ESCUELA DE INGENIERÍAS

Tema:

GUÍA PARA IMPLEMENTACIÓN DE LA ISO 27001 EN EL DEPARTAMENTO TI DE LA GOBERNACIÓN TUNGURAHUA

Proyecto de investigación previo a la obtención del título de Ingeniera en Sistemas de Información

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autora:

Paula Camila Amancha Vaca

Directora:

Mg. Teresa Milena Freire Aillón

Ambato – Ecuador

Marzo 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **PAULA CAMILA AMANCHA VACA**, con cédula de ciudadanía **1850711803**, autora del trabajo de graduación titulado: "GUÍA PARA IMPLEMENTACIÓN DE LA ISO 27001 EN EL DEPARTAMENTO TI DE LA GOBERNACIÓN TUNGURAHUA", previo a la obtención del título profesional de **INGENIERA EN SISTEMAS DE INFORMACIÓN**, en la escuela de **INGENIERÍAS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica 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 graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, marzo 2025

Paula Camila Amancha Vaca

CC. 1850711803

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

GUÍA PARA IMPLEMENTACIÓN DE LA ISO 27001 EN EL DEPARTAMENTO TI DE LA GOBERNACIÓN TUNGURAHUA

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autora:

Paula Camila Amancha Vaca

Teresa Milena Freire Aillón, Ing. Mg. f._____

CC. 0501710677

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. Mg. f._____

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____

DIRECTOR ESCUELA DE INGENIERÍAS

Diego Gonzalo Coca Chanalata, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Marzo 2025

DEDICATORIA

A mis padres, Lorena Vaca y Fabricio Amancha,

Por ser la luz que ha iluminado mi camino y el impulso detrás de cada paso que he dado.

Por su apoyo incondicional, sus sacrificios e inculcarme los valores que me han formado como la persona que soy.

Ustedes han sido mi refugio en los momentos difíciles, mi fuerza en los momentos de duda, y mi mayor inspiración para nunca rendirme. Este logro y todos los que vengan son reflejo de su amor, energía y fe en mí.

Gracias por demostrarme que el amor incondicional existe, por mover fronteras y por enseñarme que no hay meta imposible si se camina con perseverancia y con el corazón lleno de sueños.

Este logro es suyo, porque sin ustedes no lo habría conseguido.

AGRADECIMIENTO

A Dios, por ser mi guía y fortaleza en cada paso del camino, permitiéndome superar los desafíos y alcanzar este importante logro.

A mi padre, Fabricio Amancha, por ser un ejemplo de perseverancia y valentía, por enseñarme a avanzar ante los obstáculos y brindarme la oportunidad de estudiar gracias a su esfuerzo incansable. A mi madre, Lorena Vaca, quien con su amor y dedicación me ha cuidado y apoyado durante toda mi etapa estudiantil, preocupándose siempre por mi bienestar y motivándome en cada momento.

A mi sobrino, Isaac Proaño, por regalarme sus risas y abrazos que reconfortaron mi espíritu en los momentos más difíciles. A mis queridas sobrinas, María Celeste Amancha e Isabella Proaño, por su fe en mí y por recordarme que lograrlo era posible.

A mis hermanos, Alejandra Amancha y Mario Fabricio Amancha, por creer en mí, darme su ánimo constante y apoyarme con su cariño incondicional. A mi tío, Pablo Amancha, por ser un pilar de apoyo y confianza, y a todos los miembros de mi familia Amancha, por sus palabras de aliento y por regalarme momentos de alegría que aligeraron este camino.

A mi tutora, Ing. Teresa Freire, por su invaluable apoyo y orientación, por ayudarme a resolver los desafíos que surgieron a lo largo de esta ardua tarea, y por ser una docente excepcional cuyo compromiso fue clave en este proceso.

Finalmente, a mis maestros, por permitirme aprender de su conocimiento y experiencia, y por el respaldo que me brindaron a lo largo de mi camino universitario.

RESUMEN

El incremento de amenazas y ciberataques, la reciente regulación de protección de datos, la necesidad de preservar la confidencialidad, integridad y disponibilidad de la información exigen que las organizaciones adopten prácticas y estándares internacionales.

La Gobernación de Tungurahua evidencia un nivel de madurez limitado en cuanto a la seguridad de la información, por lo que, el objetivo de la investigación es diseñar una guía para implementación de la ISO 27001 en el departamento TI. Se utilizó el método analítico sintético e inductivo deductivo, con una investigación descriptiva y documental, y como instrumentos se aplicaron la encuesta y lista de chequeo que dieron como resultado hallazgos importantes los cuales, frente a los requerimientos de la norma, evidenciaron brechas de seguridad.

Con la metodología Ciclo de Deming o *Plan–Do– Check – Act*, se esquematizó la implementación de un Sistema de Gestión de Seguridad de la información que es el eje central de la misma, para realizar propuestas enfocadas en minimizar los riesgos informáticos, incrementar controles, definir políticas, establecer roles y funciones y gestionar de manera segura los elementos estructurales y funcionales del departamento de TI.

El resultado es una guía detallada y práctica para implementar todos los elementos del SGSI en base a la norma ISO 27001 en el departamento de TI de la Gobernación de Tungurahua y con ello procurar el fortalecimiento de la confiabilidad institución – ciudadano, cumplimiento de requisitos regulatorios y legales, reducción de incidentes de seguridad y protección de la reputación organizacional.

Palabras clave: guía de implementación, ISO 27001:2022, seguridad de la información, gobernación.

ABSTRACT

The increase in threats and cyberattacks, the recent regulation of data protection, the need to preserve the confidentiality, integrity and availability of information require organizations to adopt international practices and standards.

The Government of Tungurahua shows a limited level of maturity in terms of information security; therefore, the objective of the research is to design a guide for the implementation of ISO 27001 in their IT department. The synthetic analytical and inductive deductive method was used, alongside descriptive and documentary research. The survey and checklist were applied as tools that brought important findings to light, and in turn, when confronted with the requirements of the standard, showed some security breaches. The outline for the implementation of an information Security.

Management System was made, using the Deming Cycle or "Plan-Do-Check-Act" methodology, which constitutes the central axis of the said implementation, to make proposals focused on minimizing cyber security risks, increasing checkpoints, defining policies, establishing roles and tasks, to securely manage the structural and functional elements of the IT department.

The result of this work is a detailed and practical guide to implement all elements of the ISMS based on the ISO 27001 standard in the Tungurahua Government's IT department and thereby seek to strengthen the institution-citizen reliability, legal and regulatory compliance, reduction of security incidents and protection of organizational reputation.

Keywords: *Implementation guide, ISO 27001:2022, information security, governance.*

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

En la era digital, el activo más importante de una empresa es la información. Por lo que, la seguridad de esta es crucial para generar continuidad en el negocio, además de brindar confianza e integridad a los clientes. Morales, Toapanta, & Toasa (2019) mencionan que en la actualidad la protección de la información no solo conlleva el utilizar antivirus, sino se necesita una serie de técnicas para contrarrestar los nuevos ataques a los sistemas.

A nivel internacional se menciona que la seguridad es una característica importante de todo proceso que manipula información, especialmente en campos donde esta sea confidencial para ofrecer una ventaja competitiva a las empresas (Zevallos Morales, 2019). Además, los ciberataques alrededor del mundo se han vuelto más selectos y riesgosos, con consecuencias que van desde el hurto de datos y la detención del negocio hasta el deterioro de la infraestructura y la batalla cibernética.

En Colombia, Segura Barrantes (2022) analizó la necesidad de adquirir un sistema de gestión en las organizaciones públicas para mejorar procesos, brindar efectividad y mayor calidad. El problema que se presentaba fue la falta de integración de dichos sistemas normados por una ISO en este tipo de entidades, por lo que, generaba ineficiencia y sobrecarga operativa, además de que estaban sometidos a ciberataques. Es por ello, que se realizó una guía metodológica de planeación y gestión que se basó en siete dimensiones acorde a los aspectos principales de la gestión pública: talento humano, direccionamiento, gestión con valores para resultados, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación, por último, control interno. Como resultado, gracias al modelo se ofrece una perspectiva práctica para un buen desempeño institucional público.

Asimismo, ESVICSAC es una empresa peruana que brinda servicios de seguridad, vigilancia y control, no disponía de un Sistema de Gestión de Seguridad de la Información (SGSI) normado por la ISO 27001. Por lo que, se encontraban expuesto a peligros como pérdidas de información, fugas de datos e incidentes

informáticos. La solución propuesta por Arias Quispe (2020), fue la implementación de esta norma para abordar los riesgos de la información gracias a controles y políticas. Por ello, el SGSI brinda protección del activo más valioso de la empresa, la información, además, controla los riesgos y reduce las vulnerabilidades.

En cambio, Castillo Durán (2023) indica que en Ecuador existe un alto déficit en temas de ciberseguridad, es decir, no se presta la suficiente importancia a los ciberataques, en comparación a otras regiones. Por lo que, el incremento de amenazas, la creciente regulación de datos y la necesidad de preservar la confidencialidad, integridad y disponibilidad de la información hacen imperativo que las organizaciones adopten prácticas y estándares reconocidos internacionalmente.

Por tal razón, uno de los métodos para salvaguardar los datos es el Sistema de Gestión de la Seguridad de Información (SGSI), conjunto de procedimientos para sustentar la protección de la información en base a los peligros a los que se encuentra expuesta (Donoso Vargas, Calahorrano Recalde, & Donoso Vargas, 2023), en donde varias organizaciones lo implementan como resultado de una decisión estratégica. El SGSI apoya al negocio en la prevención de intrusión, difusión de datos intencional o de manera eventual y el incorrecto funcionamiento de los sistemas informáticos. Incluso, fortalece la confianza entre cliente y empresa, pues evita la pérdida de datos y el daño a la reputación de ambas partes.

Además, como la mayoría de las empresas ecuatorianas presentan vulnerabilidades informáticas, las cuales son ignoradas y con el paso del tiempo causan daño en las funciones laborales, Llano Casa, Gaibor Gavilánez, Cruz Caiza, & Cadena Moreano (2021) indican que existe la posibilidad de combatirlas por medio del diseño e implementación de la normativa ISO 27001.

Por otro lado, se menciona que para la implementación de un SGSI es recomendable trabajar en conjunto con la norma ISO 27001, estándar de valoración y administración de procedimientos que brinda parámetros para un Sistema de Gestión de Seguridad de la Información (Zaidatulnajla, 2019). Es decir, este

precepto provee una guía de referencia vigorosa y altamente reconocida para la gestión de este tipo de sistema.

En este contexto, la normativa ISO 27001 presenta un orden para los sistemas informáticos de la organización y se pueda obtener una certificación que gestione la seguridad de la información (Jácome Sánchez, 2022). También, la ISO 27001 investiga el lugar de donde se encuentra el riesgo para actuar de manera rápida y trabajarlo (Arias Quispe, 2020). En otras palabras, brinda una perspectiva sistemática para la organización en la identificación, evaluación y solución de ataques de seguridad que podrían dañar la operatividad y confidencialidad de la información.

En relación con lo antes expuesto, la situación problemática es la limitada atención y obediencia de las regulaciones necesarias para garantizar la seguridad de la información, la cual se ha convertido en un inconveniente crítico en el ambiente empresarial. Asimismo, es fundamental asegurar la confidencialidad, integridad y disponibilidad de los datos para preservar la privacidad de clientes y socios.

El director del departamento de Tecnologías de la Información y Comunicación (TIC) de la Gobernación de Tungurahua manifiesta que el principal inconveniente de la organización es la inexistencia de un Sistema de Gestión de Seguridad de la Información, en consecuencia, existe la posibilidad de que se provoquen brechas de datos, intentos de acceso no autorizado o pérdida de información sensible. También, puede ser evidente a través de auditorías internas o externas que revelen deficiencias en el cumplimiento de normativas y estándares de seguridad. Adicionalmente, la retroalimentación negativa de usuarios/ciudadanos sobre la seguridad de la información de la empresa puede indicar la existencia de inconformidad por ambos lados.

Por lo que, el no tener cuidado frente a las regulaciones y estándares oportunos, como la ISO 27001 brinda una atención sólida a la preservación de la información, que no solo expone a la Gobernación de Tungurahua a riesgos como pérdida de datos, filtraciones de información confidencial, ciberataques y sanciones legales,

sino que también tiene un impacto negativo en la reputación de credibilidad frente a los ciudadanos. Incluso, el enfoque no estructurado que se tiene para la administración de la seguridad de la información resulta en consecuencias desfavorables para la institución en términos de operatividad. En este contexto, se plantea el siguiente problema científico: ¿De qué manera se podría implementar la norma ISO 27001 en el Departamento de TI de la Gobernación de Tungurahua para evitar filtraciones de información confidencial? Y en conjunto la idea a defender, la cual es el diseño de una guía para la implementación de la ISO 27001 en la Gobernación de Tungurahua que permitirá una mejor gestión de riesgos informáticos, garantizará el cumplimiento normativo y contribuirá a la seguridad de la información.

Risco Villarreal (2021) plantea que al considerar la información como activo más valioso de una empresa, existe la obligación de implementar medidas para su protección, es así como el proyecto realizado por el autor propone la implementación de un SGSI basado en la norma ISO 27001:2005, porque el sistema favorece a la optimización de recursos, prevención de riesgos y protección de datos. En tal sentido, la presente investigación toma como referencia lo antes expuesto e indica que el objetivo general es diseñar una guía para implementación de la ISO 27001 en el Departamento TI de la Gobernación Tungurahua y como sus objetivos específicos, se presenta:

1. Sistematizar teóricamente sobre ISO 27001 y seguridad de la información.
2. Diagnosticar la situación actual sobre la seguridad de la información de la Unidad de TI de la Gobernación de Tungurahua.
3. Elaborar los elementos necesarios para la integración en una guía.

Asimismo, la investigación ocupará la metodología *Ciclo de Deming o Plan – Do – Check – Act*, pues es esencial para la ejecución de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001. Además, la metodología establece un proceso cíclico y sistemático para administrar los riesgos informáticos. Los resultados esperados en la investigación es proporcionar una guía detallada y práctica para implementar políticas de seguridad de información

basadas en la norma ISO 27001 en el departamento de TI de la Gobernación de Tungurahua. Los beneficiados directamente con el presente proyecto es el Departamento de TI, la Gobernación de Tungurahua y los ciudadanos porque se proyecta a reducir riesgos, mejorar de la gestión de seguridad y se cumplirá con los estándares internacionales de seguridad de la información. Además, los favorecidos indirectamente son los proveedores y socios estratégicos de la Gobernación, pues les brindará la debida confianza de que sus datos estarán protegidos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

El estado del arte y la práctica describe la seguridad de la información con un enfoque en el avance de los ciberataques por la dependencia de la tecnología y la importancia de la implementación de un SGSI basado en la norma ISO 27001. Además, enfatiza en proteger la información por medio de la triada de la seguridad y un enfoque exhaustivo de gestión de riesgos y amenazas cibernéticas.

1.1. Seguridad de la información

El incremento de la dependencia de las tecnologías de la información y la comunicación (TIC) en los distintos ámbitos de la vida, especialmente en el gobierno, ha generado un escenario de ciberataques más complicados y avanzados. Para ello, asegurar la información es parte fundamental para evitar actos ilegales que comprometan la legitimidad de los datos almacenados y así establecer la conocida tríada de la seguridad de la información: integridad, confidencialidad y disponibilidad para la organización (Asurza Cáceres, 2022).

La tríada de la seguridad de información o CIA cumple con establecer la integridad, facultad que se da para generar cambios en los datos de manera autorizada o no deseada; la confidencialidad, capacidad de resguardar la información de aquellos que no tienen autorización para manipularla u observarla; por último, la disponibilidad, cualidad de la información que asegura la accesibilidad de esta en cualquier momento (Vega Briceño, 2021). Al entender y poner en práctica estos principios, las empresas tienen la posibilidad de disminuir los peligros a los que está expuesta la información de sus clientes.

Asimismo, la información, especialmente la gubernamental, se encuentra amenazada por los distintos ciberataques. Las entidades del estado manejan gran cantidad de datos sensibles como financieros, personales, confidenciales e incluso, tácticas de seguridad nacional por lo que están expuestos a distintos tipos de ciberataques, Tabla 1, que causan el mal funcionamiento de redes, sitios *web* o máquinas para generar pérdida de información, (Guacho Lema, 2018).

Tabla 1. Ciberataques más comunes en empresas gubernamentales

Clasificación	Tipos	Definición
Ataques de ingeniería social	*Phishing*	El ciberdelincuente envía por medio de correo electrónico, redes sociales o mensajería instantánea avisos que suplantan a una entidad oficial.
	Baiting	Esta técnica es también conocida como "cebo", en donde el atacante infecta el equipo, por medio de USB o anuncios publicitarios, así se obtiene información personal del usuario.
Ataques a las conexiones	Ataque DDoS	El Ataque Distribuido Denegación de Servicio o DDoS, el ciberdelincuente ataque desde otros equipos al servidor web en un mismo tiempo y este deja de funcionar, por lo que podría robar los datos.
	Inyección SQL	Se inserta líneas de código en formato SQL maliciosas en la base de datos de las aplicaciones web, así se tiene acceso a la información que contiene la base de datos.
Ataques de *malware*	Virus	Tiene el objetivo de propagarse por varios dispositivos, pues se copian a sí mismos. Llega a eliminar archivos y daña datos sensibles.
	Troyano	Actúa como un *software* oficial y controla el dispositivo para robar datos e infectar con un programa malicioso.

Fuente: modificado a partir de INCIBE (2020).

Los ciberataques antes mencionados se basan en el robo de información sensible, estas amenazas a nivel mundial son consistentes pues existen distintos casos en los cuales grandes empresas han sido víctimas de estos. Por ejemplo, Equifax, empresa estadounidense que realizar informes crediticios, en julio del 2017 sufrió una inyección SQL exponiendo la información de alrededor 147 millones de personas. Los ciberdelincuentes se beneficiaron de la existencia de una brecha de seguridad en *Apache Struts* en su sitio *web*, a pesar de que la empresa creyó haber parchado dicha vulnerabilidad sufrieron un ataque (Castillo Fonseca & Zavala Juárez, 2019).

Asimismo, *WannaCry,* programa maligno de tipo *ransomware* que se clasifica como troyano*,* afectó en mayo del año 2017 a 150 países en sus empresas gubernamentales, algunos hospitales y varias organizaciones. Este ataque encriptó una serie de documentos para su decodificación solicitaba pagos en *Bitcoin*. *WannaCry* afectó datos sensibles de los gobiernos, como la colecta de impuestos, gestión del tráfico aéreo y cuidado médico (Akbanov, Vassilakis, & Logotheis, 2019).

Incluso, Ecuador ha sido víctima de una serie de ataques cibernéticos, en abril del año 2019 después de que el país tomará la decisión de quitar el asilo a Julián

Assange, un programador, periodista, activista y fundador del sitio *web WikiLeaks*, sufrió una serie de amenazas. Todos los ataques trataban de denegación de servicio, pues se sobrecargaban los servidores *web* de tráfico erróneo y esto impedía el acceso a los dispositivos. Gracias a esto se perdió datos personales que contenían empresas como la Cancellería, el Banco Central, la Presidencia y el Servicio de Rentas Internas (SRI). Hasta la actualidad no se ha podido comprobar quién o quiénes fueron los responsables de este suceso, sin embargo, se sospecha que los actores principales fueron Julián Assange y su equipo (Alvarado Chang, 2020).

Los ciberataques simbolizan riesgos crecientes en todo el mundo, presentan consecuencias significativas en organizaciones, gobiernos y sociedad. Estos ciberataques como el hurto de información en Equifax, sabotaje del *ransomware WannaCry* y los ataques de servicio en Ecuador, son pruebas necesarias para implementar medidas de ciberseguridad en todos los ámbitos.

La complejidad de los ataques y la susceptibilidad de los sistemas informáticos ponen en riesgo datos críticos, información personal, financiera y de gobierno. Frente al suceso de la empresa Equifax, la exposición de datos de millones de personas amenazó su identidad financiera e intimidad. Por otro lado, *WannaCry,* alteraron ámbitos importantes como la salud y la administración pública junto con la demostración del gran impacto de los ataques cibernéticos en los equipamientos y calidad de vida.

Además, luego de la salida de Assange, Ecuador presentó disturbios en el acceso a servicios de interés general. Este caso subraya la importancia de la protección de la información en el gobierno.

Finalmente, los ciberataques se han transformado en un peligro mundial que necesita un enfoque multisectorial para resguardar la información. Los fondos utilizados para tecnología, la instrucción del personal y la ayuda internacional son componentes importantes para luchar contra estos ataques y proteger la información digital sensible.

Por otro lado, existen riesgos físicos que provocan la inseguridad o pérdida de la información. Osorio Beltrán (2022) indica que los tipos de amenazas informáticas humanas o por desastres naturales dañan a los sistemas. Algunos de estos ejemplos se detallan en la Tabla 2.

Tabla 2. Amenazas físicas en instituciones gubernamentales

Tipo	Definición
Usuarios	Se describe como la persona que utiliza el sistema y es la principal amenaza, pues no tiene buenas prácticas de ciberseguridad y se convierte en víctima fácil. Incluso, en ocasiones es quien roba la información de manera intencional.
Intrusos	Son personas que no tienen acceso autorizado a programas, centros de cómputo o archivos a espiar, hurtar y destruir.
Siniestros	Es la acción de perder información o recursos sensibles por negligencia del personal institucional. Los siniestros más habituales son los incendios o inundaciones provocadas.
Catástrofes naturales	Son opuestos a los siniestros, pues el humano no tiene control sobre estos, se dan por causas naturales.
Fallos electrónicos	Los sistemas pueden ser afectados por fallos de energía eléctrica o por problemas que presentan los equipos.
Ingeniería social	El atacante es quien se gana la confianza de la víctima y obtiene información confidencial.

Fuente: modificado a partir de Osorio Beltrán (2022)

Estas amenazas no solo se encuentran en la teoría, sino también en la práctica. Es el caso de *Yahoo!*, en 2013 afecto a alrededor de tres mil millones de cuentas de usuarios, pues varias de las contraseñas de los usuarios eran extremadamente débiles o incluso las utilizaban en distintos servicios web y así los atacantes tuvieron la oportunidad de descifrarlas y filtrar la información. También, en 2016 se conoció un escándalo denominado "*Panama Papers",* en el cual se extrajo gran cantidad de documentos internos de clientes del estudio Mossack Fonseca y se especula que el culpable de esta sustracción fue un empleado descontento, sin embargo, la empresa no dio las razones exactas (Murguía Hughes, 2023).

Por lo tanto, las amenazas físicas a la seguridad de información abarcan riesgos humanos, como usuarios descuidados o maliciosos, además, personas con acceso no autorizado. También, los siniestros malintencionados y catástrofes naturales dañan significativamente los activos de información, a pesar de que los humanos no lo puedan controlar por completo. Es importante mencionar a las instituciones deben implementar protocolos y medidas de seguridad para evitar estos riesgos y fomentar la integridad de la información.

1.2. Sistemas de gestión de seguridad de la información

En el contexto actual, en el que la información es el activo más significativo para las empresas, resguardarla de peligros es crucial. El Sistema de Gestión de Seguridad de la Información (SGSI) surge como partidario indispensable para crear un enfoque integral de gestión de riesgos y aseguramiento de los datos.

Un SGSI es una herramienta para control de la seguridad de la información. Gracias a la implementación de este, la empresa tiene la posibilidad de conocer las amenazas a las que se someten sus activos con la intención de analizarlos y brindarles el adecuado seguimiento. Además, este tipo de sistemas sostiene una arquitectura organizacional en donde se establecen responsabilidades, tareas, recursos y roles para una precisa gestión de la seguridad de la información (Fonseca Herrera, Rojas, & Florez, 2021). En otras palabras, un SGSI además de ser una serie de procedimientos y directrices, es una doctrina de gestión que invade toda la organización. Se relaciona con etapas continuas de desarrollo que reconocen, examinan y disminuyen los peligros de la era digital.

Existen varios marcos de trabajo que complementan la implementación para un SGSI. NIST SP 800-53, brinda un catálogo de medidas de seguridad y privacidad enfocadas en la protección de los sistemas informáticos y empresas. Sin embargo, NIST no es certificable, pues únicamente es para la autorregulación, autoevaluación y un complemento de la ISO 27001 (Kurii & Opirskyy, 2022). Por otro lado, CIS *Controls*, conjunto de protocolos de ciberseguridad para la protección de información y sistemas. Este no tiene el objetivo de sustituir a ISO 27001, pues la refuerza al realizar definición de base técnica para organizar riesgos y apoyar la implementación de un SGSI, más no lo establece (Irawan, Hendi Muhammad, & Nasiri, 2024).

A partir de las opciones detallas con anterioridad, se conoce que ISO 27001 no es el único camino para establecer seguridad de la información, pero es un marco que brinda una estructura completa en cuanto a la implementación de un SGSI. Por tanto, se recomienda basarse en esta, a partir de los componentes necesarios para este sistema:

- **Límite del SGSI:** determina las estancias, vínculos, términos entre el alcance y los componentes aún no considerados.
- **Estrategias y metas de seguridad:** oficio que hace referencia al compromiso de alta dirección y el objetivo de la empresa en la administración de la seguridad de información.
- **Protocolos, procesos y manuales que apoyan al SGSI:** son los documentos y métodos que norman la estructuración, ejecución y control de los procedimientos de la seguridad de la información, además, de calibrar la eficacia de los procesos implementados.
- **Método de evaluación de amenazas:** definición de la metodología que se va a utilizar para poder realizar el análisis de peligros, vulnerabilidades, viabilidad de ocurrencia e identificación de impactos en correlación con la información. Incluso, la realización de puntos de vista para contemplar los niveles del riesgo.
- **Informe de valoración de riesgos:** presentación de resultados después de aplicar la metodología de valoración a los activos de información de la empresa.
- **Diseño de manipulación de riesgos:** documentación que conoce acciones, medios, responsabilidades y tareas importantes de alta dirección para la gestión de riesgos de seguridad de la información, en relación con los resultados de la valoración de riesgos, metas, medios disponibles, entre otros.
- **Registros:** archivos que muestren pruebas del cumplimiento de necesidades y del funcionamiento óptimo del SGSI.
- **Anuncio de control:** documentación con todas las metas de control y el seguimiento contemplados por el SGSI. (Fonseca Herrera, Rojas, & Florez, 2021)

La norma ISO 27001 brinda un modelo estructurado para la implementación de un SGSI óptimo. Al cumplir los elementos clave mencionados con anterioridad, las empresas tienen la posibilidad de contemplar un sistema integro para la protección de sus activos de información y asegurar la CIA de estos. Además, uno de los componentes clave de un Sistema de Gestión de la Seguridad de la Información es la gestión de riesgos.

La gestión de riesgos cumple con un proceso de manera continua, relacionado con las siguientes etapas:

- **Identificación**: conocer la información de la empresa y las posibles amenazas que pueden dañarlos.
- **Evaluación:** comprender la variabilidad y el impacto de cada una de las amenazas identificadas anteriormente.
- **Inducción:** llevar a cabo registros y normas para moderar las amenazar a determinado nivel de aceptación.
- **Seguimiento:** monitorear de manera periódica la valoración de amenazas y eficiencia de los controles utilizados. (Contreras Olea, 2022)

Este proceso cíclico descrito con anterioridad percibe el ambiente interno y externo de la empresa, contempla variables como el panorama de riesgos y debilidades del sistema. Asimismo, prioriza las amenazas para enfocarse en las de mayor peligro y establecer políticas de seguridad. Para que en una última instancia se realice seguimiento continuo a estas y se genere nuevas estrategias necesarias para combatirlas. La gestión de riesgos, además de ser un elemento fundamental en un SGSI, ayuda a cumplir con sus objetivos gracias al impulso que genera en la priorización de amenazas.

Los objetivos de un SGSI se describen de la siguiente manera:

- Crear conciencia y entendimiento del valor de la seguridad de la información en los empleados de una empresa para que protejan los datos de los clientes.
- Construir un consejo de seguridad de la información para capacitar a los directivos de la empresa sobre ciberataques y estrategias de prevención.
- Aplicar canales de comunicación para la discusión de dudas relacionadas con la seguridad de la información.
- Fomentar una cultura ética responsable y respetuosa sobre la privacidad de los datos personales para el bueno manejo de la información en la empresa.
- Realizar una valoración periódica de las amenazas de seguridad de la información para control de potenciales riesgos.
- Establecer un plan de gestión de riesgos dentro del proceso de implementación de los sistemas de información para el respaldo de la seguridad de la información.

- Implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para que sea efectivo y legal.
- Cumplir con un seguimiento periódico del funcionamiento del SGSI para evaluación del desempeño adecuado.

Estos objetivos establecidos para un SGSI garantizan el buen funcionamiento de este, además, ayudan a mitigar los riesgos presentes y futuros a los que se expone una empresa.

El resguardar la información es la prioridad principal de toda empresa, especialmente debería ser para el gobierno. En ese sentido, la Gobernación de Antioquia en el año 2018 implementó un Sistema de Gestión de la Seguridad de la Información con el objetivo de avalar que los ciberataques se conozcan y así gestionarlos de manera segura (Díaz Ayala & Castaño Castaño, 2020). Además, en la Gobernación de Huila cuentan con un conjunto de estrategias y normas relacionadas con las tareas del procedimiento de Gestión y Seguridad de la Información, sin embargo, Beleño García (2022), menciona que éstas no están actualizadas y no existe el personal adecuado que proteja la información. Por lo que, se podría decir que pesar de que existe un conjunto de lineamientos que establezcan el cómo actuar frente a la seguridad de la información, es necesario contratar el personal adecuado.

Asimismo, si el Sistema de Gestión de la Seguridad de la Información se rige bajo las normas de la seguridad de la información será conveniente para la institución, pues brindará a los clientes confiabilidad y ventaja competitiva frente a otras empresas. A pesar de que en reiteradas ocasiones se ha menciona a la norma ISO 27001, esta no es la única, existen otras normas, como se muestra en la Tabla 2, que contienen lineamientos acerca de la seguridad de la información.

Tabla 3. Cuadro comparativo de las normas ISO que regulan la seguridad de la información

Rasgos	ISO/IEC 27001	ISO/IEC 27002	ISO 27701	ISO 27005
Objetivo	Implementar un SGSI para contemplar la triada de la seguridad de la información.	Brinda sugerencias para el control de riesgos y proteger la información.	Basada en la norma ISO/IEC 27001, incluye los requerimientos de administración de privacidad de información.	Brinda la situación de la gestión de riesgos en base a la seguridad de la información.
¿Qué es?	Norma global de seguridad de la información.	Registro de consejos para mantener la seguridad en la información.	Norma que tiene por objetivo velar por la privacidad de los datos basada en la ISO 27001.	Manual para la implementación de un plan de gestión de riesgos de la seguridad de la información.
Certificación	Brinda una certificación a la empresa en ISO 27001.	No existe certificación alguna.	Si se obtiene la certificación de la ISO 27001, se pueden obtener de la ISO 27701	No existe certificación alguna.

Fuente: Modificado a partir de Vásquez (2023), Girbau Roque, (2022), (Guevara Arias & Soriano (2022).

En este contexto, la norma ISO/IEC 27001 es la mejor opción para implementar un SGSI, pues es la norma que abarca un esquema integral completo para ayudar con la creación de un SGSI.

A fin de cuentas, los Sistemas de Gestión de la Seguridad de la Información son instrumentos útiles que apoyan a las organizaciones a la protección de los datos, fortalecer la confianza con los clientes, fortalecer las necesidades legales y mejorar continuamente en la seguridad.

1.3. Implementación de la norma ISO/IEC 27001

En la era de la revolución digital, la información es el pilar fundamental para el éxito organizacional y protegerla es esencial. La norma ISO 27001 surge como una guía internacional para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) y una estructura sólida de la confidencialidad, integridad y disponibilidad (CIA).

La ISO 27001 es una norma creada por la Organización Internacional de Normalización (ISO) con el objetivo de administrar la seguridad de la información en una organización. La terminología correcta para referirse a este precepto es

ISO/IEC 27001, pues hace referencia a la versión inicial del año 2005, la cual se basó en la norma británica BS 7799-2:2002 (De la Rosa, 2021). Esta versión inicial se centró en el manejo de la seguridad de la información en relación con necesidades de identificación, diagnóstico y tratamiento de riesgos, instauración de gestión de seguridad y de un bucle de mejora (Castillo Plata, 2020).

Por otro lado, después de ocho años la norma se actualizó a ISO/IEC 27001:2013. Esta versión adoptó un marco sólido del Anexo SL, similar a otras normas ISO, con el objetivo de poner el foco en procedimientos de gestión de la seguridad de la información y la importancia en el contexto empresarial y liderazgo en la instauración de un SGSI (Mantilla Guerra, 2018).

Sin embargo, dentro de nueve años la norma actualiza su estructura siendo así la ISO/IEC 27001:2022, hasta el presente año es la versión más reciente. Esta incorporó cambios que se relacionan con las amenazas más evolutivas y las prácticas de seguridad de la información. Además, se dio mayor enfoque a la gestión de riesgos y protección de la privacidad (NQA, 2022).

Cabe mencionar que las empresas certificadas en la edición del 2013 de la norma ISO 27001 tenían un lapso de mutación de tres años para cumplir con los nuevos requerimientos de la última versión 2022. Al acoger la ISO/IEC 27001:2022, las empresas generan un sistema reforzado para proteger la información e instauran ventajas como, confiabilidad en los clientes, socios y proveedores; toma de decisiones; y reducción de costos en ciberseguridad. Es por ello, que surge la necesidad de conocer la estructura de esta regla basada en diez cláusulas descritas en la tabla 3 a continuación:

Tabla 4. Descripción de cláusulas de la ISO 27001:2022

N°	Nombre	Descripción
1	Alcance	Da a conocer la intención de la norma. Además, brinda información de a quiénes va dirigida y las necesidades que debe cumplir la empresa. Es importante mencionar, la ISO 27001 está orientada a cualquier modelo de organización.
2	Bases Normativas	Se refiere a otros preceptos que contengan la información similar a la ISO 27001. En este apartado solo se indica la ISO 27000 que ayuda a verificar los requerimientos bases para la implementación de un SGSI.
3	Términos y Definiciones	Se relaciona a la versión actual de la ISO 27000 – SGSI su síntesis y léxico. Cabe mencionar que en este documento existe 81 expresiones y significados que se utilizan en la ISO 27001. Además, de estos términos se usan los siguientes: control de accesos, efectividad, riesgo, evaluación de riesgos, tratamiento de riesgos y gerencia.
4	Contexto de la organización	El proteger información de una empresa dependerá del tipo de contexto: interno, procesos que maneja la empresa; externo, procesos que la empresa no maneja de manera directa. Además, el conocer las partes interesadas para analizar los problemas es fundamental, así como, documentar el alcance del SGSI.
5	Liderazgo	En este sentido el liderazgo es el papel que debe cumplir la organización en la implementación del SGSI. Esta deberá responsabilizarse por crear e implementar políticas de seguridad de la información, establecer objetivos del SGSI y especificar deberes para una rendición de cuentas. Además, tendrá la obligación de comprometerse con el SGSI.
6	Planificación	Estudia las necesidades de la evaluación de riesgos, las cuales son: reconocer los bienes de información, determinar peligros y debilidades, examinar peligros y evaluar peligros. Por otro lado, analiza los requisitos del tratamiento de riesgos para evitarlo, reducirlo, transferirlo y aceptarlo.
7	Soporte	Para implementar un SGSI se necesitan ciertos aspectos que la empresa debe cumplir: capital, competencia, concienciación, documentos de control y comunicación.
8	Operación	Se refiere a la gestión de riesgos de seguridad de la información. Por ello, se consideran aspectos relevantes como: determinar actividades frecuentes, implementación de evaluación y tratamiento de riesgos, examinar riesgos para reducirlos, otorgar tareas para la gestión de procedimientos, por último, monitorear y actualizar de manera continua los procesos.
9	Evaluación del rendimiento	Sus objetivos principales son: monitorear de procesos acerca del rendimiento de un SGSI, manejar los riesgos de seguridad de la información, evaluar el SGSI de manera periódica a través de la dirección y mejorar continuamente según las necesidades.
10	Mejora	Garantizar un SGSI eficiente, alineado a las metas de seguridad de la empresa a largo plazo y adecuado a las necesidades de la empresa.

Fuente: Modificado a partir de NQA (2022)

Además de conocer la estructura base de la norma ISO 27001, es importante comprender el modelo que se deberá seguir para su implementación. Como menciona *National Quality Assurance* (2022), este ejemplar se llama PDCA (Planificar, Hacer, Verificar y Actuar) o Ciclo de Deming, el cual es un bucle que tiene cuatro fases como se muestra en la figura 1.

Figura 1. Ciclo PDCA de un SGSI en relación con la norma ISO/IEC 27001

Fuente: Colegio Oficial de Ingenieros de Telecomunicación (2012)

Cada fase del ciclo PDCA en la figura 1 cubre una parte fundamental de la creación de un Sistema de Gestión de la Seguridad de la Información. Planificar es igual a crear el SGSI, hace referencia a la implementación y operación de este, verificar se encarga de supervisar y revisar el sistema, por último, actuar mantiene y mejora el SGSI. Además, alrededor del ciclo se contemplan las partes interesadas entre estas los requisitos, expectativas y gestión de la seguridad de la información. Sin embargo, a continuación, se detalla cada una de las etapas de acuerdo con NQA (2022):

1. **Planificar:** se relaciona con las cláusulas contexto de la organización, liderazgo y planificación. Pues, se determina las metas, recursos, requerimientos del cliente y las partes interesadas.
2. **Hacer:** se relaciona con la cláusula soporte y operaciones. Realización de procesos del SGSI en conjunto con la operatividad de políticas y controles.
3. **Verificar:** se relaciona con la cláusula de evaluación de rendimiento. Monitorear y medir el provecho de los procedimientos.
4. **Actuar:** se relaciona con la cláusula de mejora. Ejecutar medidas para actualizar el SGSI según sea necesario.

La norma ISO 27001 en conjunto con el ciclo PDCA brindan una estructura sólida para instaurar y gestionar un Sistema de Gestión de Seguridad de la Información eficiente.

Para Ecuador, las principales empresas certificadoras en la norma ISO 27001 son:

- **AENOR**: empresa pionera en la certificar acerca del Sistema de Gestión de Privacidad de la Información, además, de estar acreditada para la ISO 27001.
- **SGS**: sus servicios se basan en realizar auditorías para certificar en ISO 27001, además, de brindar consultorías y cursos de formación.
- **Bureau Veritas**: empresa líder en América Latina, presentes en 140 países. Brindan certificación en ISO / IEC 27001.

Por lo tanto, para las empresas ecuatorianas que tienen el objetivo de ofrecer protección en el manejo de su información importante y que buscan cumplir con los requisitos necesarios de seguridad, la norma expuesta con anterioridad ofrece beneficios de confidencialidad, regulación de privacidad de datos y confiabilidad hacia las partes interesadas de la organización. Además, si requieren adoptar la certificación en ISO 27001, existen varias entidades que ofrecen el servicio, por lo que, no existe excusa para ninguna organización para no proteger su activo más importante.

CAPÍTULO II. DISEÑO METODOLÓGICO

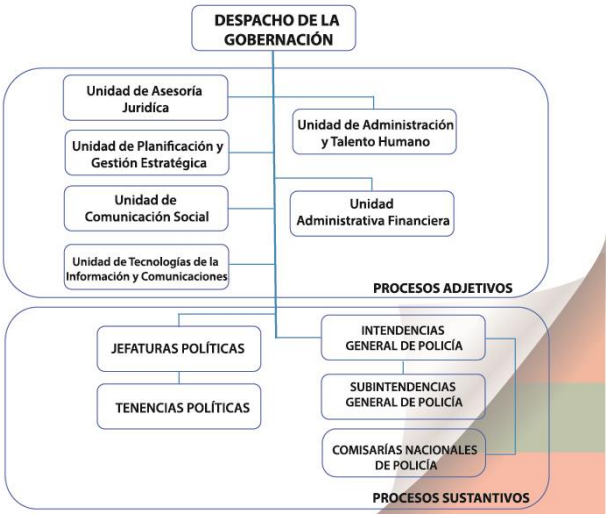
En el diseño metodológico se presenta la contextualización de la institución estudiada, Gobernación de Tungurahua, además de la metodología utilizada para el levantamiento de datos y el proceso de desarrollo del instrumento. El presente capítulo es importante porque es la etapa en donde se va a realizar la guía para la implementación de la norma ISO 27001:2022 en el Departamento TI de la Gobernación de Tungurahua, se presenta la metodología de investigación, cuestionarios de autoevaluación y lista de verificación basados en la ISO 27001, y el método de desarrollo, Planear, Hacer, Verificar y Actuar (PHVA).

2.1. Caracterización de la empresa o institución

La Gobernación de Tungurahua es una entidad pública que se encuentra ubicada en la ciudad de Ambato, Ecuador. Forma parte del estado ecuatoriano, tiene como objetivo fundamental la gestión de los recursos del gobierno y la representación de la provincia de Tungurahua. La función principal engloba roles indispensables para la supervisión y administración de la seguridad, gestión pública y conservación del orden y armonía social dentro de la provincia. Asimismo, la Gobernación no es únicamente un orden administrativo del régimen, sino cumple con responsabilidades determinantes en la implementación de protocolos para la ciudadanía tungurahuense (Gobernación de Tungurahua, 2024).

La estructura institucional de la Gobernación de Tungurahua, figura 2, se basa en el cumplimiento de la misión de gestión y representación del estado.

Figura 2. Organigrama institucional de la Gobernación de Tungurahua



Fuente: Gobernación de Tungurahua (2024)

El organigrama de la Gobernación de Tungurahua se conforma por seis unidades administrativas y con áreas operativas (Jefaturas Políticas, Tenencias Políticas, Intendencias Generales y Comisarías Nacionales). A continuación, se describe la función de las distintas áreas, según Núñez Palencia (2024):

- **Despacho de Gobernación:** liderado por el Gobernador/a de Tungurahua, quien es la máxima autoridad. Dentro del despacho se gestiona las actividades de la Gobernación y se monitorea los procesos de las otras áreas para el cumplimiento de estas.
- **Unidad de Asesoría Jurídica:** su función principal es ofrecer ayuda y orientación legal para la observancia normativa actual en todos los procesos.
- **Unidad de Planificación y Gestión Estratégica:** su deber es le administración para coordinar las actividades institucionales y la planeación de estrategias para cumplir con los objetivos propuestos.
- **Unidad de Comunicación Social:** se encarga de la distribución de información acerca de las actividades que se han realizado o se van a realizar hacia la ciudadanía mediante los distintos medios de comunicación.
- **Unidad de Administración y Talento Humano:** gestiona los recursos humanos y garantiza el bienestar del personal.

- **Unidad de Administración Financiera:** cumple con la gestión de presupuesto y finanzas para una buena operatividad de fondos.
- **Unidad de Tecnologías y Comunicaciones:** su función principal es brindar soporte técnico a los usuarios de la institución, así como, asegurar la información. Además, de gestionar todas las actividades digitales gubernamentales.

Las unidades administrativas cumplen su función dentro de la institución y son aquellas que se encargan de cumplir los procesos para que la cabeza de la Gobernación cumpla con la protección y respaldo a la ciudadanía. Por otro lado, Núñez Palencia (2024), explica que existen áreas operativas que realizan sus funciones fuera de la institución, pero colaboran a esta.

- **Jefaturas y tenencias políticas:** su objetivo principal es representar al gobierno tungurahuense en los distintos sectores de la provincia.
- **Intendencias generales:** gestionan el cumplimiento de las políticas de seguridad a la ciudadanía.
- **Comisarías:** apoyan en el control y aplicación de los protocolos públicos.

El área de estudio del presente documento es la Unidad de Tecnologías y Comunicaciones, Vladimir Robayo, director actual del área, expresa que las funciones principales de este departamento se basan en proteger la información sensible y brindar apoyo tecnológico a los distintos sistemas, como el sitio *web* institucional y los sistemas de comunicación electrónica. Las responsabilidades se detallan, a continuación:

- Crear, renovar, certificar y dar seguimiento a la implementación de manuales, guías, políticas, procesos, metodologías y/o sistemas en el contexto de TI.
- Gestionar planes para actualizar anualmente el servicio de alojamiento *web*, dominio, correo electrónico institucional, certificados de seguridad y mantenimiento del sitio *web* institucional.
- Gestionar la adquisición y actualización de equipos tecnológicos y *networking* de la Gobernación de Tungurahua.
- Gestionar del mantenimiento de equipos tecnológicos, comunicaciones y sistema de *networking* de la Gobernación de Tungurahua.

- Gestionar el mantenimiento preventivo y correctivo del sistema de video vigilancia de la Gobernación de Tungurahua.
- Realizar reportes administrativos, de monitoreo y control de capacitación, incidencias en los distintos bienes de *hardware* y *software* para brindar soluciones tecnológicas.
- Gestionar y dar seguimiento en las zonas de su competencia, el funcionamiento y operatividad de los procesos desconcentrados.
- Crear, comprobar y aprobar términos de referencia, funcionalidades y métodos para la contratación del desarrollo servicios tecnológicos, consultorías y demás en relación con TI.
- Dar seguimiento y disponer la atención para solucionar los incidentes notificados que se dan en los bienes informáticos que administra la institución.
- Administrar las redes y bienes tecnológicos de la institución.

En la actualidad, la unidad presenta inconvenientes en la aseguración de los datos, a un nivel micro la estructura es bastante limitada porque cuenta con un solo responsable, encargado de gestionar todos los bienes tecnológicos de la institución.

A detalle, las funciones de los recursos tecnológicos abarcan, lo siguiente:

- **Mantenimiento y mejora de equipamiento:** monitoreo y renovación de los dispositivos tecnológicos utilizados en la Gobernación. Incluye computadoras, laptops, impresoras, redes, *routers*, ente otros.
- **Gestión de redes:** administración de la red local de la institución, para establecer una conectividad segura y con alta disponibilidad entre las distintas áreas.
- **Seguridad de equipamiento:** instalación de sistemas de cortafuegos, VPN, antivirus, otros recursos de seguridad para protección de infraestructura contra accesos no autorizados o ciberataques.
- **Administración de sitio web institucional:** edición y actualización de información de la página oficial de la Gobernación. Control de brechas de seguridad para evitar ciberataques.

- **Copias de seguridad:** configuración de copias de seguridad periódicas de la página web e información del área, además, de soporte en el ámbito para las otras unidades.
- **Soporte técnico a usuarios:** brindar soporte a las unidades según sus necesidades para el correcto funcionamiento de la institución.
- **Planificación y gestión de proyectos:** elaboración de planes anuales y mensuales para el avance del departamento, establecer objetivos y presupuestos.

Las funciones descritas con anterioridad se ejercen en el ámbito actual del departamento TI, siendo que, lo óptimo del área sería que se encargue de la implementación de un SGSI que permitirá gestionar procedimientos de manera clara y estable para una buena seguridad de la información, además, de consolidar el cumplimiento de necesidades legales y normativas.

2.2. Metodología de investigación

Enfoque de investigación

Finol de Franco & Vera Solórzano (2020) señalan que un enfoque de investigación es la agrupación de métodos y procesos que se aplican para la recolección, análisis e interpretación de los datos. Existen dos enfoques fundamentales: el cualitativo, se concentra en entender tendencias por medio de la recolección de datos descriptivos, tales como anécdotas, opiniones y comportamientos para obtener interpretaciones amplias acorde a la situación; por otro lado, el cuantitativo, está enfocado en la obtención de datos numéricos, con el objetivo de encontrar relaciones, generalidades y patrones a través de estadísticas.

Debido a que la investigación, presenta como meta el diseño de una guía para implementar la ISO 27001, y dado que la recopilación de la información se enfoca en una población reducida, el estudio tiene un enfoque cualitativo. Esto, permite entender los procesos, hábitos y requerimientos actuales de la Unidad de TI de la Gobernación en relación con la seguridad de la información.

Método de investigación

Los métodos de investigación son un conjunto de herramientas generales que guían el proceso de obtención de datos para explorarlos e interpretarlos. Su clasificación se basa en: teórico, su objetivo principal es verificar y comprender las definiciones, tesis y bibliografía existente acerca del motivo de estudio; no obstante, existe el práctico, la adquisición de datos se la realiza por medio de encuestas, entrevistas, u otras herramientas que conceden información de una fuente primaria (Finol de Franco & Vera Solórzano, 2020).

Siendo así, el estudio utiliza métodos teóricos de tipo analítico-sintético porque se descompone los problemas de seguridad en los elementos fundamentales y unirlos para una solución (Falcón López & Ramos Serpa, 2021), por ejemplo, se divide los procedimientos de seguridad de la información en las distintas cláusulas de la norma después se unen estas partes para comprenden el fenómeno. Además, el otro método es inductivo-deductivo, pues inicia con una investigación de un caso definido para sistematizar hallazgos y así aplicar conclusiones a estos casos (Falcón López & Ramos Serpa, 2021), por ejemplo, se identifica las acciones de seguridad de la información que realizan en la Gobernación para decidir lineamientos de la ISO 27001.

Asimismo, el estudio utiliza métodos prácticos de tipo encuesta, recolección de datos de manera directa de dos representantes de las distintas unidades de Asesoría Jurídica, Planificación de Gestión Estratégica, Comunicación Social, Tecnologías y Comunicaciones, Administración y Talento Humano, Administración Financiera, Intendencias, Jefaturas, Tenencias y Comisarías de sus respectivos cantones o parroquias de Tungurahua. Otro método es la lista de chequeo porque evalúa la infraestructura en cuestiones de seguridad de la información en perspectiva del encargado del Departamento de TI.

Tipo de investigación

Cevallos Veintimilla, Polo Luna, Salgado Chasipanta, & Obrea Vergara (2017), indica que las investigaciones se clasifican como aplicada, exploratoria, de campo, entre otras. El proyecto utiliza un tipo de investigación documental, estudio de

documentos formales como orígenes de información, en el marco teórico se requirió artículos científicos, proyectos investigativos, libros y documentación oficial de la Gobernación de Tungurahua. Igualmente, adopta una investigación descriptiva, enumeración de características de la institución a estudiar y se restringe a prestar atención a lo que ocurre, pues tiene por objetivo detallar la situación de la Gobernación de Tungurahua en base a la seguridad de la información y establece bases para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Técnicas e instrumentos de investigación

La técnica de investigación es un proceso que brinda información que el investigador necesita para responder la pregunta de investigación. Las técnicas de investigación trabajan de la mano con instrumentos, herramientas útiles que ayudan a la medición de resultados (Hernández Mendoza & Duana Ávila, 2020). En este proyecto se utiliza la encuesta técnica de investigación en conjunto con el instrumento que es el cuestionario, serie de preguntas que se realiza a un número de personas (Arias Gonzáles, 2020), en este caso a dos representantes de cada dependencia. En el caso de jefaturas y comisarías políticas se realizó a nueve individuos, uno por cada cantón; por otro lado, a cuarenta y cuatro funcionarios de comisarías políticas, uno por cada parroquia. Esto da un total de sesenta y dos (62) personas encuestadas, sin embargo, no todos respondieron a la encuesta que fue habilitada durante cuatro semanas, por lo que se obtuvo cincuenta y cuatro (54) respuestas, las preguntas se basaron en encontrar las debilidades que tiene la entidad frente a la protección de información y las prácticas que cada área tiene para prevenir los riesgos y amenazas. Además, se realizó una lista de chequeo que verifica la existencia de requerimientos acorde a los que solicita la ISO 27001, como políticas de seguridad, evaluación de riesgos, documentación de la institución.

Diagnóstico de la situación actual

Resultados de la lista de chequeo

El diagnóstico de la lista de chequeo que se realizó al director de la Unidad de Tecnología de la Gobernación de Tungurahua facilita comprender la situación

actual de la entidad respecto a los requerimientos de la norma ISO 27001. Por medio de esta evaluación se conoce los recursos con los que la institución cuenta, aquellos que necesita implementarlos y los que se encuentran en proceso.

A continuación, se expone un resumen por secciones basado en los gráficos del Anexo 1, esta perspectiva brinda una visión integral de los desafíos para una implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI).

- **Contexto de la organización:** como aspecto positivo la institución reconoce de una manera sólida los puntos internos y externos fundamentales para la seguridad de la información, esto es importante porque ayuda a la comprensión de riesgos y amenazas que afectarían al SGSI. Sin embargo, en la institución no se ha regularizado la documentación acerca del alcance del SGSI, que es uno de los requerimientos principales de la norma, pues consolida que todos los implicados obtengan una visión de las metas y límites del sistema. No obstante, se encuentra en proceso el reconocimiento de las partes interesadas, así como, la recolección de los requisitos, este aspecto es importante para delimitar las funciones y responsabilidades dentro del SGSI.
- **Liderazgo:** la cabeza de la institución se encuentra en proceso de aceptación y aprobación de la implementación de un SGSI, pues el primer paso para lograrlo sería la inducción del tema por parte del departamento de TI. Por otro lado, la designación de roles y deberes aún no se encuentra implementada y esto es importante porque la ISO 27001 exige que cada integrante de la institución reconozca las responsabilidades que tiene en el sistema. De otro modo, la realización de políticas de seguridad de la información no está presente y es importante aclarar que deberán estar basadas en los lineamientos de la ISO 27001, incluso, ser aprobadas y comunicadas por la alta dirección.
- **Planificación:** Un avance importante para la implementación de un SGSI es la documentación de riesgos relacionados con la seguridad de la información, con la cual la Gobernación está en proceso de creación. Por otra parte, no cuentan con el documento de tratamiento de riesgos certificado o SoA ni mucho menos con una técnica de evaluación de riesgos, tampoco con objetivos específicos

medibles, pues esto ayuda un mejor desempeño del SGSI y generar procedimientos de acción.

- **Soporte:** La ISO 27001 solicita que en la organización existan recursos necesarios para la implementación de su sistema, para lo cual la Gobernación no ha establecido ningún medio para instaurar el sistema ni mucho menos para mantenerlo. Además, no existen procedimientos que rectifiquen que el personal tiene la capacidad de ejecutar planes de seguridad de la información. Incluso, no se cuenta con un documento que establezca los requisitos del SGSI. Por otra parte, la comunicación a los usuarios y la concientización acerca del tema se encuentra en proceso.
- **Operación:** Los procedimientos principales para la planificación y puesta en marcha del SGSI no se están realizando, cabe recalcar que esto ayuda a cumplir los objetivos según lo estipulado por la norma. Conjuntamente, los documentos que brinden información de protección de información tampoco existen. Sin embargo, los respaldos periódicos y los documentos de los hechos referentes a la seguridad de la información se encuentran en proceso.
- **Evaluación de desempeño:** La presencia de indicadores de rendimiento o KPI para la evaluación de seguridad de la información, de auditorías internas del SGSI y de educación-evaluación del sistema por parte de la alta dirección, son procesos inexistentes en la institución, a pesar, de que son requisitos que ayudan a monitorear el desempeño de un sistema y detectar las zonas de mejora. Sin embargo, al no contar con un actual SGSI, es imposible que la entidad cuente con una avaluación de desempeño.
- **Mejora:** la inexistencia de inconformidades, de procesos de continuidad y mejora continua es evidente al no contar con SGSI.
- **Anexo A:** La gobernación cuenta con políticas de seguridad de información, este es un avance clave para un sistema de seguridad, incluso, se encuentra en proceso la realización de un inventario actualizado de los activos de la entidad e implementación de medidas para contrarrestar los ciberataques. Por otro lado, la administración de accesos, evaluación de vulnerabilidades, plan de negocio con seguridad de la información y el cifrado de datos son actividades inexistentes en la organización. Lo cual, deja a las expectativas de que la entidad se encuentra vulnerable antes cualquier amenaza.

En términos generales, la evaluación de la lista de chequeo fundamenta que la Gobernación cuenta con ciertos pasos para la implementación del Sistema de Gestión de Seguridad de la Información; sin embargo, existen insuficiencias que deben ser solventadas y procesos puestos en marcha que deberán concluir de manera satisfactoria. De acuerdo con este análisis, la Gobernación queda en un escenario vulnerable ante riesgos informáticos y físicos, lo que señala lo fundamental de enfocar la alineación integral con los requerimientos de la ISO 27001 para contemplar un sistema eficiente.

2.3. Metodología de desarrollo

De acuerdo con lo que se explicó en el capítulo I, epígrafe 1.3, el PDCA (Planificar, Hacer, Verificar y Actuar) o Ciclo de Deming es la metodología adecuada porque garantiza flexibilidad, adaptabilidad y mejora sostenida al Sistema de Gestión de Seguridad de la Información (SGSI).

A continuación, se expone la propuesta de trabajo dividida por cada fase del Ciclo de Deming y subdividida por cada cláusula desde la 4 hasta la 10 y completada con los datos recolectados en la encuesta realizada a los distintos funcionarios de la Gobernación de Tungurahua, se debe tomar en cuenta que el plan de trabajo se enfoca en el Departamento de TI. Es importante mencionar que la guía no contiene las cláusulas desde 1 a la 3 porque expresan información introductoria a la norma y brindan contexto de esta, más no requerimientos específicos para la implementación del SGSI.

Fase 1: Plan

a) **Contexto de la organización**
    1. **Organigrama**

La ISO 27001:2022 indica que la unidad a la que va dirigida el Sistema de Gestión de Seguridad de la Información (SGSI), en este caso la de TI, debe contener una estructura organizacional definida. La Tabla 5, presenta los recursos que tiene la unidad y los compara con los que requiere la norma, además, presenta lo que debería implementar.

Tabla 5. Análisis de la estructura organizacional de la Unidad de TI frente al requerimiento de la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
Una sola persona que se responsabiliza de todas las actividades de la unidad definidas en el Estatuto Orgánico del Ministerio de Gobierno.	Distribución jerárquica para administrar la seguridad de la información con funciones definidas.	Estructura organizacional con funciones, se recomienda contar con, Coordinador de Ciberseguridad, Coordinador de redes, Profesional especializado en la protección de datos y Responsable para el soporte técnico.
	División de responsabilidades entre los funcionarios, en especial dentro del SGSI.	Profesionales especializados en TI, específicamente en seguridad de la información, infraestructura y soporte para abarcar las funciones que impone el Estatuto Orgánico del Ministerio de Gobierno.
	Jerarquía de entidades con responsabilidades del SGSI.	Organigrama jerárquico de subunidades de TI como: Ciberseguridad, Soporte, Proyectos, Infraestructura para una mejor gestión de roles.

Fuente: elaboración propia.

Este análisis presentado recalca las debilidades que existe en la Unidad de TI y las acciones correctivas para mejorar la redistribución de funciones y responsabilidades para una mejor administración.

La Tabla 6 presenta la comparación de las funciones que se realizan en la unidad en la actualidad y presenta lo que requiere la ISO 27001, además se expone las sugerencias a instaurar para complementar la estructura organizacional de la unidad.

Tabla 6. Análisis de funciones de la Unidad TI en base a la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
Documentación que avala que una de sus funciones es encargarse de la seguridad de la información, sin embargo, no se ejecuta la misma.	La seguridad de la información debe contener un enfoque claro para la gestión de amenazas y protección de datos.	Asignar un Coordinador de Ciberseguridad para supervisión de la instauración de políticas de seguridad.
Documentación de la función de gestión de infraestructura tecnológica de hardware. Sin embargo, la unidad cuenta con un inventario tecnológico limitado y con una sola persona que gestiona esto.	La gestión de infraestructura tecnológica no es únicamente administración de inventario de hardware sino también mantenimiento, actualización, capacitación del personal, inventario de software.	Asignar un Coordinador de infraestructura Tecnológica para administrar software, hardware, mantenimiento.
Documentación que avala que una de sus funciones es encargarse de la gestión proyectos, sin embargo, no se ejecuta la misma por escases de personal.	La gestión de proyectos tecnológicos está relacionada con la seguridad de la información.	Asignar un Coordinador de proyectos que administre propuestas y optimice recursos y procesos.
Realización de soporte a usuarios, pero en toda la institución se encuentra solo un profesional.	Existencia de un equipo de soporte técnico para mejor operatividad.	Asignar un responsable de soporte a técnico que gestione las necesidades de usuario en problemas comunes y problemas complejos, como seguridad de información.
Al existir solo una persona encargada, se encarga de algunas funciones y otras no las cumple por sobrecargo de trabajo.	Asignación de roles y responsabilidades al personal de la unidad.	Organigrama funcional que evidencie las subunidades de TI y la asignación de funciones.

Fuente: elaboración propia.

Basado en el análisis de las tablas anteriores se propone que la estructura organizacional de la Unidad de TI cuente con un director de TI que sea la cabeza del área apoyado por tres subunidades: infraestructura y redes para administrar *software, hardware,* mantenimiento, y gestión de redes; otra de seguridad y protección de datos para supervisión de la instauración de políticas de seguridad; por último, una de soporte y capacitación para gestione las necesidades de usuario en problemas comunes y problemas complejo. El director de TI será el encargado de crear propuestas de proyectos, además, optimización de recursos y procesos.

2. Funciones dentro del SGSI

A pesar del personal reducido con el que cuenta la Unidad de TI de la Gobernación, abarca la mayoría de las funciones, sin embargo, aquellas que la ISO 27001 solicita no cumplen, por lo que en la Tabla 7 de detalla los que se debe considerar.

Tabla 7. Análisis de las funciones para el SGSI de la Unidad de TI de la Gobernación frente a la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
Planificación de proyectos a nivel institucional, más no existe a nivel de Unidad de TI orientado a un SGSI.	Plan estratégico de la seguridad de información alineados a los objetivos institucionales.	Plan Estratégico de Tecnologías de Información (PETI) en base a la ISO 27001:2022
Escasez de protocolos de seguridad de la información.	Manuales, documentación de protocolos y procesos de seguridad de la información.	Crear políticas y procesos de seguridad de información alineados a la ISO 27001:2022.
La seguridad de información no está muy bien definida en la Unidad de TI ni mucho menos dentro de un SGSI.	Políticas de seguridad de la información documentadas y en ejecución.	Creación e implementación de políticas de seguridad de la información de control de acceso, plan de continuidad ante amenazas.

Fuente: elaboración propia.

Una vez analizada la información presentada en la tabla se recomienda a la Unidad TI crear un plan estratégico para poder alinear las políticas de seguridad de información a este.

3. Infraestructura Tecnológica

En términos de infraestructura tecnológica la ISO 27001 solicita ciertos implementos para una mejor gestión del SGSI, además, de la creación de documentación necesaria. En la Tabla 8, se expone lo que la Unidad TI dispone tanto a nivel de equipos electrónicos como de sistemas y lo que se sugiere implementar en el área.

Tabla 8. Análisis de la infraestructura tecnológica de la Unidad de TI frente a lo que solicita la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
Inventario tecnológico de la institución de acuerdo con la Unidad de TI, existen: 112 CPU, 109 monitores, 91 impresoras, 4 laptop, 20 reguladores de voltaje, 2 XVR. Además, se debe considerar que el 66.46% de equipos son obsoletos y el 28.49% no lo están.	Infraestructura estándar, mantenida, segura y actualizada.	Crear e instaurar un plan de actualización de equipos tecnológicos.
Red interna.	Redes seguras con control de acceso para preservar la infraestructura.	Implementar técnicas de seguridad como VPN, firewall, intervención de acceso y Administración de eventos e información de seguridad o SIEM.
Escasez de sistemas de seguridad de información.	Control de seguridad con ayuda de sistemas para proteger la infraestructura.	Implementación de sistemas como: firewall, antivirus, detección de intrusos y respaldo de datos.
El mantenimiento de equipos si se realiza, sin embargo, no existe documentación de este proceso dentro de un SGSI.	Plan de mantenimiento de equipos dentro del SGSI.	Creación de un plan de mantenimiento tanto preventivo como correctico basado en SGSI.
En ocasiones, la información sensible se maneja en papel sin controles de seguridad.	Además, de que la información digital se encuentre protegida, también la información física debe estarlo.	Creación de sistema de gestión de documentos en papel y en un futuro digitalizarlos. Gestionar controles de acceso no autorizado.

Fuente: elaboración propia

4. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Gobernación de Tungurahua está establecido por la urgencia de instaurar un sistema robusto de confidencialidad de datos dentro de la Unidad de Tecnologías de la Información y Comunicación (TI), pues es el encargado de asegurar la información en la entidad. Este SGSI empezará por implementarse en dicha unidad para una mejor gestión de infraestructura tecnológica, gestión de riesgos, administración de sistemas, procesos de respaldo y recuperación de datos y regularización de protección de datos y buenas prácticas de control de acceso.

La institución reconoce que es fundamental el proteger el activo más valioso de cualquier entidad, la información. Por ello, es imperativo la aplicación de políticas y procesos del SGSI en el área tecnológica para que los usuarios que dependen del soporte técnico de esta evidencien la existencia de integridad, confidencialidad y disponibilidad.

Por otro lado, el sistema abarcará los recursos tecnológicos como, servidores, redes, equipos; sistemas como, sitio web, sistemas de comunicación electrónica; y documentación física de procesos de la institución.

b) Liderazgo

1. Compromiso de alta dirección

Para la realización de un SGSI se requiere el compromiso e interés de la alta dirección de la institución en este caso del Gobernador a cargo. Sin embargo, la investigación se enfoca en realizar una guía para implementar la ISO 27001 en la Unidad TI, por lo que el director de TI será quien se comprometa con la gestión del SGSI, pero con la autorización de la máxima autoridad. En la tabla 9 se explica lo que deberá realizar la Unidad TI en base a lo que ya disponen.

Tabla 9. Análisis de compromiso de alta dirección de la Unidad de TI de la Gobernación frente a la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
La dirección departamental se encuentra en proceso de implementación de un SGSI. Sin embargo, necesita el apoyo institucional, que se encuentra en proceso.	La alta dirección de la entidad y de las unidades debe comprometerse activamente en la implementación del SGSI.	- Crear una capacitación para el director de la Unidad de TI acerca de la ISO 27001. - Adquirir recursos que validen el compromiso de la institución.
Inexistencia de objetivos de la seguridad de información.	Determinar objetivos basados en las políticas de seguridad de la información.	Determinación de objetivos específicos para el SGSI, como menorar riesgos de seguridad, optimizar el tiempo de respuesta ante las amenazas y resguardar la información sensible.
La administración de riesgos se encuentra en proceso, no existe una meta estructurada, tampoco un plan de tratamiento.	Plan formal de identificación y tratamiento de riesgos.	Metodología de gestión de riesgos, creación de Declaración de Aplicabilidad (SoA) y plan para tratar riesgos.
La colaboración de la Unidad TI es limitada porque solo existe un solo funcionario en el área y los recursos son menores.	El personal debe estar completamente inmerso en la planificación e implementación del SGSI.	Crear un equipo de trabajo con funciones específicas y definidas para una buena implementación del SGSI.
No existe un sistema de comunicación formal acerca de la seguridad de la información.	Sistema de comunicación periódico desde el Departamento TI hacia la alta dirección para informar sobre el estado del SGSI.	Crear un procedimiento formal que gestione un reporte de manera periódica sobre la efectividad del SGSI y los incidentes o mejoras que se han dado.

Fuente: elaboración propia.

2. Políticas de seguridad de la información

La ISO 27001 específica que las políticas deberán estar alineadas a las metas estratégicas de la organización. En este contexto se deja constancia en la Tabla 7 que no dispone ni de plan estratégico institucional ni del departamento. Por lo que, las propuestas realizadas en la presente investigación, Tabla 10, deberán oportunamente ser contrastadas con los dos elementos antes mencionados.

Tabla 10. Análisis de políticas de seguridad de la información de la Unidad de TI frente a lo que solicita la ISO 27001:2022.

La Unidad de TI de la Gobernación cuenta con:	**La ISO 27001:2022 señala que la institución debería contar con:**	**La Unidad de TI de la Gobernación debería implementar:**
Las políticas de seguridad que considera tener la unidad (políticas de uso de correo institucional y políticas de respaldo de información) no se encuentra formalmente avaladas por la alta dirección.	Políticas de seguridad avaladas por la alta dirección y alineadas a las metas estratégicas de la institución.	Crear y avalar las políticas de seguridad de información con objetivos claros, alcance y compromiso de la institución, en especial de la persona al mando, para resguardar la información. Además, la política debe incluir la triada de la información: confidencialidad, integridad y disponibilidad de los datos. Conjuntamente, las políticas de respaldo de información deberían incluir: - Respaldos periódicos y cifrados. - Plan de recuperación ante desastres con documentación.
Se encuentra en proceso la gestión de riesgos, es decir, no contienen un plan estructurado.	Proceso de gestión de riesgos: caracterización, diagnóstico y tratamiento de estos para asegurar la información.	Crear e instaurar un plan de gestión de riesgos dentro de la Unidad de TI para la mitigación de riesgos en relación con los bienes de la información. Este debe incluir: - Diagnóstico y división de incidentes. - Medidas de respuesta. - Documentos de análisis post – incidente. Asimismo, realizar la Declaración de aplicabilidad (SoA) con el detalle de los riesgos.
La administración de claves es básica, sin control formal de acuerdo con políticas de acceso.	Proceso de control de acceso: físico y lógico para proteger información.	Crear la política de control de acceso: - **Control de acceso físico:** asegurar el lugar de trabajo, máquinas y almacenamiento físico. - **Control de acceso lógico:** administración de claves, autenticación en dos pasos, gestión de permisos y tareas.
Utilización de medidas para contrarrestar el malware o ciberataques con firewall y antivirus. Sin embargo, no cuentan con políticas formales para este problema.	Implementación de medidas formales para mitigar riesgos cibernéticos.	Crear y formalizar políticas de protección contra ataques cibernéticos: - Antivirus actualizado. - Sistema de detección de intrusos.

		- Seguimiento de redes para contrarrestar amenazas.
Existe comunicación electrónica sin cifrado ni medidas de seguridad.	Políticas para asegurar las comunicaciones electrónicas con ayuda de cifrado y medidas de seguridad.	Crear y formalizar políticas de seguridad a nivel de comunicaciones: - Cifrado de correos electrónicos. - Protocolos como HTTPS y VPNs.
Las auditorías se realizan anualmente, pero no existe documentación ni se sigue un proceso sistemático.	Auditorías periódicas para evaluación de SGSI y diagnóstico de políticas.	Crear un proceso de auditorías internas: planificación, realización y seguimiento, incluso, generar la documentación de rastreo y resultados.
En ocasiones, se realizan capacitaciones no estructuradas.	Plan de concientización y capacitación regular para todo el personal acerca de las políticas de seguridad de la información.	Plan de capacitación de las políticas.

Fuente: elaboración propia

3. Asignación de funciones dentro del SGSI

La Tabla 11 consta de una base fundamental para la asignación de las funciones que impone la ISO 27001 dentro del SGSI de acuerdo con el rol sugerido y al área de la Unidad TI perteneciente a la estructura organizacional.

Tabla 11. Roles y funciones dentro del SGSI

Rol	**Funciones**	**Competencias**	**Área de la Unidad TI**
Líder del SGSI	- Diseño de Plan Estratégico de Tecnologías de Información. - Gestionar la instalación y conservación del SGSI. - Delimitar y renovar las políticas de seguridad de la información. - Monitorear la gestión de riesgos y auditorías. - Mantener informada a la alta dirección acerca del funcionamiento del SGSI.	Conocimiento de la ISO 27001.	Director de Unidad TI
Auditor interno del SGSI	- Ejecutar auditorías del SGSI. - Comprobar el cumplimiento de políticas y medidas. - Determinar irregularidades y proponer acciones de corrección.	- Auditoría de Tecnologías de Información - Conocimiento de la ISO 27001.	Director de Unidad TI
Consultor de Seguridad de información	- Crear y controlar las medidas de seguridad. - Administrar los riesgos de seguridad. - Efectuar análisis de riesgos. - Crear y formalizar las políticas de acceso.	Especialista en ciberseguridad.	Área de seguridad y protección de datos
Coordinador de redes.	- Asegurar la infraestructura tecnológica. - Instauración de firewall, sistemas de detección de intrusos y sistemas de prevención de intrusos. - Crear respaldo de información.	Administración de infraestructura de redes y comunicación.	Área de infraestructura y redes.
Coordinador de Protección de datos.	- Asegurar la utilización de normas de resguardo datos. - Monitorear el tratamiento de información sensible. - Administrar la privacidad de la información personal.	Especialista en protección de datos.	Área de seguridad y protección de datos
Coordinador de concientización y capacitación.	- Crear plan de capacitación sobre protección de información. - Incentivar a la utilización de medidas de seguridad. - Analizar resultados de efectividad de las capacitaciones.	Soporte y capacitación en áreas tecnológicas.	Área de soporte y capacitación.
Responsable de la documentación de SGSI	- Actualizar las políticas, procesos y SoA del SGSI. - Gestionar los documentos del SGSI.	Especialista en ciberseguridad.	Director de Unidad TI.

Fuente: elaboración propia

c) Planificación

Para la sección de planificación del SGSI se utiliza la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), que permite identificar, diagnosticar y tratar riesgos relacionados con sistemas de información. El objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los recursos informáticos ante las vulnerabilidades. Además, este marco ayuda a instituciones para tomar decisiones, asegurar continuidad operativa y cumplir normas de seguridad como ISO 27001 (Contreras Olea, 2022).

1. Planificación para identificación de riesgos

Determinación del contexto:

- **Encargado:** Dirección de la Unidad de TI.
- **Alcance:** analizar riesgos, identificar los sistemas, recursos de información y procedimientos a evaluar, Tabla 12.
- **Definir activos de información:** clasificar los activos de información en pública, confidencial y sensible.

Identificación de los activos de información:

- **Encargado:** Coordinador de redes
- **Alcance:** adquirir información de cuántos activos de información existen en la institución y sus características, realizar un inventario, Tabla 12.
- **Definir activos de información:** clasificar de acuerdo con la importancia.

Identificación de amenazas

- **Encargado:** Consultor de seguridad de la información
- **Alcance:** reconocer las amenazas que rompen la confidencialidad, disponibilidad e integridad, Tabla 12.
- **Definir vulnerabilidades:** diagnosticar si existe sistemas desactualizados, falta de monitoreo de acceso, entre otros.

Valoración del riesgo

- **Encargado:** Responsable del SGSI
- **Alcance:** establecer el impacto y la probabilidad de cada riesgo, Tablas 18, 19 y 20.
- **Definir un nivel de riesgo:** clasificar ente nivel medio bajo, bajo, medio, alto o crítico.

Mitigación del riesgo

- **Encargado:** responsable del SGSI
- **Alcance:** definir las medidas de prevención o detención de riesgos, Tabla 21.
- **Definir plan de tratamiento de riesgos:** este plan debe incluir medidas para contrarrestar, plan de contingencia y los recursos a adquirir necesarios para prevención de riesgos.

Monitoreo de protección de datos

- **Encargado:** Coordinador de protección de riesgos.
- **Alcance:** gestionar revisiones regulares para diagnosticar la efectividad de las medidas de mitigación de riesgos.
- Ajustar el plan de tratamiento de riesgos.

2. Identificación de riesgos

Para el de análisis de riesgos que se documenta a continuación se ha tomado como información los datos recopilados a través de la encuesta y lista de chequeo en donde se puede notar que el esquema institucional es reactivo posterior a la ocurrencia de un incidente dejando de lado la utilidad del análisis y gestión de riesgos.

Tabla 12. Identificación de riesgos, amenazas y vulnerabilidades dentro de la Gobernación.

Activo de información	Vulnerabilidad	Amenaza	Riesgo	Impacto
Sitio Web Institucional	- Desactualización de sistema. - Falta de seguimiento periódico. - Ajustes débiles de seguridad.	Ataque Distribuido Denegación de Servicios (DDoS) e inyección SQL.	Acceso no controlado a la base de información.	- Inoperatividad de servicio. - Mala imagen institucional. - Desinformación a la ciudadanía.
Sistemas de Comunicación Electrónica	- No existe capacitación para los funcionarios. - Falta de bloqueadores de spam. - Políticas de seguridad ineficaces.	Phishing y ataques de malware.	Hurto de contraseñas y/o usuarios	- Fuga de información sensible. - Trámites incongruentes.
Documentación en papel sensible	- No existe protección física para los archivos. - Políticas de control de acceso ineficientes. - No existe control de daño o destrucción de archivos.	Usuarios/intrusos sin acceso autorizado. Ingeniería social.	Propagación de información sin autorización.	- Pérdida de datos sensibles. - Alteración de información. - Pérdida de documentos.
Redes Internas	- Claves compartidas o fáciles de adivinar. - Inexistencia de cifrado de datos. - No existe segmentos de red.	Fallos electrónicos, intrusos o siniestros. Ataques de malware	Acceso no autorizado a redes internas o zona física de red.	- Intrusión de datos críticos. - Pérdida de equipos de red y de información.
Dispositivos electrónicos de usuario	- Desactualización de software y hardware. - Inexistencia de antivirus actuales. - Inexistencia de cifrado de almacenamientos de información crítica. - Inventario desactualizado e incompleto.	Malware y baiting, Acceso no autorizado.	- Propagación de troyanos y virus. - Hurto de dispositivos electrónicos.	- Robo de equipos. - Pérdida de información. - Afectación financiera.

Respaldos de Información	- Inexistencia de cifrado en respaldo de seguridad. - Inexistencia de pruebas de recuperación. - Almacenamiento en zonas expuestas.	Fallos electrónicos o catástrofes naturales. Ataque de malware.	Daño de información en respaldos.	- Pérdida de información. - Mala imagen institucional.

Fuente: elaboración propia.

3. Objetivos de seguridad de información

Los objetivos de seguridad de información, según la ISO 27001:2002, son identificados en base a los riesgos identificados con anterioridad y a las políticas establecidas, además, es importante destacar que estas metas podrán ser actualizadas en cualquier instante en relación con el contexto estratégico que presente el área de TI.

En la Tabla 13 se sugiere la implementación de tres objetivos de acuerdo con os riesgos expuestos con anterioridad, asimismo, se considera el estudio a profundidad que se ha realiza en la investigación, esto incluye las necesidades, vulnerabilidades y falencias de la Unidad TI.

Tabla 13. Definición de objetivos de seguridad de información

Objetivo	**Métrica**	**Responsable**
Asegurar la integridad de los activos de información y equipos tecnológicos para controlar el acceso físico y lógico.	Número de incidentes en relación con contraseñas, usuario o acceso no autorizado.	Coordinador de seguridad de información
Prevenir distribución de ciberataques en los activos de información y dispositivos tecnológicos.	- Número de ciberataques. - Tiempo de respuesta frente a ciberataques.	Coordinador de seguridad de información.
Mejorar la protección de respaldos de información crítica.	Cantidad de pruebas exitosas de respaldo de información.	Coordinador de seguridad de información y responsable de documentación.

Fuente: elaboración propia.

Fase 2: Hacer

d) Soporte

1. Asignación de recursos al SGSI

La asignación de recursos dentro del SGSI abarca tanto humanos como tecnológicos. En el aspecto humano, es necesario conformar un equipo multidisciplinario con roles bien definidos, además, es oportuno considerar el contexto de la Unidad TI de la Gobernación puesto que se encuentra en mejoramiento de área, por ello la presente investigación sugiere pocos roles que serían actualmente asumidos por el director de TI.

Los roles que se definen en el SGSI son los siguientes:

- Líder del SGSI
- Auditor interno del SGSI
- Consultor de Seguridad de información
- Coordinador de redes.
- Coordinador de Protección de datos.
- Coordinador de concientización y capacitación.
- Responsable de la documentación de SGSI

Por otro lado, la Tabla 14 presenta la tecnología fundamental con la que se sugiera empezar para implementar un Sistema de Gestión de Seguridad de la Información adecuado y alineado a los requerimientos de la ISO 27001. Además, se expresa sugerencias operativas del recurso para evitar malas adquisiciones.

Tabla 14. Asignación de recursos tecnológicos dentro del SGSI

Recurso Tecnológico	Cantidad
Firewall actualizado o de nueva generación (NGFW). **Recomendación:** 4 puertos GB Ethernet con funciones de VPN y filtrado de contenido.	1
Sistema de detección y prevención de intrusos o IDS/IPS **Recomendación:** capacidad de rastreo por lo menos 500 Mbps.	1
Servidor para almacenamiento de copias de seguridad. **Recomendación:** 32 GB RAM como mínimo y con almacenamiento de 8 TB RAID 5/6.	1
Antivirus empresarial con protección en tiempo real contra ciberataques. **Recomendación:** contar con por lo menos 130 dispositivos con actualización automática.	1
Sistema de Almacenamiento de Red para documentos digitales y copias de seguridad. **Recomendación:** capacidad para 20 TB de almacenamiento y acceso remoto.	1
Administración de eventos e información de seguridad (SIEM) **Recomendación:** monitoreo, gestión de logs, alertas en tiempo real, configuración de reportes.	1
Armarios seguros con resistencia a siniestros, cerradura con contraseña y con capacidad para alrededor de 1000 documentos.	3

Fuente: elaboración propia.

Los requerimientos antes detallados reflejan la condición ideal especificada por la norma, sin embargo, la institución de acuerdo con su presupuesto deberá priorizar la adquisición e implementación de estos equipos.

2. Capacitación y concientización

La capacitación y la concientización acerca de la seguridad de la información para que el personal comprenda los principios básicos del tema, además, del saber cómo actuar frente a amenazas que vulneren los datos que manejan. Por esto, en la Tabla 15. Se presenta un esquema sugerido del plan integral para la realización de este proceso junto a quién va dirigido. Además, el rol encargado de la creación e implementación de este plan será el coordinador de concientización y capacitación del área de soporte y capacitación antes descrita.

Tabla 15. Plan de capacitación y concientización de seguridad de la información

Actividad	Contenido	Dirigido a:	Tiempo estimado	Frecuencia
Inducción a la seguridad de información	- Explicar de que trata la seguridad de información - Conocer acerca de la triada de seguridad.	Funcionarios de la institución.	2 horas	Anual
Presentación de políticas de seguridad	Conocer de que trata las políticas y las responsabilidades de cada uno.	Funcionarios de la institución.	2 horas	Anual
Administración de contraseñas y autenticación	- Cómo crear una contraseña segura. - Cómo utiliza el sistema de autenticación.	Funcionarios de la institución.	1 hora	Cada seis meses
Identificación de phishing y malware	- Cómo saber que correo es fraudulento. - Conocer sobre medidas para evitar el malware. - Ejemplo de ciberataque.	Funcionarios de la institución.	1 hora	Cada tres meses
Control de acceso	- Conocer acerca de quién tiene acceso a instalaciones, documentos y sistemas. - Conocer sobre protocolos de seguridad tanto física como lógica.	Jefes de unidad.	1 hora y 30 minutos	Anual
Copias de seguridad de información	- Conocer acerca de la importancia de los respaldos de seguridad. - Conocer medidas para recuperación de datos.	Unidad de TI	2 horas	Cada seis meses
Plan de respuesta ante incidentes	- Conocer acerca del plan de respuesta ante incidentes. - Estructura para reportes de incidentes.	Jefes de Unidad	3 horas	Anual
Uso seguro de sistemas de comunicación electrónica	- Conocer sobre las políticas de comunicación. - Conocer los riesgos y sus consecuencias de mal uso de sistema comunicación.	Funcionarios de la institución.	1 hora y 30 minutos	Cada tres meses
Resguardo de documentación física y digital	- Conocer el proceso para manejo seguro de documentos. - Medidas para digitalizar de manera segura la información.	Funcionarios de la institución.	2 horas	Anual
Campaña de ingeniería social	- Conocer acerca de las diferentes técnicas de ingenierías social. - Fomentar la importancia de la seguridad de información. - Reconocer los diferentes intentos de manipulación y engaño.	Funcionarios de la institución.	1 hora	Cada seis meses.

Fuente: elaboración propia

3. Documentación del SGSI

La documentación para establecer un Sistema de Gestión de Seguridad de Información (SGSI) según la ISO 27001:2022 son aquellos que se encuentran descritos en la Tabla 16, sin embargo, no todos se van a encontrar en la guía porque es importante tomar en cuenta la confidencialidad que ciertos elementos contienen para la realización de esta documentación.

Por otro lado, existe información que debería estar documenta para una mejor implementación del SGSI, son los criterios de riesgos, la competencia del personal, la comunicación tanto interna como externa y los *indicadores* de desempeño o KPI.

Tabla 16. Clasificación de documentación del SGSI

Documento	**Realizado en la guía**	**Sugerido a realizar**	**Observación**
Propuestos por las Cláusulas de la ISO 27001:2022			
Políticas de Seguridad de la Información	X		Los documentos se encontrarán detallados en la guía.
Declaración de aplicabilidad (SoA)	X		
Evaluación y tratamiento de riesgos	X		
Plan de tratamiento de riesgos	x		
Políticas de control de acceso, gestión de riesgos y copias de seguridad de información.	X		
Documento de alcance de SGSI	X		
Objetivos de seguridad de información.	X		
Procedimientos de gestión de incidentes, auditorías internas y control de accesos.		X	Se sugiere que la Unidad TI estos procedimientos, pues son usuarios internos a la entidad y conocen a profundidad todo acerca de los incidentes, que podrían resultar confidenciales para la presente investigación.
Documentación de auditorías internas y revisiones por alta dirección.		X	La documentación seguridad deberá ser realizada por la alta dirección o por el responsable del SGSI, por lo que la presente investigación no se puede hacer cargo de esta.
Documentación de no conformidades y acciones correctivas.		X	La documentación descrita podrá ser creada, únicamente una vez creado e implementado el SGSI, por lo que al momento no sería lo ideal crearla.
Propuestos por el Anexo A de la ISO 27001:2022			
Inventario de activos		X	El inventario de activos se realiza en base a la criticidad,

			por lo que es necesario que el personal interno lo realice.
Clasificación de información		X	Es importante que el personal interno clasifique la información que maneja diariamente, pues en ocasiones podría ser de uso confidencial que no sería apropiado que un externo manipule.
Plan de continuidad de negocio		X	La institución es la única que conoce sus procesos y tiene la potestad de identificar las áreas con mayor prioridad, lo cual ayudaría a crear un mejor plan de continuidad.

Fuente: elaboración propia.

e) Operaciones

1. Controles técnicos y organizacionales

Los controles técnicos y organizacionales basados en la ISO 27001 corresponden a técnicas que se sugiere implementar para asegurar la protección de la información. Además, que son capaces de abordar los riesgos identificados con anterioridad. Por ellos, en la Tabla 17 se argumenta el cómo deberían ir estructurados estos controles en base a su clasificación y a lo solicitado por la norma.

Tabla 17. Controles técnicos y organizacionales de acuerdo con los riesgos.

Tipo de control de seguridad	Control de seguridad	Descripción
Controles Organizacionales	Políticas de seguridad de información	- Las políticas deberán administrar la información según la clasificación: confidencial, pública y sensible. - Se deberá informar al personal acerca de la utilidad fundamental de la seguridad de la información. - Indicar los procesos necesarios para la división y buen manejo de información.
	Políticas de control de acceso	- Las políticas se clasificarán en control de acceso físico para servidores, documentos críticos, equipos tecnológicos con ayuda de credenciales o sistemas de reconocimiento biométrico. - Utilización de autenticación en dos pasos.
	Plan de auditorías internas	- Las auditorías ayudarán a la estructuración de políticas de seguridad de información.

		- Ayudaran a la generación de matrices de riesgos. Ayudaran a generar documentación sobre las falencias e implementar acciones correctivas.
	Plan de gestión de riesgos	- Se logra identificar mediante MAGERIT los riesgos e incluir medidas para mitigarlos.
	Plan de capacitación de políticas.	- Crear charlas, cursos y documentos interactivos para formar al personal acerca de la seguridad de la información. - Realizar simulacros de amenazas para mejorar el nivel de respuesta.
Controles Técnicos	Políticas de proyección contra ataques cibernéticos y seguimiento de redes.	Debe contener el plan de respuesta ante incidentes y ante riesgos. Instaurar un sistema de monitoreo para conocer el tráfico extraño.
	Políticas de seguridad de comunicaciones.	- Instaurar cifrado extremo a extremo. Registrar el tráfico de red para prevención de acceso no autorizado.
	Sistemas de detección y prevención de intrusos.	- Los sistemas ayudarán a rastrear actividad sospechosa y bloquear las amenazas. Analizar las actividades sospechosas para saber los patrones.
	Respaldo de seguridad.	- Realizar respaldos de seguridad programados de manera automática. - Almacenar de manera segura en la nube o en zonas seguras.
Control Organizacional / Técnico	Plan de recuperación de incidentes.	- El plan incluye realizar simulacros para diagnosticar el funcionamiento de las medidas correctivas. - El plan comprende una estrategia que gestiona la respuesta y las medidas técnicas para mitigar incidentes, renovar operaciones y asegurar la infraestructura organizativa.

Fuente: elaboración propia.

2. Valoración de riesgos

Una vez identificadas las vulnerabilidades, las amenazas y los riesgos en base a los activos se realiza la valoración del riesgo según su probabilidad, Tabla 18, y su impacto, Tabla 19. Ambas tablas muestran la clasificación de los niveles desde el más bajo que es igual a 1 hasta el nivel crítico que es igual a 5.

Tabla 18. Tabla de probabilidad de riesgo

Nivel	Descripción	Valoración
Muy bajo	Existe improbabilidad de que la amenaza ocurra, pues necesita una combinación inusual de factores para que suceda.	1
Bajo	Existe poca probabilidad de que la amenaza ocurra. Las especificaciones para que ocurra son poco comunes.	2
Medio	Existe probabilidad moderada de que la amenaza se materialice. Las especificaciones para que ocurra son normales.	3
Alto	La amenaza es muy probable que ocurra. Las especificaciones para que ocurra es gracias a incidentes pasados.	4
Crítico	Es casi seguro que la amenaza ocurra, ha ocurrido con mayor frecuencia o no se puede evitar por el contexto en que se encuentra.	5

Fuente: Modificado a partir de (Contreras Olea, 2022)

Tabla 19. Tabla de impacto del riesgo

Nivel	Descripción	Valoración
Muy bajo	Es intrascendente el impacto, pues no afecta la operatividad.	1
Bajo	Existe un menor impacto de que la amenaza afecta a la operatividad.	2
Medio	Existe un impacto moderado de que la amenaza pierda información a corto plazo.	3
Alto	La amenaza tiene un gran impacto e interrumpe servicios con pérdida de información	4
Crítico	La amenaza produce un impacto catastrófico e interrumpe los servicios y pérdida de información a largo plazo. Además, daño en la reputación.	5

Fuente: Modificado a partir de (Contreras Olea, 2022)

- Por otro lado, la metodología MAGERIT indica que la valoración del riesgo es el producto de estas dos características como se muestra en la Tabla 19. De cierta manera, se califica con la siguiente terminología de letras según Contreras Olea (2022):
- Nivel Bajo (B) 1 – 5: rastrear de manera regular y fomentar las buenas prácticas.
- Nivel Medio (M) 6– 10: requiere acciones para prevenir el riesgo.
- Nivel Alto (A) 11 – 15: implementación de acciones correcticas de manera inmediata con monitoreo periódico.
- Nivel Crítico (C) 16-25: implementación de acciones de manera urgente con una priorización alta.

Tabla 20. Matriz de riesgo

Probabilidad	Impacto				
	Muy Bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Crítico (5)**
Muy Bajo (1)	B	B	B	B	B
Bajo (2)	B	B	M	M	M
Medio (3)	B	M	M	A	A
Alto (4)	B	M	A	C	C
Crítico (5)	B	M	A	C	C

Fuente: Modificado a partir de (Contreras Olea, 2022)

3. Mitigación del riesgo

Para la mitigación del riesgo la ISO 27001:2022 propone realizar un plan de tratamiento de riesgos, por ello en la Tabla 20 se muestra un análisis de las posibles soluciones para prevenir los riesgos analizados con anterioridad en base a la subjetividad de la presente investigación.

Tabla 21. Plan de tratamiento de riesgo

Riesgo	**Probabilidad**	**Impacto**	**Nivel de riesgo**	**Solución propuesta**	**Responsable**	**Plazo para la implementación**
Acceso no controlado a la base de información.	4	5	20	Instauración de firewall, realización de auditorías regulares y rastreo continuo.	Consultor de seguridad de información	4 meses
Hurto de contraseñas y/o usuarios	3	4	12	Instauración de autenticación en dos pasos, creación de políticas para creación de claves robustas y cambios continuos, concientización de seguridad de contraseñas. Creación de respaldo de información periódicos con almacenamiento seguro y creación de políticas de respaldo diario con pruebas de efectividad.	Consultor de seguridad de información	5 meses
Propagación de información	3	5	15	Crear e instaurar políticas de escritorio vacío,	Consultor de seguridad	3 meses

n sin autorización.				archivadores cerrados y destrucción segura. Instauración de bloqueadores de spam.	de información y auditor interno	
Acceso no autorizado a redes internas o zona física de red.	4	4	20	Creación de controles de acceso físico y lógico, sistemas de detección/prevención de intrusos y rastreo de accesos para auditorías internas.	Coordinador de redes y consultor de seguridad de información	4 meses
Propagación de troyanos y virus.	4	5	20	Instaurar virus actualizado en todos los equipos tecnológicos, crear un plan de concientización y formar políticas de navegación segura.	Consultor de seguridad de información y coordinador de protección de datos.	3 meses
Hurto de dispositivos electrónicos.	3	3	9	Crear un inventario actualizado. Acceso controlado a la institución.	Consultor de seguridad de información y coordinador de redes.	2 meses
Daño de información.	3	5	15	Creación de zona segura para almacenamiento de copias de seguridad o en la nube. Instauración de plan de continuidad operativo.	Consultor de seguridad de información	6 meses

Fuente: elaboración propia.

De acuerdo con el análisis de riesgos la mayoría de los riesgos que mayor prioridad deben tener en cualquier plan de respuesta son:

- Acceso no controlado a la información
- Daño de información
- Propagación de troyanos y virus

Pues, con base a la encuesta planteada, la lista de chequeo y la constatación realizada en la institución enfrenta retos en la seguridad de información y los riesgos más críticos podrían comprometerla en la operatividad, confiabilidad de la ciudadanía e incluso el cumplimiento normativo. Por lo que, es necesario realizar un plan estratégico para mitigar los riesgos, todo esto alineado a la ISO 27001.

Verificar

f) Evaluación de desempeño

1. Métricas para efectividad

Para medir la efectividad del SGSI en base a la norma ISO 27001 es primordial delimitar los indicadores con las cláusulas y el contexto de la institución. Además, es importante identificar los objetivos, por ejemplo: garantizar la conformidad con los controles de la ISO 27001, supervisar al sistema de seguridad de información para una mejor efectividad y reconocer las zonas de mejora en los procedimientos de seguridad.

A su vez, es necesario seleccionar los indicadores de rendimiento clave, los cuales podrían ser el cumplimiento de políticas y proceso establecidos. Asimismo, los niveles de madurez según el indicador elegido para conocer el progreso y la calidad de los controles. Por otro lado, se sugiere establecer un método de medición, la fórmula adecuada para obtener un resultado y la frecuencia temporal para realizar el cálculo.

Es por ello, que una vez implementado el SGSI lo más adecuado es identificar las métricas en base a las metas expuestas, necesidades del negocio y contexto del área.

Sin embargo, la presente investigación sugiere opciones de métricas en la Tabla 22.

Tabla 22. Métrica seguridad para la efectividad

Métrica	Fórmula
Porcentaje de incidentes de acceso no autorizado, contraseñas y/o usuarios inseguros	$\frac{\text{número de incidentes de acceso no autorizado}}{\text{número total de usuarios activos}} \times 100$
Promedio de respuesta ante ciberataques (malware, phishing, entre otros.)	$\frac{\text{tiempo de resolución ante ciberataques}}{\text{número de coberataques det e ctados}}$
Porcentaje de pruebas positivas de respaldos de información.	$\frac{\text{cantidad de pruebas positivas de respaldo de inf o rmacioón}}{\text{cantidad total de pruebas realizadas}} \times 100$

Fuente: Basado en Nurbojatmiko, y otros (2024) y Abdiraman, Goranin, Balevicius, Nurusheva, & Tumasoniene (2023).

Las métricas descritas en la Tabla 22 son sugerencias que se presenta según la investigación realizada, sin embargo, podrían variar según el área de TI. Además, las métricas presentadas se encuentran alineadas a los riesgos identificados, así como, los controles técnicos y organizacionales asociados.

1. Plan de auditorías internas

Vergara Torres (2019) indica que las auditorías se realizan para identificar si las metas, controles y procedimientos del Sistema de Gestión de Seguridad de la Información están alineados a la norma ISO 27001. En el contexto de la investigación, debido a la complejidad del proceso no se define dentro del alcance, sin embargo, se sugiere algunas consideraciones en base a algunos criterios de varios autores. Además, propone que la frecuencia adecuada a realizarlas deberá ser mínimo dos veces al año para que el estado del sistema sea el más apto. Por ello, la investigación propone la realización de un plan de auditorías internas para la detección de brechas e implementar acciones correctivas que mejoren la seguridad de la información de la entidad y en específico de la Unidad TI.

En primer lugar, se plantea definir el objetivo de la auditoría, analizar la efectividad de la implementación de los controles de seguridad de la información alineados a la ISO 27001:2022 para la obtención de procesos alineados con las necesidades de la institución y de la Unidad TI. Otro punto es la realización de tipos de auditorías: de diagnóstico, en las cuales se determinan las brechas y conocer el estado del SGSI en comparación a los requerimientos de la norma; de seguimiento, se constata progresos y desempeño de los controles implementados; por último, de evaluación final , se conoce si el SGSI es apto para una posible certificación

Además, la frecuencia con la que se sugiere realizar es una vez al completar la implementación del SGSI y después una anualmente con revisiones cada seis meses para zonas de alto impacto como respaldo de seguridad de información y control de acceso (León Ardila & Melo Gamez, 2024).

Por otro lado, León Ardila & Melo Gamez (2024) propone la utilización del análisis GAP, técnica para conocer el estado de madurez que presenta la institución acerca de la seguridad de la información alineada a la ISO 27001:2013 (Ramírez Benavides, 2021), para comparar los requisitos de la norma contra lo que tiene la unidad mediante técnicas como entrevistas, observación directa y análisis de documentos, con la ayuda de una lista de chequeo basada en el anexo A de la norma.

Además, se sugiere utilizar el modelo ADKAR, que es un método para administrar el cambio individual que se utiliza una vez identificado el mismo para después gestionarlo en cinco fases: conciencia, deseo de apoyar, conocimiento, capacidad para instaurar y reforzar (Loáisiga Tórrez, 2021). Por lo que, León Ardila & Melo Gamez (2024), expone que este modelo mejorará los cambios dentro de cada funcionario para que acepten las recomendaciones de la auditoría. Conjuntamente, se presentarán informes que detallen los resultados de las observaciones y acciones correctivas. Es importante destacar que en el plan de auditorías se determinan los indicadores de desempeño o KPIs, los cuales pueden ser porcentaje de controles instaurados alineado a la norma, cantidad de no conformidades determinadas y resueltas, por último, porcentaje de madurez del SGSI.

Actuar

g) Mejora

1. Documentación de las no conformidades y acciones correctivas

Una vez que el plan de auditorías internas es aprobado por la máxima autoridad de la institución, con el personal de la Unidad TI se debe ejecutar este proceso, en donde se identificaran las no conformidades, desviación de los requerimientos y procesos alineados a la ISO 27001; los cuales se deben clasificar según la gravedad. Se realiza la respectiva documentación para implementar las acciones

correctivas para cada una de las no conformidades, por lo que, la investigación sugiere la siguiente estructura.

Yungán Cazar & Narváez Contero (2022) propone que después de identificar y clasificar la no conformidad se utilice el diagrama Ishikawa para poder identificar la causa principal de estas. Este diagrama tiene forma de un esqueleto de pez, el cual tiene seis ramificaciones que representan las 6 M (material, mano de obra, método de trabajo, maquinaria, medio ambiente y mantenimiento), las cuales son las posibles causas; y en la cabeza se indica la no conformidad, es decir el problema (Valdiviezo Leon, 2023). Después de identificar las causas se definen las acciones correctivas para prevenir la reincidencia del problema y afrontar desde la raíz.

Todo este proceso debe ser documentado y aprobado por los responsables, en este caso la Unidad TI y el Despacho de la Gobernación. Posteriormente, se implementarán las medidas propuestas y el consultor de auditoría interna tendrá la función de supervisar su ejecución dentro del plazo establecido (Yungán Cazar & Narváez Contero, 2022).

Si existe el caso de que las acciones correctivas no brinden resultados positivos, el auditor emitirá un nuevo informe para planificar nuevas soluciones y una vez que se verifiquen como efectivas, las no conformidades finalizan el proceso y se archivan.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Resultados

El resultado de la investigación es la “Guía para Implementación de la ISO 27001 en el Departamento TI de la Gobernación Tungurahua”, que se encuentra en el anexo 3. Cabe indicar que, la propuesta de trabajo se documenta y desarrolla en el capítulo II, epígrafe de la metodología de desarrollo, con la respectiva esquematización y contenido técnico.

3.2. Evaluación y validación

Para la evaluación y validación de la guía se diseñó una matriz que se muestra en la Tabla 23, y que valora aspectos como: alcance, coherencia con la ISO 27001, viabilidad, claridad y coherencia, aplicabilidad, compatibilidad, reducción de riesgos e incidentes, por último, monitoreo y evaluación, debido a que es importante valorar el contenido técnico, la estructura interna, la pertinencia de las propuestas y si es un instrumento de trabajo usable y fácil de manejar. Para el efecto, se solicitó la participación del Director de la Unidad TI de la Gobernación de Tungurahua, pues es quién será el responsable de la implementación del SGSI.

Tabla 23. Matriz de evaluación de guía

Criterio de evaluación	**Descripción**	**1**	**2**	**3**	**4**	**5**
Alcance	La guía se encuentra alineada a los requerimientos y riesgos de la Gobernación.					
Coherencia con la ISO 27001	La guía contiene los requerimientos y estructura de la ISO 27001.					
Viabilidad	La guía propone políticas, estándares, recursos y herramientas factibles en el contexto de la Gobernación.					
Coherencia y claridad	La guía contiene información fácil de entender y precisa para el personal de la Unidad TI.					
Aplicabilidad	La guía propone procesos realistas para la operatividad de la Gobernación.					
Compatibilidad	Las sugerencias de la guía son compatibles con los sistemas e información que contiene la Gobernación.					
Reducción de riesgos e incidentes	La guía propone sugerencias que ayudarán a cumplir los objetivos de seguridad y prevenir riesgos e incidentes.					
Monitoreo y evaluación	La guía presenta métricas e indicadores de rendimiento que ayudarán calcular la efectividad del SGSI.					
Valoración global						

Fuente: elaboración propia

La matriz contiene ocho criterios de evaluación, los cuales ayudan a confirmar si la guía es una herramienta útil para la Gobernación y para quién será el encargado de implementar el SGSI.

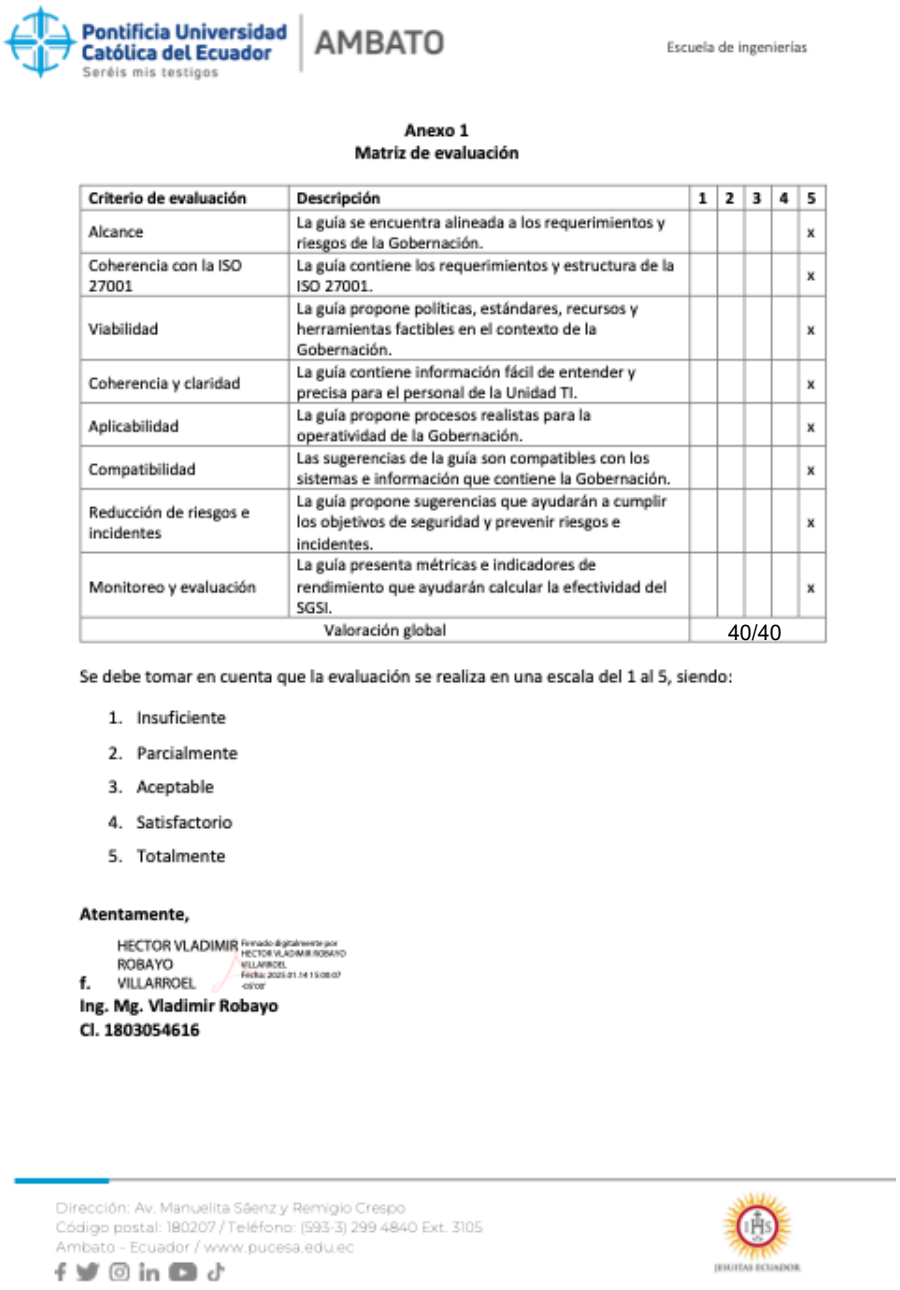
Se debe tomar en cuenta que la evaluación se realiza en una escala del 1 al 5, siendo:

1. Insuficiente
2. Parcialmente
3. Aceptable
4. Satisfactorio
5. Totalmente

Resultados de la validación

Una vez realizada la evaluación, el director de la Unidad TI dio a conocer sus apreciaciones sobre la guía para la implementación de la ISO 27001.

Figura 4. Resultado de la evaluación a la guía de implementación ISO 27001



Pontificia Universidad Católica del Ecuador
Seréis mis testigos
AMBATO
Escuela de ingenierías

Anexo 1
Matriz de evaluación

Criterio de evaluación	Descripción	1	2	3	4	5
Alcance	La guía se encuentra alineada a los requerimientos y riesgos de la Gobernación.					x
Coherencia con la ISO 27001	La guía contiene los requerimientos y estructura de la ISO 27001.					x
Viabilidad	La guía propone políticas, estándares, recursos y herramientas factibles en el contexto de la Gobernación.					x
Coherencia y claridad	La guía contiene información fácil de entender y precisa para el personal de la Unidad TI.					x
Aplicabilidad	La guía propone procesos realistas para la operatividad de la Gobernación.					x
Compatibilidad	Las sugerencias de la guía son compatibles con los sistemas e información que contiene la Gobernación.					x
Reducción de riesgos e incidentes	La guía propone sugerencias que ayudarán a cumplir los objetivos de seguridad y prevenir riesgos e incidentes.					x
Monitoreo y evaluación	La guía presenta métricas e indicadores de rendimiento que ayudarán calcular la efectividad del SGSI.					x
Valoración global		40/40				

Se debe tomar en cuenta que la evaluación se realiza en una escala del 1 al 5, siendo:

1. Insuficiente
2. Parcialmente
3. Aceptable
4. Satisfactorio
5. Totalmente

Atentamente,

f. HECTOR VLADIMIR ROBAYO VILLARROEL

Ing. Mg. Vladimir Robayo
CI. 1803054616

Dirección: Av. Manuelita Sáenz y Remigio Crespo
Código postal: 180207 / Teléfono: (593-3) 299 4840 Ext. 3105
Ambato - Ecuador / www.pucesa.edu.ec

Fuente: elaboración propia

De acuerdo con los criterios emitidos por el profesional evaluador, todos los parámetros analizados tienen la valoración máxima de “Totalmente”. Es decir, que la guía satisface al 100% las expectativas y los criterios técnicos necesarios para su implementación.

CONCLUSIONES

- En términos de teoría se comprende que la parte fundamental de la investigación es la norma ISO 27001, pues es un conjunto de requisitos que la entidad debe recolectar para la correcta implementación de un Sistema de Gestión de la Seguridad de la Información. Además, de ser la regulación principal frente a otras ISO porque brinda certificación y esto es reconocido ante distintos tipos de empresas. La ISO 27001 es completa y se enfoca en mantener los tres principios básicos: confidencialidad, integridad y disponibilidad que ayudan a asegurar la información que es el principal activo de cualquier organización y que debe ser preservado ante cualquier tipo de ataque tanto cibernético como físico.

- La situación actual de la Unidad TI de la Gobernación de Tungurahua en relación a la seguridad de la información es preocupante porque para la implementación de un Sistema de Gestión de Seguridad de Información deben contar con una estructura organizacional y funcional definida, la cual es ineficiente pues únicamente existe un responsable en el área. Además, la alta dirección de la entidad se encuentra en proceso de aceptación ante este proyecto, así como la creación de: plan de gestión de riesgos, inventario de *hardware* y *software*, políticas de seguridad de información, objetivos de esta, entre otros, son inexistentes. Por lo tanto, es poco probable que exista un proceso de mejora continua y medición de efectividad para lo cual es indispensable crear una planificación clara a larga plazo para que la implementación de un SGSI se vuelva realidad.

- La guía de implementación de la ISO 27001 en la Gobernación de Tungurahua está compuesta por todos los documentos necesarios para una buena estructura del SGSI. A pesar de que la norma se constituye de diez clausulas, el contenido del instrumento se basa en las siete cláusulas de la norma: contexto de la organización, liderazgo, planificación, soporte, operaciones, evaluación de rendimiento y mejora, por otro laso las tres restantes (alcance, bases normativas, y términos - definiciones) no fueron

necesarias incluirlas, pues describen de lo que se trata más no los requisitos específicos. Asimismo, los elementos necesarios se basaron en: organigrama funcional, declaración de aplicabilidad, plan de tratamiento de riesgos, políticas de seguridad de información, objetivos de seguridad de la información, asignación de recursos, entre otros. Además, de las estructuras de los distintos documentos como: inventario, plan de continuidad de negocio, plan de gestión de incidentes, entre otros. Lo que permitirá a la Unidad TI construir de forma clara un SGSI.

RECOMENDACIONES

- Crear un plan estratégico de tecnologías de la información alineado a los objetivos institucionales como punto de partida en el diseño e implementación de un SGSI.

- Ejecutar de manera obligatoria el plan de capacitación inmerso en el proceso de implementación del SGSI para crear una cultura de seguridad de la información en la institución.

- Invertir en herramientas de seguridad de la información que permitan mitigar las amenazas y detectar las vulnerabilidades de los activos tecnológicos.

- Digitalizar la información física para tener un mejor manejo de información.

BIBLIOGRAFÍA

Abdiraman, A., Goranin, N., Balevicius, S., Nurusheva, A., & Tumasoniene, I. (2023). Application of Multicriteria Methods for Improvement of Information Security Metrics. *Sustainability 2023*.

Akbanov, M., Vassilakis, V., & Logotheis, M. (2019). *WannaCry Ransomware: analysis of infection, persistence, recovery prevention and propagation mechanisms.* Disponible en: https://acortar.link/pS7dwg.

Alvarado Chang, J. E. (2020). *Análisis de ataques cibernéticos hacia el Ecuador.* Disponible en: https://acortar.link/5Rap95.

Arias Gonzáles, J. L. (2020). *Técnicas e instrumentos de investigación científica.* Enfoques Consulting EIRL.

Arias Quispe, E. S. (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao.* Disponible en: https://acortar.link/8399k6.

Asurza Cáceres, J. D. (2022). *Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing S.A.C. en 2021.* Disponible en: https://acortar.link/tKwyhJ.

Beleño García, B. A. (2022). *Propuesta de un Modelo de Gestión de Seguridad y Privacidad de la Información para la Gobernación del Huila .* Disponible en: https://acortar.link/zIjsI1.

Castillo Durán, E. F. (2023). *Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001.* Disponible en: https://acortar.link/3T3Fbi.

Castillo Fonseca, J. M., & Zavala Juárez, B. (2019). *Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos.* Disponible en: https://acortar.link/mi2ede.

Castillo Plata, A. R. (2020). *Actualización norma ISO/IEC 27001:2005 para la versión 2013 en Caracol Televisión.* Bogotá: Fundación Universitaria Los Libertadores.

Cevallos Veintimilla, A. F., Polo Luna, E. F., Salgado Chasipanta, D. J., & Obrea Vergara, M. S. (2017). *Métodos y técnicas de investigación.* Instituto Superior Tecnológico Corporativo Edwards Deming.

Colegio Oficial de Ingenieros de Telecomunicación. (2012). *Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001.* Disponible en: https://acortar.link/UgyMc.

Contreras Olea, G. A. (2022). *Análisis comparativo entre las metodologías de gestión de riesgos de los sistemas de gestión de seguridad de la información (SGSI): Magerit y octave.* Disponible en: https://acortar.link/KNsOoy.

De la Rosa, M. T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, 492-506.

Díaz Ayala, S. E., & Castaño Castaño, D. A. (2020). *Componente de seguridad de la información en el Ciclo de Vida del Desarrollo de Software aplicado al procedimiento PR-M7-P5-033 en la Gobernación de Antioquia .* Disponible en: https://acortar.link/oL9CVq.

Donoso Vargas, D., Calahorrano Recalde, C., & Donoso Vargas, S. (2023). *Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador. Revista Universidad y Sociedad.* Disponible en: https://acortar.link/OU6WtJ.

Falcón López, A., & Ramos Serpa, G. (2021). Acerca de los métodos teóricos y empíricos de investigación: significación para la investigación educativa. *Revista Conrado*, 22-31.

Finol de Franco, M., & Vera Solórzano, J. L. (2020). *Paradigmas, enfoques y métodos de investigación: análisis teórico.* Disponible en: https://acortar.link/4CG5fZ.

Fonseca Herrera, O., Rojas, A., & Florez, H. (2021). *A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard.* Disponible en: https://acortar.link/0i8DUF.

Girbau Roque, C. D. (2022). *Diseño de un sistema de gestión de protección de datos personales basado en la norma ISO/IEC 27701:2019.* Disponible en: https://acortar.link/fjAL6U.

Gobernación de Tungurahua. (2024). *Misión – Visión – Valores*. Obtenido de Gobernación de Tungurahua: https://www.gobernaciontungurahua.gob.ec/?p=475

Gobernación de Tungurahua. (2024). *Organigrama*. Obtenido de Gobernación de Tungurahua: https://www.gobernaciontungurahua.gob.ec/?p=472

Guacho Lema, M. J. (2018). *Análisis de los ciberataques realizados en América Latina.* Disponible en: https://acortar.link/nhTofh.

Guevara Arias, V. I., & Soriano, S. D. (2022). *La nube en Pymes mediante las normas ISO 27005.* Disponible en: https://acortar.link/fYbkMi.

Hernández Mendoza, S. L., & Duana Ávila, D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, 51-53.

INCIBE. (2020). *Guía de ciberataques.* Disponible en: https://acortar.link/ZO6ZT7.

Irawan, H., Hendi Muhammad, A., & Nasiri, A. (2024). Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8. *Journal Inovtek Polbeng*, 126-139.

Jácome Sánchez, A. P. (2022). *Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001.* Disponible en: https://acortar.link/ognxkX.

Kurii, Y., & Opirskyy, I. (2022). *Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013.* Lviv Polytechnic National University.

León Ardila, J. M., & Melo Gamez, L. Y. (2024). *Metodología para el diagnóstico y cumplimiento de la norma ISO 27001:2022.* Universidad Cooperativa de Colombia.

Llano Casa, A. C., Gaibor Gavilánez, M. L., Cruz Caiza, C. C., & Cadena Moreano, J. A. (2021). *Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador.* Disponible en: https://acortar.link/hDREO5.

Loáisiga Tórrez, C. A. (2021). *Propuesta de definición de un sistema de gestión de la seguridad de la información bajo el estándar de la norma ISO/IEC 27001:2013 para intituciones de educación superior en Nicaragua.* Univeridad Iberoamericana Ciudad de México.

Mantilla Guerra, A. R. (2018). *Gestión de seguridad de la información con la norma ISO 27001:2013.* Disponible en: https://acortar.link/zSY79A.

Morales, F., Toapanta, S., & Toasa, R. (2019). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información.* Disponible en: https://acortar.link/GmOjG6.

Murguía Hughes, J. (21 a 23 de junio de 2023). Mantener la privacidad de la información aun cuando la seguridad haya sido vulnerada. *In Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad: Vigo*, págs. 213-220.

NQA. (2022). *ISO 27001:2013 Guía de Implantación.* Disponible en: https://acortar.link/xoHfq8.

Núñez Palencia, M. R. (2024). *Acuerdo Ministerial Nro.155.* Ministerios de Gobierno.

Nurbojatmiko, N. A., Wasiqi, N. C., Alfajri, M. F., Ulinnuha, Z., Purwati, Y. K., Ayu, I. K., & Yasmin, N. A. (2024). Risk assessment maturity level of academic information system using ISO 27001 system security engineering- capability maturity model. *Journal of Applied Engineering and Technological Science (JAETS)*, 941-954.

Osorio Beltrán, J. A. (2022). *Diseño de un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013 para el área de tecnología en la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá.* Universidad Piloto de Colombia Facultad de Ingeniería Especialización en Seguridad Informática Bogotá.

Porras Ruiz, M. Á. (2019). *Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información.* Disponible en: https://acortar.link/wS3JfK.

Ramírez Benavides, J. P. (2021). *Diseño de un sistema de gestión de seguridad de la información para los procesos de soporte y desarrollo de software en la empresa ALFCOM S.A basado en la norma ISO/IEC 27001:2013.* Universidad Piloto de Colombia.

Risco Villarreal, E. G. (2021). *Sistema de Gestión para la Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021.* Universidad César Vallejo.

Segura Barrantes, J. C. (2022). *Guía metodológica para la articulación de las normas ISO 9001:2015, ISO 45001:2018 E ISO 27001:2013 a partir del modelo integrado de planeación y gestión (MIPG) en Colombia.* Bogotá: Convenio Universidad Santo Tomás e ICONTEC Facultad de Ingeniería Mecánica Maestría en Calidad y Gestión Integral Bogotá D.C.

Valdiviezo Leon, K. K. (2023). *Implementación de un sistema web basada en las políticas de la norma ISO 27001 para mejorar la gestión de servicios de soporte técnico en una empresa de reparación de efectos personales en Lima -2023.* Universidad Tecnológica del Perú.

Vásquez, J. D. (2023). *ISO/IEC 27000.* Disponible en: https://acortar.link/5J3RMi.

Vega Briceño, E. (2021). *Seguridad de la Información.* Disponible en: https://acortar.link/VajvVr.

Vergara Torres, O. H. (2019). Mejorando la implantación de la ISO 27001 en las organizaciones . *Universidad Piloto de Colombia*.

Yungán Cazar, J. C., & Narváez Contero, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, 1025-1041.

Zaidatulnajla, H. (2019). *A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors.* Disponible en: https://acortar.link/SKB9OL.

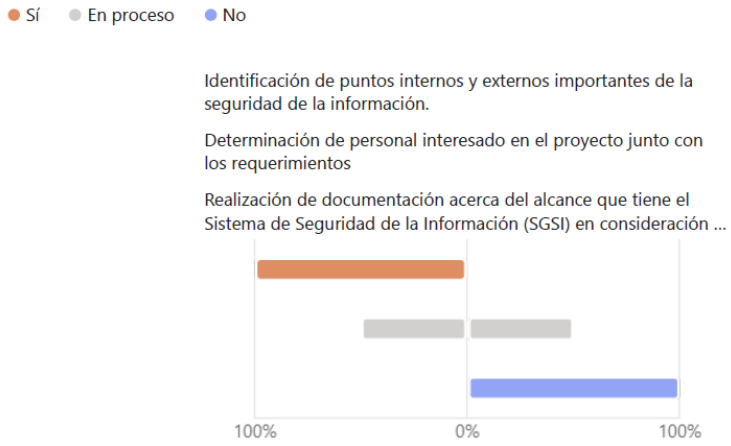
Zevallos Morales, M. N. (2019). *Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte.* Disponible en: https://acortar.link/sSRSBm.

ANEXOS

Anexo 1. Resultados de lista de chequeo de la verificación de aspectos de seguridad de la información de la norma ISO 27001.

Contexto de la organización

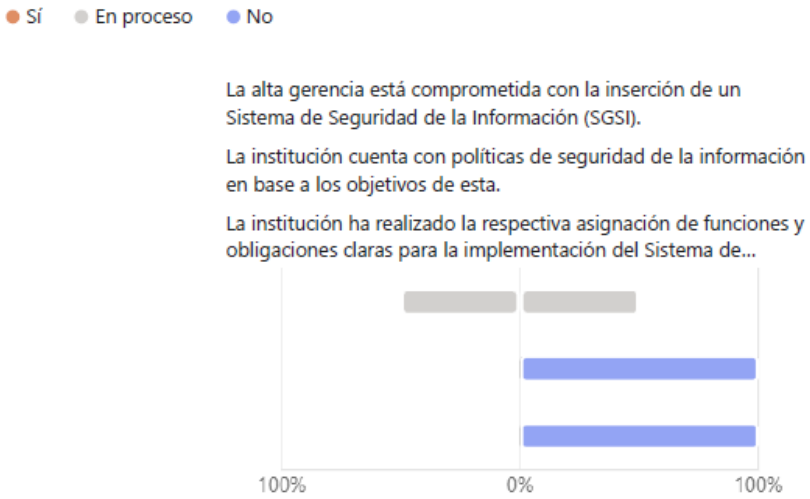
Figura 5. *Gráfico estadístico del Contexto de la organización*



Fuente: elaboración propia

- **Liderazgo**

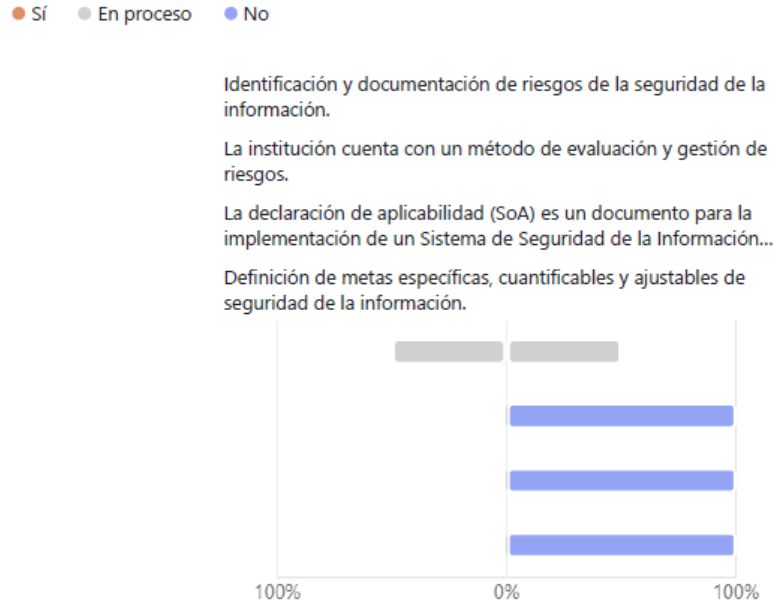
Figura 6. Gráfico estadístico del Liderazgo



Fuente: elaboración propia

- **Planificación**

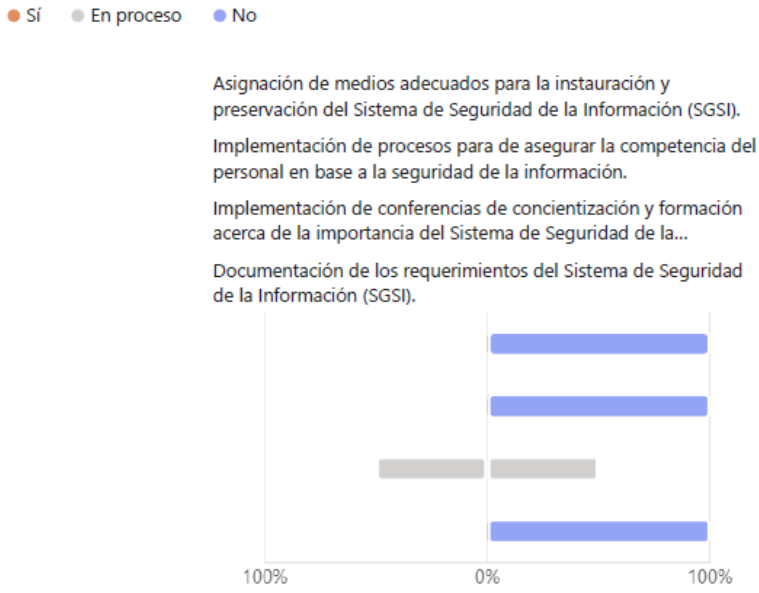
Figura 7. Gráfico estadístico de Planificación



Fuente: elaboración propia

- **Soporte**

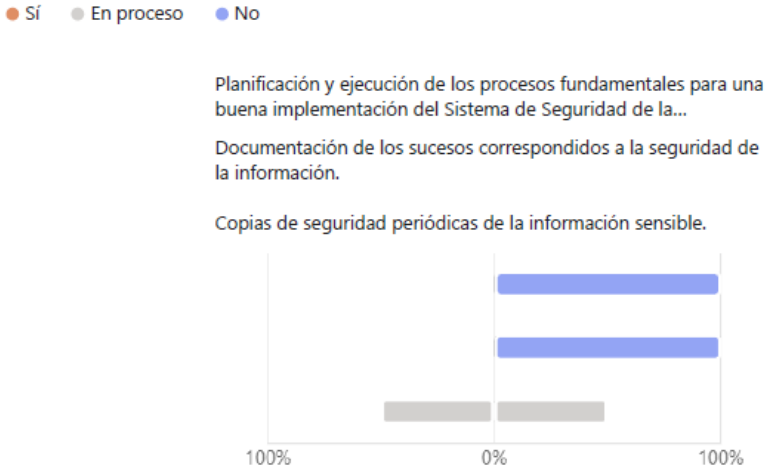
Figura 8. Gráfico estadístico de Soporte



Fuente: elaboración propia

- **Operación**

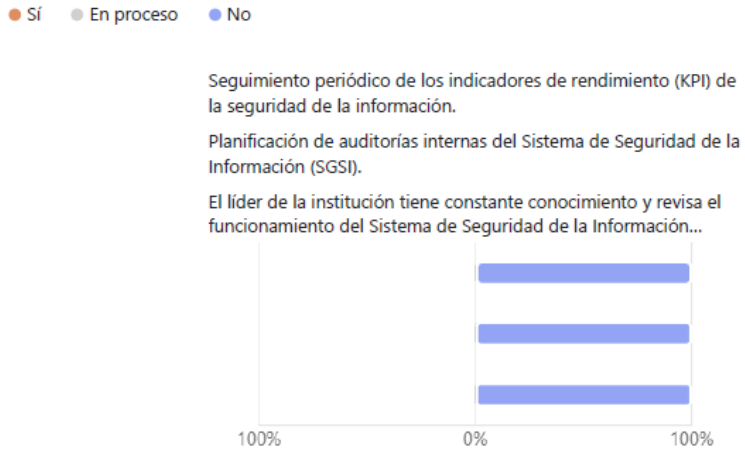
Figura 9. *Gráfico estadístico de Operación*



Fuente: elaboración propia

- **Evaluación de desempeño**

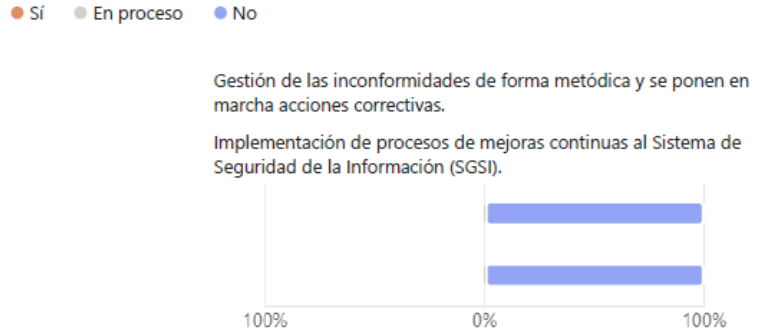
Figura 10. Gráfico estadístico de Evaluación de desempeño



Fuente: elaboración propia

- **Mejora**

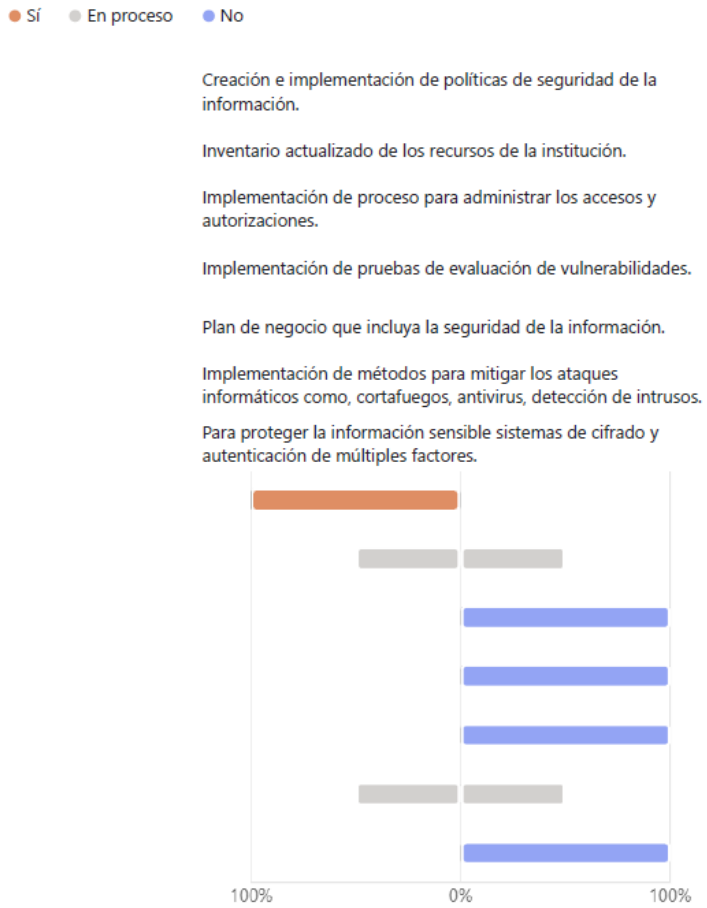
Figura 11. *Gráfico estadístico de mejora*



Fuente: elaboración propia

- Anexo A

Figura 12. Gráfico estadístico de Anexo A



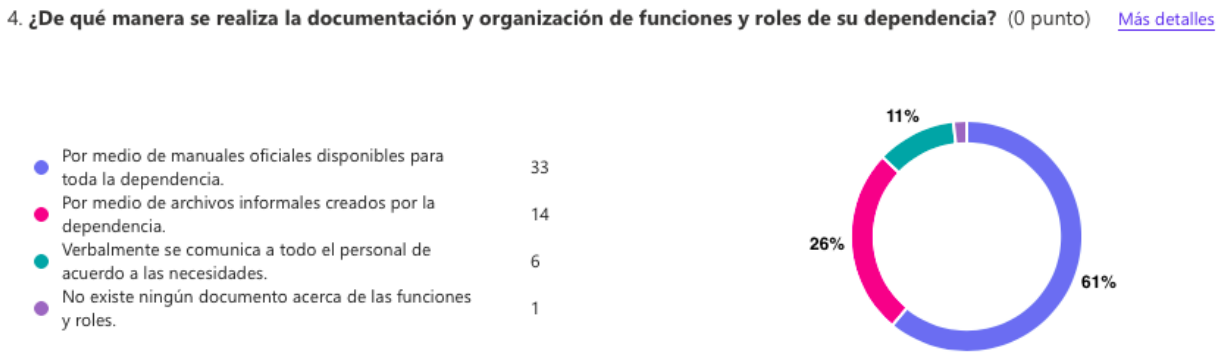
Fuente: elaboración propia

Anexo 2

Interpretación de resultados de encuesta realizada a las distintas áreas de la Gobernación de Tungurahua. Las tres primeras preguntas no se representan en los grafico a continuación, pues están orientadas a la identificación de cada encuestado.

- Pregunta 1, muestra opciones de la dependencia a la cual pertenece.
- Pregunta 2, muestra opciones del cantón al que pertenece el encuestado si es de la dependencia de jefatura o comisaria políticas.
- Pregunta 3, muestra opciones de parroquia al que pertenece la encuesta si es de la dependencia de tenencia política.

Figura 13. Gráfico de tabulación de datos acerca de documentación de roles y funciones.

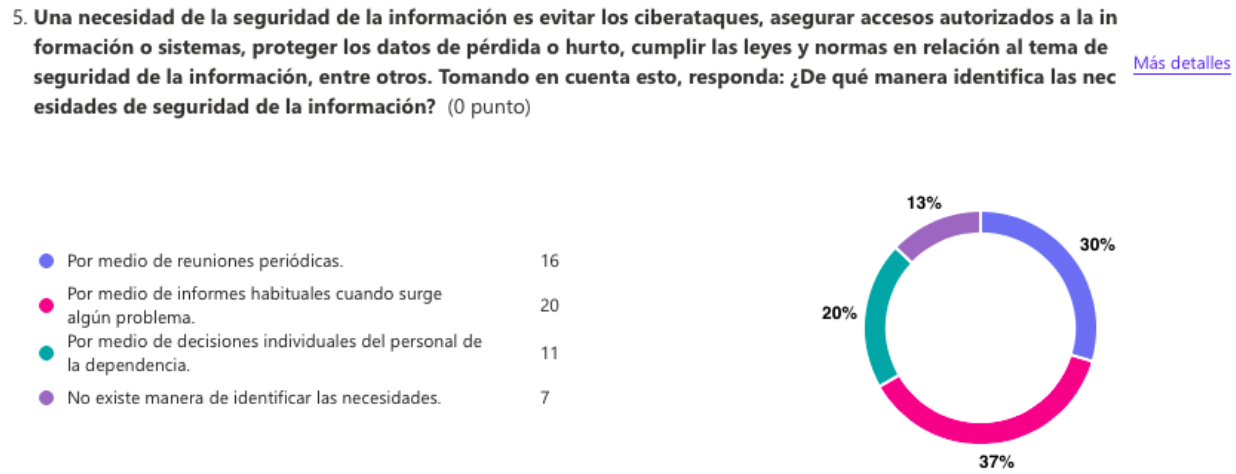


Fuente: elaboración propia

La documentación que utiliza la institución para la definición de funciones y roles para la mayoría de los usuarios (61%) se basan en manuales oficiales, sin embargo, al realizar la investigación se solicitaron dichos manuales y lo que supieron manifestar es, que se basan en el Código Orgánico Penal, más no en un manual estructurado por ellos. Por lo que, se logra entender por qué el resto de encuestados respondieron que utilizan archivos informales (26%), seguido de comunicados verbales de acuerdo con las necesidades (11%). Por otra parte, el 2% indica que no existe documento alguno para establecer funciones y roles.

En conclusión, se refleja la falta de estandarización definida, pues la ISO 27001 solicita una estructura institucional clara que sea avalada por documentación formal.

Figura 14. Gráfico de tabulación acerca de la identificación de necesidades de seguridad de información



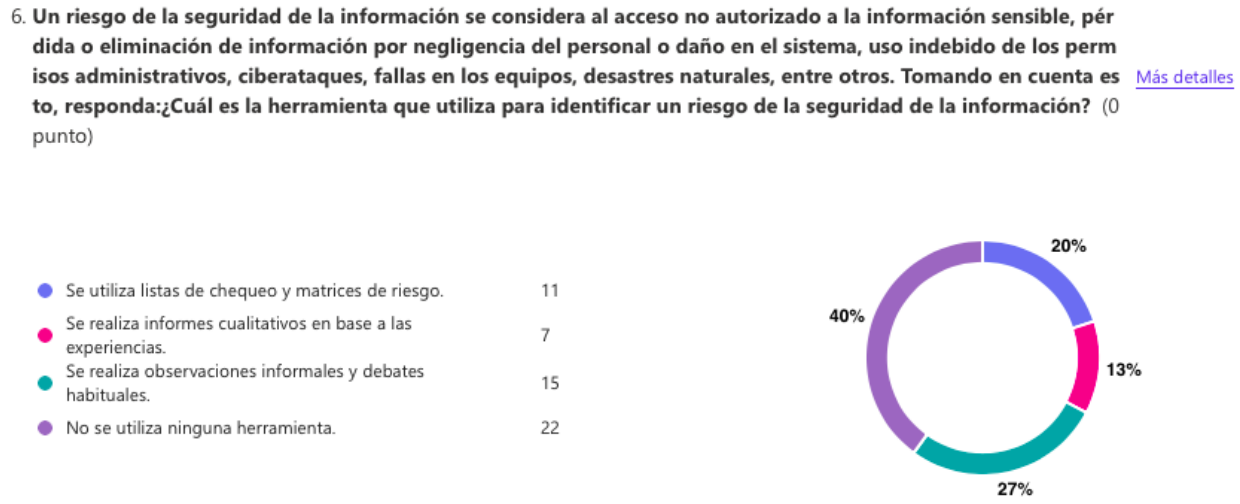
Fuente: elaboración propia

La identificación de necesidades de seguridad de la información se la realiza por medio de informes habituales cuando surge el problema, según el 37% de los encuestados. Esto presenta un porcentaje considerable en el que, si surge un problema se reúnen los funcionarios para comentarlo, sin embargo, no están prevenidos.

Por otro lado, el 30% lo realizan mediante reuniones periódicas. El 20% indica que cada funcionario de la dependencia toma la decisión según sus necesidades y el 13% no tiene manera alguna de identificarlos.

En conclusión, la entidad no cuenta con una herramienta formal para el análisis sistemático ni con una planificación estratégica para comprender las necesidades de la seguridad de información.

Figura 15. Gráfico de tabulación de datos acerca de herramientas para identificación de riesgos relacionados con la seguridad de información.

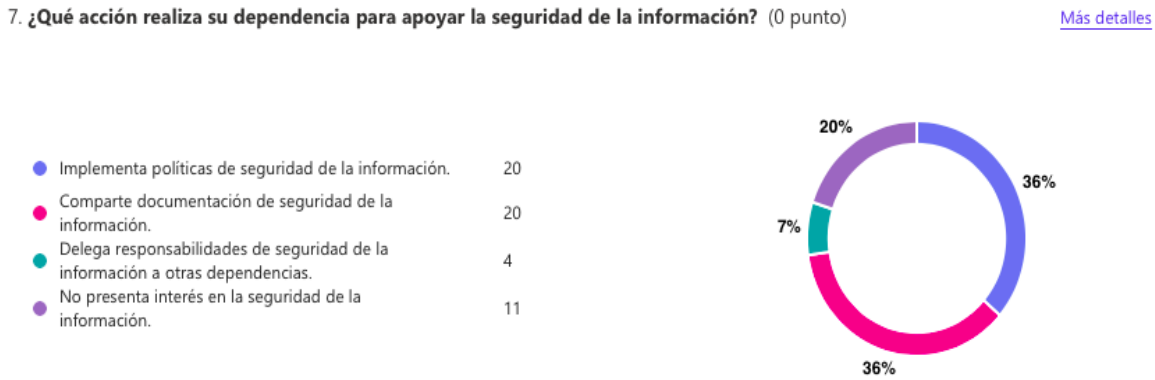


Fuente: elaboración propia

La identificación de riesgos de la seguridad de información es preocupante, pues el 40% de los encuestados no cuenta con una herramienta para poder determinar un riesgo. En cambio, el 27% realiza observaciones y debates informales habitualmente, por lo que se podría decir que cuentan con una forma de identificar los riesgos, pero no la ideal. Las dos opciones formales que ayudan a la identificación de riesgos son listas de chequeo y matrices de riesgo con un 20%, por otro lado, los informes cualitativos según experiencias con un 13%, es decir que no cuentan con prevención sino actúan conforme pasa el problema.

En resumen, la Gobernación no cuenta con una cultura institucional clara, por los que es vulnerable ante amenazas tanto físicas como lógicas.

Figura 16. Gráfico de tabulación de datos acerca de apoyo a la seguridad de información



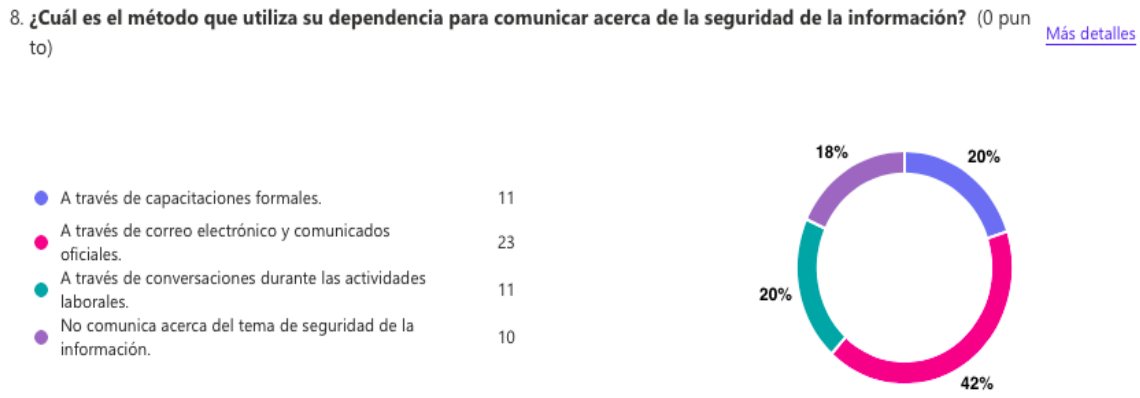
Fuente: elaboración propia

La implementación de políticas de seguridad de la información es uno de los requisitos clave para implementar un SGSI y el 36% de los encuestados afirma que cuentan con ella y por otro lado el 36% cuenta con documentación de seguridad de información. Sin embargo, se solicitó dicha documentación y entregaron documentos de manual de uso de correo institucional, políticas de respaldo de información y políticas de uso de correo institucional, sin embargo, estos documentos no cumplen con requisitos alineados a la ISO 27001.

En cambio, el 20% considera que la dependencia no presenta interés por la seguridad de la información y el otro 7% delega esta responsabilidad a otra dependencia.

Por lo tanto, el personal de la entidad tiene conocimiento limitado acerca de la buena estructura de políticas de seguridad de información, siendo para el ambiente organizacional un riesgo ante cualquier amenaza.

Figura 17. *Gráfico de tabulación de datos acerca de método de comunicación de seguridad de la información*

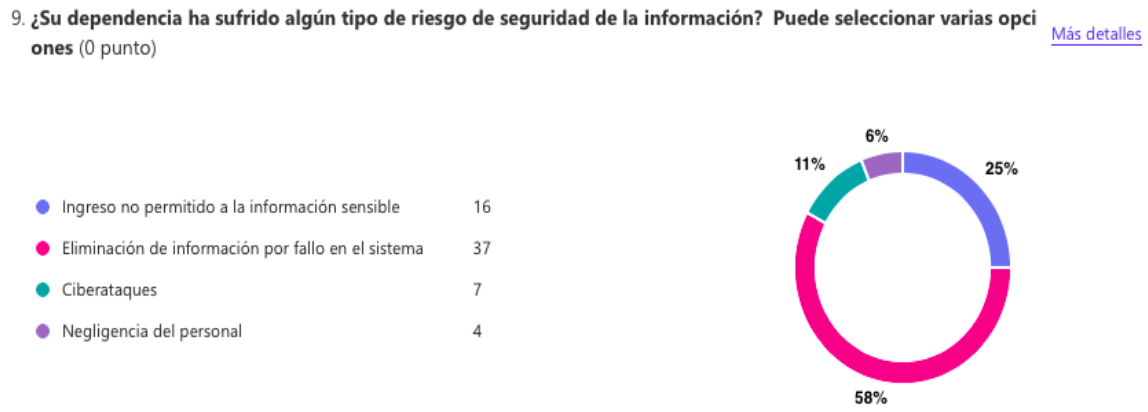


Fuente: elaboración propia

Para la implementación exitosa de un SGSI, es necesario que el personal de la institución conozca acerca de la seguridad de la información, por ello el requerimiento de la ISO 27001 es realizar capacitaciones formales, en la encuesta se obtiene que el 20% lo realiza. Por otra parte, el 42% obtiene información vía correo electrónico y el 20% por medio de conversaciones informales en el contexto laboral. Además, el 18% no comunica acerca del tema. Se concluye, que el porcentaje más alto adquiere información digital, sin embargo, es necesario realizar un plan de capacitación para todo el personal.

En otras palabras, para prevenir cualquier tipo de negligencia por parte del personal es necesario capacitarlos acerca de las buenas prácticas de seguridad de información, sin embargo, la Gobernación no cuenta con programas de concientización ni capacitación lo que es un problema.

Figura 18. Gráfico de tabulación de datos acerca de sufrir riesgo de seguridad de información

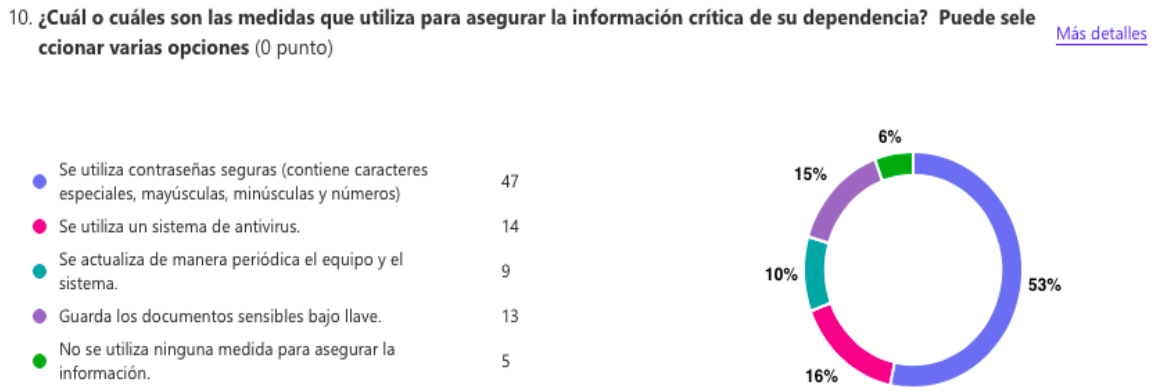


Fuente: elaboración propia

En esta ocasión es preocupante conocer que más de a mitad de los encuestados (58%) ha sufrido eliminación de información por fallo en el sistema, lo que se concluye que no existe métodos de prevención, ni respaldo de información. Además, el 25% contempla el ingreso no permitido a la información crítica, es decir, que no contienen barrera de seguridad ni autenticación en dos pasos. El 11% ha sufrido ciberataques y el 6% negligencia del personal, por lo que es necesario implementar sistemas de prevención de *malware* y otros, así como, control de acceso.

En términos generales la institución requiere planes de contingencia para prevenir cualquier amenaza y evitar pérdida de información o daño en los equipos.

Figura 19. Gráfico de tabulación de datos acerca de seguridad de información crítica.

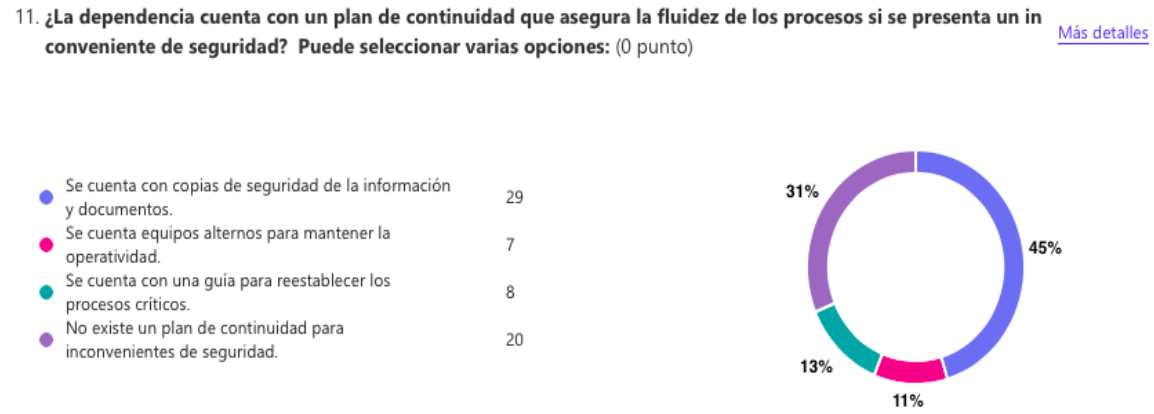


Fuente: elaboración propia

A pesar de que el 53% de los encuestados respondió que utilizan contraseñas seguras, que es una práctica ideal, se realizó una visita a los lugares de trabajo y ciertos funcionarios utilizan notas adhesivas en su computador con sus contraseñas escritas. El 16%, porcentaje considerable, utiliza antivirus. Por otro lado, en términos de documentación física, se utiliza la protección bajo llave, pero con un 15%. Incluso, un 6% no usa ninguna herramienta para asegurar la información.

Por lo que, frente a estos resultados se concluye que la institución no cuenta con medidas, buenas prácticas ni priorización ante la seguridad de información.

Figura 20. Gráfico de tabulación de datos acerca del plan de continuidad ante información.



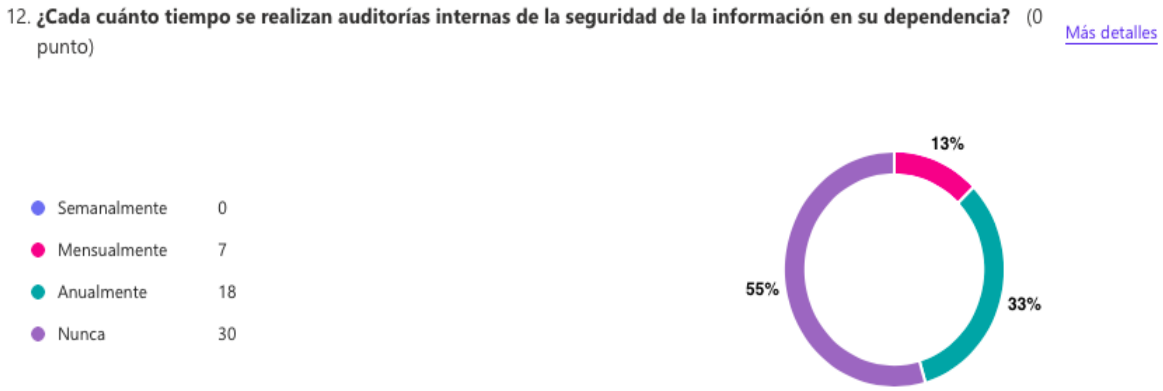
Fuente: elaboración propia.

El 45% de los encuestados dan a conocer que si existe algún fallo existen copias de seguridad de la información, sin embargo, la información que dice ser respalda

se encuentra en los mismos equipos. En cambio, el 31% no tiene ningún plan de continuidad. Pero es interesante conocer que el 13% cree tener una guía para reestablecer procesos críticos, la cual se solicitó, pero no fue entregado ningún documento que evidencie esta respuesta.

En conclusión, los funcionarios no comprenden en su totalidad la necesidad de un plan de continuidad para evitar la inoperatividad de la institución y trabajan bajo un conocimiento limitado de esto.

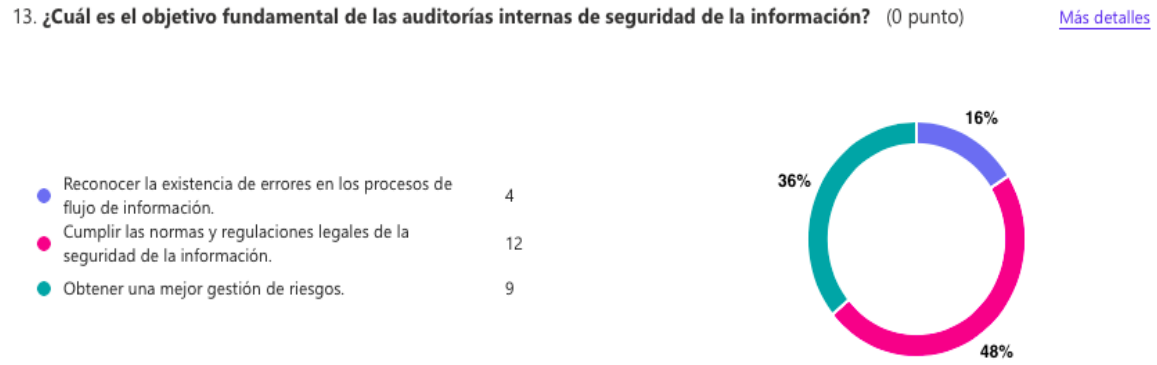
Figura 21. Gráfico de tabulación de datos acerca de auditorías internas.



Fuente: elaboración propia

Es preocupante conocer que más de la mitad de los encuestados no realizan auditorías en sus dependencias, solo el 33% las realiza anualmente y el 13% mensualmente. Sin embargo, se solicitó documentación que evidencia la realización de dichas auditorías y muestran datos de auditorías internas no relacionadas con la seguridad de información. En conclusión, los funcionarios no comprendieron el tema de seguridad de información a pesar de que se detalló de manera explícita. Por otro lado, es alarmante conocer que no se realiza ningún método para monitorear el flujo de datos.

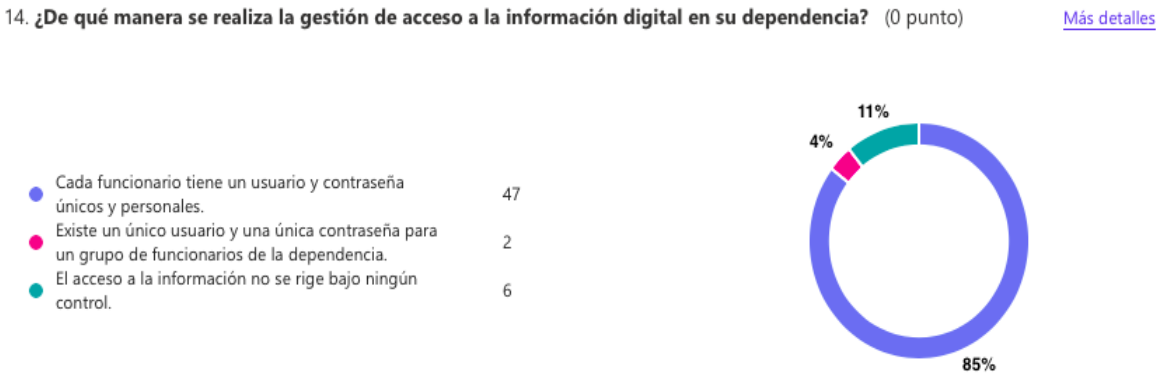
Figura 22. Gráfico de tabulación de datos acerca de función de auditorías.



Fuente: elaboración propia

La presente pregunta dependía de la anterior, por lo que, los encuestados que seleccionaron la opción" nunca" no les apreció esta. Mientras tanto, el 48% menciona que una auditoría tiene por objetivo cumplir el reglamento legas, el 36% gestiona mejor los riesgos y el 16% para recocer los errores humanos. Sin embargo, gracias a las anteriores preguntas y a la documentación solicitada por el presente autor, se logra conocer que los encuestados se contraponen en sus respuestas ya sea porque no tienen conocimiento de ello o por la no comprensión de la buena cultura organizacional frente a la seguridad de información.

Figura 23. Gráfico de tabulación de datos acerca de control de acceso a información física.



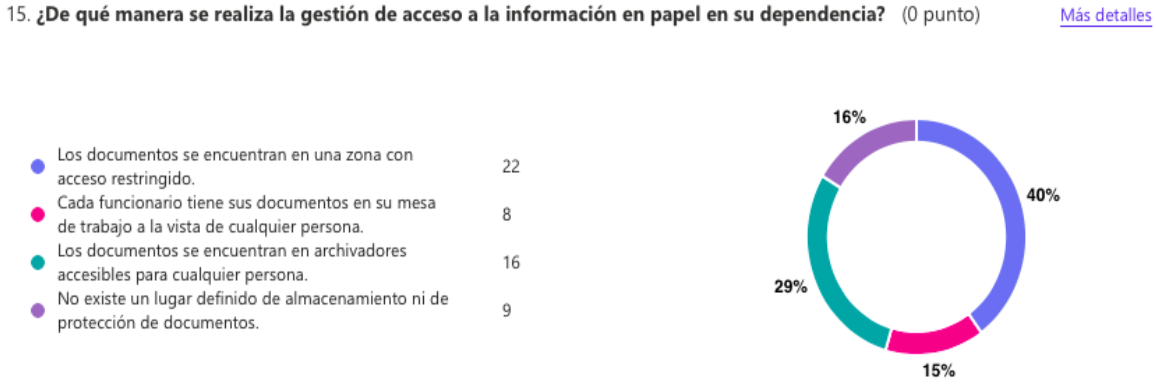
Fuente: elaboración propia

Para el control de acceso a la información la opción más habitual (85%) es el uso de contraseñas para cada usuario, sin embargo, en anteriores preguntas se concluye que no tiene propósito alguno, pues usuarios escriben sus contraseñas

en notas adhesivas en sus monitores. Por otro parte, el 11% no se rige bajo ningún control y es preocupante porque la información no se encuentra protegida.

En conclusión, la entidad no establece una política de control de acceso, lo que transmite que uno de los principios básicos de la ISO 27001, confidencialidad, no se cumple y esto genera desconfianza para la ciudadanía e involucrados.

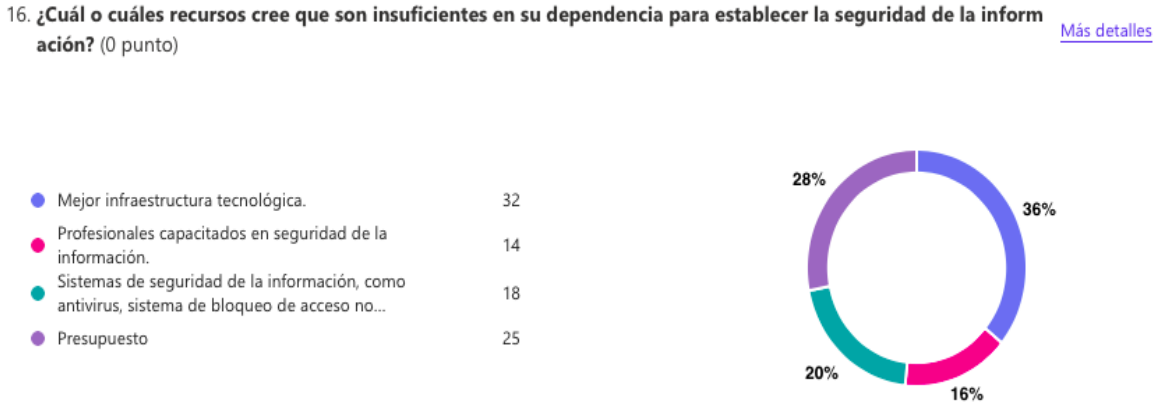
Figura 24. Gráfico de tabulación de datos acerca de control de acceso a información física.



Fuente: elaboración propia

La Gobernación cuenta con una serie de proceso manuales, por lo que gestionan gran cantidad de documentos físicos, es por ellos que el control de acceso es fundamental. La encuesta muestra que el 40% cuentan con una zona restringida para estos archivos, seguido del 29%, que indica que se encuentran al alcance de cualquier persona. Por lo que, menos de la mitad de los funcionaros no cuentan con una zona definida para sus documentos sensibles, sin embargo, es necesario generar un plan de acción para solventarlo.

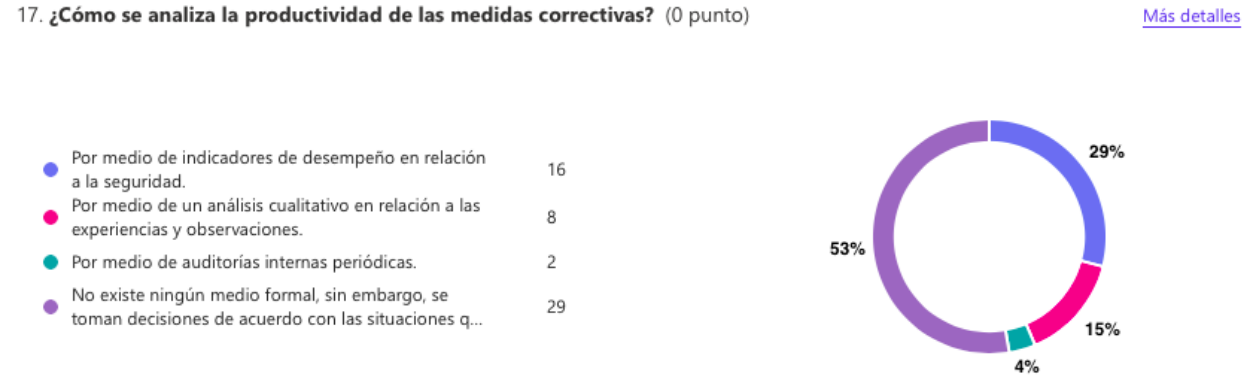
Figura 25. Gráfico de tabulación de datos acerca de recursos para una mejor seguridad de la información.



Fuente: elaboración propia

Es interesante conocer que los funcionarios creen que se necesita mejor infraestructura tecnológica, la presente investigación solicitó el inventario tecnológico de la entidad y se confirma que la mayoría de los equipos son obsoletos. No obstante, la otra parte de encuestados responden que existe falta de presupuesto, por lo que se concluye que por ese motivo la Gobernación no podría actualizar su equipo tecnológico. Además, de que no existen sistemas para prevenir amenazas y poco personal capacitado, pues la Unidad TI está conformado por una sola persona.

Figura 26. Gráfico de tabulación de datos acerca de medidas correctivas.

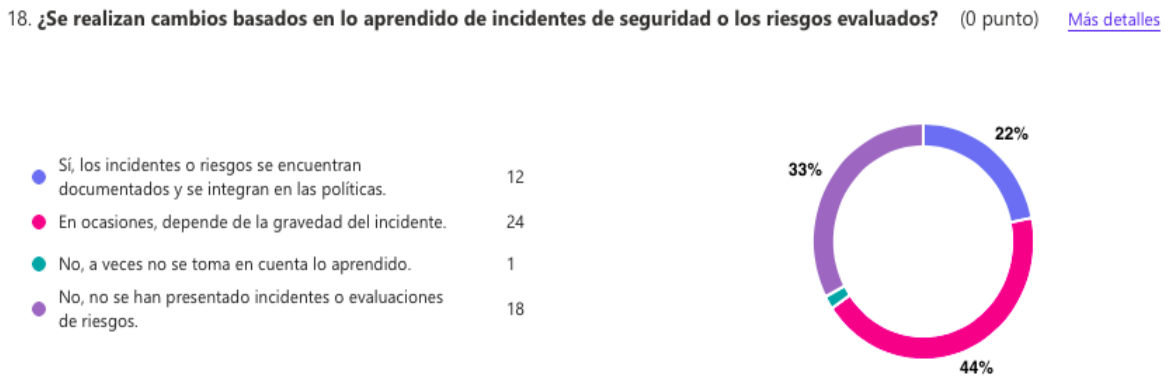


Fuente: elaboración propia

Es importante lo que se detalla en esta pregunta, pues más de la mitad de encuestados no utilizan ningún medio formal para la realización de medidas, pero actúan después de que sucede el problema. En cambio, pocos son quiénes utilizan indicadores de desempeño en relación con la seguridad. Sin embargo, es curioso

entender como utilizan los KPI si no cuentan con un sistema de identificación de riesgos. Por lo que, se concluye que el personal no tiene conocimiento alguno acerca del tema y solo actúan si les pasa algún problema más no previenen el mismo.

Figura 27. Gráfico de tabulación de datos acerca de cambios en caso de incidente.



Fuente: elaboración propia

La ISO 27001 requiere la documentación y un análisis de incidentes para establecer acciones correctivas, sin embargo, la institución no cuenta con la debida estructura de riesgos ni análisis de estos, lo ideal sería que más de la mitad si no es todos identifiquen las amenazas.

PUCE | AMBATO

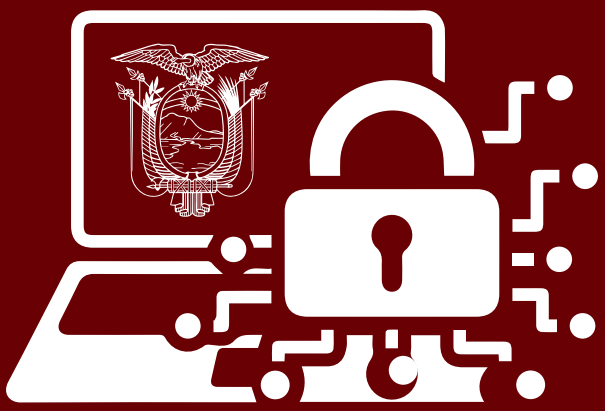
GUÍA PARA LA IMPLEMENTACIÓN ISO 27 001 2022

AUTOR
CAMILA AMANCHA

DIRECTOR
ING. MG. TERESA FREIRE

ESCUELA DE INGENIERÍAS

PUCE | AMBATO



GUÍA PARA LA IMPLEMENTACIÓN ISO 27 001 2022

CONTENIDO

01 INTRODUCCIÓN

ANTECEDENTES

OBJETIVO DE LA GUÍA

Brindar un instrumento práctico que posibilite la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Unidad de Tecnología de la Información (TI) de la Gobernación de Tungurahua, basándose en los parámetros establecidos por la norma ISO 27001: 2022.

Además, este documento se enfoca en ser una referencia para otras organizaciones públicas del Ecuador de similar estructura, que confronta retos similares en el proceso de mantener la información segura. El optar por un SGSI permite la protección de la información en todas sus formas, además, incrementa la confianza de los ciudadanos y una administración segura y eficiente de los datos sensibles.

La Gobernación de Tungurahua es una entidad pública cuya máxima autoridad es el gobernador o gobernadora, quien es el representante del Presidente de la República del Ecuador en la provincia, encargado de coordinar y controlar las políticas del gobierno nacional, además, de dirigir las actividades de funcionarios y representantes de la Función Ejecutiva en cada provincia. La estructura institucional de la entidad se basa en Despacho de Gobernación, Unidad de Asesoría Jurídica, Unidad de Planificación y Gestión Estratégica, Unidad de Comunicación Social, Unidad de Tecnologías de la Información y Comunicaciones, Unidad de Administración y Talento Humano, Unidad de Administración Financiera, además, cuenta con área operativas: Jefaturas Políticas, Tenencias Políticas, Comisarías de Policía, Intendencia General de Policía de Tungurahua.
La Unidad de Tecnologías de la Información y Comunicación de la Gobernación de Tungurahua, en la actualidad está conformado por un solo responsable. Las actividades que se cumplen en esta Unidad de Gestión son:

- Crear, renovar, certificar y dar seguimiento a la implementación de manuales, guías, políticas, procesos, metodologías y/o sistemas en el contexto de TI.
- Gestionar planes para actualizar anualmente el servicio de alojamiento web, dominio, correo electrónico institucional, certificados de seguridad y mantenimiento del sitio web institucional.
- Gestionar la adquisición y actualización de equipos tecnológicos y networking de la Gobernación de Tungurahua.
- Gestionar del mantenimiento de equipos tecnológicos, comunicaciones y sistema de networking de la Gobernación de Tungurahua.
- Gestionar el mantenimiento preventivo y correctivo del sistema de video vigilancia de la Gobernación de Tungurahua
- Realizar reportes administrativos, de monitoreo y control de capacitación, incidencias en los distintos bienes de hardware y software para brindar soluciones tecnológicas.
- Gestionar y dar seguimiento en las zonas de su competencia, el funcionamiento y operatividad de los procesos desconcentrados
- Crear, comprobar y aprobar términos de referencia, funcionalidades y métodos para la contratación del desarrollo servicios tecnológicos, consultorías y demás en relación con TI.
- Administrar las redes y bienes tecnológicos de la institución.
- Dar seguimiento y disponer la atención para solucionar los incidentes notificados que se dan en los bienes informáticos que administra la institución.

La limitación de personal y recursos presenta un desafío para avalar la seguridad de la información, por lo que, la Gobernación se encuentra vulnerable antes amenazas y riesgos.

La Gobernación al no contar con seguridad que permita proteger su información y ante la ausencia de flujo de información centralizado, pues cada área manipula su información de manera independiente, dificulta la trazabilidad y el manejo efectivo de los datos. Este problema aumenta el riesgo de pérdida, mal uso o el acceso no autorizado de la información crítica.

Por lo tanto, para mitigar estas deficiencias, es necesario implementar un Sistema de Gestión de Seguridad de la Información bajo la norma ISO 27001. Este ayuda a establecer procesos claros y consistentes para gestionar los datos y avalar el cumplimiento de requerimientos legales y normativos.

De acuerdo con los hallazgos encontrados gracias a la investigación realizada en la Gobernación de Tungurahua, tiene una estructura limitada en su Unidad de Tecnología, pues cuenta con una sola persona que se responsabiliza de todas las actividades de la unidad definidas en el Estatuto Orgánico del Ministerio de Gobierno.

Además, cuenta con un inventario tecnológico básico, tiene una planificación de proyectos a nivel institucional anual y no a largo plazo, presenta escasez de protocolos de seguridad de la información, cuenta con una red interna y sistemas de seguridad de información escasos, la información sensible se maneja en papel sin controles de seguridad. Por otro lado, la dirección de la Unidad TI de la Gobernación de Tungurahua, se encuentra en proceso de implementación de un SGSI. Incluso, los objetivos de la seguridad de información, la administración de riesgos, el plan de tratamiento, plan estratégico de TI, plan de continuidad de negocio, entre otros, no se encuentran definidos.

Estas observaciones y más son problemas para el proceso de implementación de un Sistema de Gestión de Seguridad de Información, pues la ISO 27001:2022 requiere una distribución jerárquica con funciones definidas, especialmente para el SGSI. La seguridad de la información debe contener un enfoque claro para la gestión de amenazas y protección de datos. Asimismo, entender que la gestión de infraestructura tecnológica no es únicamente administración de inventario de hardware sino también mantenimiento, actualización, capacitación del personal, inventario de software para mejor operatividad.

ALCANCE

El alcance de esta guía se enfoca en adoptar un SGSI en la Unidad de Tecnologías de la Información y Comunicación de la Gobernación de Tungurahua. Este alcance engloba tanto los activos de información manipulados por TI, como los procesos de cada una de las unidades de la institución

La responsabilidad del manejo de la información es compartida entre la Unidad de Tecnología de Información y los directores departamentales de las diferentes unidades de la Gobernación; en tal sentido, es importante la participación de todos para que el SGSI tenga éxito.

El Sistema de Gestión de Seguridad de la Información propuesto incluye la protección de los activos de TI más importantes de la Gobernación, como el sitio web oficial, información del Quipux y la base de datos que se utilicen para almacenar información importante. Además, abarca interacciones entre las unidades para que el flujo de información sea más seguro y centralizado.

02

FUNDAMENTOS DE LA NORMA ISO 27001

¿QUÉ ES UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN? SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un método estructurado para administrar información crítica de una institución, de esta manera se garantiza confidencialidad, integridad y disponibilidad.

Además, el sistema utiliza políticas y controles creados para la protección de la información frente a amenazas y asígarantizar la estabilidad de la empresa. La implementación de un SGSI abarca el reconocimiento de riesgos y vigilancia constante del cumplimiento de normativas establecidas.

Es importante conocer que un SGSI no solo incluye recursos tecnológicos de la seguridad de la información, sino también recursos humanos y de organización, como usuarios, procedimientos y activos fundamentales de la seguridad. Esto es esencial en el contexto de la Gobernación de Tungurahua, pues se presenta la escasez de elementos y personal especializado, por lo que se indispensable mejorar la eficiencia y continuidad en la gestión de información.

ISO 27001 2022

Es considerada una referencia internacional que brinda una arquitectura detallada para la inserción, conservación y avance de un Sistema de Gestión de Seguridad de la Información.

La versión actualizada de la norma contribuye a un enfoque más versátil y moldeable, por lo que, las instituciones tienen la opción de personalizar las políticas de seguridad según sus necesidades y contexto en el que se operan. En el contexto de las organizaciones públicas, específicamente la Gobernación de Tungurahua, la ISO 27001 contempla reglas y políticas para asegurar la información crítica, menorar las vulnerabilidades y optimizar los procedimientos.

RELEVANCIA DE ISO 27001 PARA LA GOBERNACIÓN DE LA PROVINCIA DE TUNGURAHUA

La norma ISO 27001 se ha convertido en una regulación relevante para las instituciones públicas porque se manipula numerosa cantidad de información pública, interna y confidencial de trascendencia social que necesita un máximo nivel de protección.

De igual manera, la instauración de un SGSI enfocado en la ISO 27001 promueve el cumplimiento de exigencias legales y normativas de regulación de seguridad de información en el ámbito público en Ecuador.

También, refuerza la credibilidad de las instituciones hacia los ciudadanos, pues se garantiza que sus datos estén protegidos.

En otras palabras, si se adopta la ISO 27001 en la Gobernación de Tungurahua y en otras entidades públicas similares, se fortalecerá la eficiencia y transparencia de los procesos gubernamentales, e incluso contribuirá a generar consciencia a nivel de seguridad de la información en el país

03 CONTEXTO DE LA ORGANIZACIÓN

El contexto de la organización determina las condiciones mínimas necesarias para la implementación de la ISO 27001:2022, por lo que se detalla a continuación las propuestas de como formar una estructura clara y definida para un mejor orden en la entidad.

3.1 ORGANIGRAMA FUNCIONAL

DIRECTOR DE UNIDAD TI	FUNCIONES		
	Coordinar y organizar recursos recursos tecnológicos	Gestionar contratos tecnológicos	Elaborar planes estratégicos de TIC

SUBUNIDAD DE INFRAESTRUCTURA Y REDES **Coordinador de ciberseguridad y redes**	FUNCIONES	Proveer recursos tecnológicos Monitorear y aplicar esquema de seguridad tecnológica Examinar diagramas de red e infraestructura	Planificar y ejecturar el mantenimiento - monitoreo de infraestructura tecnológica
SUBUNIDAD DE SEGURIDAD Y PROTECCIONES **Coordinador de protección de datos**	FUNCIONES	Aplicar normas de seguridad tecnológica Desarrollar y monitorear matrices de riesgo Gestionar políticas de seguridad	
SUBUNIDAD DE SOPORTE Y CAPACITACIÓN **Responsable de soporte técnico**	FUNCIONES	Coordinar mantenimiento preventivo y correctivo Gestionar cuentas de usuarios Gestionar mesa de ayuda	

El organigrama que se propone sea implementado en la Unidad de TI, se basa en el contexto actual de la misma, dentro de la estructura organizacional y con lo mínimo requerido para definir un esquema enfocado en la seguridad de la información y para mejorar la estructura actual

Se sugiere que la Unidad de TI conste de un director de TI que sea la cabeza del área apoyado por tres subunidades: infraestructura y redes para administrar software, hardware, mantenimiento, y gestión de redes; otra de seguridad y protección de datos para supervisión de la instauración de políticas de seguridad; por último, una de soporte y capacitación para gestione las necesidades de usuario en problemas comunes y problemas complejo. El director de TI será el encargado de crear propuestas de proyectos, además, optimización de recursos y procesos.

3.2 FUNCIONES DENTRO DEL SGSI

Para elaborar un Sistema de Gestión de seguridad de información (SGSI), es importante elaborar ciertos elementos que ayudarán a una mejor efectividad.

3.2.1. Elaborar un Plan Estratégico de Tecnologías de Información (PETI)

Si bien dentro de la presenta guía, no se contempla especificar el contenido del PETI, en función de la norma ISO se propone unos lineamientos mínimos para su desarrollo.

INTRODUCCIÓN
Breve descripción acerca del propósito que tiene el PETI en la Unidad TI y en la Gobernación de Tungurahua. Además, de un contexto organizacionales en relación con las tecnologías de información.

ALCANCE
Dar a conocer los límites del PETI en conjunto con los procedimientos, unidades y funciones dentro de la Gobernación.

PRINCIPIOS Y CONSIDERACIONES
Describir la base conceptual de la transformación tecnológica que tendrá la Gobernación, alineados a los objetivos específicos previamente definidos y a las políticas ecuatorianas y provinciales.

DIAGNÓSTICO
Identificar las unidades que requieren actualizaciones tecnológicas de acuerdo con el FODA.

ESTRUCTURA DE UNIDAD TI
Determinar una organización para administrar la unidad con la asignación de roles y funciones

MONITOREO Y CONTROL
Establecer los indicadores de desempeño o KPIs para medir la efectividad del PETI. Además, estructurar un plan de seguimiento y control una vez al año.

OBJETIVOS
Establecer un objetivo general que describa el enfoque estratégico del PETI. También, determinar objetivos específicos que abarquen la adaptación tecnológica, digitalización y actualización de recursos tecnológicos.

CONTEXTO DE LA ORGANIZACIÓN
Redactar la situación actual de la Unidad TI de la Gobernación y realizar el proceso de FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)

PETI - PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN
Adjuntar los documentos necesarios como, hoja de ruta, cronograma de propuestas tecnológicas; plan de trabajo, soluciones para prevenir o resolver los problemas detectados en el FODA; presupuesto, recursos previstos para cada solución; y, cronograma fechas para determinar el inicio y el fin de las tareas.

ESTRUCTURA DE SEGURIDAD DE INFORMACIÓN
Plan para asegurar la información alineado a la gestión de riesgos.

PLAN DE COMUNICACIÓN
Estrategia para socializar el PETI con los funcionarios de la entidad

3.2.2. Elaborar políticas de seguridad de la información

Las políticas que se definan deben enmarcarse en los siguientes puntos:

PROPÓSITO Y ALCANCE
Describir los límites de las políticas y el objetivo que tiene para garantizar la seguridad de la información. Así como, el compromiso de la alta dirección frente al tema.

POLÍTICAS GENERALES
Describir el marco legal nacional relacionado con la seguridad de información para las instituciones públicas.

ROLES Y RESPONSABILIDADES
Establecer las funciones que deben cumplir los involucrados principales Unidad TI, usuarios de las unidades y la alta dirección.

POLÍTICAS DE CONTROL DE ACCESO
Dividir el control de acceso a zonas lógicas, administración de contraseñas y permisos a sistemas de información; control de acceso a zonas físicas, registrar visitas a zonas críticas y administración de permisos

CLASIFICACIÓN DE INFORMACIÓN
Describir la importancia de la información, ya sea lógica y física, de acuerdo con la sensibilidad.

POLÍTICAS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE INFORMACIÓN
Informar del número de copias que se deberán realizar según el nivel de clasificación de información.

POLÍTICAS DE GESTIÓN DE RIESGOS
Estructurar un plan de gestión de riesgos alineado a una metodología acorde al contexto de la situación actual de la entidad.

POLÍTICAS DE CONTINUIDAD DE NEGOCIO
Asegurar que los procesos mantendrán su operatividad ante cualquier circunstancia.

POLÍTICAS DE ESCRITORIO LIMPIO
Determinar procesos para mantener el espacio de trabajo ordenado y limpio.

CUMPLIMIENTO Y SANCIONES
Describir las sanciones por incumplimiento de las políticas para mantener su practicidad.

POLÍTICAS DE ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN
Describir el plazo para actualizar el inventario de recursos tecnológicos y la necesidad de clasificar la información.

POLÍTICAS CONTRA CIBERATAQUES
Enumerar herramientas necesarias para mitigar los ciberataques de acuerdo con los activos de información que contiene la Gobernación.

POLÍTICAS DE USO DE CORREO ELECTRÓNICO
Describir las limitaciones del uso del correo electrónico institucional y formas de evitar ciertas amenazas.

POLÍTICAS DE DOCUMENTACIÓN FÍSICA
Gestionar prácticas para asegurar los documentos físicos de acuerdo con la clasificación de la información.

POLÍTICAS DE AUDITORÍAS INTERNAS
Describir un marco para probar la efectividad de las auditorías internas.

REVISIÓN Y ACTUALIZACIÓN
Describir el plazo de vigencia de las políticas y de mejora por un determinado tiempo.

3.3 INFRAESTRUCTURA TECNOLÓGICA

Para mantener el orden en la infraestructura tecnológica de la entidad es necesario comprender ciertos formatos para una mejor operatividad.

3.3.1. Elaborar un inventario tecnológico actualizado

Según la norma, el inventario debe estructurarse de manera clara y ordenada en una tabla con columnas que permitan conocer el estado, durabilidad y caracterización del activo, de la siguiente manera

CÓDIGO DE EMPRESA
Código que la empresa asigna a cada recurso para identificar cada activo tecnológico.

NOMBRE
Nombre con el que se identifica al activo.

CUSTODIO
Nombre de usuario a quién pertenece el activo y se hace responsable de este.

PARROQUIA
Nombre de parroquia de Tungurahua en donde se encuentra el activo.

DESCRIPCIÓN
Breve descripción que detalle el objetivo del activo.

TIPO
Clasificación del activo como: hardware, software, información o infraestructura.

CANTÓN
Nombre de cantón de Tungurahua en donde se encuentra el activo.

UNIDAD
Dependencia a la cual pertenece el activo.

FECHA DE ADQUISICIÓN
Fecha corta en el que el activo llegó a la Gobernación.

FECHA FIN DE VIDA ÚTIL
Fecha corta en el que se estipule la obsolescencia del activo.

ESTADO
Clasificación del activo de acuerdo con su condición (activo, obsoleto o en mantenimiento)

OBSERVACIÓN
Comentarios por parte del experto.

CARACTERÍSTICAS
En caso de ser hardware, RAM, disco duro, almacenamiento, etc.; software, versión, licencia, compatibilidad, etc.; información, formato, volumen, ubicación, etc.; por último, infraestructura, ancho de banda, ubicación física, redundancia, etc. Esta columna podría dividirse en sub-columnas para mejor entendimiento.

Para mantener el orden en la infraestructura tecnológica de la entidad es necesario comprender ciertos formatos para una mejor operatividad.

3.3.2. Implementar herramientas de seguridad de información

Para asegurar los sistemas de información de la Gobernación: correo electrónico, Quipux, sitio web institucional, equipos computacionales, entre otros, es necesario contemplar la utilidad de ciertas herramientas, como:

RED PRIVADA VIRTUAL (VPN)

Lo ideal es implementar un servidor en el centro de cómputo y configurarlo para que enrute todo el tráfico por medio de una conexión segura. Además, para los sistemas de comunicación es necesario configurar la VPN para que solo utilice puertos SMTP, IMAP y POP3. Por otro lado, para el sitio web institucional, se restringirá el panel de acceso y deberá permitir únicamente la navegación por HTTPS. Por último, los equipos de los usuarios se configurarán con la VPN para que el tráfico pase por medio de un túnel cifrado.

HERRAMIENTA SIEM

Sistema que se utiliza para administrar la información y los incidentes de seguridad para analizarlos en tiempo real por medio de alertas y deteczción proactiva de peligros y amenazas

FIREWALL DE PRÓXIMA GENERACIÓN (NGFW)

Implementar un NGFW para los activos de información y controlar el tráfico entrante y saliente, así como, evitar ataques cibernéticos.

ANTIVIRUS

Utilizar un antivirus que proteja contra ciberataques y monitoreo la actividad de los dispositivos.

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS (IDS/IPS)

Tiene la capacidad de centralizar la información de logs y sirve como barrera de control de acceso.

COPIAS DE SEGURIDAD

Realizar el respaldo de datos de acuerdo con las políticas de seguridad de la información.

3.3.3. Elaborar un plan de mantenimiento preventivo y correctivo

Un plan de mantenimiento tanto preventivo y correctivo para los recursos tecnológicos se debe llevar a cabo Zen base a una estructura relacionada al presupuesto y contexto de la Gobernación:

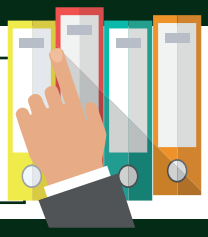
MANTENIMIENTO PREVENTIVO

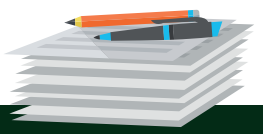
El mantenimiento preventivo se realizará cada 6 meses a los equipos antiguos o que ya no cuenten con garantía, de acuerdo con el presupuesto destinado por la alta dirección. Por otro lado, para los equipos que contengan garantía, únicamente se destinara un mantenimiento lógico y limpieza profunda. Antes de cualquier tipo de mantenimiento, el usuario deberá respaldar la información por cualquier percance e incluso describirá los problemas que ha sufrido durante el tiempo de uso para justificar el cambio de partes. El mantenimiento preventivo abarcará: en el CPU, un desmontaje, limpieza profunda tanto interior como exterior, aspirado, comprobación de tarjetas, limpieza de controladores. Comprobar y garantizar los vínculos de red (conexiones, cables, conectores). Revisión y limpieza del teclado y monitor. Verificar la instalación de antivirus y configurarlo en caso de ser requerido. Eliminar caché y vaciar la papelera.

MANTENIMIENTO CORRECTIVO

Si existe algún tipo de desperfecto en el equipo se recurrirá al mantenimiento correctivo, para ello, el usuario tendrá que contactarse vía correo electrónico con la Unidad TI y explicar el descontento para que el jefe de TI pueda proceder con su necesidad. En el caso de que el equipo cuente con garantía se deberá poner en contacto con la empresa proveedora del equipo y gestionar la corrección lo más pronto posible para evitar inoperatividad.

3.3.4. Crear un sistema de gestión de documentos en papel





Este sistema se alineará a las políticas de seguridad de información, específicamente las políticas de documentación física y control de accesos, pues en primer lugar se deberá clasificar la información de acuerdo con los niveles de sensibilidad para luego etiquetarlos. Estos pasos ayudaran a conocer la cantidad de documentos que se manejan dentro de cada dependencia y el flujo de información que se maneja. Después, se tendrá que verificar la ubicación exacta. Todo esto para crear un índice maestro que contemplará: el tipo, ubicación exacta y la fecha de emisión y recepción del documento.

03

3.4 ALCANCE DEL SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Gobernación de Tungurahua está establecido por la urgencia de instaurar un sistema robusto de confidencialidad de datos dentro de la Unidad de Tecnologías de la Información y Comunicación (TI), pues es el encargado de asegurar la información en la entidad. Este SGSI empezará por implementarse en dicha unidad para una mejor gestión de infraestructura tecnológica, gestión de riesgos, administración de sistemas, procesos de respaldo y recuperación de datos y regularización de protección de datos y buenas prácticas de control de acceso.

La institución reconoce que es fundamental el proteger el activo más valioso de cualquier entidad, la información. Por ello, es imperativo la aplicación de políticas y procesos del SGSI en el área tecnológica para que los usuarios que dependen del soporte técnico de esta evidencien la existencia de integridad, confidencialidad y disponibilidad

Por otro lado, el sistema abarca los recursos tecnológicos como, servidores, redes, equipos; sistemas como, sitio web, sistemas de comunicación electrónica; y documentación física de procesos de la institución.

04

LIDERAZGO

El liderazgo compromete a la alta dirección, Despacho de la Gobernación, a formar parte de la implementación y operatividad del SGSI, siendo este uno de los principales actores junto con el director de la Unidad TI. Para ello es necesario, establecer objetivos y esquematizar documentos necesarios para el SGSI.

4.1 COMPROMISO DE ALTA DIRECCIÓN

La alta dirección ayudará con la aprobación y gestión de una capacitación acerca de la ISO 27001:2022 para la Unidad TI, a través de empresas certificadoras de la norma, y de ser posible participará de igual manera para conocer el objetivo de la normativa, así como la importancia de esta.
Esta capacitación podrá ser de empresas que certifiquen, pues tendrán un mayor conocimiento del tema. Por otro lado, la alta dirección tendrá la responsabilidad de emitir un documento que certifique la aprobación de la implementación del SGSI en la Gobernación de Tungurahua, Unidad TI para avalar su compromiso con la protección de datos.

04 ES NECESARIO DETERMINAR OBJETIVOS ESPECÍFICOS PARA EL SGSI

1. Disminuir los riesgos de seguridad de la información para ser una entidad confiable, integra y disponible.
2. Optimizar el tiempo de respuesta ante las amenazas lógicas y físicas
3. Asegurar la información crítica y sensible con la ayuda de políticas de seguridad.

Estos objetivos son una sugerencia basados con el contexto de la Gobernación de Tungurahua, sin embargo, podrán ir cambiando conforme las necesidades de la Unidad TI.

La Unidad TI se compromete a enviar un reporte periódico acerca de la efectividad del SGSI, de los incidentes y mejoras que se han ejecutado. El informe deberá contener:

PORTADA
Identificación del informe (título, fecha, autor

MÉTRICAS DE EFECTIVIDAD
Resultado y la frecuencia temporal del cálculo de la fórmula de la métrica.

RESUMEN
Explicar a breve rasgos el estado del SGSI, la cantidad total de los incidentes detectados y tratados, así como, la cantidad de mejoras implementadas.

ESTADO DE LOS CONTROLES DEL SoA
Describir si se implementó o actualizó un control e indicar los controles pendientes

RESUMEN DE INCIDENTES
Detallar los incidentes reportados, análisis de incidentes críticos.

MEJORAS
Descripción de mejoras y el impacto que van a ocasionar

PLAN DE ACCIÓN
Detallar actividades que quedan pendientes hasta el nuevo reporte.

CONCLUSIONES Y RECOMENDACIONES

4.2 DECLARACIÓN DE APLICABILIDAD (SoA)

La declaración de aplicabilidad se realizará acorde con las necesidades de la Gobernación y en base a los controles establecidos por el Anexo A de la ISO 27001:2022. Este documento será zuna matriz con las siguientes columnas:

SECCIÓN	DESCRIPCIÓN	ESTADO ACTUAL
Número que identifica al control de acuerdo con el Anexo A.	Nombre del control que se establece en el Anexo A.	Clasificación, por implementar o implementado, según corresponda.

04

DECLARACIÓN DE APLICABILIDAD (SoA)			
N°	**SECCIÓN**	**DESCRIPCIÓN**	**ESTADO ACTUAL**
CONTROLES DE SEGURIDAD			
1	5.1	Políticas de seguridad de información	Por implementar
2	5.2	Funciones y responsabilidades de seguridad de información	Por implementar
3	5.5	Contacto con las autoridades	Implementado
4	5.9	Inventario de información y otros activos asociados	Por implementar
5	5.12	Clasificación de la información	Por implementar
6	5.13	Etiquetado de la información	Por implementar
7	5.51	Control de acceso	Por implementar
8	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Por implementar
9	5.26	Respuesta a incidentes de seguridad de la información	Por implementar
10	5.27	Aprender de los incidentes de seguridad de la información	Por implementar
11	5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Por implementar
12	5.34	Privacidad y protección de la información de identificación personal (PII)	Por implementar
13	5.36	Cumplimiento de políticas, reglas y estándares para la seguridad de la información	Por implementar
CONTROLES DE PERSONAS			
14	6.1	Chequeo	Por implementar
15	6.2	Términos y condiciones de empleo	Implementado
16	6.3	Concienciación, educación y capacitación sobre seguridad de la información	Por implementar
17	6.6	Acuerdos de confidencialidad o no divulgación	Implementado
18	6.8	Informes de eventos de seguridad de la información	Por implementar
CONTROLES FÍSICOS			
19	7.1	Perímetros de seguridad física	Por implementar
20	7.2	Entrada física	Por implementar
21	7.3	Asegurar oficinas, habitaciones e instalaciones	Por implementar

DECLARACIÓN DE APLICABILIDAD (SoA)			
N°	**SECCIÓN**	**DESCRIPCIÓN**	**ESTADO ACTUAL**
22	7.4	Monitoreo de seguridad física	Por implementar
23	7.5	Protección contra amenazas físicas y ambientales	Por implementar
24	7.7	Escritorio claro y pantalla clara	Por implementar
CONTROLES TECNOLÓGICOS			
25	8.1	Dispositivos de punto final de usuario	Implementado
26	8.2	Derechos de acceso privilegiados	Por implementar
27	8.3	Restricción de acceso a la información	Por implementar
28	8.5	Autenticación segura	Por implementar
29	8.7	Protección contra malware	Por implementar
30	8.13	Copia de seguridad de la información	Por implementar
31	8.15	Registro	Por implementar
32	8.20	Seguridad de redes	Por implementar

Estos 32 controles seleccionados son los que se sugieren implementar en la Gobernación en base a la simplicidad de sus operaciones.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.3

PROPÓSITO Y ALCANCE

Las presentes políticas constituyen directrices para fomentar la triada de la seguridad: confidencialidad, integridad y disponibilidad de los activos de información de la Gobernación de Tungurahua, rigiéndose con lo establecido en la ISO 27001:2022. Además, se aplican a todas las áreas administrativas, funcionarios y toda persona que interactúa con la información de la entidad. Por lo tanto, la alta dirección de la Gobernación de Tungurahua realiza el compromiso de:

1. Implantar metas de seguridad de la información de manera clara para la protección de la información y la eficacia del SGSI
2. Cumplir con los requerimientos normativos de la seguridad de la información
3. Implementar mejoras para el SGSI con la ayuda de reuniones periódicas, auditorías y gestión de riesgos
4. Transmitir las presentes políticas a todo el personal y partes interesadas según corresponda.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.3 ROLES Y RESPONSABILIDADES

La Gobernación de Tungurahua se compromete a asegurar los activos bajo la responsabilidad con la ayuda de las políticas necesarias de acuerdo con la normativa y leyes aplicables.

Tanto la Gobernación como la Unidad TI y las unidades específicas deberán asignar un responsable para determinar, instaurar y monitorear las políticas de seguridad de información. Esta persona encargada deberá reportar acerca de incidentes a la comisión de auditorías para que junto con la alta dirección se provea de acciones correctivas.

La alta dirección aprueba y asegura la implantación de las presentes políticas y será quien proveerá de recursos para la seguridad de información.

Además, la Unidad TI será la encargada de implementar las políticas de seguridad, administrar incidentes y realizar las evaluaciones de riesgos, asimismo, ayudará con el monitoreo de controles de acceso físicos y digitales.

Por otro lado, los usuarios deberán cumplir con las políticas, se comprometerán a reportar cualquier incidente o detección sospechosa a la Unidad TI, por último, tendrán que asistir de manera obligatoria a las capacitaciones sobre la seguridad de información

POLÍTICAS GENERALES

- Las políticas muestran la normativa legal que instituye el Gobierno ecuatoriano para las entidades públicas
- Hay que asegurar todo procedimiento y tarea en relación con la seguridad de la información se encuentre alineada con leyes locales, regulaciones internacionales y requerimientos de la norma ISO 27001:2022
- Actualizar los documentos de las normas legales y procesos de acuerdo con los cambios de innovación y judiciales
- Utilizar técnicas de monitoreo y análisis para garantizar el cumplimiento continuo
- Alinearse con el Artículo 66, numeral 19 de la Constitución del Ecuador que asegura el derecho a la protección de datos individuales

Poner en práctica los requerimientos y postulados de la Ley Orgánica de Protección de Datos Personales para un mejor tratamiento de información de la ciudadanía.

- Incluir pruebas de impacto y asignación de roles para protección de datos en base a los fundamentos del Reglamento General a la Ley Orgánica de Protección de Datos Personales
- Incluir acciones estratégicas y administrativas de acuerdo con la Ley de Seguridad Pública y del Estado para asegurar la infraestructura confidencial

POLÍTICAS DE CONTROL DE ACCESO

- El control de acceso a los activos digitales de información es necesario contemplar para evitar cualquier tipo de amenaza:
- Cada usuario debe contar con un usuario y contraseña única para cada activo de información digital.
- Se restringe el uso compartido del usuario y contraseña.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.3

"Art.66.19 El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" (Constitución de la República del Ecuador, Art.66.19, 2021).

POLÍTICAS DE CONTROL DE ACCESO

La contraseña de cada usuario debe contener una estructura definida para una mayor robustez

- Caracteres especiales (*,@,- entre otros).
- Caracteres numéricos
- Mayúsculas
- Minúsculas
- Longitud mínima de 12 caractéres

El acceso a cualquier activo de información debe ser revisado trimestralmente por el personal de la Unidad TI o del responsable de cada unidad.

Implementación de autenticación en dos pasos para el acceso a la información más sensible.

Por otro lado, el control de acceso a zonas físicas es vital para un mejor manejo de la confidencialidad y confiabilidad:

Las zonas que contienen equipos tecnológicos sensibles como servidores, equipos de red, respaldos, entre otros, deberán ser restringidas con un sistema de videovigilancia y de control de acceso

El acceso a estas zonas deberá ser registrado en bitácoras y revisadas de manera periódica.

CLASIFICACIÓN DE INFORMACIÓN

Para mantener la confidencialidad, integridad y disponibilidad de información se deberá establecer un método de clasificación de información alineado a la Política de administración de activos.

Para mantener la confidencialidad, integridad y disponibilidad de información se deberá establecer un método de clasificación de información alineado a la Política de administración de activos.

PÚBLICA
Cualquier persona puede acceder a la información y no existe riesgo para los intereses de la Gobernación de Tungurahua

INTERNA
Información que puede acceder solo funcionarios de la Gobernación.

LIMITADA
La información únicamente puede ser manipulada por la unidad para evitar la utilización fraudulenta.

RESERVADA
Información que es conocida por el propietario y si se divulga, existe riesgo de perjuicios

CONFIDENCIAL
Información que es manipulado por un grupo reducido de funcionarios.

SECRETA
Información que si se comunica sin autorización afecta a los intereses de la institución y el valor de esta.

La información obtendrá su nivel de clasificación según la sensibilidad de esta.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.3

POLÍTICAS DE ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

Mantener actualizado el inventario de los activos de información al menos una vez al año.

Cada uno de los activos tienen un custodio, responsable de la gestión y protección.

De acuerdo a la clasificación de la información será almacenada en zona segura y con cifrado de datos.

Toda la información física deberá ser etiquetada y almacenada en zonas de acceso restringido.

POLÍTICAS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE INFORMACIÓN

Los respaldos de información se realizarán de acuerdo con el nivel de clasificación dado, tomando en cuenta que la información crítica se copiará semanalmente.

Los respaldos de información deberán ser cifrados y ser almacenados en zonas separadas

Para evitar la inoperatividad de la institución los respaldos se deberán realizar en horario no laboral.

Realizar pruebas cada tres meses para una restauración para garantizar la integridad y accesibilidad de las copias

POLÍTICAS CONTRA CIBERATAQUES

Cada uno de los activos de información deben contener con herramientas de seguridad: antivirus, cortafuegos y sistemas de detección y prevención de intrusos actualizados

Los funcionarios recibirán capacitaciones acerca de prevención contra de ciberataques como phishing, malware, DDoS, entre otros

Gestionar un monitoreo de redes para controlar los movimientos sospechosos en tiempo real.

Si ocurre un incidente de seguridad de información se deberá reportar de manera inmediata a la Unidad TI por medio de canales formales y oficiales (correo electrónico o Quipux).

POLÍTICAS DE GESTIÓN DE RIESGOS

Realizar identificación y evaluación de riesgos cada seis meses para conocer las amenazas y vulnerabilidades.

Cada riesgo deberá ser clasificado por el impacto y la probabilidad de su ocurrencia, acorde a la metodología MAGERIT.

Establecer un plan de mitigación de riesgos conforme al nivel de riesgo.

Gestionar documentación de evaluación de riesgos para la toma de decisiones por la alta dirección.

POLÍTICAS DE USO DE CORREO ELECTRÓNICO

La utilización de correo institucional únicamente se utilizará para fines organizacionales.

Monitoreo de uso de correo electrónico para detectar vulnerabilidades de seguridad de información.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.3

Se restringe el envió de información confidencial sin cifrado de datos.

Cada usuario deberá actualizar la contraseña del correo cada determinado tiempo (semestralmente).

POLÍTICAS DE CONTINUIDAD DE NEGOCIO

La Gobernación de Tungurahua deberá realizar un plan de continuidad para una mejor operatividad ante los incidentes.

Cada proceso crítico tendrá su plan de recuperación documentado.

Para la evaluación de efectividad de cada plan se realizará simulacros cada año.

El plan de continuidad contendrá comunicación con personas externas.

POLÍTICAS DE DOCUMENTACIÓN FÍSICA

Cada documento físico también deberá ser clasificado según su nivel de confidencialidad.

La información de nivel reservado, confidencial o secreta será almacenado en un archivador bajo llave con acceso restringido

Se registrará el acceso autorizado a los documentos en una bitácora para mayor control.

Los documentos no válidos o erróneos deberán ser destruidos por la técnica de trituración.

POLÍTICAS DE ESCRITORIO LIMPIO

Cada equipo tecnológico deberá ser bloqueado cuando el funcionario abandone su puesto, ya sea de manera automatizada con el bloqueo de pantalla o manualmente

El entorno de trabajo deberá estar ordenado y despejado de documentos al finalizar la jornada, sin papeles a la vista según la clasificación de la información.

POLÍTICAS DE AUDITORÍAS INTERNAS

Cada año se deberá realizar una auditoría interna para diagnosticar la efectividad y el cumplimiento de las políticas de seguridad de información.

Al realizar la auditoría se realizará un informe de resultados para presentar a la alta dirección y establecer medidas correctivas.

La auditoría incluirá control de accesos, copias de seguridad y el cumplimiento de las políticas.

CUMPLIMIENTO Y SANCIONES

Ante cualquier tipo de violación de la Política de Seguridad de la Información resulta en acciones disciplinarias correspondientes de acuerdo con lo que establezca la institución. Además, de que es responsabilidad de cada funcionario de la Gobernación transmitir al responsable asignado de la unidad afecta cualquier incidente o actividad sospechosa que afectará a la seguridad de información

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

REVISIÓN Y ACTUALIZACIÓN

Las presentes políticas serán revisadas una vez cada año para asegurar que se encuentren alineadas a las actualizaciones tecnológicas, normativas y operativas de la Gobernación de Tungurahua

La información será accesible para cada funcionario y externo, además, deberá ser comunicada dentro de la entidad.

4.4 ASIGNACIÓN DE FUNCIONES DENTRO DEL SGSI

ROL	FUNCIONES	COMPETENCIAS	ÁREA DE LA UNIDAD TI
Líder del SGSI	◆ Diseño de Plan Estratégico de Tecnologías de Información. ◆ Gestionar la instalación y conservación del SGSI. ◆ Delimitar y renovar las políticas de seguridad de la información. ◆ Monitorear la gestión de riesgos y auditorías. ◆ Mantener informada a la alta dirección acerca del funcionamiento del SGSI.	Conocimiento de la ISO 27001.	Director de Unidad TI
Auditor interno del SGSI	◆ Ejecutar auditorías del SGSI. ◆ Comprobar el cumplimiento de políticas y medidas. Determinar irregularidades y proponer acciones de ◆ corrección.	Auditoría de Tecnologías de Información Conocimiento de la ISO 27001	Director de Unidad TI
Consultor de Seguridad de Información	◆ Crear y controlar las medidas de seguridad. ◆ Administrar los riesgos de seguridad. ◆ Efectuar análisis de riesgos. ◆ Crear y formalizar las políticas de acceso.	Especialista en ciberseguridad	Área de seguridad y protección de datos
Coordinador de Protección de datos	◆ Asegurar la utilización de normas de resguardo datos. ◆ Monitorear el tratamiento de información sensible. ◆ Administrar la privacidad de la información personal.	Especialista en protección de datos	Área de seguridad y protección de datos
Coordinador de concientización y capacitación	◆ Crear plan de capacitación sobre protección de información. ◆ Incentivar a la utilización de medidas de seguridad. ◆ Analizar resultados de efectividad de las capacitaciones	Soporte y capacitación en áreas tecnológicas	Área de seguridad y protección de datos
Responsable de la documentación de SGSI	◆ Actualizar las políticas, procesos y SoA del SGSI. ◆ Gestionar los documentos del	Especialista en ciberseguridad	Director de Unidad TI

05 PLANIFICACIÓN

5.1 OBJETIVOS DE SEGURIDAD DE INFORMACIÓN

OBJETIVO	MÉTRICAS	RESPONSABLE
Asegurar la integridad de los activos de información y equipos tecnológicos para controlar el acceso físico y lógico.	Número de incidentes en relación con la clasificación de incidentes	Coordinador de seguridad de información
Prevenir distribución de ciberataques en los activos de información y dispositivos tecnológicos.	Número de ciberataques	Coordinador de seguridad de información
	Tiempo de respuesta frente a ciberataques	
Mejorar la protección de respaldos de información crítica.	Cantidad de pruebas exitosas de respaldo de información	Coordinador de seguridad de información y responsable de documentación

5.2 PLAN DE IDENTIFICACIÓN DE RIESGOS

DETERMINACIÓN DEL CONTEXTO

ENCARGADO	ALCANCE	DEFINIR ACTIVOS DE INFORMACIÓN
Dirección de la Unidad de TI	Analizar riesgos, identificar los sistemas, recursos de información y procedimientos a evaluar.	Clasificar los activos de información en pública, confidencial y sensible.

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

ENCARGADO	ALCANCE	DEFINIR ACTIVOS DE INFORMACIÓN
Coordinador de redes	Adquirir información de cuántos activos de información existen en la institución y sus características, realizar un inventario	Clasificar de acuerdo con la importancia

IDENTIFICACIÓN DE AMENAZAS		
ENCARGADO Consultor de seguridad de la información	**ALCANCE** Reconocer las amenazas que rompen la confidencialidad, disponibilidad e integridad.	**DEFINIR ACTIVOS DE INFORMACIÓN** Diagnosticar si existe sistemas desactualizados, falta de monitoreo de acceso, entre otros.

VALORACIÓN DE RIESGO		
ENCARGADO Responsable del SGSI	**ALCANCE** Establecer el impacto y la probabilidad de cada riesgo	**DEFINIR ACTIVOS DE INFORMACIÓN** Clasificar ente nivel medio bajo, bajo, medio, alto o crítico.

MITIGACIÓN DEL RIESGO		
ENCARGADO Responsable del SGSI	**ALCANCE** Definir las medidas de prevención o detención de riesgos.	**DEFINIR ACTIVOS DE INFORMACIÓN** Este plan debe incluir medidas para contrarrestar, plan de contingencia y los recursos a adquirir necesarios para prevención de riesgos.

MONITOREO DE PROTECCIÓN DE DATOS		
ENCARGADO Coordinador de protección de riesgos	**ALCANCE** Gestionar revisiones regulares para diagnosticar la efectividad de las medidas de mitigación de riesgos.	Ajustar el plan de tratamiento de riesgos.

5.3 IDENTIFICACIÓN DE RIESGOS

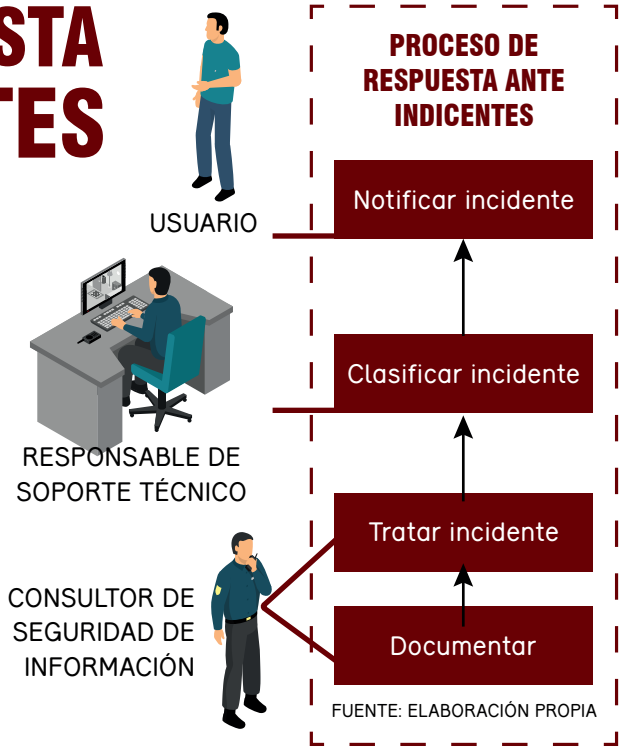
ACTIVO DE INFORMACIÓN	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO
SITIO WEB INSTITUCIONAL	◆ Desactualización de sistema. ◆ Falta de seguimiento periódico. ◆ Ajustes débiles de seguridad	Ataque Distribuido Denegación de Servicios (DDoS) e inyección SQL.	Acceso no controlado a la base de información.	◆ Inoperatividad de servicio. ◆ Mala imagen institucional. ◆ Desinformación a la ciudadanía
SISTEMAS DE COMUNICACIÓN ELECTRÓNICA	◆ No existe capacitación para los funcionarios. ◆ Falta de bloqueadores de spam. ◆ Políticas de seguridad de ineficaces.	Phishing y ataques de malware.	Hurto de contraseñas y/o usuarios.	◆ Fuga de información sensible. ◆ Trámites incongruentes

ACTIVO DE INFORMACIÓN	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO
DOCUMENTACIÓN EN PAPEL SENSIBLE	◆ No existe protección física para los archivos. ◆ Políticas de control de acceso ineficientes. ◆ No existe control de daño o destrucción de archivos.	Usuarios/intrusos sin acceso autorizado. Ingeniería social.	Propagación de información sin autorización	◆ Pérdida de datos sensibles. ◆ Alteración de información. ◆ Pérdida de documentos
REDES INTERNAS	◆ Claves compartidas o fáciles de adivinar. ◆ Inexistencia de cifrado de datos. ◆ No existe segmentos de red	Fallos electrónicos, intrusos o siniestros Ataques de malware	Acceso no autorizado a redes internas o zona física de red.	◆ Intrusión de datos críticos. ◆ Pérdida de equipos de red y de información.
DISPOSITIVOS ELECTRÓNICOS DE USUARIO	◆ Desactualización de software y hardware ◆ Inexistencia de antivirus actuales. ◆ Inexistencia de cifrado de almacenamientos de información crítica. ◆ Inventario desactualizado.	Malware y baiting Acceso no autorizado	Propagación de troyanos y virus Hurto de dispositivos electrónicos	◆ Robo de equipos. ◆ Pérdida de información. ◆ Afectación financiera.
RESPALDOS DE INFORMACIÓN	◆ Inexistencia de cifrado en respaldo de seguridad. ◆ Inexistencia de pruebas de recuperación. ◆ Almacenamiento en zonas expuestas.	Fallos electrónicos o catástrofes naturales. Ataque de malware	Daño de información de respaldos	◆ Pérdida de información. ◆ Mala imagen institucional.

5.4 PLAN DE RESPUESTA ANTE INCIDENTES

Para el plan de respuesta ante incidentes se deberá seguir el siguiente proceso:

1. El usuario deberá notificar acerca del incidente vía correo electrónico especificando detalladamente lo sucedido. **NOTA : para mejor entendimiento revisar el glosario ubicado en la página 35.**
2. La subunidad de soporte y capacitación de la Unidad TI tendrá la responsabilidad de clasificar el incidente como confidencial, divulgación de información; integridad, afectación a la confiabilidad de la información; disponibilidad, daño a los servicios de información; por último, incidentes de cumplimiento, sucesos que no cumplen con las regulaciones legales establecidas.



FUENTE: ELABORACIÓN PROPIA

5.4

3. Una vez clasificado el incidente se tratará los confidenciales en primer lugar, seguidos de los incidentes de integridad y disponibilidad, para concluir con lo de incumplimiento de leyes.
4. Después de solucionar el incidente el encargado de la gestión de estos, consultor de la seguridad de información, realizará un informe detallado para presentar a la dirección de la Unidad TI, este informe en el que se detalla la cantidad de incidentes reportados, en proceso de solución y solucionados. Además, del proceso de mejora que se utiliza para el mismo.

Por otro lado, un modelo de matriz para manejo de incidentes con las siguientes columnas:

FECHA DE INCIDENTE	Fecha en la que ocurrió el incidente.
CÓDIGO DE INCIDENTE	Número continuo para identificar el incidente.
CLASIFICACIÓN	Clasificar como confidencial, integridad, disponibilidad e incidentes de cumplimiento.
DESCRIPCIÓN	Detallar lo que ocurrió en el incidente.
IMPACTO	Nivel en que el incidente afecta a la institución (Bajo, medio, alto o crítico).
PRIORIDAD	Nivel en que el incidente requiere atención (Bajo, medio, alto o crítico).
ESTADO	Describir si el incidente se encuentra en proceso, resuelto o en espera.
FECHA DE RESOLUCIÓN	Fecha en la que se solucionó el incidente.
RESPONSABLE	Funcionario encargado de solventar el incidente.
ACCIÓN IMPLEMENTADA	Medida tomada para resolver el incidente.
CAUSA	Causa principal que ocasionó el incidente.
MEJORA	Acción preventiva que impedirá que vuelva a ocurrir el incidente.

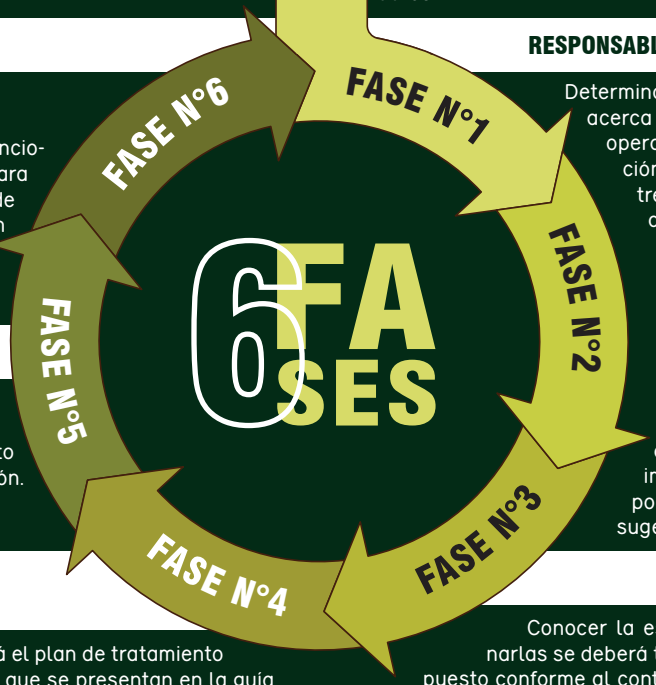
5.5 PLAN DE CONTINUIDAD DE NEGOCIO

PROCESO O CICLO

Para mantener la operatividad de la institución es necesario crear un plan de continuidad de negocio basado en el plan de tratamiento de riesgos, plan de respuesta ante incidentes y los objetivos tanto de la seguridad de la información como del SGSI.

La estructura para este documento se base en 6 fases:

CICLO



RESPONSABLE: COORDINADOR DE PROTECCIÓN DE DATOS

Se realiza la determinación del alcance, es decir, cualquier tipo de activo de información, sistema tecnológico, servicios u otros. Por lo general, el alcance son los activos de información que tienen mayor criticidad y que causarán mayor impacto en caso de pérdida de datos.

RESPONSABLE: FUNCIONARIOS DE LA UNIDAD TI

Determinar el análisis de la institución, conocer acerca de las circunstancias tecnológicas, operativas y de los recursos de la Gobernación. Esto se llevará a cabo por medio de tres tareas: reuniones, conforme al alcance seleccionado recolectar información de los usuarios finales para conocer las necesidades y así identificar el nivel de criticidad; analizar el impacto que generará sobre el negocio, conocer el tiempo de recuperación, recursos humanos y tecnológicos, tiempo máximo de caída, nivel mínimo de recuperación, dependencias afectadas y el nivel de impacto sobre la pérdida de información; por último, realizar un análisis de riesgo, sugerencia realizada en esta guía.

RESPONSABLE: DIRECTOR TI

Conocer la estrategia de continuidad para determinarlas se deberá tomar en cuenta la viabilidad y el presupuesto conforme al contexto del incidente.

RESPONSABLE: COORDINADOR DE PROTECCIÓN DE DATOS

Respuesta a la contingencia, se realizará el plan de tratamiento de riesgos e incidentes que se presentan en la guía

RESPONSABLE: SOPORTE TÉCNICO

Realización de pruebas, mantenimiento y revisión.

RESPONSABLE: DIRECTOR TI

Concienciación, dar a conocer a los funcionarios acerca del plan de continuidad para que contemple la importancia de respuesta ante incidentes y prevención de riesgos.

06 SOPORTE

Es importante conocer los recursos necesarios y básicos para la implementación del SGSI tanto tecnológicos como documentos. Por lo que se propone ciertas características y estructuras a continuación.

6.1 ASIGNACIÓN DE RECURSOS AL SGSI

RECURSO TECNOLÓGICO		CANTIDAD
Firewall de nueva generación (NGFW).	RECOMENDACIÓN: 4 puertos GB Ethernet con funciones de VPN y filtrado de contenido.	1
Sistema de detección y prevención de intrusos o IDS/IPS	RECOMENDACIÓN: capacidad de rastreo por lo menos 500 Mbps.	1
Servidor para almacenamiento de copias de seguridad.	RECOMENDACIÓN: 16 GB RAM como mínimo y con almacenamiento de 8 TB RAID 5/6.	1
Antivirus empresarial con protección en tiempo real contra ciberataques.	RECOMENDACIÓN: contar con por lo menos 130 dispositivos con actualización automática.	1

RECURSO TECNOLÓGICO		CANTIDAD
Sistema de Almacenamiento de Red para documentos digitales y copias de seguridad.	RECOMENDACIÓN: capacidad para 10 TB de almacenamiento y acceso remoto.	1
Armarios seguros con resistencia a siniestros, cerradura con contraseña y con capacidad para alrededor de 1000 documentos.		3
Administración de eventos e información de seguridad (SIEM).	RECOMENDACIÓN: monitoreo, gestión de logs, alertas en tiempo real, configuración de reportes.	1

6.2 CAPACITACIÓN Y CONCIENTIZACIÓN

ACTIVIDAD	CONTENIDO	DIRIGIDO A:	TIEMPO ESTIMADO	FRECUENCIA
INDUCCIÓN A LA SEGURIDAD DE INFORMACIÓN	◆ Explicar de que trata la seguridad de información. ◆ Conocer acerca de la triada de seguridad.	Funcionarios de la institución	2 HORAS	Anual
PRESENTACIÓN DE POLÍTICAS DE SEGURIDAD	Conocer de que trata las políticas y las responsabilidades de cada uno.	Funcionarios de la institución	2 HORAS	Anual
ADMINISTRACIÓN DE CONTRASEÑAS Y AUTENTICACIÓN	◆ Cómo crear una contraseña segura. ◆ Cómo utiliza el sistema de autenticación.	Funcionarios de la institución	1 HORA	Cada seis meses
IDENTIFICACIÓN DE PHISHING Y MALWARE	◆ Cómo saber que correo es fraudulento. ◆ Conocer sobre medidas para evitar el malware. ◆ Ejemplo de ciberataque.	Funcionarios de la institución	1 HORA	Cada tres meses
CONTROL DE ACCESO	◆ Conocer acerca de quién tiene acceso a instalaciones, documentos y sistemas. ◆ Conocer sobre protocolos de seguridad tanto física como lógica	Jefes de unidad	1 hora y 30 minutos	Anual
COPIAS DE SEGURIDAD DE INFORMACIÓN	◆ Conocer acerca de la importancia de los respaldos de seguridad. ◆ Conocer medidas para recuperación de datos.	Unidad de TI	2 HORAS	Cada seis meses
PLAN DE RESPUESTA ANTE INCIDENTES	◆ Conocer acerca del plan de respuesta ante incidentes. ◆ Estructura para reportes de incidentes.	Jefes de unidad	3 HORAS	Anual

ACTIVIDAD	CONTENIDO	DIRIGIDO A:	TIEMPO ESTIMADO	FRECUENCIA
USO SEGURO DE SISTEMAS DE COMUNICACIÓN ELECTRÓNICA	◆ Conocer sobre las políticas de comunicación. ◆ Conocer los riesgos y sus conce-cuencias de mal uso de sistema comunicación.	Funcionarios de la institución	1 hora y 30 minutos	Cada tres meses
RESGUARDO DE DOCUMENTACIÓN FÍSICA Y DIGITAL	◆ Conocer el proceso para manejo seguro de documentos. ◆ Medidas para digitalizar de manera segura la información.	Funcionarios de la institución	2 HORAS	Anual
CAMPAÑA DE INGENIERÍA SOCIAL	◆ Conocer acerca de las diferentes técnicas de ingenierías social. ◆ Fomentar la importancia de la seguridad de información. ◆ Reconocer los diferentes intentos de manipulación y engaño.	Funcionarios de la institución	1 HORA	Cada seis meses

6.3 DOCUMENTACIÓN DEL SGSI

DOCUMENTO	NÚMERO DE PÁGINA DONDE SE ENCUENTRA	LA INSTITUCIÓN DEBERÁ REALIZAR EN BASE A LA ESTRUCTURA DE LA PÁGINA
PROPUESTOS POR LAS CLÁUSULAS DE LA ISO 27001 : 2022		
Políticas de Seguridad de la Información	15 - 20	
Declaración de aplicabilidad (SoA)	13 - 15	
Evaluación y tratamiento de riesgos	21 - 23	
Plan de tratamiento de riesgos	29 - 30	
Políticas de control de acceso, gestión de riesgos y copias de seguridad de información.	16 - 18	
Documento de alcance de SGSI	12	
Objetivos de seguridad de información.	21	
Procedimiento de gestión de incidentes		23 - 24
Procedimiento de auditorías internas.		31 - 32
Documentación de no conformidades y acciones correctivas.		32 - 33

DOCUMENTO	NÚMERO DE PÁGINA DONDE SE ENCUENTRA	LA INSTITUCIÓN DEBERÁ REALIZAR EN BASE A LA ESTRUCTURA DE LA PÁGINA
PROPUESTOS POR EL ANEXO A DE LA ISO 27001 : 2022		
Inventario de activos		10
Clasificación de información		17
Plan de continuidad de negocio		24 - 25

07 OPERACIONES

En base a la planificación del SGSI, es posible realizar los controles técnicos y organizacionales que se presentan a lo largo de la guía, asimismo, se realiza la evaluación de riesgos para su tratamiento.

7.1 CONTROLES TÉCNICOS Y ORGANIZACIONALES

TIPO DE CONTROL DE SEGURIDAD	CONTROL DE SEGURIDAD	DESCRIPCIÓN
CONTROLES ORGANIZACIONALES	Políticas de seguridad de información	◆ Las políticas deberán administrar la información según la clasificación: confidencial, pública y sensible. ◆ Se deberá informar al personal acerca de la utilidad fundamental de la seguridad de la información. ◆ Indicar los procesos necesarios para la división y buen manejo de información.
	Políticas de control de acceso	◆ Las políticas se clasificarán en control de acceso físico para servidores, documentos críticos, equipos tecnológicos con ayuda de credenciales o sistemas de reconocimiento biométrico. ◆ Utilización de autenticación en dos pasos.
	Plan de auditorías internas	◆ Las auditorías ayudarán a la estructuración de políticas de seguridad de información. ◆ Ayudaran a la generación de matrices de riesgos. ◆ Ayudaran a generar documentación sobre las falencias e implementar acciones correctivas.
	Plan de gestión de riesgos	Se logra identificar mediante MAGERIT los riesgos e incluir medidas para mitigarlos.
	Plan de capacitación de políticas.	◆ Crear charlas, cursos y documentos interactivos para formar al personal acerca de la seguridad de la información. ◆ Realizar simulacros de amenazas para mejorar el nivel de respuesta

TIPO DE CONTROL DE SEGURIDAD	CONTROL DE SEGURIDAD	DESCRIPCIÓN
CONTROLES TÉCNICOS	Políticas de proyección contra ataques cibernéticos y seguimiento de redes	Debe contener el plan de respuesta ante incidentes y ante riesgos. Instaurar un sistema de monitoreo para conocer el tráfico extraño.
	Políticas de seguridad de comunicaciones	◆ Instaurar cifrado extremo a extremo. ◆ Registrar el tráfico de red para prevención de acceso no autorizado.
	Sistema de detección y prevención de intrusos	◆ Los sistemas ayudarán a rastrear actividad sospechosa y bloquear las amenazas. ◆ Analizar las actividades sospechosas para saber los patrones.
	Respaldo de seguridad	◆ Realizar respaldos de seguridad programados de manera automática. ◆ Almacenar de manera segura en la nube o en zonas seguras.
	Plan de capacitación de políticas.	◆ El plan incluye realizar simulacros para diagnosticar el funcionamiento de las medidas correctivas. ◆ El plan comprende una estrategia que gestiona la respuesta y las medidas técnicas para mitigar incidentes, renovar operaciones y asegurar la infraestructura organizativa.
CONTROL ORGANIZACIONAL / TÉCNICO	Plan de respuesta de incidentes	◆ El plan incluye realizar simulacros para diagnosticar el funcionamiento de las medidas correctivas. ◆ El plan comprende una estrategia que gestiona la respuesta y las medidas técnicas para mitigar incidentes, renovar operaciones y asegurar la infraestructura organizativa.

7.2 MITIGACIÓN DE RIESGOS

El nivel de riesgo es el producto de la probabilidad por el impacto. Tomando en cuenta que los valores son del 1 al 5 siendo 1 el más bajo y 5 el nivel crítico.

RIESGO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	SOLUCIÓN PROPUESTA	RESPONSABLE	PLAZO PARA LA IMPLEMENTACIÓN
Acceso no controlado a la base de información.	4	5	20	Instauración de firewall, realización de auditorías regulares y rastreo continuo.	Consultor de seguridad de información	4 MESES

7.2

RIESGO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	SOLUCIÓN PROPUESTA	RESPONSABLE	PLAZO PARA LA IMPLEMENTACIÓN
Hurto de contraseñas y/o usuarios	3	4	12	Instauración de autenticación en dos pasos, creación de políticas para creación de claves robustas y cambios continuos, concientización de seguridad de contraseñas. Creación de respaldo de información periódicos con almacenamiento seguro y creación de políticas de respaldo diario con pruebas de efectividad.	Consultor de seguridad de información	5 MESES
Programación de información sin autorización	3	5	15	Crear e instaurar políticas de escritorio vacío, archivadores cerrados y destrucción segura. Instauración de bloqueadores de spam.	Consultor de seguridad de información y auditor interno	3 MESES
Acceso no autorizado a redes internas o zona física de red	4	4	20	Creación de controles de acceso físico y lógico, sistemas de detección/prevención de intrusos y rastreo de accesos para auditorías internas.	Coordinador de redes y consultor de seguridad de información	4 MESES
Propagación de troyanos y virus	4	5	20	Instaurar virus actualizado en todos los equipos tecnológicos, crear un plan de concientización y formar políticas de navegación segura.	Consultor de seguridad de información y coordinador de protección de datos.	3 MESES
Hurto de dispositivos electrónicos	3	3	9	Crear un inventario actualizado. Acceso controlado a la institución.	Consultor de seguridad de información y coordinador de protección de datos.	2 MESES

7.2

RIESGO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	SOLUCIÓN PROPUESTA	RESPONSABLE	PLAZO PARA LA IMPLEMENTACIÓN
Daño de información	3	5	15	Creación de zona segura para almacenamiento de copias de seguridad o en la nube. Instauración de plan de continuidad operativo.	Consultor de seguridad de información	6 MESES

08 EVALUACIÓN DE RENDIMIENTO

Al momento en que la Gobernación implemente el SGSI se debe medir la efectividad por medio de fórmulas sugeridas y establecer un plan de auditorías internas para su mejora.

8.1 MÉTRICAS PARA EFECTIVIDAD

MÉTRICA	FÓRMULA
Porcentaje de incidentes de acceso no autorizado, contraseñas y/o usuarios inseguros.	$\frac{\text{Número de incidentes de acceso no autorizado}}{\text{Número total de usuarios activos}} \times 100$
Promedio de respuesta ante ciberataques (malware, phishing, entre otros.)	$\frac{\text{Tiempo de resolución ante ciberataques}}{\text{Número de ciberataques detectados}}$
Porcentaje de pruebas positivas de respaldos de información.	$\frac{\text{Cantidad de pruebas positivas de Respaldo de información}}{\text{Número total de usuarios activos}} \times 100$

8.2 PLAN DE AUDITORÍAS INTERNAS

Para la realización de auditorías internas es necesario definir el objetivo de la auditoría, analizar la efectividad de la implementación de los controles de seguridad de la información alineados a la ISO 27001:2022 para la obtención de procesos alineados con las necesidades de la institución y de la Unidad TI. Otro punto es la realización de tipos de auditorías: de diagnóstico, en las cuales se determinan las brechas y conocer el estado del SGSI en comparación a los requerimientos de la norma; de seguimiento, se constata progresos y desempeño de los controles implementados;

Por último, de evaluación final , se conoce si el SGSI es apto para una posible certificación. Además, la frecuencia con la que se sugiere realizar es una vez al completar la implementación del SGSI y después una anualmente con revisiones cada seis meses para zonas de alto impacto como respaldo de seguridad de información y control de acceso. Esta frecuencia también dependerá de las políticas de seguridad de información.

Por otro lado, se utilizará la técnica de análisis GAP para comparar los requisitos de la norma contra lo que tiene la unidad mediante técnicas como entrevistas, observación directa y análisis de documentos, con la ayuda de una lista de chequeo basada en el anexo A de la norma ISO 27001:2022.

Además, se sugiere utilizar el modelo ADKAR que se utiliza para identificar el cambio por medio de la conciencia, deseo de apoyar, conocimiento y capacidad. Por último, se presentará, informes que detallen los resultados de las observaciones y acciones correctivas. Es importante destacar que en el plan de auditorías se determinan los indicadores de desempeño o KPIs, los cuales pueden ser porcentaje de controles instaurados alineado a la norma, cantidad de no conformidades determinadas y resueltas, por último, porcentaje de madurez del SGSI.

09 MEJORA

Al implementar el plan de auditorías internas se debe realizar evaluación de no conformidades y sus posibles soluciones de acuerdo a una estructura.

9.1 DOCUMENTACIÓN DE LAS NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Una vez que el plan de auditorías internas es aprobado por la máxima autoridad de la institución, con el personal de la Unidad TI se debe ejecutar este proceso, en donde se identificaran las no conformidades, desviación de los requerimientos y procesos alineados a la ISO 27001; los cuales se deben clasificar según la gravedad. Se realiza la respectiva documentación para implementar las acciones correctivas para cada una de las no conformidades.

Identificar y clasificar la no conformidad con la ayuda del diagrama Ishikawa para poder identificar la causa principal de estas. Este diagrama tiene forma de un esqueleto de pez, el cual tiene seis ramificaciones que representan las 6 M (material, mano de obra, método de trabajo, maquinaria, medio ambiente y mantenimiento), las cuales son las posibles causas; y en la cabeza se indica la no conformidad, es decir el problema. Después de identificar las causas se definen las acciones correctivas para prevenir la reincidencia del problema y afrontar desde la raíz.

Todo este proceso debe ser documentado y aprobado por los responsables, en este caso la Unidad TI y el Despacho de la Gobernación. Posteriormente, se implementarán las medidas propuestas y el consultor de auditoría interna tendrá la función de supervisar su ejecución dentro del plazo establecido.

Si existe el caso de que las acciones correctivas no brinden resultados positivos, el auditor emitirá un nuevo informe para planificar nuevas soluciones y una vez que se verifiquen como efectivas, las no conformidades finalizan el proceso y se archivan.

Además, se indica un posible esquema de la matriz en donde se incluirán las no conformidades y sus acciones correctivas.

FECHA	Fecha en la que se identificó la no conformidad.
N°	Número consecutivo e identificativo para la conformidad
PUNTO DE NORMA AFECTADO	Indicar que parte de las políticas de seguridad de información fue afectada.
DESCRIPCIÓN	Detallar la no conformidad
ESTADO DE LA NC	Momento de la no conformidad (cerrada, abierta o en proceso)
UNIDAD	Unidad en la que se dio la no conformidad
ACCIÓN CORRECTIVA	Detallar la acción que se implementa
RESPONSABLE	Encargado de sobrellevar la no conformidad
ESTADO DE LA AC	Indicar si la acción correctiva se implementó (implementada, en proceso, no implementada)

10 GLOSARIO

TRIADA DE LA INFORMACIÓN

Es un conjunto de tres pilares que apoyan a la ciberseguridad, estos son confidencialidad, integridad y disponibilidad.

CONFIDENCIALIDAD

Brindar un control de acceso autorizado a la información.

INTEGRIDAD

Mantener la información accesible en el momento en que se requiera.

DISPONIBILIDAD

mantener la información accesible en el momento en que se requiera.

AMENAZA

Acción que causa daño al sistema o a la información.

CONTROLES DE ACCESO

Prevenciones que tienen por objetivo manejar los permisos de acceso a la información y a los sistemas para el cumplimiento del principio de la confidencialidad e integridad.

ACTIVO DE INFORMACIÓN

Es un recurso que contiene información valiosa para la entidad y que si sufre algún daño afecta de manera negativa a la operatividad de esta.

MAGERIT

Es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), que permite identificar, diagnosticar y tratar riesgos relacionados con sistemas de información.

VULNERABILIDAD

Es una debilidad que tiene el sistema y que es posible que se explote por un atacante.

RIESGO

Es aquella posibilidad de que una amenaza se materialice y el impacto que ocasionaría en la empresa.

INCIDENTE

Es el hecho que afecta a la información y a los sistemas.

MALWARE

se refiere a un software malicioso que está diseñado para causar daño a un dispositivo tecnológico.

PHISHING

El ciberdelincuente envía por medio de correo electrónico, redes sociales o mensajería instantánea avisos que suplantan a una entidad oficial.

DDoS

Ataque Distribuido Denegación de Servicio o DDoS, el ciberdelincuente ataque desde otros equipos al servidor web en un mismo tiempo y este deja de funcionar, por lo que podría robar los datos.

INYECCIÓN SQL

Se inserta líneas de código en formato SQL maliciosas en la base de datos de las aplicaciones web, así se tiene acceso a la información que contiene la base de datos.

USUARIOS INTRUSOS

Persona que utiliza el sistema y es la principal amenaza, pues no tiene buenas prácticas de ciberseguridad y se convierte en víctima fácil. Incluso, en ocasiones es quien roba la información de manera intencional.

INGENIERÍA SOCIAL

El atacante es quien se gana la confianza de la víctima y obtiene información confidencial.

FALLO ELECTRÓNICO

Sistemas pueden ser afectados por fallos de energía eléctrica o por problemas que presentan los equipos.

SINIESTRO

Acción de perder información o recursos sensibles por negligencia del personal institucional. Los siniestros más habituales son los incendios o inundaciones provocadas.

CATÁSTROFE NATURAL

Opuestos a los siniestros, pues el humano no tiene control sobre estos, ya que se dan por causas naturales.

BAITING VIRUS

Esta técnica es también conocida como "cebo", en donde el atacante infecta el equipo, por medio de USB o anuncios publicitarios, así se obtiene información personal del usuario.

Tiene el objetivo de propagarse por varios dispositivos, pues se copian a sí mismos. Llega a eliminar archivos y daña datos sensibles.

TROYANO

Actúa como un software oficial y controla el dispositivo para robar datos e infectar con un programa malicioso.

AUTOR
CAMILA AMANCHA

DIRECTOR
ING. MG. TERESA FREIRE

DISEÑO
LIC. MARISSA ALBÁN