de información**

    Procurar que la seguridad sea una parte integral de los sistemas de información asegurando que en etapas tempranas de los proyectos de desarrollo de software se consideren requisitos de seguridad, validación para el adecuado procesamiento de datos, criptografía, datos de prueba, archivos sensibles y críticos de las aplicaciones, asegurando los códigos fuente, gestionando y probando todo cambio realizado, restricciones de acceso o gestión de vulnerabilidades técnicas. (Gobierno Electrónico, 2020)

11. **Relaciones con proveedores**

Es una medida importante en la seguridad de la información, ya que implica establecer y mantener relaciones seguras y confiables con los proveedores de productos y servicios de tecnología de la información. Este control se centra en garantizar que los proveedores cumplan con los requisitos de seguridad de la información de la organización y que sean capaces de mantener un nivel adecuado de protección de los datos. (Gobierno Electrónico, 2020)

12. Gestión de Incidentes de seguridad de Información

Este dominio se orienta a asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción oportuna tanto para mitigar el impacto, así como para dar una solución definitiva encaminada a que no se vuelva a dar el evento, es por eso que, debe existir un canal conocido y habilitado para reportar incidentes de seguridad de la información, así mismo, deben estar claramente definidos los responsables para dar tratamiento a dichos Incidentes. (Gobierno Electrónico, 2020)

13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Este control se enfoca en identificar y evaluar los riesgos de seguridad de la información asociados con la interrupción de las operaciones y establecer medidas para prevenir o mitigar estos riesgos. Esto incluye la implementación de planes de continuidad del negocio que contengan procedimientos para la protección y recuperación de la información, la realización de copias de seguridad periódicas, la designación de equipos de respuesta a emergencias y la realización de pruebas y simulacros de respuesta a desastres. (Gobierno Electrónico, 2020)

14. Cumplimiento regulatorio

Su objetivo es evitar que la organización incumpla cualquier ley, estatuto, obligación, reglamento u obligación contractuales, así como, cualquier aspecto regulatorio que pudiera aplicar, como, propiedad intelectual, ley de contratación pública, ley de comercio electrónico y firma digital, Acuerdo 166, Constitución de la República del Ecuador, etc. (Gobierno Electrónico, 2020)

CAPÍTULO III

MARCO METODOLÓGICO

Este marco metodológico se constituye como el plano estratégico que orientará la recopilación, análisis y aplicación de datos para lograr los objetivos establecidos. En esta sección, se delineará la metodología de investigación, destacando la selección de herramientas y técnicas específicas, así como la justificación detrás de estas elecciones. Además, se describe el enfoque para la recopilación de datos, la identificación de variables críticas y la validación de resultados. La transparencia y coherencia en cada etapa del proceso metodológico se consideran esenciales para garantizar la replicabilidad y confiabilidad de los resultados obtenidos.

Naturaleza de la investigación

En el presente trabajo de titulación tiene un enfoque cuantitativo que se fundamenta en paradigma positivista, el cuál según Rodríguez y Pérez (2022), asume la objetividad como única vía para alcanzar el conocimiento, enfatiza que la información se puede traducir en números, busca explicar, predecir y controlar los fenómenos, así como verificar teorías y fundamenta el análisis en la estadística descriptiva e inferencial.

La investigación sería aplicada porque se busca diseñar una metodología basada en el EGSI con el propósito de implementarla en una empresa privada. El objetivo es utilizar los conocimientos y las mejores prácticas establecidas por el gobierno en materia de seguridad de la información y adaptarlas a las necesidades y características específicas de la empresa.

Además, la investigación tendría un enfoque descriptivo, ya que se busca comparar, describir y explicar cómo se diseñará y desarrollará la metodología basada en el EGSI. Esto implica identificar los componentes clave del EGSI, analizar su relevancia para la empresa y proponer recomendaciones específicas para su implementación.

Población

Según García (2020) establece que “La población se refiere al conjunto de cosas, objetos u sujetos que guardan una característica en común y la muestra implica un subconjunto representativo de la población” (pág. 82). Para el presente trabajo de

investigación se centra en los directivos de la empresa TOC Systems, con una atención específica en la figura que desempeña el papel crucial de responsable de seguridad de la información dentro de la organización. Debido al tamaño reducido y la especificidad de la población, se prescinde del concepto de muestra en este contexto. La delimitación precisa de esta población se justifica por la naturaleza estratégica de los directivos y su influencia directa en la toma de decisiones relacionadas con la seguridad de la información. La focalización en esta población específica permitirá una exploración detallada y personalizada de las percepciones, necesidades y desafíos inherentes a la implementación de la metodología basada en el EGSI en el entorno empresarial de TOC Systems.

Técnica e instrumento de recolección de datos

Para llevar a cabo la recolección de datos, se emplea una técnica que combina la revisión documental, observación directa y la evaluación mediante un instrumento específico.

Luego de revisar documentación disponible en libros, artículos científicos y sitios web se determinó la adaptación del Modelo de Diagnóstico de Seguridad de la Información según ISO 27001 creado por la Alta Consejería Distrital de TIC del Municipio de Bogotá, Colombia (Alta Consejería Distrital de TIC, 2020). Dicho instrumento, un aplicativo desarrollado en Microsoft Excel, permite determinar el nivel de madurez del SGSI, a través de un cuestionario estructurado en tres partes, denominados logros.

La herramienta, previamente validada y estructurada, para verificar el cumplimiento de los 14 controles de seguridad del EGSI. Este instrumento, cuidadosamente elaborado, se convertirá en un mecanismo eficiente para evaluar de manera sistemática la implementación de los controles en la organización TOC Systems. Combinar estas técnicas y usar el instrumento en Excel aseguran una recopilación de datos precisa y estructurada, facilitando una evaluación detallada del nivel según los controles de seguridad establecidos por el EGSI.

El instrumento se encuentra almacenado en la nube (Ver Anexo 6)

Mientras que la operacionalización de variables está estructurada de la siguiente forma como se muestra en la Tabla 2.

Tabla 2: *Operacionalización de variables*

Variable	Definición	Dimensión	Indicador	Instrumento
Conocimiento de la empresa sobre el Esquema Gubernamental de Seguridad de la Información.	Se refiere al grado de comprensión y familiaridad que tiene una organización con respecto a las directrices, políticas y prácticas establecidas en el marco de seguridad de la información diseñado por el gobierno.	- Conocimiento teórico - Conocimiento práctico	Escala de medición nominal	Aplicativo desarrollado en Microsoft Excel
Cumplimiento de la empresa con los estándares del Esquema Gubernamental de Seguridad de la Información	El grado en que la empresa sigue y aplica los estándares y medidas de seguridad del bernamental de Seguridad de la Información.	-Políticas y procedimientos - Implementación técnica y - Monitorización y mejora continua.	Escala de medición nominal	Aplicativo desarrollado en Microsoft Excel
Implementación de controles de seguridad en la empresa	El grado en que la empresa ha aplicado y establecido los controles y medidas de seguridad para proteger la información.	-Cobertura de controles -Madurez de los controles -Resiliencia y adaptabilidad	Escala de medición nominal	Aplicativo desarrollado en Microsoft Excel
Metodología de la seguridad de la información	La metodología de seguridad de la información se enfoca en establecer procesos sistemáticos para proteger la confidencialidad, integridad y disponibilidad de los datos.	Fundamentación en la Norma.	Norma ISO 27001	Aplicativo desarrollado en Microsoft Excel

Fuente: *Elaboración Propia*

Procedimiento de análisis de datos

Según García y López (2020), "se describen las distintas operaciones a las que serán sometidos los datos que se obtengan: clasificación, registro, tabulación y codificación si fuere el caso" (pág. 125). En el presente trabajo de investigación, para analizar la información que se obtuvo a través del instrumento en Excel se utilizará la técnica de

estadística descriptiva, la cual según Sánchez y Martínez (2021), "es un proceso mediante el cual se recopila, organiza, presenta, analiza e interpreta datos de manera que describa fácil y rápidamente las características esenciales de dichos datos mediante el empleo de métodos gráficos, tabulares o numéricos" (pág. 20).

Consideraciones éticas

La confiabilidad de un instrumento según Pérez y Gómez (2022) es el “Grado en que un instrumento produce resultados consistentes y coherentes” (pág. 198). Esto va a permitir determinar cuán confiables son los resultados obtenidos.

Se garantiza el cumplimiento de los principios éticos en la investigación:

- **Consentimiento informado:** Antes de la participación en la lista de verificación se obtendrá el consentimiento informado de todos los participantes.
- **Confidencialidad:** Todos los datos recopilados serán tratados de manera confidencial y solo se utilizarán con fines académicos y de investigación.

Metodología del producto

El proceso de implementación del Plan Piloto en TOC Systems se llevará a cabo de manera estructurada y progresiva, siguiendo las mejores prácticas establecidas en la norma ISO 27001:2013. Este plan tiene como objetivo evaluar la efectividad y viabilidad de la implementación del SGSI en la empresa.

A continuación, se describe el proceso detallado:

Fase 1: Preparación Inicial

1. Formación del Equipo de Implementación: Se designará un equipo de implementación compuesto por miembros clave de diferentes áreas de la empresa, incluyendo representantes de la alta dirección, personal de TI, seguridad de la información y otros roles relevantes.
2. Concientización y Capacitación:

- Se llevará a cabo una sesión de concientización sobre la importancia de la seguridad de la información y la norma ISO 27001 para todo el personal de la empresa.

- Se proporcionará capacitaciones específicas sobre los requisitos de la norma SO 27001 a los miembros del equipo de implementación.

Fase 2: Evaluación Inicial

- Análisis de Brechas: Se realizará un análisis de brechas para identificar las áreas en las que TOC Systems cumple con los requisitos de la norma ISO 27001 y las áreas que necesitan mejoras.
- Adaptación del Instrumento: El instrumento en Excel se adaptará para reflejar las especificidades y necesidades de TOC Systems, permitiendo una evaluación detallada.

Fase 3: Personalización del SGSI para TOC Systems

- Desarrollo de Documentación: Se elaborarán los documentos necesarios para establecer el SGSI, incluyendo la política de seguridad de la información, procedimientos operativos estándar, y registros de seguridad.
- Personalización de Controles de Seguridad: Se personalizan los controles de seguridad de acuerdo con la estructura y operaciones específicas de TOC Systems, asegurando una integración efectiva.

Fase 4: Implementación del Plan Piloto

- Aplicación del Instrumento en Excel: Se utilizará un instrumento en Excel para llevar a cabo evaluaciones y seguimientos durante la implementación del SGSI, enfocándose en los 14 controles de seguridad definidos en la norma ISO 27001.
- Implementación Gradual de Controles: Se implementarán gradualmente los controles de seguridad, comenzando por aquellos que requieran acciones inmediatas y avanzando hacia medidas más complejas.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

El análisis bibliográfico del EGSI vigente en Ecuador revela una estructura integral destinada a asegurar la protección de los datos manejados por entidades gubernamentales. Este esquema abarca políticas, procedimientos, y tecnologías orientadas a la prevención de incidentes de seguridad, asegurando la confidencialidad, integridad, y disponibilidad de la información.

Al considerar la transferencia de aspectos del EGSI al ámbito empresarial, se identifican varias áreas de potencial aplicación. Entre ellas, la implementación de políticas de seguridad de la información, la adopción de estándares para la gestión de riesgos, y el desarrollo de planes de respuesta ante incidentes. Estos elementos pueden adaptarse para fortalecer las estrategias de seguridad en empresas privadas, promoviendo un enfoque proactivo en la protección de datos críticos.

La evaluación de las necesidades de seguridad de la información en empresas privadas debe partir de un análisis de riesgos detallado, que considere tanto amenazas internas como externas. Este proceso permitirá identificar las áreas críticas que requieren atención inmediata, así como establecer un plan de acción para mitigar riesgos. La adaptación de prácticas y principios del EGSI puede proporcionar un marco robusto para esta evaluación, asegurando que se aborden de manera efectiva los desafíos específicos del entorno empresarial.

El marco metodológico desarrollado con los principios del EGSI, ajustado a las empresas privadas, implica la personalización de estrategias y herramientas para alinearlas con los objetivos y necesidades específicas del sector privado. Esto incluye la adaptación de políticas de seguridad, la implementación del SGSI basados en normativas internacionales (como ISO/IEC 27001), y el fortalecimiento de la cultura organizacional en torno a la seguridad de la información. Este enfoque integrado facilita una protección efectiva de los activos de información, al tiempo que promueve la resiliencia organizacional frente a amenazas y vulnerabilidades emergentes.

Análisis de resultados

Para evaluar el impacto de la metodología implementada, se utilizarán indicadores de desempeño relacionados con la seguridad de la información en la empresa. Algunos de los indicadores a considerar pueden incluir:

- Porcentaje de empleados capacitados en temas de seguridad de la información.
- Nivel de cumplimiento de las políticas y procedimientos de seguridad por parte del personal.
- Tiempo de respuesta ante incidentes de seguridad de la información.
- Número de vulnerabilidades identificadas y corregidas.
- Reducción en la incidencia de brechas de seguridad o ataques informáticos.

Además de los indicadores cuantitativos, se realizará una evaluación cualitativa mediante encuestas de satisfacción y retroalimentación de los empleados sobre la percepción de la seguridad de la información en la empresa.

Inventario de activos

La Tabla 3 presenta el inventario de activos de información de la organización de Toc Systems.

Tabla 3: *Inventario de activos de información*

N.	*Tipo*	*Descripción*	*Observaciones*
1	Físico	Mueble	Almacena documentos y dispositivos
2	Físico	Oficinas	Lugar en el cual se lleva a cabo las actividades directivas y empleados
3	Físico	Mochilas	Permite el transporte de los dispositivos de manera cómoda y fácil.
	Físico	Rack	Lugar donde se puede alojar equipamiento electrónico, informático y de comunicaciones
4	Humano	Secretaria	Persona la cual prestan apoyo administrativo a los directivos y otros profesionales
5	Humano	Empleados	Personas que desempeñan actividades diarias la cual permite aumentar el crecimiento de la organización
6	Humano	Guardia de seguridad	Control de ingreso/salida física y vehicular de personas
7	Humano	Gerente	Persona encargada de planear y dirigir el trabajo de un grupo de individuos
8	Humano	Presidente	Persona que define el propósito, la misión y la visión. Y es el responsable de proveer los recursos necesarios.
9	Lógico	Sistema Operativo	Conjunto de programas que realizan funciones básicas y permiten el desarrollo de otros programas. (Linux, Windows)
10	Lógico	Proyectos de software	Implica la creación y gestión de componentes intangibles, como el código fuente, la arquitectura del sistema, la documentación, los diseños y otros artefactos asociados con el desarrollo y mantenimiento del software
11	Lógico	Servidores	procesamiento, almacenamiento y aplicaciones
12	Tecnológico	Computadora	Permite almacenar información, obtener datos importantes, para sostener procesos de negocio a través de Internet
13	Tecnológico	Celular	Permite la comunicación y la toma de decisiones ágil gracias a la comunicación instantánea
14	Físico	Mouse	Dispositivo de entrada diseñado para manipular objetos en la pantalla de la computadora

Tabla 3: (cont.)

N.	*Tipo*	*Descripción*	*Observaciones*
15	Físico	Mouse Pad	Superficie sobre la que se apoya y se desliza el mouse de la computadora
16	Físico	Tarjetas	Permiten el acceso a las instalaciones
17	Físico	Audífono	Permiten que los asesores puedan concentrarse en su conversación y aislarse del ruido

Fuente: *TocSystem*

Inseguridades Iniciales

La evaluación de la inseguridad se ha desglosado en tres categorías clave: personas, tecnología y procesos, cada una asignada con un porcentaje específico. En este análisis, se ha determinado que la inseguridad a nivel de personas es del 20%, la inseguridad relacionada con la tecnología es del 40%, y la inseguridad en los procesos internos alcanza el 60%. La combinación de estos valores proporciona un índice global de inseguridad para la empresa del 40%.

Este enfoque de desglose permite identificar las áreas específicas de la operación empresarial que presentan mayores desafíos en términos de seguridad. Por ejemplo, la inseguridad a nivel de procesos, evaluada en un 60%, indica que hay aspectos críticos en los procedimientos internos que requieren atención y mejoras.

Con un índice global de inseguridad del 40%, existe la oportunidad de implementar estrategias y medidas correctivas para abordar estas áreas de vulnerabilidad y fortalecer la postura general de seguridad de la empresa. Este análisis proporciona una base sólida para tomar decisiones informadas sobre cómo mejorar la seguridad de la información, la infraestructura y la gestión de los empleados dentro de la empresa colaborada. (Ver Anexo 4)

Figura 3: *Seguridad e inseguridad global*

Fuente: *TocSystem*

Inseguridad a Nivel de Personas:

Una inseguridad del 20% en este aspecto podría sugerir que se necesitan medidas adicionales para mejorar la conciencia y la capacitación en seguridad entre los empleados. Se podría considerar un enfoque específico en programas de formación para mitigar las amenazas relacionadas con errores humanos o prácticas inseguras.

Inseguridad de Tecnología:

La inseguridad del 40% en tecnología indica una necesidad crítica de fortalecer las medidas de seguridad en el ámbito tecnológico. Esto podría implicar la implementación de soluciones de seguridad avanzadas, actualizaciones regulares de software, y la adopción de prácticas de seguridad cibernética robustas.

Inseguridad de Procesos:

La inseguridad del 60% en procesos destaca la importancia de revisar y mejorar los procedimientos internos relacionados con la seguridad de la información. Esto podría incluir la revisión y actualización de políticas de seguridad, la implementación de controles de acceso adecuados y la creación de procesos que mitiguen riesgos potenciales.

Uso de la herramienta estandarizada

La herramienta estandarizada de evaluación del SGSI se ha diseñado para abordar tres logros específicos con sus respectivos objetivos. A continuación, se detallan las instrucciones para el uso efectivo de la herramienta, junto con los puntos clave a evaluar en cada logro:

1. Definición de Marco de Seguridad y Privacidad de la Entidad (30%)

Objetivo: Evaluar la efectividad en la planificación y definición del marco de seguridad y privacidad del SGSI.

Puntos Clave a Evaluar:

- Cumplimiento de la planificación del SGSI.
- Documentación y socialización del marco de seguridad.
- Definición y aplicación del alcance del SGSI.

2. Implementación del Plan de Seguridad y Privacidad de la Información (40%)

Objetivo: Evaluar la efectividad en la implementación práctica del plan de seguridad y privacidad de la información.

Puntos Clave a Evaluar:

- Cumplimiento de requisitos de la norma ISO 27001.
- Efectividad en la gestión de controles de seguridad.
- Aprobación y aplicación de políticas y roles.

3. Monitoreo y Mejoramiento Continuo (30%)

Objetivo: Evaluar la efectividad en las fases de verificación y actuación para el monitoreo y mejora continua del SGSI.

Puntos Clave a Evaluar:

- Metodología de seguimiento y análisis permanente.
- Realización de auditorías internas y programas de auditoría.
- Respuestas y gestión de no conformidades.
- Revisión de eficacia de acciones correctivas.
- Procesos documentados de mejora continua.

Al utilizar la herramienta, asegúrese de considerar detenidamente cada punto clave en relación con los objetivos y metas establecidos para cada logro. Proporcione respuestas claras y específicas, reflejando la situación actual del SGSI de la entidad en cada fase. Este proceso de evaluación ayudará a identificar áreas de mejora y a fortalecer el sistema de seguridad de la información según los estándares y mejores prácticas que podremos evidenciar al analizar cada logro.

Autodiagnóstico SGSI logro 1: Definición de marco de seguridad y privacidad de la entidad

Luego se analizan los resultados obtenidos por el logro uno de acuerdo a las métricas establecidas en la siguiente tabla.

Tabla 4: *Reglas de valorización del logro 1*

Estado	Descripción
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

Fuente: *Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)*

En la Tabla 5 podemos evidenciar el desglose de los datos obtenidos en porcentajes sobre las preguntas que compone el logro 1.

Tabla 5: *Resumen del marco de seguridad y privacidad - logro 1*

Resumen del marco de seguridad y privacidad - logro 1			
Preguntas	**Valorización**	**Total**	**Peso**
6 a 15	Cumple satisfactoriamente	6	9,23%
5 a 15	Cumple parcialmente	5	3,85%
2 a 15	No cumple	2	0,00%
1 a 15	Autodiagnóstico	1	2,50%
1 a 15	Plan de trabajo	1	2,50%
	Total	15	18,08%

Fuente: *Elaboración Propia*

El análisis de los datos proporcionados revela un panorama detallado de la valorización de las preguntas en el contexto del Logro 1 del Marco de Seguridad y Privacidad.

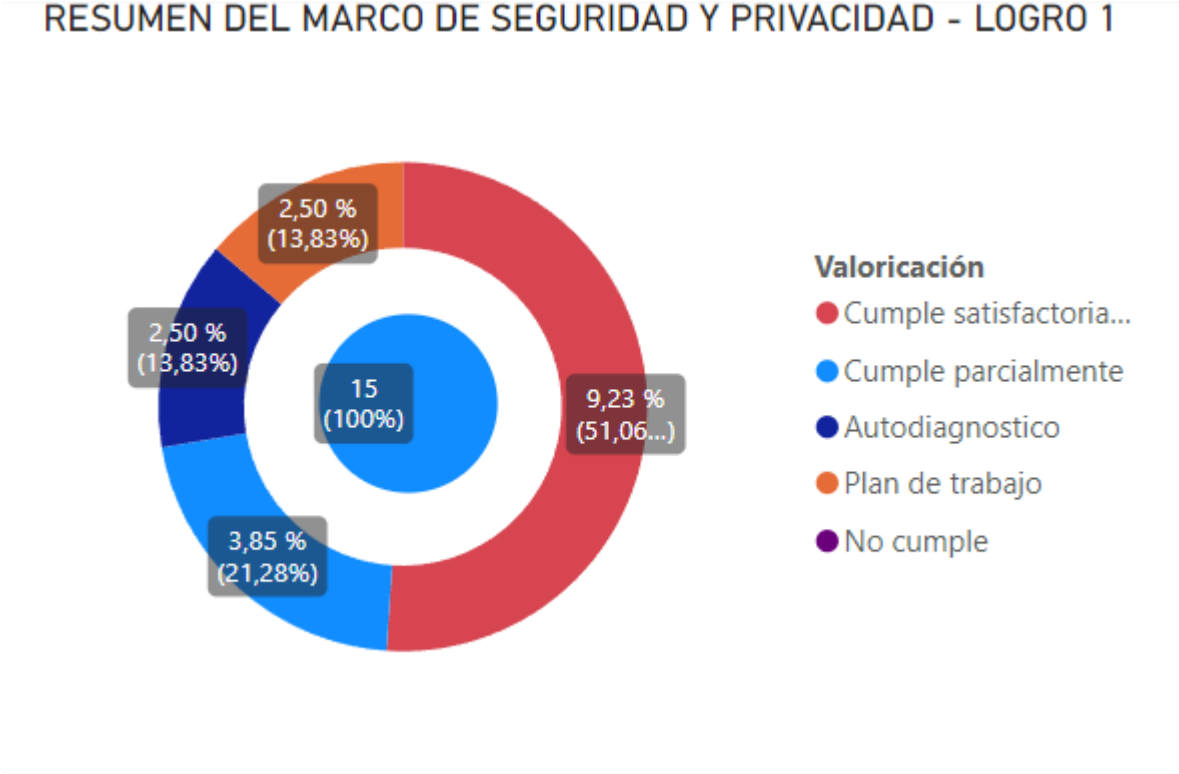


Figura 4: *Resumen del marco de seguridad y privacidad logro #1*

Fuente: *Elaboración Propia*

Las preguntas, evaluadas como "cumple satisfactoriamente" revelan una base sólida para la implementación exitosa del SGSI. La participación y aprobación de la dirección, la meticulosa identificación de aspectos internos y externos, la consideración detallada de las partes interesadas y la evaluación precisa de objetivos destacan como elementos críticos para el logro del éxito en esta iniciativa. Además, la existencia de un Comité de Seguridad de la Información y una política debidamente aprobada subraya un enfoque estructurado y respaldado por la dirección en la efectiva gestión de la seguridad de la información, consolidando así la fundación sólida para un SGSI eficaz.

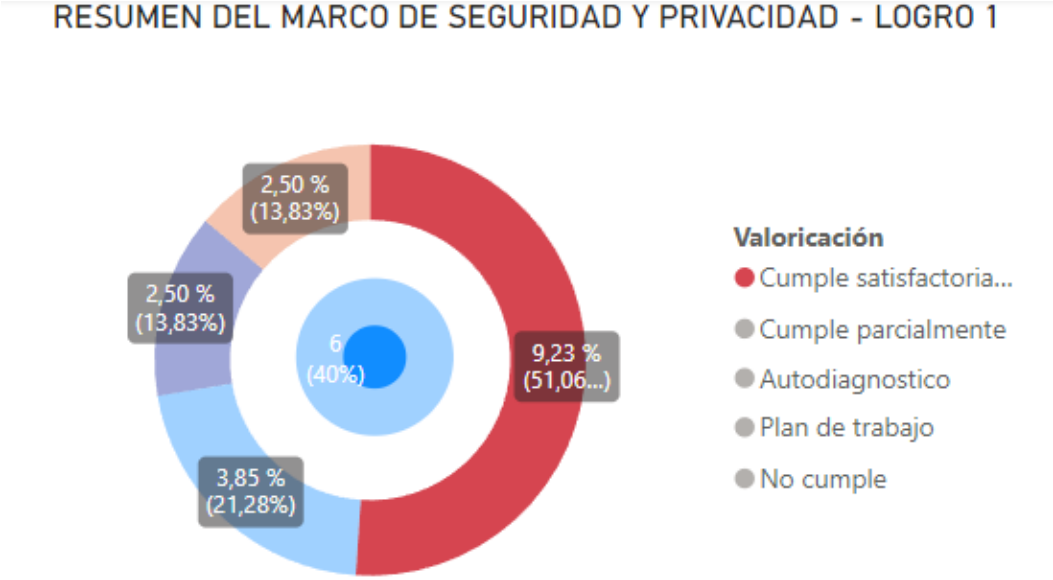


Figura 5: *Porcentaje de preguntas satisfactorias*

Fuente: *Elaboración Propia*

Estas prácticas exitosas proporcionan una base sólida para continuar avanzando en la implementación del SGSI, asegurando alineación con objetivos organizacionales y estándares de seguridad.

Autodiagnóstico SGSI logro 2: Implementación del plan de seguridad y privacidad de la información

Tabla 6: *Reglas de valorización del logro 2*

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Fuente: *Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)*

En la Tabla 7 podemos evidenciar el desglose de los datos obtenidos en porcentajes sobre las preguntas que compone el logro 2 en base a los 144 controles analizados.

Tabla 7: *Resumen del plan de seguridad y privacidad de la información logro 2*

Resumen del plan de seguridad y privacidad de la información -logro 2			
Preguntas	**Valorización**	**Total**	**Peso**
38 a 144	Cumple satisfactoriamente	38	13,33%
67 a 144	Cumple parcialmente	67	11,75%
9 a 144	No cumple	9	0,00%
0 a 15	No aplica	0	0,00%
	No. Controles que le aplican	114	
	Total	15	25,09%

Fuente: *Elaboración Propia*

El análisis de los datos proporcionados revela un panorama detallado de la valorización de las preguntas en el contexto del Logro 2 del Plan de Seguridad y Privacidad de la información.

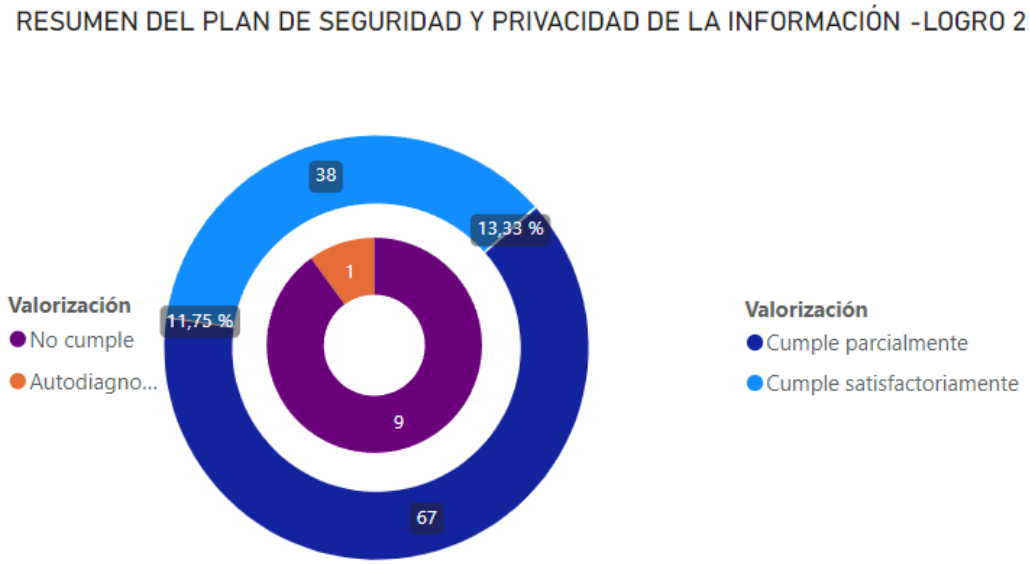


Figura 6: *Resumen del plan de seguridad y privacidad logro #2*

Fuente: *Elaboración Propia*

La valorización del 25,09% indica un progreso significativo en la implementación de controles de seguridad y privacidad de la información. Es alentador que el 13,33% de los controles cumpla satisfactoriamente, evidenciando una gestión efectiva y completa, documentación adecuada y cumplimiento por parte de todos los involucrados. Sin embargo, la presencia del 11,75% de controles valorizados como "cumple parcialmente" destaca áreas que necesitan mayor atención y mejoras para lograr un cumplimiento total.

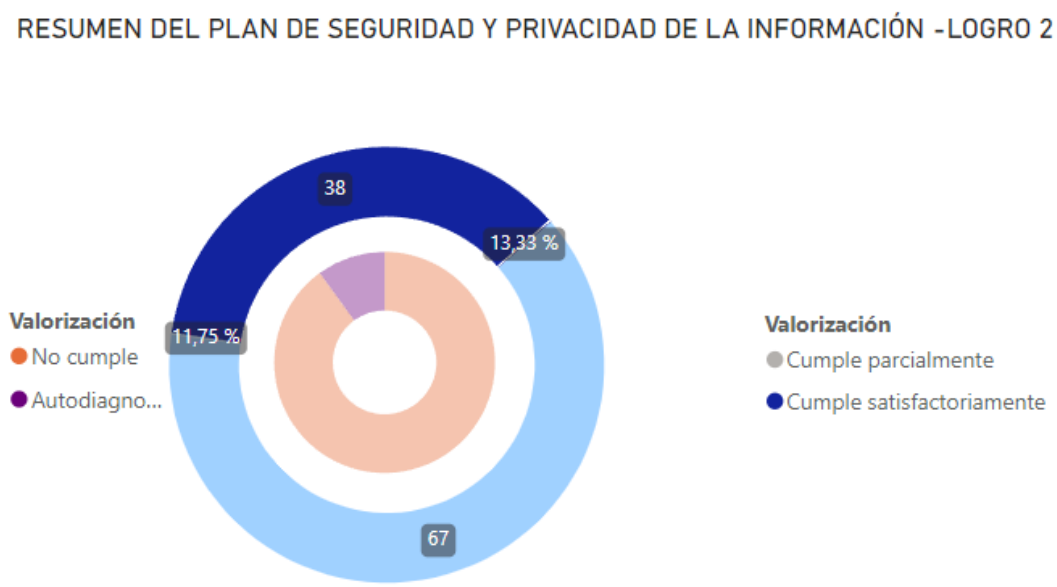


Figura 7: *Porcentaje de preguntas satisfactorias*

Fuente: *Elaboración Propia*

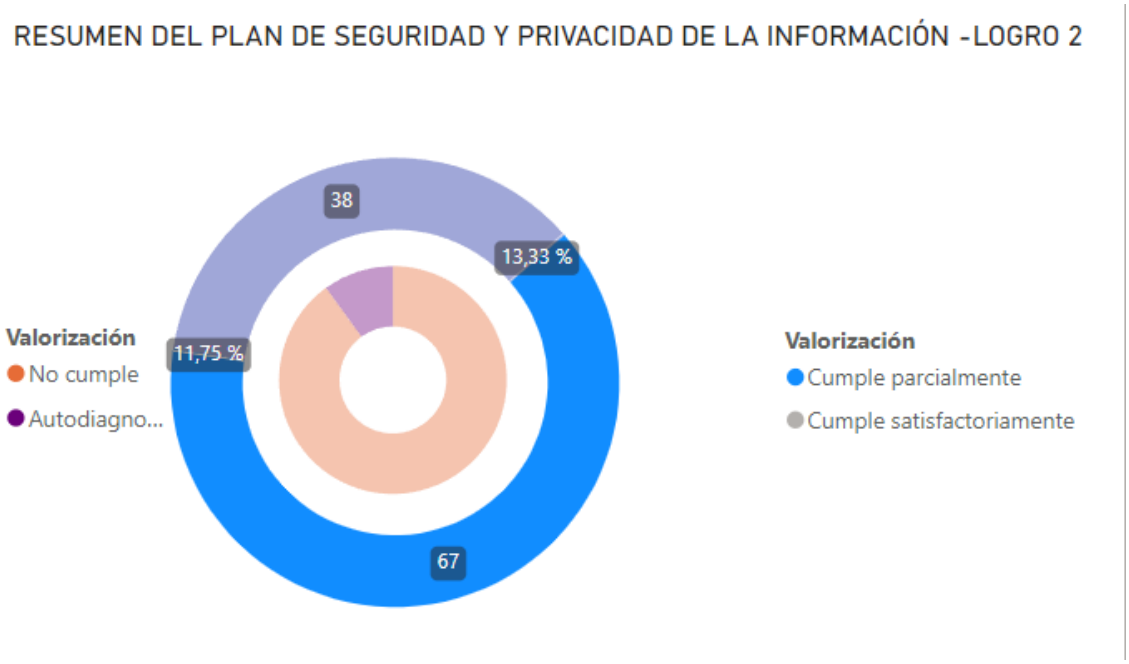


Figura 8: *Porcentaje de preguntas parciales*

Fuente: *Elaboración Propia*

La valorización de "no cumple" en el 0,00% es positiva, indicando que no hay controles completamente ausentes, aunque aún existen 9 controles que requieren acción inmediata para cumplir con los estándares de seguridad establecidos. La valorización de "no aplica" muestra una evaluación justificada de la no aplicabilidad de ciertos controles, lo cual es una práctica aceptable en la gestión de seguridad de la información.

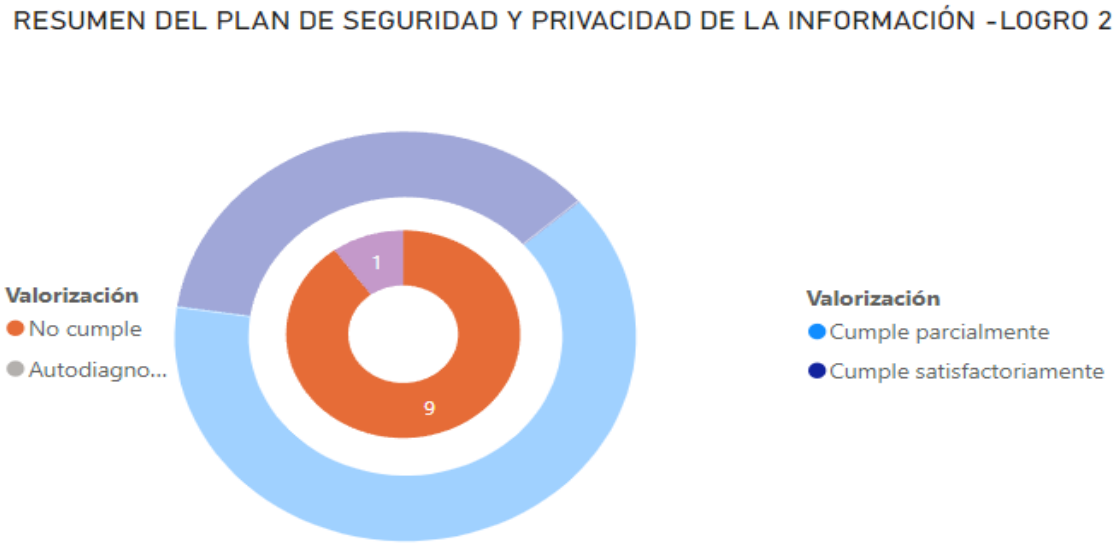


Figura 9: *Porcentaje de preguntas que no cumplen*

Fuente: *Elaboración Propia*

Autodiagnóstico SGSI logro 3: Monitoreo y mejoramiento continuo

Tabla 8: *Reglas de valorización del logro 3*

Estado	Descripción
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

Fuente: *Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)*

En la Tabla 9 podemos evidenciar el desglose de los datos obtenidos en porcentajes sobre las preguntas que compone el logro 3.

Tabla 9: *Resumen del plan de monitoreo y mejora continua -logro 3*

Resumen del plan de monitoreo y mejora continua -logro 3				
	Verificar		**Actuar**	
Valorización	**Total**	**Peso**	**Total**	**Peso**
Cumple satisfactoriamente	0	0,00%	0	0,00%
Cumple parcialmente	4	5,00%	2	2,50%
No cumple	2	0,00%	4	0,00%
Total		5,00% Total		2,50%

Fuente: *Elaboración Propia*

El análisis general de los datos del Logro 3 sobre el Plan de Monitoreo y Mejora Continua indica una valorización total del 5,00% en la fase de Verificar y del 2,50% en la fase de Actuar. A continuación, se analizan los resultados específicos de las preguntas y las categorías de valoración:

Fase de Verificar:

En esta fase, la entidad ha mostrado una valorización del 5,00%. Se observa que, aunque hay aspectos positivos, como revisiones realizadas por la dirección y reconocimiento de la necesidad de retroalimentación, existen desafíos notables. La falta de auditorías internas y la ausencia de programas estructurados de auditoría indican una brecha crítica en la verificación del SGSI. Además, las valorizaciones parciales en la metodología de seguimiento y análisis permanente, así como en la documentación de revisiones de la dirección, sugieren áreas que requieren fortalecimiento. Se recomienda implementar auditorías internas periódicas, establecer programas de auditoría detallados y mejorar la formalización de los procesos de revisión de la alta dirección para garantizar una verificación más completa y efectiva.

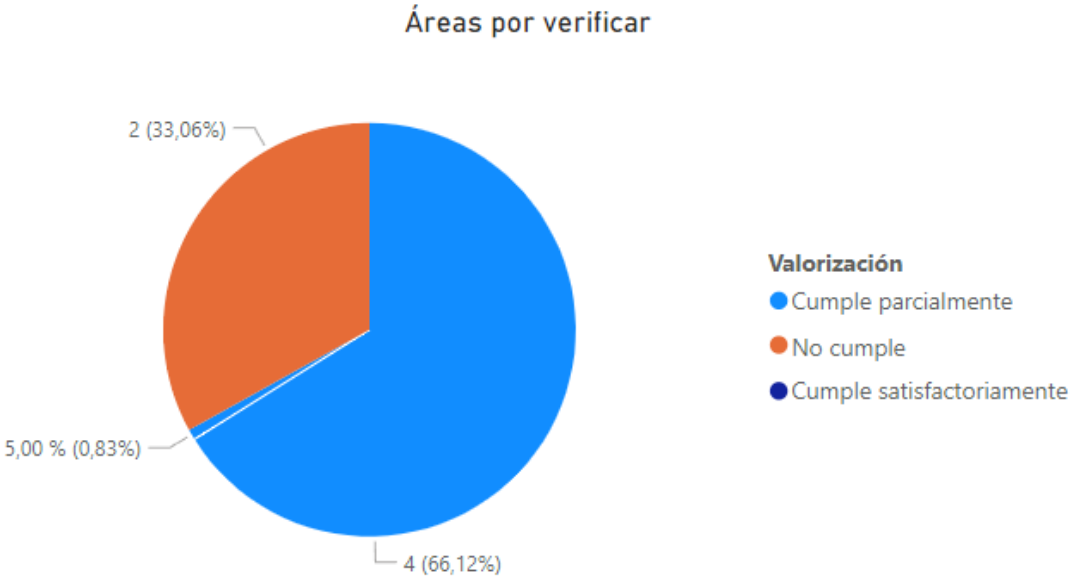


Figura 10: *Detalle de preguntas de acuerdo a su valorización en la fase de verificación*

Fuente: *Elaboración Propia*

Fase de Actuar:

En la fase de Actuar, la entidad muestra una valorización del 2,50%. Aunque se observa un cumplimiento parcial en la implementación de acciones correctivas y en la realización de procesos de mejora continua, existen desafíos críticos en otras áreas. La falta de respuestas a las no conformidades, la ausencia de revisión de la eficacia de las acciones correctivas y la no documentación de acciones correctivas y cambios en el SGSI indican debilidades importantes en el ciclo de mejora continua. Se recomienda priorizar la implementación efectiva de acciones correctivas, establecer procesos para evaluar la eficacia de estas acciones y documentar de manera exhaustiva los procesos de mejora continua. Estos pasos son fundamentales para impulsar la eficacia del SGSI y garantizar un enfoque sólido en la fase de Actuar para la mejora continua.

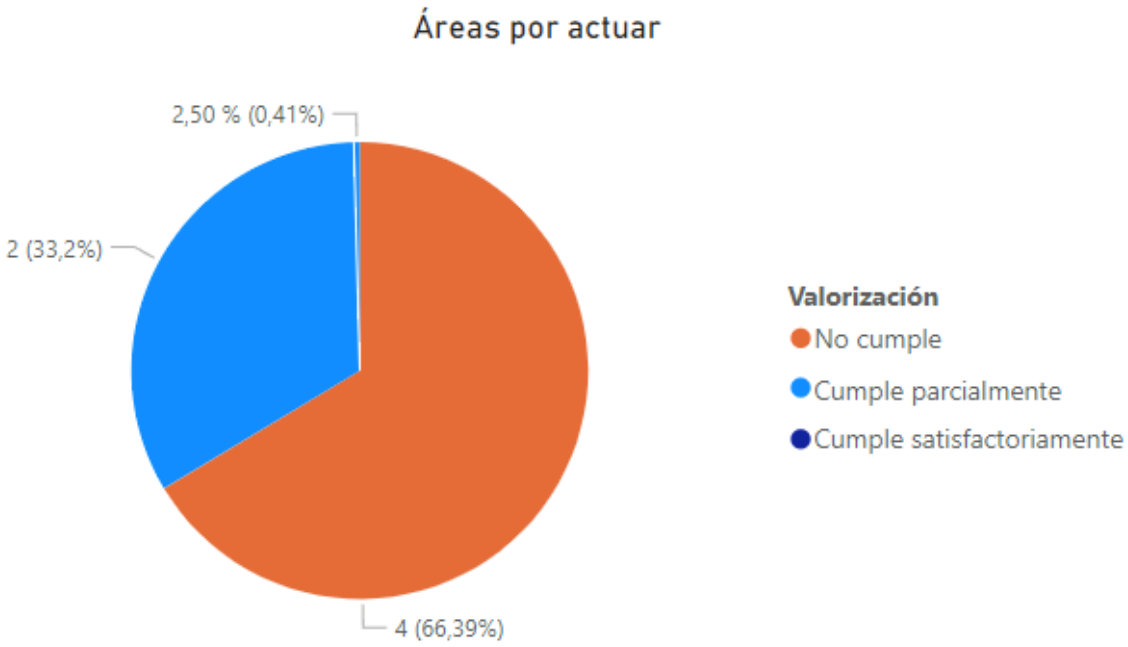


Figura 11*: Detalle de preguntas de acuerdo a su valorización en la fase de actuación*

Fuente: *Elaboración Propia*

A pesar de algunos puntos positivos, como las revisiones realizadas por la dirección y esfuerzos en mejora continua, la entidad enfrenta desafíos notables en auditorías internas, gestión de no conformidades y documentación de acciones correctivas. Se recomienda enfocarse en la implementación de auditorías internas regulares, establecer programas detallados de auditoría y mejorar la gestión de no conformidades con respuestas efectivas y revisiones de eficacia. La documentación estructurada de procesos y acciones se identifica como crucial, sugiriendo la necesidad de establecer prácticas documentadas para las revisiones de la dirección, las acciones correctivas y los procesos de mejora continua. Este enfoque integral es esencial para fortalecer la efectividad del SGSI y abordar las áreas críticas de mejora identificadas.

Resultados iniciales de la empresa

El análisis de los datos de cada logro en relación con las metas establecidas se presenta a continuación:

Logro 1 - "Planear" (Ejecutado: 18,1%):

La fase "Planear" del Logro 1 se ubica en un 18,1%, quedando por debajo de la meta establecida del 30%. Aunque hay avances en la planificación del SGSI, se identifica un espacio significativo para mejorar y alcanzar la meta propuesta.

Logro 2 - "Hacer" (Ejecutado: 25,1%):

La fase "Hacer" del Logro 2 alcanza un 25,1%, superando la meta del 40% establecida. Este resultado indica un progreso sustancial en la implementación de controles de seguridad y privacidad de la información. Aunque hay áreas de mejora identificadas, el desempeño general en esta fase es positivo.

Logro 3 - "Verificar" (Ejecutado: 5,0%) y "Actuar" (Ejecutado: 2,5%):

Las fases "Verificar" y "Actuar" del Logro 3 se sitúan en 5,0% y 2,5%, respectivamente. Ambas fases quedan por debajo de las metas establecidas del 15%. Estos resultados indican desafíos notables en las áreas de monitoreo y mejora continua del SGSI. Se destaca la necesidad de fortalecer las prácticas de verificación y actuar para cumplir con los estándares y mejorar la efectividad del sistema.

Total ejecutado (50,7%):

El total ejecutado para los tres logros es del 50,7%, revelando un rendimiento general a medio camino entre las metas establecidas. Aunque el Logro 2 muestra un desempeño positivo, los Logros 1 y 3 requieren una atención especial para cerrar las brechas identificadas y alinearse más estrechamente con las metas propuestas.

Tabla 10: *Resultados finales de los logros aplicados*

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	18,1%
LOGRO2	HACER	40%	25,1%
LOGRO3	VERIFICAR	15%	5,0%
	ACTUAR	15%	2,5%
	TOTAL	100%	50,7%

Fuente: *Elaboración Propia*

En los cuales se han evaluado diversos dominios de control en aspectos como:

- Controles que aplican
- Peso controles implementados y parcialmente implementados
- Implementados
- Parcialmente
- No cumple
- No aplica

De los cuales hemos obtenido la siguiente información identificando el dominio con mayor y menor relevancia según los valores obtenidos de cada logro aplicado según cada aspecto.

Controles que aplican:

- Mayor importancia: Seguridad física y del entorno (15 controles aplican).
- Menor importancia: Criptografía (2 controles aplican).

Peso controles implementados y parcialmente implementados:

- Mayor importancia: Seguridad de los recursos humanos (5.5 de ponderación).

- Menor importancia: Relación con los proveedores (1.5 de ponderación).

Implementados:

- Mayor importancia: Seguridad de los recursos humanos (4 implementados).
- Menor importancia: Varios dominios (0 implementados).

Parcialmente:

- Mayor importancia: Seguridad de los recursos humanos (2 parcialmente implementados).
- Menor importancia: Relación con los proveedores (0 parcialmente implementados).

No cumple:

- Mayor importancia: Seguridad física y del entorno (0 no cumple).
- Menor importancia: Varios dominios (3 no cumplen).

No aplica:

- Mayor importancia: Varios dominios (0 no aplica).
- Menor importancia: Criptografía (0 no aplica).

Tabla 11: *Dominios evaluados en todos los controles aplicados*

POR DOMINIO DE CONTROL						
Nombre dominios de control	**Controles que aplican**	**Peso controles implementados y parcialmente implementados**	**Implementados**	**Parcialmente**	**No cumple**	**No aplica**
Dominio 5 - políticas de seguridad de la información	2	1	0	2	0	0
Dominio 6 - organización de la seguridad de la información	7	5,5	4	3	0	0
Dominio 7 - seguridad de los recursos humanos	6	5	4	2	0	0
Dominio 8 - gestión de activos	10	7	4	6	0	0

Dominio 9 - control de acceso	14	9	4	10	0	0
Dominio 10 - criptografía	2	0	0	0	2	0
Dominio 11 - seguridad física y del entorno	15	10,5	6	9	0	0
Dominio 12 - seguridad de las operaciones	14	7	3	8	3	0
Dominio 13 - seguridad de las comunicaciones	7	4	1	6	0	0
Dominio 14 - adquisición, desarrollo y mantenimiento de sistemas	13	9	5	8	0	0
Dominio 15 - relación con los proveedores	5	1,5	0	3	2	0
Dominio 16 - gestión de incidentes de seguridad de la información	7	5,5	4	3	0	0

Tabla 11: (Cont.)

POR DOMINIO DE CONTROL						
Nombre dominios de control	**Controles que aplican**	**Peso controles implementados y parcialmente implementados**	**Implementados**	**Parcialmente**	**No cumple**	**No aplica**
Dominio 17 - aspectos de seguridad de la información de la gestión de continuidad de negocio	4	3,5	3	1	0	0
Dominio 18 - seguridad de las comunicaciones	8	3	0	6	2	0
	114					

Fuente: *Elaboración Propia*

Los dominios del Sistema de Gestión de Seguridad de la Información (SGSI) se analizaron en función de la cantidad de controles que aplican, proporcionando insights

valiosos sobre la importancia relativa de cada dominio en la implementación de medidas de seguridad. A continuación, se presenta un resumen ordenado de mayor a menor importancia:

Seguridad de los recursos humanos (6 controles):

- Alta importancia, destacando la necesidad crítica de establecer medidas de seguridad relacionadas con el personal, su capacitación y gestión de acceso.

Seguridad de las operaciones (14 controles):

- Importancia moderada, resaltando la relevancia de abordar aspectos operativos para mantener la seguridad de la información.

Control de acceso (14 controles):

- Importancia moderada, esencial para garantizar la integridad y confidencialidad de la información mediante una gestión adecuada de acceso.

Adquisición, desarrollo y mantenimiento de sistemas (13 controles):

- Importancia moderada, subrayando la necesidad de seguridad en la adquisición y desarrollo de sistemas para evitar vulnerabilidades.

Seguridad física y del entorno (15 controles):

- Alta importancia, indicando la necesidad crítica de proteger los entornos físicos para garantizar la seguridad de la información.

Gestión de incidentes de seguridad de la información (7 controles):

- Importancia moderada, reflejando la necesidad de gestionar eficazmente incidentes para garantizar la continuidad operativa

Organización de la seguridad de la información (7 controles):

- Importancia moderada, esencial para una organización efectiva que asigna roles y responsabilidades en seguridad.

Seguridad de las comunicaciones (7 controles):

- Importancia moderada, esencial para proteger la transmisión de información sensible, tanto interna como externamente.

Gestión de activos (10 controles):

- Alta importancia, indicando la necesidad crítica de gestionar activos para salvaguardar la información y garantizar la continuidad operativa.

Seguridad de las comunicaciones (8 controles):

- Importancia moderada, crucial para garantizar la seguridad en las comunicaciones internas y externas.

Políticas de seguridad de la información (2 controles):

- Baja importancia, con una cantidad limitada de controles, indicando un impacto menor en la aplicación de medidas de seguridad.

Relación con los proveedores (5 controles):

- Importancia moderada, relevante para garantizar la seguridad en las relaciones con proveedores externos.

Aspectos de seguridad de la información de la gestión de continuidad de negocio (4 controles):

- Importancia moderada, vital para mantener la operatividad en situaciones adversas.

Criptografía (2 controles):

- Baja importancia, indicando un impacto relativamente menor en la aplicación de medidas de seguridad.

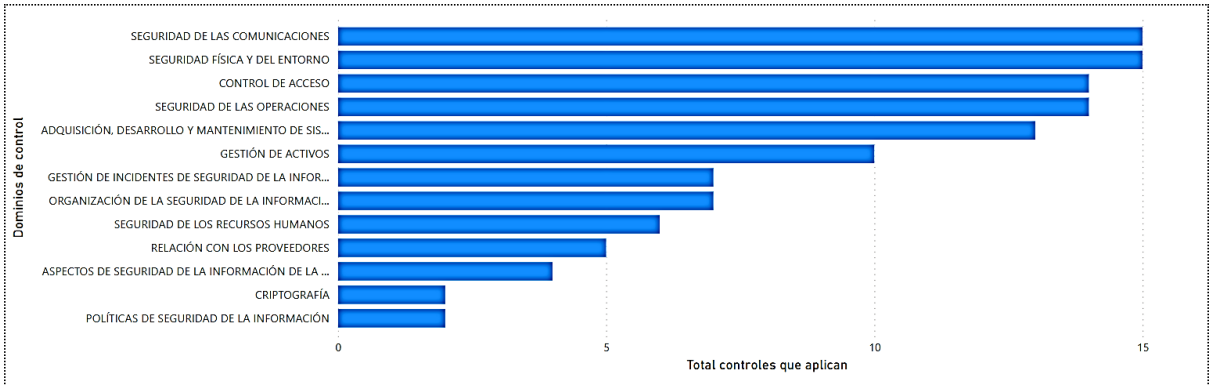


Figura 12: *Total de controles aplicados por dominio*

Fuente: *Elaboración Propia*

Los dominios en los cuales se han identificado controles parcialmente implementados son los siguientes, junto con el número de controles parcialmente implementados en cada uno:

Seguridad de las operaciones (8 controles parcialmente implementados):

- Este dominio destaca por la mayor incidencia de controles parcialmente implementados, indicando áreas que requieren mejoras específicas en las prácticas de seguridad operativa.

Control de acceso (10 controles parcialmente implementados):

- El dominio de Control de Acceso también muestra una alta incidencia de controles parcialmente implementados, resaltando la necesidad de fortalecer la gestión de acceso para garantizar la seguridad de la información.

Adquisición, desarrollo y mantenimiento de sistemas (8 controles parcialmente implementados):

- Se observa una incidencia moderada en este dominio, señalando áreas específicas que requieren atención para mejorar la seguridad durante la adquisición, desarrollo y mantenimiento de sistemas.

Gestión de incidentes de seguridad de la información (3 controles parcialmente implementados):

- Aunque la incidencia es menor en comparación con otros dominios, se destaca la necesidad de mejorar la gestión de incidentes para garantizar una respuesta efectiva.

Organización de la seguridad de la información (5,5 controles parcialmente implementados):

- Aunque la incidencia es moderada, este dominio indica áreas que podrían beneficiarse de mejoras en la organización de la seguridad de la información.

Seguridad de las comunicaciones (4 controles parcialmente implementados):

- Existe una incidencia moderada, indicando áreas específicas que necesitan atención para fortalecer las prácticas de seguridad en las comunicaciones.

Este análisis resalta los dominios que presentan controles parcialmente implementados, señalando áreas críticas que requieren atención inmediata para mejorar la eficacia del SGSI.

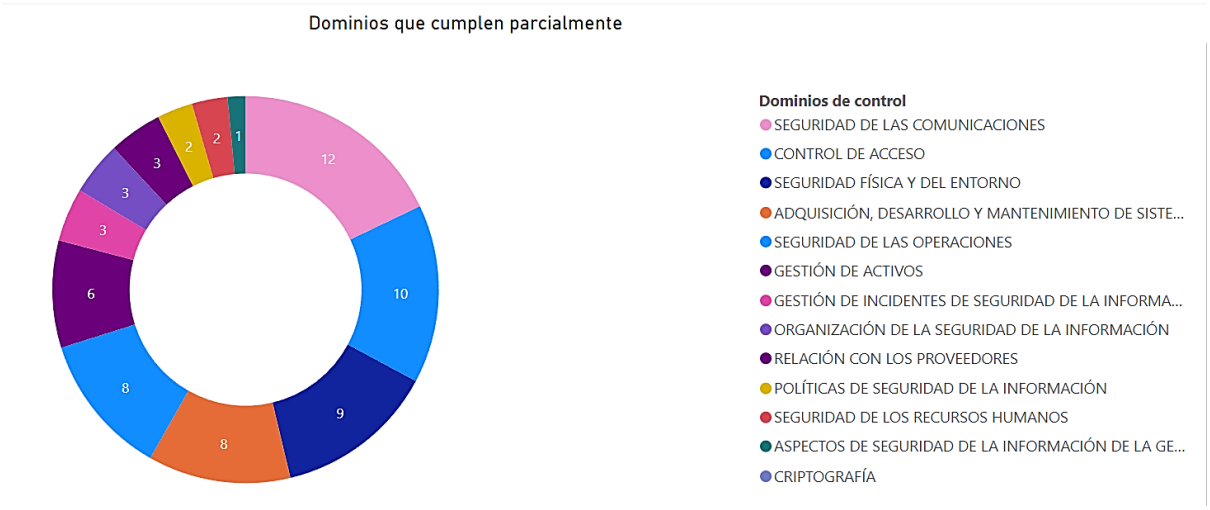


Figura 13: *Total de dominios que se cumplen parcialmente*

Fuente: *Elaboración Propia*

Modelo propuesto para la Metodológico para la Implementación de Seguridad de la Información en Empresas Privadas

Paso 1. Comprensión del Contexto Empresarial

1.1 Diagnóstico Preliminar:

- **Identificación de la estructura organizativa:** La primera fase del diagnóstico preliminar se centra en una minuciosa identificación de la estructura organizativa de la empresa. Este proceso implica el mapeo detallado de departamentos, unidades, y roles dentro de la organización. Se busca comprender la jerarquía, las relaciones de autoridad y responsabilidad, así como la distribución funcional de las áreas. Este análisis proporcionará una visión integral de la dinámica organizacional, permitiendo identificar posibles puntos de acceso a la información sensible y establecer claramente los responsables de la seguridad de la información en cada nivel. Esta comprensión profunda de la estructura organizativa es esencial para desarrollar estrategias y políticas de seguridad que se integren de manera efectiva en el entramado operativo de la empresa.
- **Análisis de la infraestructura tecnológica existente:** En esta etapa, se procede al examen minucioso de la infraestructura tecnológica preexistente en la empresa. Esto implica la identificación de sistemas operativos, plataformas, aplicaciones y servicios utilizados en la gestión diaria. Además, se evalúan las configuraciones de red, la topología tecnológica y las medidas de seguridad implementadas hasta el momento. Este análisis de la infraestructura tecnológica arrojará luz sobre posibles puntos de vulnerabilidad, redundancias y áreas que requieren actualización. Al comprender la base tecnológica actual, se sientan las bases para la posterior implementación de medidas específicas que fortalezcan la seguridad de la información, garantizando así la compatibilidad de las soluciones propuestas con la infraestructura existente.
- **Evaluación de los activos de información críticos:** La evaluación de activos de información críticos constituye un paso crucial en la identificación de los recursos más valiosos para la organización. Se clasifican y se analizan los

datos y activos que poseen un valor estratégico o sensible. Este proceso implica determinar la confidencialidad, integridad y disponibilidad de la información, así como identificar su relevancia para los procesos operativos. Al comprender qué activos de información son más críticos para la empresa, se puede priorizar la aplicación de medidas de seguridad adecuadas. Además, esta evaluación sirve como base para la posterior clasificación de la información y el establecimiento de niveles de protección acorde con la importancia de cada activo para el funcionamiento de la organización.

1.2 Identificación de Amenazas y Vulnerabilidades:

- **Análisis de posibles amenazas cibernéticas:** En esta fase, se lleva a cabo un análisis exhaustivo de las posibles amenazas cibernéticas que podrían afectar la seguridad de la información en el entorno empresarial. Esto implica la identificación de amenazas comunes, como malware, ataques de phishing, ingeniería social, entre otros. Se examina la naturaleza de estas amenazas, su prevalencia en el sector y su potencial impacto en los activos de información críticos. Este análisis proactivo permite a la organización anticipar posibles escenarios de riesgo y diseñar estrategias preventivas para mitigar amenazas potenciales, contribuyendo así a fortalecer la postura de seguridad cibernética de la empresa.
- **Evaluación de vulnerabilidades específicas del entorno empresarial:** En esta etapa, se realiza una evaluación minuciosa de las vulnerabilidades específicas presentes en el entorno empresarial. Esto incluye la revisión de configuraciones de red, sistemas operativos, aplicaciones y servicios utilizados. Se lleva a cabo un análisis de vulnerabilidades conocidas y potenciales, considerando la actualización de software, la configuración segura y las mejores prácticas de seguridad. Esta evaluación identifica las debilidades existentes que podrían ser explotadas por amenazas cibernéticas, proporcionando así información esencial para el desarrollo de estrategias de mitigación específicas y la aplicación de medidas correctivas que refuercen la resiliencia del entorno tecnológico de la empresa.
- **Valoración del nivel de exposición a riesgos: según el análisis de amenazas y vulnerabilidades, se valora el nivel de exposición a riesgos.**

Este proceso implica asignar una ponderación a las amenazas identificadas y evaluar la probabilidad de su materialización y el impacto potencial en los activos de información. La combinación de estos factores permite cuantificar el riesgo y determinar áreas críticas que requieren una atención inmediata. Esta valoración proporciona a la empresa una visión clara de sus puntos débiles y la ayuda a priorizar recursos y esfuerzos para implementar medidas de seguridad de manera efectiva, minimizando así la exposición a riesgos cibernéticos.

Paso 2. Fase de Adaptación del EGSI al Contexto Empresarial

2.1 Revisión de Principios del EGSI:

- **Análisis detallado de los principios del Esquema Gubernamental de Seguridad de la Información:** En esta fase, se lleva a cabo un análisis exhaustivo de los principios establecidos en el EGSI. Se examinan detalladamente los pilares fundamentales de esta normativa gubernamental, que abarcan desde la clasificación de información hasta la gestión de incidentes. Se busca comprender la esencia de cada principio, los objetivos que persiguen y la relación entre ellos. Este análisis detallado no solo proporciona una visión profunda de las directrices gubernamentales, sino que también sienta las bases para su posterior adaptación y aplicación en el contexto empresarial. Cada principio se desglosa para comprender su aplicabilidad y relevancia en la protección de los activos de información, permitiendo una integración más efectiva en el marco metodológico diseñado.
- **Identificación de elementos aplicables y ajustes necesarios para empresas privadas:** En esta etapa, se procede a la identificación de elementos específicos del EGSI que son directamente aplicables al ámbito empresarial. Se evalúa la relevancia de cada principio en el contexto de las empresas privadas, considerando sus particularidades y necesidades. Además, se lleva a cabo un análisis crítico para determinar los posibles ajustes necesarios para garantizar la efectividad y aplicabilidad en el entorno empresarial. Este proceso de adaptación implica considerar las diferencias operativas, estructurales y de riesgo entre el sector gubernamental y el privado.

La meta es integrar los principios del EGSI de manera coherente, respetando su esencia, pero ajustándolos estratégicamente para asegurar su funcionalidad y relevancia en la gestión de la seguridad de la información en empresas privadas.

2.2 Clasificación de la Información Empresarial:

- **Desarrollo de un sistema de clasificación de datos específico para la empresa:** En esta fase, se procede al desarrollo de un sistema de clasificación de datos que se ajuste a las necesidades y particularidades de la empresa. Esto implica identificar las categorías de información existentes, asignar niveles de sensibilidad y establecer criterios claros para la clasificación. Se consideran factores como la criticidad de la información, su valor estratégico y el impacto potencial en caso de acceso no autorizado. Al definir este sistema de clasificación personalizado, se facilita la aplicación de medidas de seguridad proporcionales a la importancia de cada tipo de información. Este enfoque contribuye a una gestión más eficiente y focalizada de los recursos de seguridad, optimizando la protección de los datos críticos de la empresa.
- **Definición de niveles de confidencialidad, integridad y disponibilidad:** Como parte del proceso de clasificación, se procede a definir claramente los niveles de confidencialidad, integridad y disponibilidad de la información empresarial. Cada nivel se adapta a la naturaleza de los datos y a los requisitos operativos de la empresa. La confidencialidad establece quién puede acceder a la información, la integridad asegura la precisión y confiabilidad de los datos, y la disponibilidad garantiza que la información esté accesible cuando sea necesario. Estos niveles son esenciales para la posterior implementación de controles de seguridad, ya que permiten una asignación adecuada de recursos para proteger y preservar la información crítica de la empresa.

2.3 Definición de Políticas y Procedimientos:

- **Creación de políticas de seguridad de la información adaptadas a la realidad empresarial:** En esta fase, se procede a la creación de políticas de seguridad de la información que se alineen con la realidad operativa y los objetivos estratégicos de la empresa. Estas políticas abarcan desde la gestión

de contraseñas hasta la gestión de incidentes, asegurando que cada directriz sea clara, específica y aplicable a las operaciones diarias. Se consideran las características únicas de la empresa, sus activos de información críticos y las regulaciones sectoriales pertinentes. La creación de políticas adaptadas contribuye a la construcción de una cultura de seguridad interna, donde los empleados comprenden y adoptan las prácticas necesarias para preservar la confidencialidad e integridad de la información.

- **Establecimiento de procedimientos operativos estándar:** Junto con la creación de políticas, se establecen procedimientos operativos estándar que detallan cómo implementar y seguir cada política. Estos procedimientos ofrecen un enfoque sistemático para abordar situaciones específicas, desde la gestión de accesos hasta la respuesta a incidentes. Al establecer estos procedimientos, se proporciona una guía práctica para el personal, asegurando la consistencia en la aplicación de las políticas y facilitando la respuesta efectiva ante posibles amenazas o incidentes de seguridad. La combinación de políticas bien definidas y procedimientos operativos estandarizados sienta las bases para una implementación efectiva y coherente de las medidas de seguridad de la información en toda la organización.

Paso 3. Fase de Implementación y Despliegue del Marco Metodológico

3.1 Planificación de Implementación:

- **Elaboración de un plan detallado de implementación, considerando fases graduales:** En esta etapa, se desarrolla un plan de implementación meticuloso que guiará la integración de la metodología en la empresa. El plan se estructura en fases graduales para facilitar una adopción progresiva y efectiva. Cada fase se define claramente, especificando los objetivos, actividades y plazos correspondientes. Se consideran cuidadosamente las interdependencias entre las diferentes etapas para garantizar una transición fluida. La planificación detallada también incluye la identificación y asignación de recursos críticos, tanto humanos como tecnológicos, y la asignación de responsabilidades a equipos específicos. Este enfoque estratégico facilita la gestión efectiva de la

implementación, asegurando que cada paso contribuya al logro de los objetivos generales de seguridad de la información.

- **Asignación de recursos y responsabilidades:** En el proceso de implementación, se asignan los recursos necesarios para garantizar el éxito de cada fase del plan. Esto implica la asignación de personal, tecnologías, presupuesto y cualquier otro recurso relevante para la ejecución de las medidas de seguridad. Además, se definen claramente las responsabilidades de cada miembro del equipo, asegurando una distribución equitativa y eficiente de tareas. La asignación de recursos y responsabilidades se realiza en función de las habilidades y capacidades individuales, aprovechando al máximo los talentos dentro de la organización. Este enfoque garantiza que todos los aspectos de la implementación estén respaldados por los recursos adecuados y que exista una claridad total sobre quién es responsable de cada tarea.

3.2 Desarrollo de Capacidades Internas:

- **Capacitación del personal en las nuevas políticas y procedimientos:** Una parte integral de la implementación es el desarrollo de las capacidades internas del personal. Se lleva a cabo una capacitación exhaustiva sobre las nuevas políticas de seguridad de la información y los procedimientos operativos estandarizados. Esta formación no solo se centra en la comprensión teórica, sino también en la aplicación práctica de las medidas de seguridad. Los empleados son capacitados en el uso de herramientas de seguridad, reconocimiento de posibles amenazas y la correcta respuesta ante incidentes. La capacitación contribuye a la creación de una cultura de seguridad sólida, donde cada miembro del personal se convierte en un defensor activo de la protección de la información.
- **Sensibilización sobre la importancia de la seguridad de la información:** Junto con la capacitación técnica, se realiza un esfuerzo significativo en la sensibilización del personal sobre la importancia de la seguridad de la información. Este componente busca crear conciencia sobre las amenazas cibernéticas, los riesgos asociados y la contribución individual en la protección de la información de la empresa. Se implementan campañas de sensibilización,

se ofrecen seminarios y se fomenta la participación activa de los empleados en la seguridad informática. La sensibilización no solo fortalece el conocimiento del personal sobre las mejores prácticas de seguridad, sino que también crea una cultura proactiva en la que cada individuo comprende su papel en la preservación de la integridad y confidencialidad de la información.

3.3 Integración de Tecnologías de Seguridad:

- **Evaluación e implementación de herramientas tecnológicas de seguridad: En esta fase crítica, se evalúan las tecnológicas disponibles en el mercado para determinar cuáles son más apropiadas para las necesidades específicas de la empresa.** Se analizan soluciones como antivirus, sistemas de prevención de pérdida de datos (DLP), cifrado de datos y otras tecnologías relevantes. La selección se realiza en base a criterios de eficacia, compatibilidad con la infraestructura existente y capacidad para abordar amenazas identificadas durante el análisis de vulnerabilidades. Posteriormente, se implementan estas herramientas, asegurando una integración sin inconvenientes con los sistemas preexistentes y garantizando su capacidad para proporcionar una capa robusta de defensa contra amenazas cibernéticas.
- **Configuración de firewalls, sistemas de detección de intrusiones y sistemas de gestión de identidades: para implementar medidas de seguridad, se configuran con precisión los firewalls, sistemas de detección de intrusiones (IDS) y sistemas de gestión de identidades (IAM).** Los firewalls se configuran para controlar el tráfico de red, garantizando la protección contra accesos no autorizados. Los sistemas de detección de intrusiones se ajustan para monitorear de manera proactiva las actividades en la red y responder rápidamente a posibles amenazas. Además, los sistemas de gestión de identidades se implementan para administrar de manera eficiente los accesos de los usuarios, garantizando que cada individuo tenga permisos apropiados y se sigan las políticas de seguridad establecidas. La configuración precisa de estas tecnologías constituye una barrera esencial contra ataques cibernéticos, asegurando la integridad y confidencialidad de la información empresarial.

Paso 4. Fase de Evaluación y Mejora Continua

4.1 Auditorías de Seguridad:

- **Realización de auditorías periódicas para evaluar la efectividad del marco metodológico: En esta fase crucial, se realizan auditorías de seguridad regularmente para evaluarlas del marco metodológico implementado.** Estas auditorías se diseñan para examinar la adhesión a las políticas de seguridad, la eficacia de los controles implementados y la detección de posibles brechas en la seguridad. A través de este proceso, se identifican áreas de mejora y se evalúan las medidas existentes para garantizar su relevancia continua. Los hallazgos de la auditoría proporcionan información valiosa para la toma de decisiones estratégicas, permitiendo la corrección proactiva de posibles desviaciones y la optimización constante del marco metodológico para mantener la máxima seguridad de la información.
- **Identificación de áreas de mejora y corrección de posibles desviaciones: Como resultado de las auditorías, se identifican las áreas de mejora y se corrigen posibles desviaciones detectadas al implementar el marco metodológico.** Este proceso implica una revisión crítica de los resultados de la auditoría, priorizando las áreas que requieren atención inmediata y ajustes. Las correcciones se realizan con la participación activa de los responsables del marco de seguridad y otros interesados, garantizando una respuesta ágil y efectiva. La identificación y corrección proactiva de desviaciones asegura que el marco metodológico se mantenga alineado con los objetivos de seguridad, proporcionando una base sólida para la gestión continua de la seguridad de la información.

4.2 Gestión de Incidentes:

- **Implementación de un sistema de gestión de incidentes:** En esta fase, se establece un sistema integral de gestión de incidentes para abordar de manera efectiva eventos de seguridad adversos. El sistema comprende protocolos claros para la identificación, notificación, análisis y respuesta a incidentes de seguridad. Se designan roles y responsabilidades específicos dentro del equipo de gestión de incidentes, garantizando una respuesta coordinada y

eficiente. Los protocolos también incluyen medidas de recuperación para minimizar el impacto y restaurar la normalidad operativa. La implementación de este sistema proporciona una estructura sólida para abordar y mitigar incidentes de seguridad de manera oportuna, reduciendo al mínimo el impacto potencial en la empresa.

- **Establecimiento de protocolos de respuesta y recuperación:** Junto con la implementación del sistema de gestión de incidentes, se establecen protocolos detallados para guiar la respuesta y recuperación ante incidentes de seguridad. Estos protocolos incluyen pasos específicos a seguir, roles y responsabilidades claramente definidos, y criterios para evaluar el impacto y la gravedad de un incidente. Se garantiza una comunicación efectiva durante todo el proceso, tanto interna como externamente según sea necesario. Establecer protocolos sólidos no solo facilita una respuesta rápida y coordinada, sino que también contribuye a la mejora continua del marco metodológico al aprender de cada incidente y ajustar las estrategias de seguridad en consecuencia.

4.3 Actualización Periódica:

- **Para garantizar la vigencia y efectividad continua del marco metodológico, se hace una revisión periódica en respuesta a cambios en el entorno empresarial y la evolución de las amenazas cibernéticas.** Se monitorean constantemente las tendencias del sector, las nuevas tecnologías y las regulaciones pertinentes. Cualquier cambio significativo en el entorno operativo o nuevas amenazas identificadas se abordan mediante la actualización o ajuste del marco metodológico. Este enfoque proactivo asegura que la empresa esté preparada para enfrentar los desafíos emergentes y mantiene la relevancia de las medidas de seguridad implementadas en el marco de la protección de la información empresarial.

Paso 5. Fase de Documentación y Comunicación

5.1 Documentación Detallada:

- **Elaboración de manuales y documentación detallada del marco metodológico:** La elaboración de manuales y documentación detallada del

marco metodológico es un componente esencial para garantizar la comprensión y aplicación efectiva de las políticas de seguridad de la información en la organización. Estos documentos actúan como guías completas que ofrecen detalles específicos sobre la implementación de medidas de seguridad, procedimientos operativos y protocolos de actuación. Cada componente del marco metodológico se documenta de manera exhaustiva, proporcionando información clara sobre roles y responsabilidades, procesos de gestión de riesgos, y pasos a seguir en situaciones de seguridad. Esta documentación no solo sirve como recurso de referencia para el personal, sino que también facilita la coherencia en la aplicación de las políticas y medidas de seguridad en toda la organización.

- **Creación de materiales educativos para el personal:** La creación de materiales educativos adaptados al personal es fundamental para promover la comprensión y adhesión a las políticas de seguridad de la información. Estos materiales van más allá de los manuales formales y pueden incluir presentaciones interactivas, videos informativos y sesiones de capacitación. Los materiales educativos se diseñan con un enfoque pedagógico, asegurando que el personal no solo comprenda las políticas, sino también la importancia de su papel en la protección de la información. Se utilizan ejemplos prácticos y escenarios relevantes para garantizar una aplicación efectiva de las medidas de seguridad. Estos materiales educativos son herramientas valiosas para fomentar una cultura de seguridad proactiva y facilitar el aprendizaje continuo en temas relacionados con la seguridad de la información.

5.2 Comunicación Interna y Externa:

Desarrollo de estrategias de comunicación para informar a los empleados sobre las nuevas políticas: Para asegurar la efectividad de las nuevas políticas de seguridad, se desarrollan estrategias de comunicación interna dirigidas a informar y educar a los empleados sobre los cambios y expectativas. Estas estrategias incluyen la creación de mensajes claros y accesibles que destaquen la importancia de la seguridad de la información, los beneficios para la organización y el papel crucial que desempeña cada miembro del personal en la protección de los activos de información. Se utilizan diversos canales de

comunicación, como correos electrónicos, intranet, reuniones y sesiones de capacitación, para garantizar una amplia comprensión y aceptación de las nuevas políticas de seguridad entre los empleados.

Establecimiento de canales de comunicación con partes interesadas externas: Además de la comunicación interna, se establecen canales de comunicación efectivos con partes interesadas externas, como clientes, proveedores y otras entidades relevantes. Estos canales se diseñan para informar sobre las medidas de seguridad implementadas, reforzar el compromiso de la empresa con la protección de la información y proporcionar garantías de seguridad a las partes externas. La transparencia y la comunicación efectiva contribuyen a construir y mantener la confianza con las partes interesadas externas, asegurando que estén informadas y tranquilas acerca de las medidas adoptadas para salvaguardar la información y proteger sus intereses.

La metodología concebida, en concordancia con el análisis exhaustivo y los resultados obtenidos, emerge como una herramienta estratégica y efectiva para la gestión de la seguridad de la información en entidades empresariales. Basada en el Esquema Gubernamental de Seguridad de la Información versión 2 (EGSI v2) y alineada con la norma ISO 27001:2013, esta metodología fusiona la solidez normativa gubernamental con estándares internacionales reconocidos. Su flexibilidad y adaptabilidad la posicionan como un recurso valioso para empresas tanto del sector privado como público. Al ser diseñada con la premisa de ajustarse fácilmente a diversas necesidades, el marco metodológico se erige como un instrumento dinámico, capaz de ser moldeado según los requisitos específicos de cada organización. Su aplicabilidad abarca desde pequeñas empresas hasta grandes corporativos, consolidándose como una guía estructurada que trasciende los límites sectoriales. Con esta metodología, se busca proporcionar a las organizaciones una herramienta práctica y holística que promueva la seguridad de la información como una piedra angular para el éxito operativo y la preservación de la confianza de los stakeholders.

Análisis de riesgos

El análisis de riesgos presentado se basa en evaluar la probabilidad de ocurrencia de diversos factores de riesgo y el nivel de impacto que estos podrían tener en la organización. La tabla proporciona una clasificación de los riesgos según su nivel (Alto, Medio, Bajo), su frecuencia de ocurrencia (Siempre, A veces, Nunca) y calcula el riesgo resultante como el producto de estas dos variables. A continuación, se ofrece un análisis detallado de los resultados:

Tabla 12: *Factores de riesgo*

	Factores de riesgo	**Nivel de riesgo**	**X**	**Frecuencia de ocurrencia**	**Y**	**Riesgo = X * Y**
1	Hackeo	Alto	3	Siempre	3	9
2	Control de software operacional	Alto	3	A veces	2	6
3	Protección de los datos usados para prueba	Medio	2	Siempre	3	6
4	Divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios	Medio	2	A veces	2	4
5	Pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Medio	2	A veces	2	4
6	Suplantación de identidad	Medio	2	Nunca	1	2
7	Daño a los equipos informáticos	Medio	2	Nunca	1	2
8	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores	Medio	2	Nunca	1	2
9	Acceso físico no autorizado	Medio	2	Nunca	1	2
10	Acceso a información y a instalaciones de procesamiento de información.	Medio	2	Nunca	1	2
11	Cortes de luz	Bajo	1	Nunca	1	1
12	Pérdida de datos	Bajo	1	Nunca	1	1
13	Incendio	Bajo	1	Nunca	1	1

Tabla 12: (Cont.)

	Factores de riesgo	Nivel de riesgo	X	Frecuencia de ocurrencia	Y	Riesgo = X * Y
14	Desastres naturales	Bajo	1	Nunca	1	1

Fuente: *Elaboración Propia*

Resultados obtenidos

A continuación, se describe cada uno de los riesgos más críticos, donde se considera críticos a los que obtiene un valor mayor o igual a 4.

Hackeo: Con un nivel de riesgo alto y una frecuencia de ocurrencia constante ("Siempre"), el hackeo se identifica como el riesgo más crítico con una puntuación de 9. Esto indica una necesidad urgente de medidas robustas de seguridad cibernética para mitigar este riesgo.

Control de software operacional y Protección de los datos usados para prueba: Ambos con un riesgo calculado de 6, pero con diferentes frecuencias de ocurrencia. Mientras que el control de software operacional ocurre "A veces", la protección de datos para prueba es un riesgo constante. Esto sugiere la importancia de implementar prácticas de seguridad tanto en el uso cotidiano del software como en los entornos de prueba.

Divulgación, modificación, retiro o destrucción no autorizados de información y Pérdida, daño, robo o compromiso de activos: Estos riesgos tienen una puntuación de 4, indicando un nivel medio de riesgo con una ocurrencia "A veces". Resaltan la necesidad de controles efectivos sobre la información y los activos físicos.

Suplantación de identidad, Daño a los equipos informáticos, Protección de activos accesibles a proveedores, Acceso físico no autorizado, y Acceso a información y a instalaciones de procesamiento de información: Todos con una puntuación de 2, reflejan riesgos medios que actualmente tienen una baja frecuencia

de ocurrencia ("Nunca"). Sin embargo, aún requieren atención para evitar que aumenten su frecuencia o impacto.

Cortes de luz, Pérdida de datos, Incendio, y Desastres naturales: Estos representan los riesgos con la puntuación más baja (1), clasificados como de nivel bajo y con una ocurrencia "Nunca". Aunque son menos prioritarios, es esencial no descuidar la preparación frente a estos riesgos, ya que sus impactos podrían ser significativos.

Una vez tenemos los datos mapeados se procede a ordenarlos de mayor a menor para así obtener un diagrama de dispersión de los factores con mayor incidencia sobre la escala de evaluación que parte del 1 al 3 con una frecuencia final obtenido de la multiplicación del riesgo con su frecuencia la cual se evaluará los factores de riesgo que tengan un valor similar o mayor a 4.

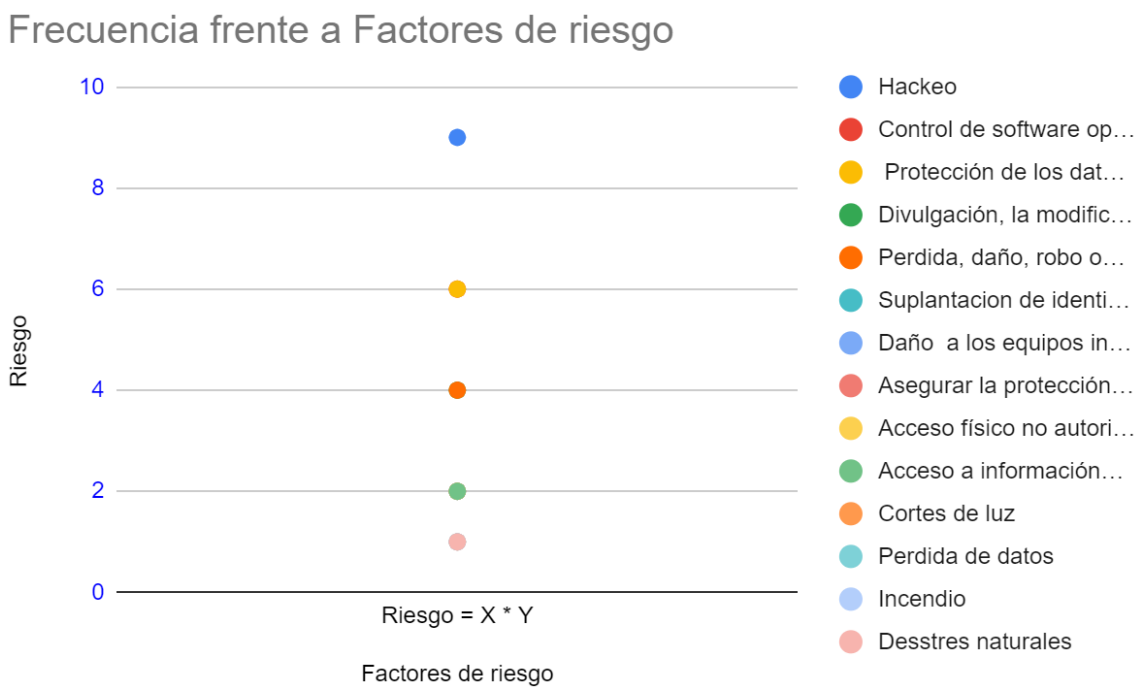


Figura 14: *Evaluación de frecuencia de factores de riesgo*

Fuente: *Elaboración Propia*

En el gráfico anterior se pudo evidenciar diversos factores los cuales tienen un mayor grado de afectación a la seguridad de la información dentro y fuera de la empresa, las acciones a realizar por cada factor de riesgo son las siguientes:

Hackeo

- **Acción 1:** Implementar medidas avanzadas de seguridad informática, como firewalls robustos, sistemas de detección de intrusiones y actualizaciones regulares de software para proteger contra ataques cibernéticos.
- **Acción 2:** Realizar auditorías de seguridad periódicas y pruebas de penetración para identificar vulnerabilidades y asegurar que los sistemas estén actualizados y protegidos.

Control de software operacional: Realizar inspecciones y revisiones manuales, modelado de amenazas, revisión de código y pruebas de intrusión

Protección de los datos usados para prueba: Establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios

Divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios: Implementar medidas de seguridad como políticas, procedimientos para incidentes (prevención, detección, respuesta y recuperación), concientización y colaboración

Pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización: Implementar medidas de seguridad como análisis de datos en herramientas, controles o procesos de seguridad digital, políticas, procedimientos para incidentes (prevención, detección, respuesta y recuperación), concientización y colaboración. Además, se pueden identificar y evaluar cada uno de los riesgos que posee la organización en la actualidad y mejorar las políticas de seguridad informática

De acuerdo a las diversas acciones a realizar para mitigar los riesgos dentro de la organización de acuerdo al análisis previamente realizado se ha optado por realizar las siguientes acciones realizadas por nuestra mano:

- Documentar procesos de análisis, diseño, desarrollo, pruebas y despliegue de proyectos de desarrollo de software
- Realizar un acta de los pasos a seguir para brindar una capacitación de seguridad de la información de acuerdo al EGSI a todos los empleados

Las acciones realizadas por parte de la empresa son las siguientes:

- Controles de seguridad para la utilización de los activos de la empresa
- Medición de desempeño de los empleados

Los controles que parten de la herramienta utilizada que han sido resueltos con el uso de las acciones mencionadas con anterioridad son los siguientes:

Logro 1:

13. La entidad ha evaluado las competencias de las personas que realizan, bajo su control, ¿un trabajo que afecta el desempeño de la seguridad de la Información?

Logro 2:

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

A12.1.1 Procedimientos de operación documentados

A12.7.1 Controles de auditorías de sistemas de información

A18.2.1 Revisión independiente de la seguridad de la información

A9.4.4 Procedimiento de ingreso seguro

A10.1.1 Política sobre el uso de controles criptográficos

A10.1.2 Gestión de llaves

A12.5.1 Instalación de software en sistemas operativos

A12.6.2 Restricciones sobre la instalación de software

Logro 3:

2. La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?

3. La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?

Los controles en los cuales se han realizados las diversas acciones planteadas dan apertura a que en la empresa se procure la seguridad de la información en diversos aspectos, los cuales la preparan para futuras auditorías internas y externas que se llegaran a realizar por parte de la organización.

Estas acciones realizadas por parte de ambos colaboradores han logrado incrementar en un 4,6% los esquemas de seguridad dentro de la organización lo cual lo podemos evidenciar en la siguiente tabla:

Tabla 13: *Incremento de seguridad de la información*

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	18,8%
LOGRO2	HACER	40%	26,5%
LOGRO3	VERIFICAR	15%	7,5%
	ACTUAR	15%	2,5%
	TOTAL	100%	55,3%

Fuente: *Elaboración Propia*

Con estos primeros pasos realizados dentro de la organización damos entrada a futuras aplicaciones del EGSI y de auditorías las cuales permitirán mitigar y afianzar la seguridad dentro de la información dentro de la organización.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Basándose en los resultados obtenidos durante el proceso de investigación, se presentarán las siguientes conclusiones y recomendaciones en correspondencia con los objetivos planteados.

Conclusiones

El trabajo de investigación ha logrado diseñar un marco metodológico basado en el EGSI para su implementación en empresas privadas. La exhaustiva revisión bibliográfica sobre el contenido del EGSI vigente en Ecuador proporcionó los cimientos necesarios para comprender a fondo las directrices gubernamentales en materia de seguridad de la información. Además, el análisis de las prácticas exitosas tanto a nivel nacional como internacional permitió identificar elementos transferibles al ámbito empresarial, enriqueciendo así el proceso de diseño metodológico.

La evaluación de las necesidades de seguridad de la información en empresas privadas ha sido fundamental para adaptar el enfoque del EGSI a las particularidades de cada entidad, considerando la diversidad de datos, modelos de negocio y amenazas cibernéticas a las que se enfrentan. Como resultado, el marco metodológico desarrollado no solo refleja los principios fundamentales del EGSI, sino que también se ha adaptado de manera flexible para garantizar su aplicabilidad efectiva en el contexto empresarial.

Este logro no solo contribuye al ámbito académico, sino que también ofrece una herramienta valiosa para el fortalecimiento de la seguridad de la información en el sector privado. La metodología propuesta proporciona una guía detallada y práctica para la implementación de medidas efectivas de seguridad, consolidando así una respuesta proactiva y robusta frente a las crecientes amenazas cibernéticas en el entorno empresarial. En última instancia, este trabajo sienta las bases para la promoción de una cultura de seguridad informática en el sector privado, alineada con las mejores prácticas y estándares gubernamentales, contribuyendo a la protección

de la información sensible y la resiliencia de las organizaciones frente a posibles riesgos y ataques.

Con respecto al primer objetivo específico del presente trabajo se ha logrado una comprensión profunda del EGSI en Ecuador mediante el análisis bibliográfico. Este conocimiento es fundamental para entender las directrices y normativas actuales que rigen la seguridad de la información a nivel gubernamental.

En cuanto a la revisión de las prácticas exitosas de implementación del EGSI en Ecuador y en otras jurisdicciones ha proporcionado valiosas lecciones aprendidas y estrategias efectivas, que permiten identificar aspectos transferibles al ámbito empresarial ayudando a que la aplicación de los principios de seguridad de la información sea más efectiva.

Con respecto al tercer objetivo la evaluación de las necesidades de seguridad de la información en empresas privadas ha permitido comprender las particularidades de las entidades en términos de datos, modelos de negocio y amenazas cibernéticas. La adaptación eficiente de la metodología basada en EGSI a estas necesidades específicas es esencial para garantizar su aplicabilidad práctica y su capacidad para abordar las amenazas de manera efectiva. Al considerar estas particularidades, el marco metodológico resultante se convierte en una herramienta personalizada y dinámica que se ajusta a las demandas cambiantes del entorno empresarial.

Por último, se ha logrado desarrollar un marco metodológico detallado que incorpora principios del Esquema Gubernamental de Seguridad de la Información, adaptados a las características específicas de las empresas privadas. Este marco no solo se limita a una simple adaptación superficial, sino que se sumerge en la comprensión profunda de las dinámicas empresariales, asegurando así su relevancia y eficacia. Al incorporar principios fundamentales del EGSI, como la clasificación de la información, control de accesos y gestión de incidentes, adaptados a las características específicas del sector privado, se ha creado una guía estructurada y flexible. Este marco no solo establece directrices claras para la implementación de medidas de seguridad, sino que también incorpora elementos escalables y adaptables para garantizar su utilidad a medida que evolucionan las tecnologías y las amenazas. La resultante combinación de robustez gubernamental y flexibilidad empresarial convierte a este marco en una herramienta

integral para la gestión proactiva de la seguridad de la información en empresas privadas.

Recomendaciones

- Se sugiere adaptar la metodología basada en el EGSI para satisfacer las necesidades y características específicas de las empresas. Esto incluirá ajustar los controles de seguridad, políticas y procedimientos según los activos de información y el nivel de riesgo de software.
- Se recomienda el total apoyo y compromiso de la alta dirección de la empresa para garantizar el éxito de la implementación. Esto incluirá la asignación de recursos adecuados y la designación de responsables para liderar la gestión de la seguridad de la información.
- Se sugiere realizar evaluaciones periódicas de la efectividad de la metodología y su adecuación a los cambios en el entorno de riesgo. Estas evaluaciones permitirán identificar áreas de mejora y realizar ajustes necesarios para mantener la seguridad de la información en constante evolución.
- Es importante reconocer las limitaciones de este estudio, que incluyen la disponibilidad limitada de recursos y el tiempo acotado para la implementación. Además, debido a la naturaleza específica de la empresa TOC Systems, los resultados y recomendaciones pueden no ser completamente generalizables a otras organizaciones
- Se recomienda establecer canales de colaboración con entidades gubernamentales responsables del EGSI para garantizar la alineación continua entre las normativas gubernamentales y las prácticas de seguridad implementadas en el ámbito empresarial. La colaboración activa en la revisión y actualización periódica de las normativas garantizará que la metodología diseñada permanezca actualizada y efectiva frente a las amenazas emergentes. Además, esta asociación estratégica proporcionará un marco para compartir las lecciones aprendidas, las mejores prácticas y los hallazgos relevantes entre el sector público y privado, fomentando así una cultura de seguridad de la información más robusta y resiliente en el panorama gene

Bibliografía

AMBIT - *BST*. (2021, May). *AMBIT - BST*. Recuperado el 20 de Junio de 2020, de *https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases*

Aplicabilidad de la norma ISO 27001 en los problemas más frecuentes. (2019, diciembre). *ISOTools*. Recuperado el 07 de Junio de 2023, de https://www.isotools.us/2018/12/17/aplicabilidad-norma-iso-27001-problemas-comunes-empresas/

Certificación ISO 27001 - *Consultoría para la ISO 27001*. (2020). Innevo. Recuperado el 07 de Junio de 2023, de https://info.innevo.com/es-mx/obtenga-la-certificacion-iso27001

Cuervo, J. (2021, febrero). *Acuerdo Ministerial nº 166. Esquema Gubernamental de Seguridad de la Información EGSI*. Informática Jurídica. Recuperado el 03 de Julio de 2023, de https://www.informatica-juridica.com/acuerdo/acuerdo-ministerial-no-166-esquema-gubernamental-de-seguridad-de-la-informacion-egsi-de-19-de-septiembre-de-2013/

EGSI. (2020, enero). *Edición especial sumario*: Recuperado el 07 de Junio de 2023, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

EGSI. (2023, julio). *EGSI*. Recuperado el 03 de Julio de 2023, de https://www.proquest.com/openview/f4b193b46ccb16a251428b15a52d084a/1?pq-origsite=gscholar&cbl=1006393

López, F. (2019), *Autodiagnóstico SGSI. Bogotá D.C., Colombia.* Implementación de una Metodología para Gestión de Riesgos de Información basada en las normas ISO/IEC 27001 y 27002.

Pérez, J., & Gómez, L. (2022). Evaluación de Instrumentos de Medición en Investigación Científica.

Hernández, R., Fernández, C., & Baptista, P. (2020). Metodología de la investigación. McGraw-Hill Education.

Rodríguez, M., & García, L. (2020). "Improving Information Security Awareness: Strategies and Best Practices". Journal of Cybersecurity Education

Smith, J. (2021). "Understanding Cyber Attacks: Threats and Solutions". International Journal of Cybersecurity.

García, A., & López, M. (2020). "Physical Security Threats to Information Systems: A Case Study Analysis". Journal of Cybersecurity Management.

Wang, Q., & Li, C. (2021). "Network Security Vulnerabilities and Countermeasures: A Comprehensive Review". International Journal of Network Security.

Chen, X., & Kim, Y. (2020). "Insider Threats in Information Security: Patterns, Prevention, and Detection Techniques". Journal of Information Systems Security.

Patel, R., & Kumar, S. (2021). "Mobile Device Security: Risks and Mitigation Strategies". International Journal of Mobile Security.

EGSI | Cascante. (julio, 2020). *Academia.edu*. Recuperado el 03 de Julio de 2023, de https://www.academia.edu/37787824/ESQUEMA_GUBERNAMENTAL_DE_SEGURIDAD_DE_LA_INFORMACION_EGSI

Esquema de Seguridad de la Información de Ecuador | *GSS*. (2022). GlobalSuite Solutions. Recuperado el 03 de Julio de 2023, de https://www.globalsuitesolutions.com/es/analisis-esquema-gubernamental-seguridad-informacion-ecuador-correcta-implantacion/

Rodríguez, M., & García, L. (2020). "Improving Information Security Awareness: Strategies and Best Practices". Journal of Cybersecurity Education

Gobierno electrónico. (2020, enero). *Edición especial sumario*: Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

Grupo STT. (2021, noviembre). *Grupo STT.* Recuperado el 20 de Junio de 2023, de https://grupostt.com/2021/11/23/la-importancia-de-la-seguridad-de-la-informacion-en-nuestra-vida/

ISO *27001 - Software ISO 27001 de Sistemas de Gestión*. (2022). ISOTools. Recuperado el 29 de Mayo de 2023, de https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

ISO/IEC *27001*. (2023, marzo). Wikipedia. Recuperado el 29 de Mayo de 2023, de https://es.wikipedia.org/wiki/ISO/IEC_27001

López, M. (2023, marzo). *Esquema Gubernamental de Seguridad de la Información (EGSI)*. GlobalSuite Solutions. Obtenido de https://www.globalsuitesolutions.com/es/egsi-nueva-version-esquema-gubernamental-seguridad-informacion/

López, T. (2022, June 17). *ISO 27001*. El blog de Innevo. Recuperado el 07 de Julio de 2023, de https://blog.innevo.com/seguridad-sin-iso-27001

Mes de la Concientización de la ciberseguridad. (2022). *SEPS*. Recuperado el 07 de Junio de 2023, de https://www.seps.gob.ec/wp-content/uploads/PresentacionCharlaMINTEL.pdf

Rodríguez, A., & Pérez, B. (2022). Métodos de investigación en ciencias sociales: Enfoques y técnicas. Editorial Académica.

Sánchez, A., & Martínez, M. (2021). Metodología de análisis de datos: Métodos gráficos, tabulares y numéricos. Editorial Académica.

García, J. (2020). Metodología de la investigación: Conceptos fundamentales. Editorial Académica.

Ministerio de telecomunicaciones y de la sociedad de la información. (2022, abril). *Reporte No. 9 - Avances de la implementación del EGSI v2*. Gobierno Electrónico. Recuperado el 03 de Julio de 2023, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/05/Reporte-No.-10-Avances-de-la-implementacion-del-EGSI-V2.pdf

ORCA Software *GRC*. (2019, enero). *Blog ORCA GRC*. Recuperado el 20 de Junio de 2023, de https://blog.orcagrc.com/diferencias-seguridad-informatica-seguridad-de-la-informacion

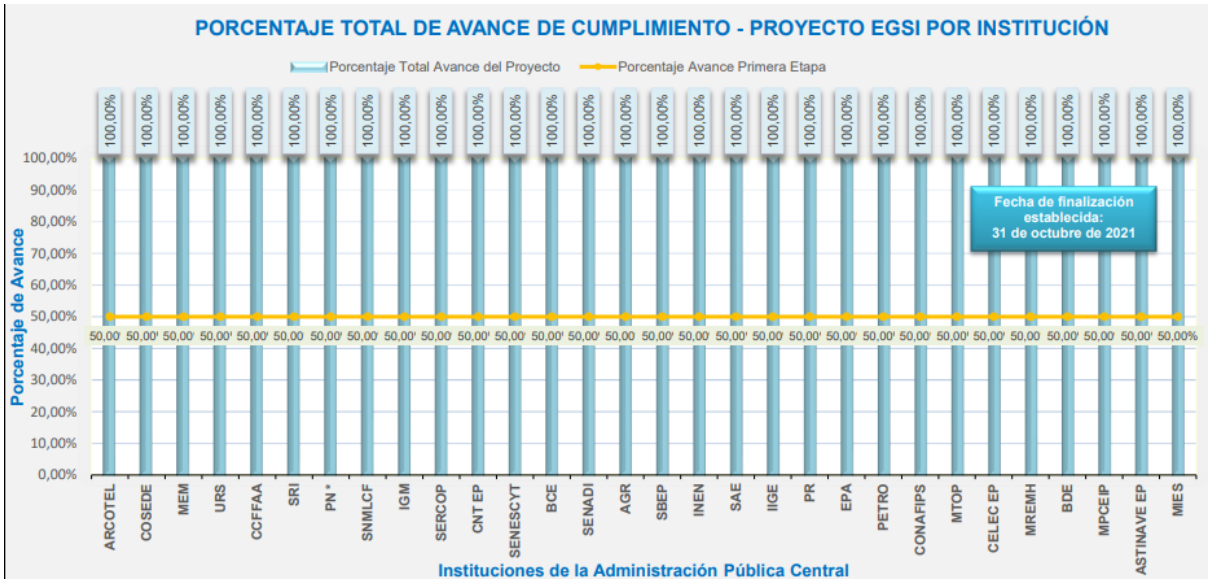
Raquel Toro, SSI, R. (2017, enero). *¿Seguridad informática o seguridad de la información?* PMG SSI. Recuperado el 20 de Junio de 2023, de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Seguridad de la Información. (2017). *Fortra*. Recuperado el 20 de Junio de 2023, de https://www.fortra.com/es/soluciones/seguridad-informatica/seguridad-de-informacion

SGSI. (2023). *ISO27000.es.* Recuperado el 20 de Junio de 2023, de https://www.iso27000.es/sgsi.html

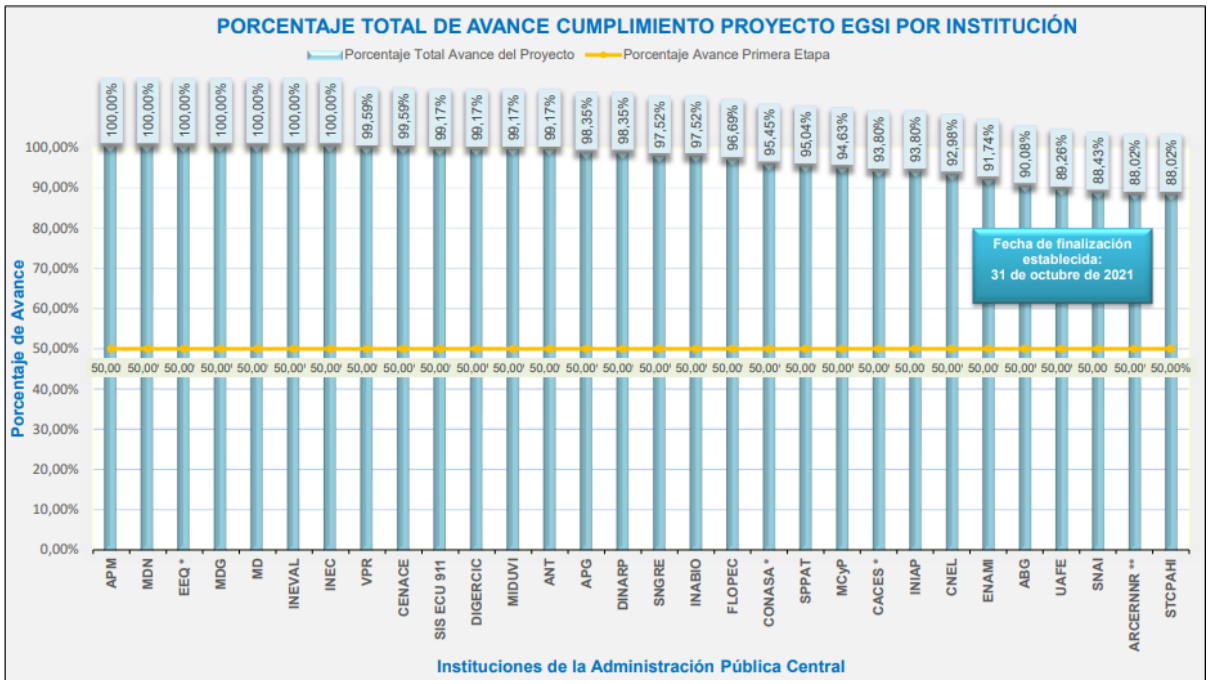
ANEXOS

Anexos 1: *Proyecto EGSI por institución*



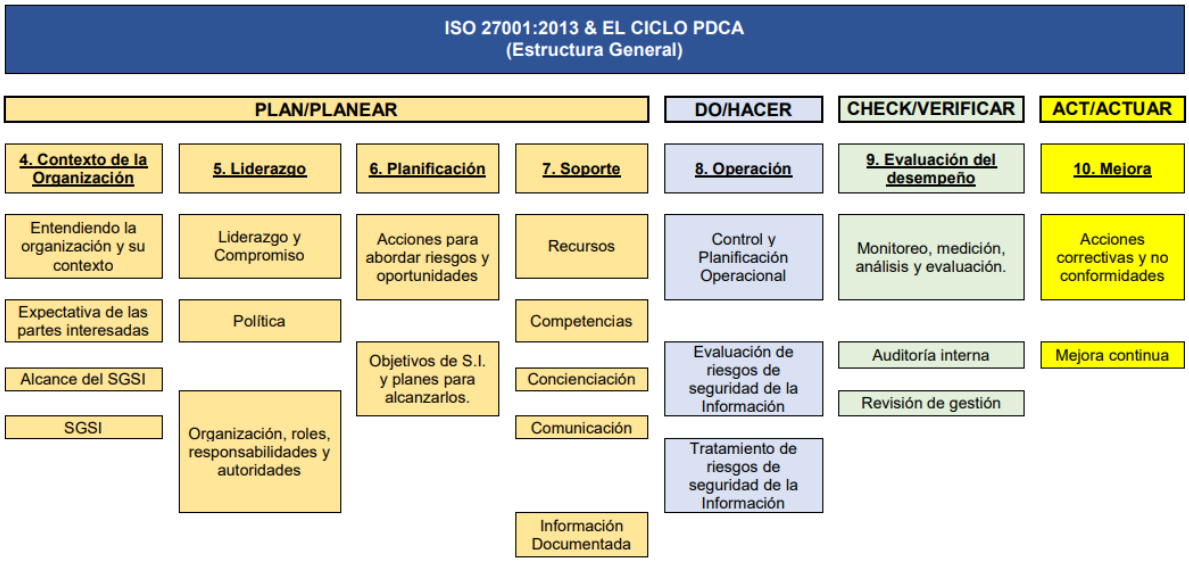
Fuente: *(Ministerio de telecomunicaciones y de la sociedad de la información, 2022)*

Anexos 2: *Proyecto EGSI por institución - 2*



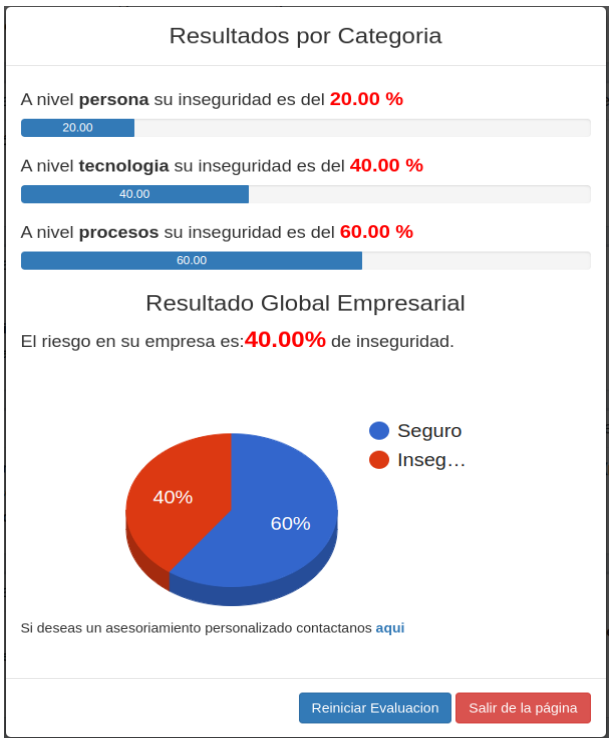
Fuente: *(Ministerio de telecomunicaciones y de la sociedad de la información, 2022)*

Anexos 3: *Ciclo PDCA*



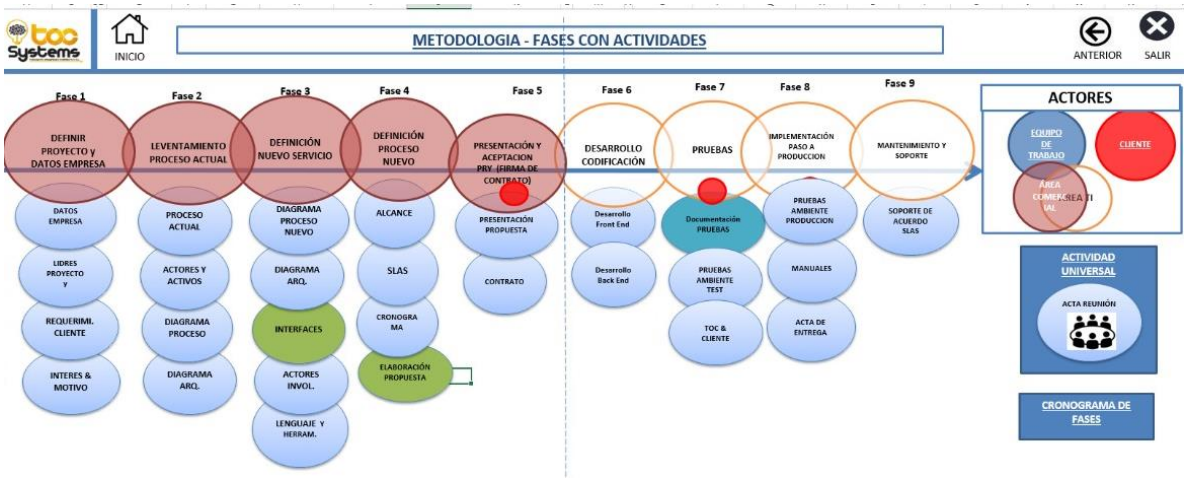
Fuente: *(Guía para la implementación del EGSI. Abril 2020)*

Anexos 4*: Herramienta de cálculo de seguridad empresarial*



Fuente: *(Empresa TocSystem)*

Anexos 5: *Herramienta de cálculo de seguridad empresarial*

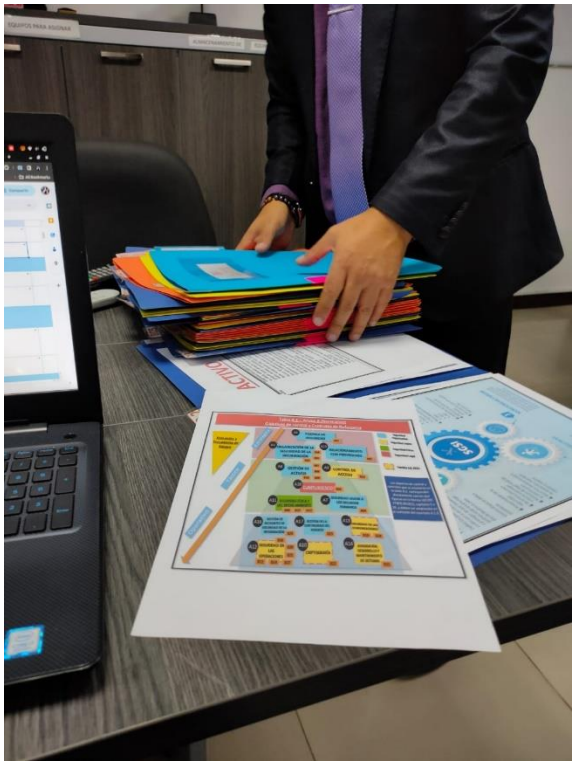


Fuente: *(Empresa TocSystem)*

Anexos 6: *Instrumento*

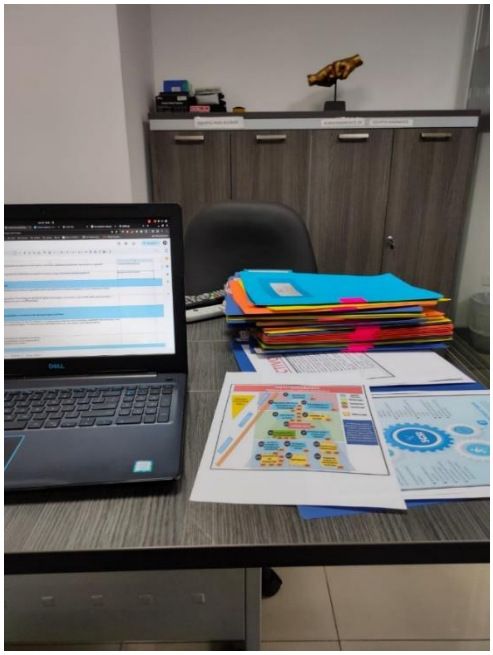
URL*:* https://docs.google.com/spreadsheets/d/1kT5-hJNDjN1Pp_RFCPXN54SNwwRp3B7j/edit?rtpof=true&sd=true

Anexos 7: *Evidencia de la aplicación del instrumento*



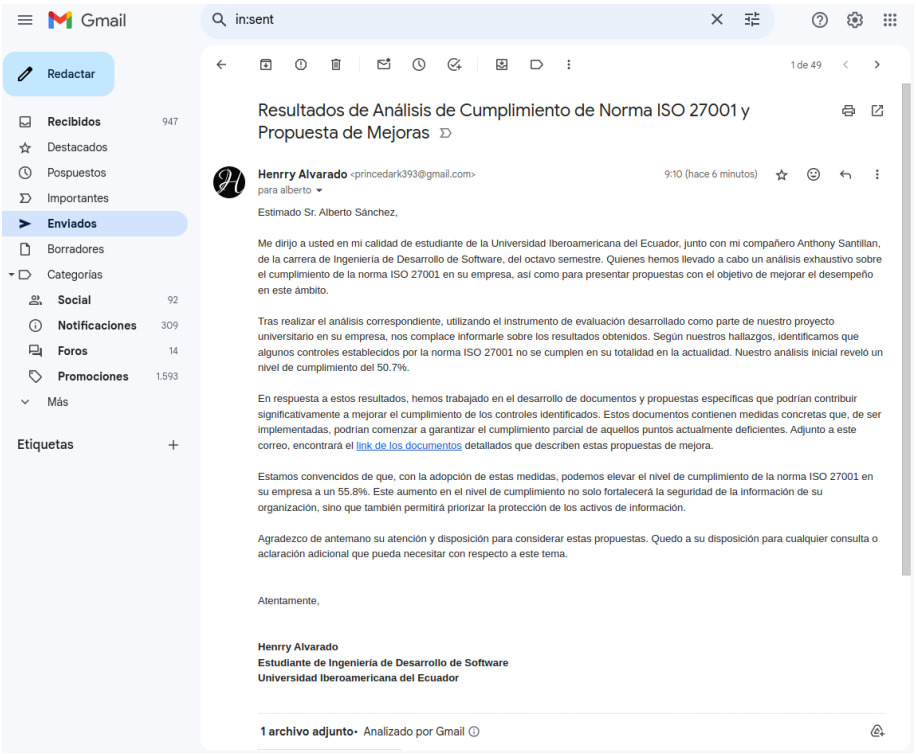
Fuente: *(Empresa TocSystem)*

Anexos 8: *Evidencia de la aplicación del instrumento*



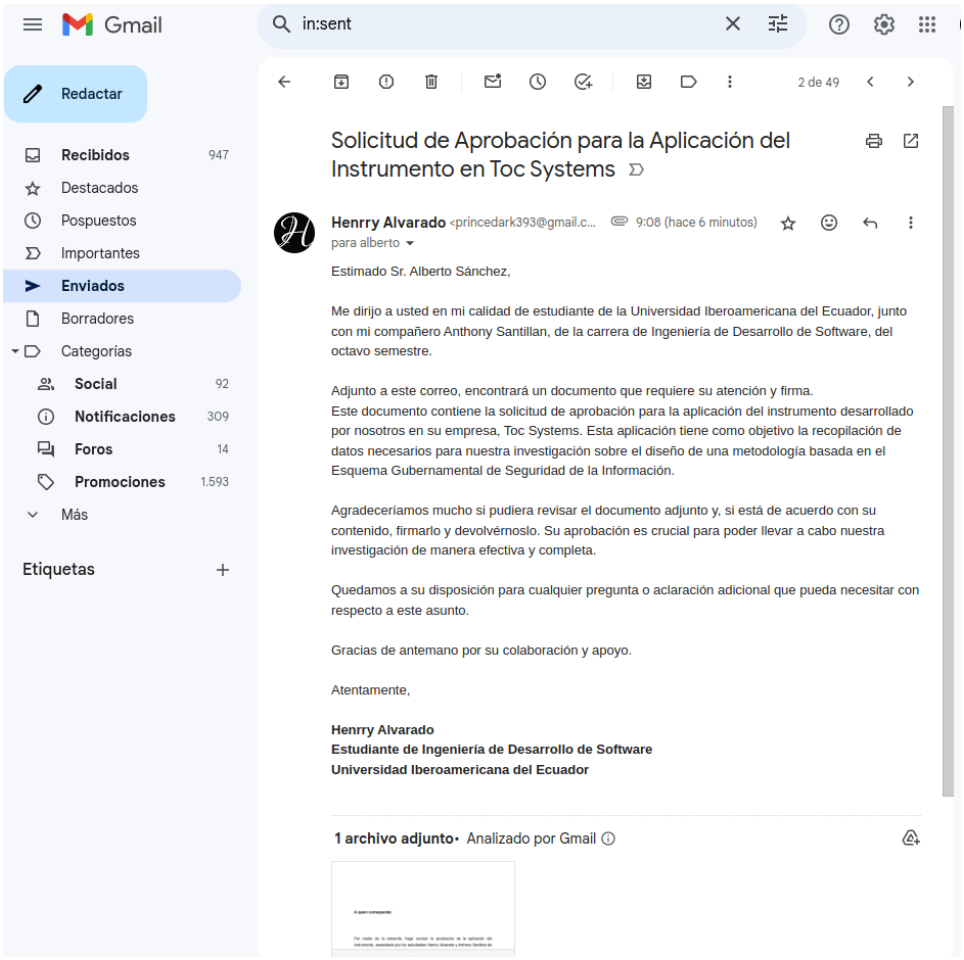
Fuente: *(Empresa TocSystem)*

Anexos 9: *Evidencia del envió de los resultados obtenidos a la empresa.*



Fuente: *Elaboración Propia*

Anexos 10: *Evidencia del envió de la solicitud de aprobación del instrumento para aplicar en la empresa.*



Fuente: *Elaboración Propia*

Anexos 11: *Aprobación de aplicación de instrumento*

A quien corresponda:

Por medio de la presente, hago constar la aprobación de la aplicación del instrumento, presentado por los estudiantes Henrry Alvarado y Anthony Santillan de la Universidad Iberoamericana del Ecuador de la carrera de Ingeniería de Desarrollo de Software, del octavo semestre, quienes lo realizan en la empresa Toc Systems para la recopilación de datos necesarios para su investigación, sobre el tema de diseño de una metodología basada en el Esquema Gubernamental de Seguridad de la Información para posterior implementación en una empresa privada.

A petición de los interesados y para los fines que estime conveniente, se extiende la presente en la ciudad de Quito a los 09 días de febrero del 2024.

Atentamente,

ALBERTO PAUL SANCHEZ CHAVEZ

Firmado digitalmente por ALBERTO PAUL SANCHEZ CHAVEZ
Nombre de reconocimiento (DN): c=EC, serialNumber=1716766058, cn=SANCHEZ CHAVEZ, cn=ALBERTO PAUL SANCHEZ CHAVEZ, 1.3.6.1.4.1.37942.10.4=1716766058, ou=Certificado Persona Natural EC (FIRMA), givenName=ALBERTO PAUL, email=alberto@toc.com.ec, 2.5.4.13=Certificado para Persona Natural, st=PICHINCHA, l=MARISCAL SUCRE
Fecha: 2024.02.14 22:44:59 -05'00'
Versión de Adobe Acrobat Reader: 2023.008.20533

Alberto Sanchéz

Responsable de seguridad de la información

Fuente: *Elaboración Propia*

Anexos 12: *Recepción de resultados*

TOC Systems

Dir.: Av. 12 de Octubre N24-739 y Av. Colón Ed. Torre Boreal Piso: 6, Of.608

Quito, 09 de febrero del 2024

Estimados Henrry Alvarado y Anthony Santillan,

Por medio de la presente carta, la empresa TOC Systems confirma oficialmente haber recibido los resultados obtenidos y las propuestas presentadas por ustedes en relación con la investigación realizada sobre el diseño de una metodología basada en el esquema gubernamental de seguridad de la información.

Agradecemos sinceramente el tiempo, esfuerzo y dedicación que han invertido en este proyecto, así como la calidad de los resultados y propuestas presentadas. Reconocemos la importancia estratégica de esta investigación para nuestra organización y la valoramos profundamente.

Entendemos que, según lo acordado, las acciones a tomar basadas en los análisis realizados quedan bajo nuestra responsabilidad. Nos comprometemos a revisar detenidamente los resultados y propuestas presentadas y a tomar las acciones apropiadas de acuerdo con las necesidades y objetivos de la empresa.

Quedamos a su disposición para cualquier consulta adicional o aclaración que puedan necesitar en relación con este asunto.

Agradecemos nuevamente su contribución y esperamos poder trabajar juntos en futuros proyectos.

Atentamente,

ALBERTO PAUL SANCHEZ CHAVEZ

Firmado digitalmente por ALBERTO PAUL SANCHEZ CHAVEZ
Nombre de reconocimiento (DN): c=EC, serialNumber=1716766058, sn=SANCHEZ CHAVEZ, cn=ALBERTO PAUL SANCHEZ CHAVEZ, 1.2.6.1.4.1.37942.10.4=1716766058, ou=Certificado Persona Natural EC (FIRMA), givenName=ALBERTO PAUL, email=alberto@toc.com.ec, 2.5.4.12=Certificado para Persona Natural, st=PICHINCHA, l=MARISCAL SUCRE
Fecha: 2024.02.14 22:56:04 -05'00'
Versión de Adobe Acrobat Reader: 2021.008.20533

Alberto Sanchéz
Responsable de seguridad de la información
TOC Systems
alberto@toc.com.ec

Fuente: *Elaboración Propia*