ESCUELA DE INGENIERÍAS

Tema:

ANÁLISIS DEL ALCANCE Y CAMPO DE APLICACIÓN DE LAS NORMAS ISO/IEC27001:2022 EN EL GAD PÍLLARO

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

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

Autora:

Nadia Jamileth Cuyago Moreta

Directora:

Mg. Liliana del Rocío Mena Hernández

Ambato – Ecuador

Agosto 2025

DECLARACIÓN DE AUTENTICIDAD Y RESONSABILIDAD

Yo: **NADIA JAMILETH CUYAGO MORETA**, con cédula de ciudadanía **1804527701**, autora del trabajo de integración curricular titulado: "ANÁLISIS DEL ALCANCE Y CAMPO DE APLICACIÓN DE LAS NORMAS ISO/IEC27001:2022 EN EL GAD PÍLLARO", 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, agosto 2025

Nadia Jamileth Cuyago Moreta

CC. 1804527701

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

ANÁLISIS DEL ALCANCE Y CAMPO DE APLICACIÓN DE LAS NORMAS ISO/IEC27001:2022 EN EL GAD PÍLLARO

Línea de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor:

Nadia Jamileth Cuyago Moreta

Liliana del Rocío Mena Hernández, Ing. Mg. f._____
CC. 1802729077
CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____
CALIFICADOR

Galo Mauricio López Sevilla, 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
SECRETARIA GENERAL
PROCURADURÍA

Ambato – Ecuador

Agosto 2025

DEDICATORIA

Este trabajo está dedicado especialmente a mis padres, Klever y Liliana, quienes han sido el pilar fundamental a lo largo de mi vida. Gracias por su amor incondicional, por su apoyo constante, y por creer en mi incluso en los momentos más difíciles. Cada uno de sus sacrificios ha sido una fuente de inspiración en esta linda etapa de mi formación.

A ustedes les debo todo mi ser y todo lo que he logrado, gracias por ser mi guía, e inculcarme valores y principios, por incentivarme a dar siempre lo mejor de mí y por acompañarme en cada paso que he dado aun siendo el más mínimo.

Este logro no es solo mío, también es suyo.

AGRADECIMIENTO

Agradezco a Dios y la Virgen Santísima del Carmen por guiar mi caminar, por darme fortaleza en cada instante de adversidad y por concederme lograr esta meta tan importante en mi vida.

Quiero agradecer a toda mi familia por su constante apoyo, especialmente a mi padre, Klever Cuyago, por ser un ejemplo de perseverancia, esfuerzo y valentía, por motivarme a luchar siempre por mis sueños y nunca rendirme. A mi madre, Liliana Moreta le agradezco por su amor y dedicación incondicional. Ella ha sido mi refugio seguro, su apoyo constante me ha motivado a seguir adelante.

A mi hermano Robinson, gracias por siempre estar presente, por tu compañía, confianza y tu apoyo incondicional en todo este camino. A Karlita gracias por siempre estar presente, por tu compañía tu confianza, palabras de aliento y sobre todo tu apoyo incondicional en mi vida que valoro profundamente.

A Malu, gracias infinitas por ser como una hermana para mí, por tu cariño, tus consejos y por tu constante presencia en cada etapa de este proceso, tu apoyo me ha sostenido y tu amistad me ha dado fuerzas para continuar

A mis amigos de la universidad, el mejor grupo que la vida me pudo regalar. Gracias por cada experiencia vivida, por las risas, los aprendizajes y el buen compañerismo que nos ha unido. Me llevo conmigo lo mejor de cada uno. De manera especial quiero agradecer a Kim, Mela, Nico, Abraham, Raimi y Jonathan por dejar cada una de sus huellas imborrables en mi corazón.

Al departamento de Tecnologías de la Información de la PUCESA, mi más sincero agradecimiento por compartir sus conocimientos y depositar su confianza en mí. Su apoyo ha sido esencial para mi crecimiento personal y profesional.

Agradezco a mi tutora, Ing. Liliana Mena por su valioso apoyo y por ayudarme a enfrentar los desafíos que aparecieron durante esta ardua tarea y por ser una excelente docente cuyo compromiso fue fundamental en este proceso.

RESUMEN

En la investigación se analiza el alcance y campo de aplicación de la Norma ISO/IEC: 27001:2022 en el GAD de Píllaro, para la correcta identificación y seguridad de la información crítica de la institución, por la creciente necesidad de responder a los problemas relacionados a la seguridad informática en la institución pública, misma que maneja datos sensibles; por lo que es de vital importancia proteger la información de posibles vulnerabilidades del entorno digital actual dentro de la municipalidad. La investigación es necesaria, busca identificar los aspectos de la seguridad de los datos, minimización de riesgos de la información y consecuentemente permitir el cumplimiento normativo.

Se aplica la metodología en base al ciclo PDCA (*Plan-Do-Check-Act*) también conocido como ciclo de Deming, se inicia a partir de una revisión teórica de los SGSI (Sistemas de Gestión de Seguridad de la Información), seguido de un diagnóstico de la situación actual de la seguridad tecnológica en el GAD de Píllaro y el diseño de un mapa de procesos que delimite el alcance del SGSI. Como resultado se obtiene una guía que sirve como referencia para la gestión de la seguridad de la información en la institución.

Palabras clave: ciberseguridad, sgsi, iso/iec: 27001, protección de datos, gad Píllaro

ABSTRACT

The study analyzes the scope and field of application of the ISO/IEC 27001:2022 standard in the Gad Municipality of Píllaro to correctly identify and secure the institution's critical information. This arises from the growing need to address cybersecurity-related issues in the public institution, which handles sensitive data. Therefore, it is vital to protect information from potential vulnerabilities in the current digital environment within the municipality. This research is necessary as it seeks to identify key aspects of data security, minimize information risk, and ultimately ensure regulatory compliance.

The methodology is based on the PDCA (Plan-Do-Check-Act) cycle, also known as the Deming Cycle. It begins with a theoretical review of ISMS (Information Security Management Systems), followed by an assessment of the current state of technological security in GAD Municipality of Píllaro and the design of a process map to define the scope of the ISMS. The result is a guide that serves as a reference for managing information security within the institution.

Keywords*: cybersecurity, isms. iso/iec 27001, data protection, gad Píllaro*

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

En el ámbito **internacional** se destacan los siguientes trabajos:

En la investigación de Ramos, Cahuaya y Llanqui, (2023), la seguridad de la información es fundamental , se refiere a un conjunto de acciones preventivas y reactivas tanto de las entidades como sistemas tecnológicos que buscan proteger la información con el objetivo de preservar su privacidad, disponibilidad e integridad de datos, además, promueve la implementación de buenas prácticas de seguridad en los procesos internos y externos de las entidades, garantiza que los activos de información estén protegidos. Se concuerda que la seguridad de la información no es solo un requisito técnico, sino un componente crítico de la gestión organizacional que debe ser abordado de manera integral y constante.

Por el contrario, Nieves (2017), señala que los datos y procesos que realizan las empresas y organizaciones están expuestos a varios peligros que pueden afectar su confidencialidad, integridad y acceso a los datos, estos peligros no solo afectan la continuidad de las operaciones, sino que también pueden causar pérdidas importantes, como económicas, legales y de reputación, por esta razón, es importante adoptar un enfoque completo en la gestión de la seguridad de la información, que incluya la evaluación de peligros, el desarrollo de políticas de seguridad, la formación del personal, la aplicación de tecnologías avanzadas, la vigilancia constante y un plan de respuesta a incidentes, permitiendo así identificar, evaluar y reducir proactivamente estos peligros y reforzar la resistencia de la organización ante posibles amenazas. Su fortaleza radica en comunicar con claridad la importancia de la seguridad de la información como un pilar estratégico para las empresas, destaca tanto los riesgos asociados como los beneficios de una gestión eficiente.

En cambio, Risco Villarreal (2021), se enfoca en las variables y la aplicación de la metodología, detalla como realizo la selección de la población y muestra para el estudio, así como los pasos que se siguieron, aparte, se nombran las formas de mirar los datos y se considera la moral ligada al estudio, lo que ayuda a asegurar la confidencialidad y el no dar los nombres de los que participan, y también a cuidar la información. Al final, el estudio enseña una buena unión entre lo técnico y lo moral, lo

que es vital para sacar resultados seguros y que tengan valor para todos.

Por otra parte, en el ámbito **nacional** se destaca lo siguiente:

Según Ramos, Cahuaya y Llanqui, (2023) a nivel nacional, se subraya que la seguridad de la información es crucial para la integridad de cualquier organización, ya sea una empresa, entidad o institución, esto se debe a que protege datos importantes de posibles amenazas; la norma ISO 27001, que es una norma internacional muy reconocida, se divide en varias áreas que abordan aspectos clave de la gestión de la seguridad de la información, misma que incluye políticas de seguridad que describe pautas generales para manejar la seguridad; gestión de actividades, permite aclarar y garantizar la protección de los recursos preciosos de la organización; el control de acceso que rige quién puede ver la información que se clasifica de manera similar. La norma ISO 27001 se compone de varias partes esenciales que garantizan una buena gestión de la seguridad de la información, misma que es importante tratar la seguridad desde diferentes perspectivas, como las políticas de la organización, el manejo de recursos humanos y la seguridad física.

Según Angulo Chica (2024) adoptar la ISO 27001 facilita la implementación de un sistema de gestión de riesgos, dando así los medios claves para la protección de activos, la cual no solo ayuda a disminuir los riesgos, sino que también da confianza a clientes y socios comerciales, dando una mejor imagen corporativa en un mundo donde la tecnología avanza y hay peligros todo el tiempo, tener sistemas nuevos y alineados con estándares internacionales es muy importante para que la información esté segura y la empresa siga funcionando. Se concluye que se puede afirmar que implementar esta medida representa una decisión estratégica clave para las organizaciones, porque no solo garantiza la seguridad de sus recursos más valiosos a través de una administración de riesgos completa, sino que también consolida la confianza de los usuarios y colaboradores, lo cual robustece de manera notable la imagen de la compañía.

En la investigación de Flores Urgilés, Flores Urgilés, Carrillo Zenteno y Andrade Cárdenas (2023) se destaca que, a través de una recolección de datos de tipo cuantitativo, la norma ISO establece un marco fundamental para implementar un sistema de gestión de la seguridad de la información (SGSI) en las organizaciones,

esto permite de manera objetiva recolectar y examinar los datos, facilitando así la evaluación del cumplimiento de las políticas de seguridad. Se puede citar a la ISO 27001, la cual proporciona un enfoque bien organizado para gestionar y optimizar la seguridad de la información; esta norma no solo identifica los riesgos, sino que también considera las vulnerabilidades que pueden presentarse, por otro lado, la norma ISO 27002 ofrece recomendaciones sobre cómo maximizar la seguridad, esto le ayuda a las empresas en la implementación y revisión de si las medidas de seguridad son adecuadas para sus objetivos. Asimismo, el método utilizado posibilita verificar de manera clara si se están cumpliendo y respetando las normas de seguridad, lo que motiva e impulsa a las empresas a aplicar buenas prácticas y a garantizar que la información se encuentre siempre protegida.

Situación problemática

En el GAD Municipal de Píllaro, la protección de la información se ha vuelto en un desafío significativo, por lo que se gestionan los datos de manera constante, mismos que son delicados respecto a los ciudadanos, procedimientos administrativos y servicios públicos. Para abordar este desafío, es esencial identificar los riesgos y garantizar una protección adecuada de la información.

El problema científico se centra en la necesidad de analizar cómo se implementan las normas ISO/IEC 27001:2022 en el ámbito del GAD Píllaro, con la finalidad de establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que facilite identificar y proteger los datos y la información sensible de manera efectiva. Este análisis resulta esencial para garantizar que las medidas adoptadas aborden todas las vulnerabilidades presentes y se adapten a las particularidades operativas de la institución, lo cual, a su vez mejorará la seguridad de la información y asegurará el cumplimiento de las normativas internacionales.

Preguntas científicas

1. ¿Cuáles son los principales referentes teóricos que relacionan la seguridad de la información con las normas ISO/IEC 27001:2022?
2. ¿Cuáles son las metodologías utilizadas para la recolección de datos en el

análisis del alcance de la aplicación de las normas ISO/IEC 27001:2022?

3. ¿Cuáles son los puntos clave del análisis del alcance de las normas ISO/IEC 27001:2022?
4. ¿Cómo se puede determinar la información a proteger en base a las normas ISO/IEC 27001:2022?

Objetivo general

Analizar el alcance y campo de aplicación de las normas ISO/IEC 27001:2022 en el GAD Píllaro que permita la identificación de la información a proteger.

Objetivos específicos

- Fundamentar teóricamente los SGSI (Sistemas de Gestión de Seguridad de la Información) y su relación con las normas ISO/IEC mencionadas.
- Diagnosticar la situación actual de la seguridad tecnológica de los aspectos a considerar en base a la norma ISO/IEC27001:2022 y Seleccionar la metodología.
- Recopilar datos claves del análisis para determinar el alcance de la aplicación de la norma ISO/IEC27001:2022.
- Desarrollar una guía del alcance y diseño de un mapa de procesos del alcance del SGSI para un control en los flujos de información.

Modelo de la investigación

El ciclo PDCA, conocido también como Ciclo de Deming, es una metodología administrativa cuyo objetivo es la mejora continua de los procesos, la metodología PDCA es un modelo muy utilizado en la gestión de la seguridad de la información, como lo establece las normas ISO/IEC 27001:2022, además, este modelo es altamente estructurado y fiable para la identificación de riesgos, el diseño e implementación de controles adecuados y la evaluación continua del efecto de las medidas adoptadas y poseer así una mejora continua, y por lo tanto, la protección de la información.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Ciberseguridad de la información

La ciberseguridad conocida también como seguridad informática, es el área de la ciencia en computación encargada en el desarrollo e implementación de mecanismos de protección a la información digital y sistemas de acceso no autorizados, en esencial busca garantizar la confiabilidad, integridad y disponibilidad de la información.

La historia de la ciberseguridad de la información se ha constituido como un fiel retrato de la evolución de la informática e internet, dos campos que han modificado el manejo de la información y las conexiones de las personas y de las organizaciones a nivel internacional, en sus inicios, durante las décadas de 1950 y 1960, las computadoras eran enormes y costosas, limitadas a círculos gubernamentales o académicos, en ese entonces, la seguridad no era una prioridad, las redes no existían tal como las conocemos hoy, las instituciones gestionaban información restringida en medios físicos como tarjetas perforadas o cintas magnéticas, lo que hacía que las amenazas a la seguridad fueran bastante mínimas, aunque también limitaba la conectividad entre las máquinas. Esta evolución resalta la necesidad de adaptar continuamente las estrategias de seguridad a los avances tecnológicos, garantizando así la protección de la información en un mundo cada vez más interconectado (Casado Robledo, 2020).

Según la investigación de Casado Robledo (2020), el surgimiento de la conectividad de redes en los años 1970 y 1980, junto con la expansión de Internet en el transcurso de los años 1990, trajo consigo una serie de nuevas amenazas informáticas, los primeros virus y el mal uso de los sistemas informáticos crearon en las organizaciones la necesidad de pensar en la protección de los datos y de la infraestructura digital, es decir, durante la existencia de este escenario en el cual emergen las primeras herramientas de seguridad como antivirus, cortafuegos (*firewalls*) y sistemas de detección de intrusiones, con el avance de las tecnologías, la evolución del cibercriminal también obliga a la creación de leyes y normativas para regular y sancionar los delitos informáticos, las últimas dos décadas han mostrado cómo la continua expansión del comercio electrónico, del Internet de las Cosas (IoT), de las redes sociales y otros avances, han contribuido tanto a ampliar las posibilidades como

a aumentar los peligros, lo que ha obligado a las empresas y gobiernos a reforzar sus sistemas.

Al pasar los años, la ciberseguridad se ha convertido en una disciplina muy compleja, que abarca no sólo las herramientas técnicas, sino también marcos normativos, sistemas de gestión de riesgos y capacitación prolongada, con objeto de hacer frente a nuevas amenazas emergentes como, por ejemplo: los ataques avanzados de día cero, el *ransomware* y las violaciones de datos masivas (Casado Robledo, 2020). La creación de herramientas de seguridad y leyes para regular los delitos informáticos ha sido indispensable, , la ciberseguridad es una disciplina compleja que integra tecnologías, marcos normativos y gestión de riesgos, para enfrentar las amenazas emergentes y los ataques avanzados.

En la investigación de Urcuqui, García, Osorio y Navarro (2018), la ciberseguridad se define como la práctica de defender los dispositivos, redes, programas informáticos, sistemas esenciales y datos frente a potenciales amenazas digitales, las entidades tienen el deber de proteger la información para preservar la confianza del cliente y acatar las regulaciones, emplean estrategias y recursos de ciberseguridad para salvaguardar la información sensible del acceso no permitido, además de prevenir interrupciones en las operaciones de la empresa debido a una actividad de red no planificada. Las entidades aplican la ciberseguridad al mejorar la protección digital entre los individuos, los procedimientos y las tecnologías.

Tal como lo mencionan Adedoyin y Christiansen (2023), la ciberseguridad también es uno de los desafíos en el mundo actual, debido a su complejidad y aspectos políticos, así como la tecnología; su objetivo principal es garantizar la confiabilidad, integridad de los datos y privacidad en todo el sistema empresarial frente a los ataques cibernéticos globales escalados. Las operaciones de ciberseguridad son aptas para los sistemas de las empresas, analizan los riesgos de la actualidad a los sistemas modernos desde el punto de vista de una empresa; se analizan los riesgos del momento, se ponen en marcha las medidas operativas a nivel corporativo y a nivel sistemático para mantener la confianza, asegurar la integridad, garantizar la confidencialidad de la información y proteger la honestidad de los datos, sobre todo en un mundo digital vulnerable.

En la actualidad, la ciberseguridad se ha vuelto crucial para la protección de información y garantizar el buen funcionamiento de los gobiernos y organizaciones, por lo que es importante implementar medidas de seguridad eficientes debido al aumento de amenazas cibernéticas, tales como el robo de identidad, el *phishing* y los ataques de *ransomware*; la ciberseguridad permite la preservación completa de la integridad de toda la información, asegurando que la totalidad de los datos permanezca indestructible ante cualquier agente malicioso, una sólida seguridad impulsa notablemente la adopción de nuevas tecnologías digitales. Muchas iniciativas de concienciación y educación en ciberseguridad enseñan a los usuarios a identificar y disminuir riesgos, promoviendo así un uso responsable de internet. Al implementar medidas de seguridad efectivas frente a las amenazas cibernéticas se fomenta la confianza en las tecnologías digitales y promueve un uso responsable de internet (Tapia, Ruiz, & Vega, 2021).

Según, Bala, Costales, Yñota, Jamis y Ramirez (2022) la ciberseguridad de la información es fundamental para las operaciones comerciales, , los ciberataques son muy frecuentes y provocan importantes pérdidas económicas, la inteligencia artificial beneficia notablemente a la ciberseguridad, y este progreso incrementa considerablemente la importancia de la ética profesional en dicho campo; para desarrollar e implementar prácticas y tecnologías de ciberseguridad, es fundamental considerar los aspectos éticos de la seguridad de la información. La ciberseguridad es importante para las empresas comerciales, los ciberataques pueden generar pérdidas económicas significativas (Ramírez Alba, 2023).

El incremento del comercio digital favorece al trabajo remoto y a la conexión global, además ofrece un entorno adecuado para nuevas vulnerabilidades que los ciberdelincuentes aprovechan de varias formas; como el realce del comercio digital extiende el número de transacciones en línea, ocasiona mayores riesgos de ataques, fraudes y robo de datos confidenciales. El teletrabajo ha ampliado la superficie de ataque al permitir que los empleados y socios se conecten a redes corporativas desde ubicaciones remotas, a menudo desde dispositivos personales menos seguros, esta descentralización de sistemas también dificulta la gestión de la seguridad, por lo que las empresas deben garantizar la protección en todas sus oficinas y en entornos

distribuidos. Ramírez Alva (2023), indica que el comercio digital y el trabajo remoto han incrementado las amenazas cibernéticas, lo que expone a las empresas y a los usuarios a un mayor riesgo de fraude y sustracción de datos.

Un ataque de ciberseguridad contra una empresa puede tener graves consecuencias, no sólo resultando en la pérdida de información confidencial y dinero, sino también dañando la reputación de la empresa. Cuando ocurre una violación de datos, la confianza del cliente se daña gravemente, lo que puede resultar en pérdida de clientes, gastos administrativos adicionales e interrupción de servicios críticos, además, la integridad de los sistemas de información mantenidos por la compañía se comprometería, lo que podría causar daños a largo plazo a su capacidad para operar y proporcionar servicios confiables; en este contexto, garantizar la seguridad cibernética ya no es una opción, sino que se ha convertido en una prioridad, que requiere medidas preventivas, uso de tecnologías de detección y respuesta; y, actualizaciones periódicas de las políticas de seguridad para protegerse contra brotes de amenazas. El implementar medidas preventivas y tecnologías de detección es clave para proteger la estabilidad y operatividad de la empresa (Ramírez Alba, 2023).

La ciberseguridad en la actualidad, además de ser una herramienta para la creación de herramientas defensivas, tiene que lidiar con distintos tipos de peligros que amenazan su existencia y la de sus usuarios. Las amenazas cibernéticas más comunes y relevantes son las siguientes:

- ***Phishing***: Consiste en un método utilizado para engañar a las personas y obtener información confidencial, como contraseñas o datos de tarjetas de crédito. Estos ataques se dirigen a correos electrónicos falsos, mismos que se ejecutas en las organizaciones ilegales que buscan aprovecharse de la situación (Urcuqui, García, Osorio, & Navarro, 2018).
- ***Ransomware***: Es un tipo de *software* malicioso que, al infiltrarse, encripta la información tanto empresarial como de los usuarios. Este tipo de ataques se ha vuelto bastante conocido, especialmente por el impacto que pueden tener en la economía y en las operaciones diarias de las organizaciones (Casado Robledo, 2020).
- ***Malware***: Es un grupo ampliado que abarca programas dañinos, como virus,

troyanos, gusanos y software espía. Estos programas están diseñados para infiltrarse en los sistemas de computación, provocar inconvenientes, robar información o eliminar datos sin que el usuario lo identifique. El *malware* puede trabajar de manera autónoma o como parte de un ataque particular (Adedoyin & Christiansen, 2023).

- **Ataques de día cero (*Zero-Day*)**: Estos ataques se benefician de las debilidades desconocidas o que han sido recién descubiertas en los sistemas, lo que significa que no hay soluciones disponibles para protegerse de ellos. Dado que los defectos son desconocidos por los fabricantes, se trata de una amenaza grave e imperativa para ser abordada (Ramírez Alba, 2023).
- **Ataques de denegación de servicio distribuido (DDoS)**: Estos ataques se dan cuando un servidor, red o sistema se inunda con una gran cantidad de tráfico ilegal. Esto puede hacer que el sistema se caiga y que los servicios dejen de funcionar. Aunque no siempre revelan información, pueden generar pérdidas financieras y dañar la reputación de una empresa (Tapia, Ruiz, & Vega, 2021).
- **Ingeniería social**: Este es un método que se centra en influir en las personas para que compartan información confidencial o hagan cosas que puedan poner en peligro la seguridad del sistema. Su uso es frecuente junto con otros métodos, como el *phishing*, para hacer que ambos sean más efectivos (Bala, Costales, Yñota, & Ramirez, 2022).

Las amenazas requieren que se implementen políticas de seguridad, la formación continua al personal y que al mismo tiempo se garantice los sistemas informáticos se encuentren actualizados de manera constante. La prevención y la respuesta rápida a estos peligros son elementos esenciales de una estrategia integral de ciberseguridad.

1.2. SGSI (Sistema de Gestión de Seguridad de la Información)

En la actualidad, la información de las empresas se ha vuelto uno de los activos más valiosos, por lo que es de vital importancia proteger las posibles amenazas. En este sentido, el SGSI se convierte en un aliado importante, , ofrece un al proporcionar un enfoque integral para la gestión de riesgos y la protección efectiva de los datos.

Un SGSI es un conjunto de políticas de administración de la información, tiene como objetivo proteger la disponibilidad, integridad y confidencialidad de los datos, además, garantiza que la información crítica para el negocio no se vea expuesta a amenazas y vulnerabilidades. El SGSI consiste en un proceso de gestión de riesgos que se enfoca en identificar los activos, analizar las amenazas y determinar los controles que se van a implantar para evitar los riesgos (Nieves, 2017).

El SGSI está fundamentado en la protección de tres principios básicos: confidencialidad, integridad y disponibilidad, grupo también denominado como CID, la Figura 1 muestra estos principios y su interrelación, y cada uno de ellos se define a continuación (Mogollón Jiménez, 2022):

- **Confidencialidad**: La información sensible solo puede estar a disposición de los usuarios que están autorizados, impidiendo así la reducción de la misma y el uso de forma inapropiada.
- **Integridad**: La información tiene que ser exacta y completa. Ha de protegerse en todo momento de modificaciones de datos hechas por personas que no están autorizadas para ello.
- **Disponibilidad**: La información tiene que ser accesible de forma adecuada para los usuarios autorizados.

Figura 1. Principios de la Seguridad Informática

Fuente: Ministerio de Telecomunicaciones y la Sociedad de la información (2020)

El proceso de digitalización expone a las organizaciones a riesgo de ciberseguridad y

diversas vulnerabilidades, con el avance continuo de las amenazas y ataques, se hace aún más necesaria la implementación de medidas de seguridad que protejan activos valiosos y mantengan la confianza en el entorno digital. Para poder establecer un SGSI, las organizaciones deben obtener un método para implementar una adecuada administración de la seguridad de la información y garantizar la continuidad del negocio. Para facilitar el procedimiento de evaluación y análisis de riesgos, es importante comprender algunos conceptos esenciales de acuerdo con Risco Villarreal (2021):

- **Riesgo**: se refiere a la posibilidad de que una amenaza específica use una vulnerabilidad lo que podría resultar en una perdida significativa de un recurso de información. Generalmente, se entiende como la relación entre la probabilidad de que ocurra un evento y las consecuencias que este podría acarrear.
- **Amenaza**: Causa potencial de un accidente, que puede resultar en un perjuicio a un sistema, individuo u organización.
- **Vulnerabilidad**: La debilidad de un activo o control que puede ser aplicado por una o varias amenazas.
- **Impacto**: Es el resultado que surge de la concretización de una amenaza hacia un activo. Hace referencia al costo que un suceso, independientemente de su envergadura, puede generar para la entidad, el cual puede evaluarse no solo en aspectos económicos (como la pérdida de reputación, consecuencias legales, entre otros).
- **Riesgo inherente**: Este peligro existe y es inherente a cada actividad, sin que se establezcan controles.
- **Riesgo residual**: Se refiere al riesgo que persiste tras la implementación de acciones para mitigar el riesgo.

El proceso de gestión de riesgos de la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo. El enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. Por otro lado, proporciona un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, lo que incluso garantiza

que los riesgos de alto impacto se evalúen correctamente. En la Tabla 1 se describe este proceso.

Tabla 1. Pasos de las actividades del proceso de gestión del riesgo

Proceso para la SGRSI (Gestión del Riesgo de Seguridad de la Información)	
Actividades	**Pasos**
Establecimiento del contexto	1. Consideraciones Generales – Recolección de datos preliminares 2. Fijar normas fundamentales para la Administración de Riesgos 3. Determinar la extensión y restricción de la Gestión del Riesgo 4. Establecer una entidad para el funcionamiento del SGRSI
Valoración del Riesgo	5. Detectar Activos de Información 6. Identificar las amenazas y las vulnerabilidades 7. Establecer los controles actuales 8. Detectar repercusiones 9. Valorar las consecuencias 10. Evaluar los sucesos 11. Evaluar la capacidad de estimación del riesgo 12. Evaluar los riesgos
Tratamiento de Riesgo	13. Seleccionar controles
Aceptación de Riesgo	14. Responder a los riegos
Comunicación del Riesgo	15. Informar los riegos
Monitoreo y Revisión del Riesgo	16. Monitorear y evaluar los riegos

Fuente: Ministerio de Telecomunicaciones y la Sociedad de la información (2020)

Para desarrollar un SGSI se requiere de la identificación de políticas de seguridad, identificar activos importantes y aplicar medidas de control. Esto se da gracias a la administración de riesgos que fomenta en estándares como la ISO/IEC 27001:2013, que fue desarrollada por la Organización Internacional de la Normalización (ISO) y la Comisión Electrónica Internacional (IEC). Para asegurar el correcto funcionamiento y supervisión de un SGSI, es recomendable adoptar buenas prácticas, pues facilitan informar al personal acerca de la relevancia de la seguridad, tener el respaldo de los líderes de la organización y aplicar un enfoque estructurado que promueva el mejoramiento continuo de la seguridad de los datos (Haufe, Colomo, Dzombeta, Brandis, & Stantchev, 2016).

Dentro del ámbito de la seguridad informática las metodologías de análisis de riesgos constituyen una disciplina que se desarrolla en el SGSI de las organizaciones, llevando a cabo importantes escaneos de vulnerabilidades una vez más a partir de

una serie de modelos y procesos para proponer una forma más adecuada de proteger la información y los recursos de TI, algunos de los propósitos de las metodologías de análisis de riesgos son: planificación de la reducción de los riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información (Paula, 2024),

En la investigación de Busto Pérez (2024), una Política de Seguridad de la Información constituye un documento que define los lineamientos y normas para un organismo para proteger sus activos de información, su finalidad es principalmente proteger la confidencialidad, integridad y disponibilidad de la información, es necesario que esta política sea explícita y comunicada a todos los empleados, donde se delimiten roles y responsabilidades.

Además, Busto Pérez (2024), dice que deben estar detallados, al menos, los procedimientos para la gestión de incidentes de seguridad y los usos que se le pueden dar a los recursos informáticos, la política necesita ser revisada y actualizada periódicamente para adecuarse a nuevos riesgos y tecnologías emergentes y en la medida en que se hace, las organizaciones pueden reducir igualmente la probabilidad de brechas de seguridad y aumentar la confianza por parte de los clientes y socios.

Cabe recalcar que la gestión de incidentes de seguridad se convierte en un aspecto fundamental en la seguridad de la información pues, aunque se lleven a cabo medidas para evitar su ocurrencia, seguramente pueden suceder brechas de datos o ataques cibernéticos (Tasa Cantanzaro, Maquera Quispe, Rojas Bujaico, & Delgado Rospigliosi, 2022). Por lo que un SGSI debe contener un plan de respuesta que permita actuar de una manera rápida y eficiente, donde se contemple la identificación de incidentes, el proceso de notificación, la evaluación de daños, la contención y las acciones correctivas, además debe tener en cuenta que hay que garantizar una correcta comunicación con los interesados y fomentar la mejora continua de dicho sistema para evitar que se produzcan incidentes similares.

El SGSI es importante para contribuir, no solo al cumplimiento de requisitos y normativas, sino a la implementación del mismo con un efecto en la imagen de la

organización (Yungán & Narváez, 2022).Con un SGSI la organización evidencia su empeño por la seguridad de la información, lo que puede mejorar mucho su imagen. Esta percepción favorable puede dar lugar a una mayor confianza de los clientes y socios, quienes aprecian la adecuación con que la organización se toma la protección de los datos.

La implementación de un SGSI puede dar como resultado varios beneficios competitivos, además, se puede promover la atracción de nuevos clientes, , las empresas pueden diferenciase de un segmento de mercado saturado, posicionándose como proveedores confiables anticipando la seguridad de la información. Además, dicha credibilidad puede propiciar alianzas estratégicas y contratos que puedan contribuir al crecimiento y desarrollo de la empresa en un entorno de negocio en continuo movimiento (Yungán & Narváez, 2022). A continuación, se explica y se presenta cada uno de los pasos que se debe seguir para implementar un Sistema de Gestión de Seguridad de la Información:

1. **Definir la política de seguridad**

   Se definen los objetivos, el marco general, los requisitos legales y los criterios que se utilizarán para evaluar los riesgos. Para ello, es necesario establecer la metodología, la cual debe contar con la aprobación de la dirección o de la junta directiva.

2. **Definir el alcance del SGSI**

   Es fundamental tener claridad sobre los resultados que se obtendrán una vez que se implemente el plan de acción en la organización; para ello, se deben considerar los activos, las tecnologías y la descripción de cada uno de ellos.

3. **Identificar los riesgos**

   En esta fase es necesario identificar las amenazas potenciales a las que la empresa podría estar sujeta, quiénes son los responsables inmediatos, a qué aspectos son susceptibles y cuál sería el efecto si se llegara a comprometer la confidencialidad, la integridad y la disponibilidad de los activos informativos.

4. **Analizar y evaluar los riesgos**

   Se analiza el impacto que podría tener alguno de los riesgos en caso de que se materialice, se identifica la probabilidad de su ocurrencia y se evalúa cómo esto podría influir en los controles que ya están en funcionamiento. Asimismo, se verifica si el riesgo puede ser aceptado o si debe ser mitigado.

5. **Hacer un tratamiento de riesgos**

   Es decir, implementar los controles apropiados, categorizar los niveles de riesgo, prevenirlos o transferirlos a terceros si es factible.

6. **Declarar la aplicabilidad**

   Se establecen los objetivos de control y se eligen los controles que se implementarán.

7. **Realizar la gestión**

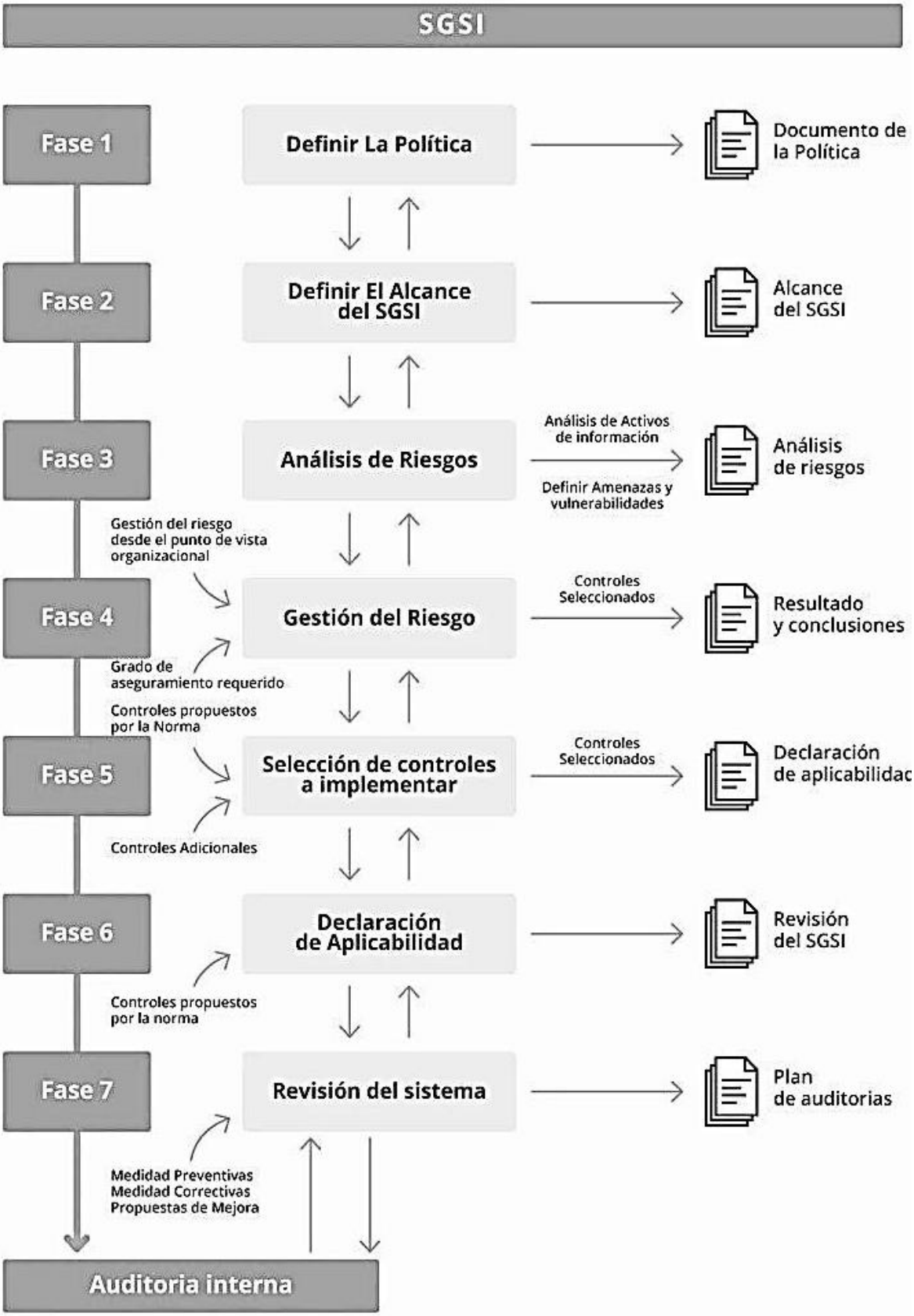
   Se trata de establecer cómo se abordarán los riesgos, aplicar dicho tratamiento considerando los controles identificados y las responsabilidades de cada individuo, implementar los controles, definir el sistema de métricas, crear conciencia en la organización y promover una cultura que asegure que todos los empleados estén familiarizados con el SGSI. Además, se debe gestionar su operación y utilizar los recursos necesarios para garantizar su cumplimiento.

8. **Monitorear**

   Se sugiere realizar una revisión periódica del SGSI para determinar si se está

cumpliendo con lo estipulado por la norma ISO 27001, con los objetivos establecidos y si es eficaz. Asimismo, es importante reportar las mejoras necesarias y las acciones que se llevarán a cabo para alcanzarlas (PIRANI, 2024).

Figura 2. Pasos para implementar un SGSI



Fuente: PIRANI (2024)

1.3. Normas ISO/IEC 27001:2022 como marco de referencia

La norma ISO 27001 es un estándar global para manejar la seguridad de la información; básicamente, ayuda a las empresas a blindar la privacidad, la corrección y el acceso a sus datos. Brinda una estructura para identificar riesgos, implementar controles y garantizar la continuidad del negocio frente a amenazas. Este estándar ha sido desarrollado por la ISO (*International Organization for Standardization*) u Organización Internacional de Normalización y por la IEC (*International Electrotechnical Commission*), Comisión Electrotécnica Internacional (UNIR, 2019).

Asimismo, la norma ISO/IEC 27001 tiene como objetivo disminuir los riesgos de daños e interferencias a la información y a las operaciones de la organización, misma que le ayudará a cumplir con las exigencias de implementación de los SGSI dentro de cualquier empresa. Un SGSI representa un planteamiento ordenado para la administración de la información en las empresas, , busca garantizar su protección y permanencia en un entorno que salvaguarde la Confidencialidad, la Integridad y la Disponibilidad de la misma. Para las organizaciones, los datos son su principal y más preciado activo; y, resguardarlos es fundamental para el buen funcionamiento de la empresa (Duarte & Monges, 2018).

La norma ISO/IEC 27001:2022 está diseñada para aplicar a todo tipo de organizaciones, sin importar lo grande o pequeña que sea, a qué se dedique ni a qué mercado opere. Esta norma se adapta a cualquier tipo de empresa, ya sea pública o privada. Asimismo, permite modelar las medidas de seguridad para que se ajusten a las condiciones de cada necesidad empresarial, proporcionando una estructura sólida para manejar la seguridad de la información, minimizar los riesgos y garantizar la privacidad, la precisión y la accesibilidad de datos importantes (Lolemi, 2024).

La norma ISO 27001:2022 incorpora actualizaciones dirigidas a los retos que las organizaciones afrontan en seguridad hoy en día y a los frentes de reciente avance tecnológico, convirtiéndose en un recurso clave para aquellas organizaciones que quieren reforzar su estrategia de ciberseguridad (Rajeshwari, 2024).

La norma ISO/IEC 27001 nació en el año 2005 y se destacó por su enfoque en la

gestión de seguridad de la información. Su principal objetivo es la identificación, análisis y tratamiento de riesgos, además de la implementación de un sistema de gestión de seguridad y un ciclo de mejora continua (Consultores ISO, 2024).

En 2013, se actualizó la norma ISO/IEC 27001:2013. Esta nueva versión incluye el marco del Anexo SL, conocido como "Estructura de Alto Nivel". Esto facilita la integración con otras nomas del sistema ISO. Esta actualización resaltó la importancia de crear procedimientos adecuados para gestionar la seguridad de la información en las organizaciones. Además, destacó la relevancia del liderazgo en la implementación y el cuidado del SGSI (Mantilla, 2017).

En 2022, se llevó a cabo una revisión y actualización de la norma ISO/IEC 27001:2022. Esta nueva versión incluye cambios importantes que incluye cambios significativos que reflejan la evolución frente a amenazas más sofisticadas y para implementar nuevas prácticas en seguridad de la información. Asimismo, se mejoró la atención en la gestión de riesgos y la protección de privacidad de la información (Mantilla, 2017). Según un estudio de Consultores ISO (2024), la norma ISO 270001 es muy importante para gestionar la protección de la información por varias razones:

- **Protección de los activos de información**: La norma ISO 27001 ayuda a las empresas a identificar y clasificar de manera adecuada sus activos de información para protegerlos. El estándar establece un proceso claro para proteger recursos esenciales como los datos personales de los clientes y los secretos de negocio, mismo que se logra mediante el uso de diversos protocolos de seguridad y estrategas de protección.
- **Mitigación de riesgos**: El el enfoque principal de esta normativa. La norma ISO 27001 ayuda a las entidades a identificarse, valoración y gestión de los riesgos vinculados a la seguridad de los datos. Esto incluye tanto los peligros externos, como los ataques cibernéticos, el malware y los hackeos, como los peligros internos, que comprenden el daño de información o el acceso no permitido. Al implementar controles para minimizar estos peligros, las entidades pueden reducir considerablemente tanto la posibilidad como el efecto de los incidentes de seguridad.
- **Cumplimiento normativo y regulatorio**: Con el aumento en las regulaciones

de protección de datos y privacidad del GDPR (Reglamento General de Protección de Datos) en Europa, es necesario que las organizaciones deban cumplir con una serie de leyes que exigen una adecuada salvaguarda de la información. La ISO 27001 asiste a las organizaciones en el cumplimiento de estas normativas al definir políticas y procesos transparentes sobre la gestión de la información y su correcta protección.

- **Mejora continua**: Con el aumento de las regulaciones sobre la protección de datos y la privacidad, como el GDPR en Europa, las organizaciones se ven obligadas a cumplir con diversas normativas legales que exigen una adecuada protección de la información. La norma ISO 27001 es una herramienta clave que ayuda a las organizaciones a alinearse con estas leyes, estableciendo políticas y procedimientos claros para manejar y proteger la información de manera efectiva.
- **Confianza y reputación**: Para las organizaciones, una de las principales ventajas de adoptar la ISO 27001 es la confianza que se establece entre clientes, proveedores y otras partes interesadas. Obtener la certificación ISO 27001 es una clara señal del compromiso de la organización con la seguridad de la información, y puede ser un factor diferenciador crucial en mercados competitivos. En un mundo donde las violaciones de datos pueden causar estragos en la reputación de una empresa, la certificación ISO 27001 actúa como un respaldo de que la organización está tomando medidas proactivas para proteger la información sensible.
- **Ventaja competitiva**: La adopción de la ISO 27001 ofrece una ventaja competitiva considerable. Las empresas que obtienen esta certificación pueden presumir de haber implementado los más altos estándares en seguridad de la información, lo que puede ser un factor clave para atraer clientes y conseguir contratos, especialmente cuando se trata de aquellos que manejan grandes volúmenes de datos sensibles o que operan en sectores muy regulados, como la banca, la salud o la tecnología.

La norma ISO/IEC 27001:2022 estructura sus requisitos principales en las cláusulas 4 al 10, que abordan aspectos clave como el contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua:

1. **Cláusula 4 – Contexto de la organización**: Requisitos y expectativas de los interesados tanto a nivel interno como externo y que influirán en el SGSI y determinación del alcance de este.
2. **Cláusula 5 – Liderazgo**: Importancia de la implicación de la gerencia con el sistema, mediante el establecimiento de políticas, integrando el SGSI en los procesos de la organización, y asegurando los recursos necesarios.
3. **Cláusula 6 – Planificación**: Es imprescindible detectar, analizar y valorar los riesgos de seguridad de la información tomando como referencia los umbrales aceptables de riesgo de la organización (apetito al riesgo), así como planificar estrategias de respuesta (mitigación).
4. **Cláusula 7 – Soporte**: Recursos necesarios para la capacitación y concienciación del personal, además de la importancia de la comunicación y la propia información.
5. **Cláusula 8 – Operación**: Se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
6. **Cláusula 9 – Evaluación de desempeño**: Se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del SGSI, para asegurar que funciona según lo planificado.
7. **Cláusula 10 – Mejora**: Se centra en cómo abordar las no conformidades con la norma, las acciones correctivas que hay que implementar y la mejora periódica del SGSI (UNIR, 2019).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

El cantón Santiago de Píllaro tiene una historia interesante que comienza antes de la llegada de los españoles. En ese entonces, vivían en la zona grupos indígenas como los Píllaros y los Puruháes. Estos pueblos se destacaban por su forma de vida en comunidad y por sus métodos de agricultura que se adaptaban a las montañas de los Andes. La llegada de los conquistadores españoles en el siglo XVI hizo que la región se convirtiera en un símbolo de resistencia y orgullo. Esto se debió a Rumiñahui, quien lideró la defensa del territorio y logró detener el avance de los conquistadores. Sin embargo, al final, se inició un proceso de colonización que incluyó la evangelización y un cambio en las estructuras sociales y económicas. (Cerón, 2023).

Durante la época republicana, Píllaro se estableció como un relevante núcleo agrícola y comercial de la provincia de Tungurahua, famoso por la fertilidad de sus territorios y la producción de maíz, patatas y frutas del Andino. El 29 de julio de 1860, fue ascendido a la condición de cantón, fortaleciendo así su identidad política y administrativa. Con el paso del tiempo, las costumbres culturales se han preservado, entre las que sobresale la Diablada Pillareña, catalogada como Patrimonio Cultural del Ecuador, mismo que, representa la riqueza simbólica y festiva de su pueblo. En la actualidad, Píllaro intenta balancear su crecimiento con la conservación de sus valores culturales y la protección del medio ambiente. (Cerón, 2023).

El Gobierno Autónomo Descentralizado Municipal (GAD) de Santiago de Píllaro es una entidad pública que forma parte de la estructura estatal del país y su propósito fundamental es garantizar el bienestar de la colectividad, impulsando el desarrollo social, económico, cultural y ambiental mediante una gestión participativa, transparente y eficiente; sus funciones abarcan la gestión de vigilancia y seguridad, la administración pública; y, la preservación del orden y la paz social en el cantón. La misión del GAD de Píllaro es: “Impulsar las acciones institucionales para la consecución de un adecuado desarrollo social, económico y cultural de la población, con la participación directa y efectiva de todos los actores sociales dentro de un marco de transparencia, ética y el uso óptimo del talento humano altamente comprometido,

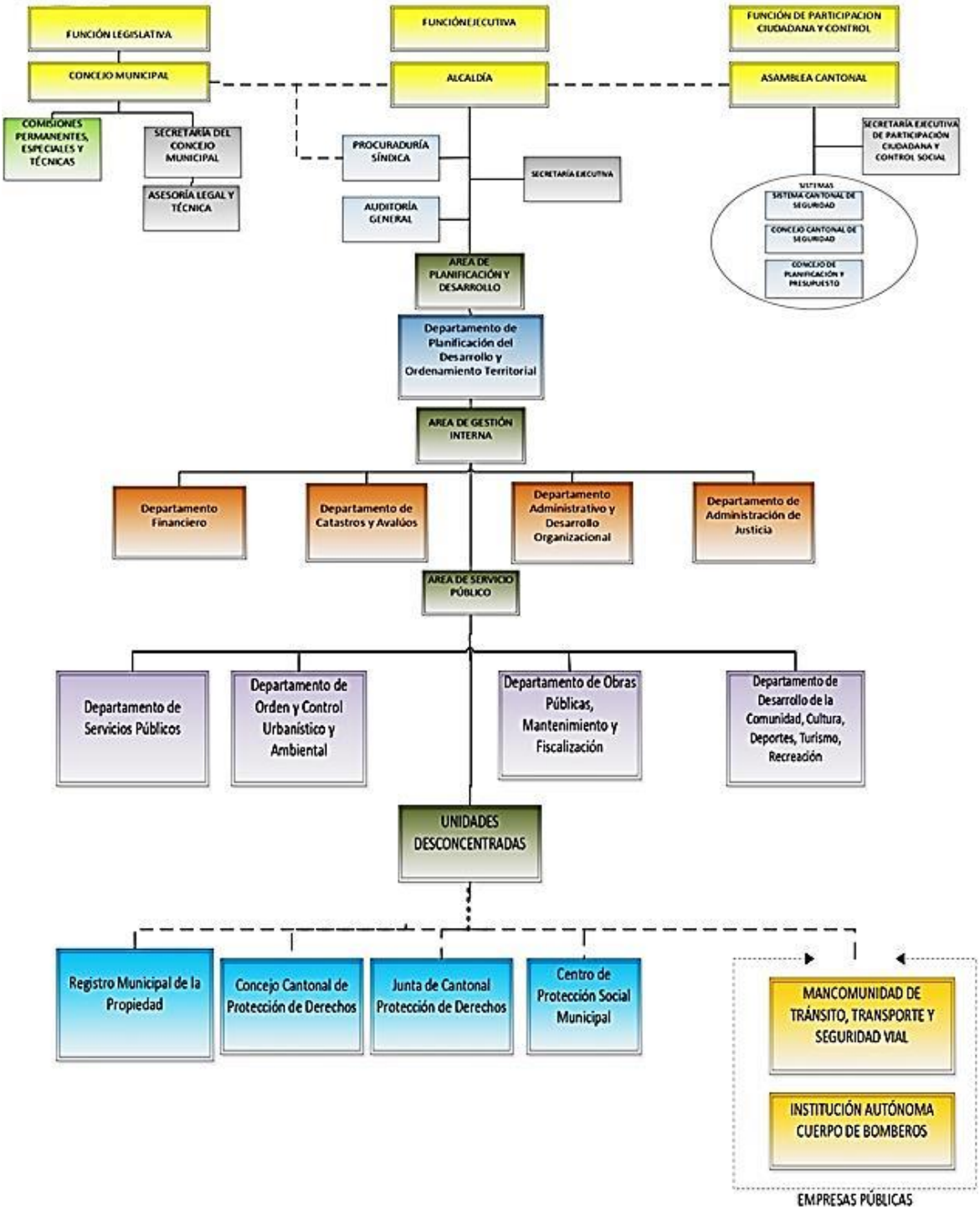
capacitado y motivado” (GAD Santiago de Píllaro, 2025).

La visión del GAD es: “Convertir el Cantón Santiago de Píllaro, en un referente dinámico de cambio, cuyas características de crecimiento, estén marcadas por la activa participación de sus habitantes, dentro de un marco de planificación que implique la responsabilidad social de sus entes y organizaciones, y cuyas actividades productivas optimicen el talento humano, tecnológicos y naturales, permitiendo el desarrollo integral del cantón, en una armónica relación hombre naturaleza, que vaya consolidando su identidad de pueblo trabajador, hospitalario y alegre” (GAD Santiago de Píllaro, 2025).

La misión y la visión del GAD Santiago de Píllaro destacan su dedicación al crecimiento social, económico y cultural de la comunidad. Esto se logra a través de la participación activa de todos los involucrados, la claridad en las acciones y el uso efectivo de las habilidades de las personas y la tecnología disponible. Para lograr estos objetivos, es fundamental asegurar la protección de la información institucional. Los sistemas digitales y los datos importantes son esenciales para planificar, ofrecer servicios públicos y tomar decisiones estratégicas. Por lo tanto, al proteger la confidencialidad, la integridad y la disponibilidad de la información, se fortalece la confianza de los ciudadanos, se mejora la transparencia en la administración y se ayuda a establecer un modelo de gestión moderno y responsable que cumpla con estándares internacionales. La aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 es fundamental para alcanzar la misión y visión de la institución. Esto promueve el desarrollo completo del cantón, al mismo tiempo que se actúa con responsabilidad social y se asegura la sostenibilidad tecnológica.

El GAD de Píllaro cuenta con una estructura organizacional encabezada por el Alcalde, apoyado por el Concejo Municipal y diversas direcciones y departamentos. Entre sus áreas principales destacan: Procuraduría Síndica Municipal, Auditoría General, Planificación del Desarrollo y Ordenamiento Territorial, Finanzas, Catastros y Avalúos, Obras Públicas, Servicios Públicos, Desarrollo Social y Comunitario, y la Administración de Justicia. La Figura 3 muestra el organigrama estructural del GAD.

Figura 3. Organigrama estructural del GAD de Píllaro



Fuente: GAD Santiago de Píllaro (2025)

Las principales funciones de cada área o departamento se describen a continuación (GAD Santiago de Píllaro, 2022):

- **Procuraduría Síndica Municipal**: Su objetivo es ofrecer apoyo y asesoría legal al Gobierno Autónomo Descentralizado (GAD) en asuntos judiciales y fuera de los tribunales, para salvaguardar los intereses del municipio. Se ocupa de

participar en audiencias, trámites y reuniones, asegurando que se apliquen adecuadamente las normas y protegiendo la seguridad legal de la institución.

- **Auditoría General**: Ejerce el control interno conforme a lo estipulado por la Contraloría General del Estado. Realiza auditorías y evaluaciones, y brinda asesoría técnica al GAD para garantizar la transparencia en el uso de los recursos públicos.
- **Planificación del Desarrollo y Ordenamiento Territorial**: Formula y coordina la planificación estratégica del desarrollo cantonal, administra el uso del suelo, propone políticas de seguridad civil y fomenta la participación ciudadana en programas de desarrollo sostenible.
- **Financiero**: Administra los recursos económicos del GAD, define políticas y metas financieras, elabora y controla el presupuesto municipal, gestiona la inversión pública y asegura el cumplimiento de los objetivos financieros.
- **Catastros y Avalúos**: Se encarga de la investigación técnica y legal sobre bienes urbanos y tenencia de la tierra, para regularizar la propiedad y mantener actualizados los registros catastrales para la administración territorial.
- **Administrativo y Desarrollo Organizacional**: Coordina políticas institucionales y programas de crecimiento organizacional, administra los servicios de atención al público, logística, transporte, mantenimiento de instalaciones y zonas verdes.
- **Orden y Control Urbanístico y Ambiental**: Supervisa permisos y licencias urbanas y ambientales, controla canteras y minas y elabora planes de gestión del suelo y del medio ambiente.
- **Servicios Públicos**: Planifica y gestiona la prestación de servicios públicos municipales (recolección de residuos, mantenimiento de espacios públicos, cementerios, terminales y mercados), regula el comercio informal y la tenencia responsable de animales.
- **Obras Públicas, Mantenimiento y Fiscalización**: Diseña, ejecuta y supervisa la obra pública municipal, gestiona contratos, garantiza el mantenimiento preventivo y correctivo de la infraestructura y supervisa la calidad de materiales, equipos y personal involucrado en las construcciones.
- **Desarrollo Social y Comunitario, Cultural, Deportivo, Turístico y Emprendimiento**: Promueve el desarrollo social y económico del cantón

mediante programas comunitarios, culturales, turísticos y deportivos, fomenta la economía popular y solidaria; y, apoya emprendimientos para mejorar la calidad de vida de la población.

- **Administración de Justicia**: Garantiza el debido proceso y la legítima defensa, mediante resoluciones sancionatorias o absolutorias; y, contribuye al orden y la paz social en el territorio cantonal.
- **Tecnologías de la Información (TI):** Brinda soporte a los sistemas institucionales, la página web y la comunicación electrónica; se encarga de velar por la seguridad de la información.

El área de Tecnologías de la Información (TI) enfrenta limitaciones que afectan la seguridad de la información, entre ellas se puede mencionar la carencia de políticas formales de seguridad, la ausencia de procedimientos documentados para recuperación de datos ante incidentes, la obsolescencia tecnológica de sus servidores, la falta de un análisis formal de riesgos y de un inventario digital actualizado de activos informáticos. Estas carencias generan vulnerabilidades en la protección de datos sensibles, por lo que, se ha vuelto una necesidad imperativa la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, que incluya políticas claras, procedimientos de respaldo y recuperación, capacitación del personal, actualización tecnológica y mecanismos de monitoreo continuo.

2.2. Metodología de investigación

Enfoque de investigación

El enfoque adoptado en esta investigación es cualitativo, porque explora las necesidades, limitaciones y oportunidades de mejora en el GAD de Píllaro, de forma contextualizada e integral. Además, de acuerdo con Hernández Sampieri (2018), este enfoque posibilita indagar en los factores humanos, organizacionales y tecnológicos que intervienen en la gestión de la información; por lo que resultó adecuado para diseñar una guía de alcance y mapas de procesos del SGSI, pues implicó analizar la manera en que fluye la información a través de los distintos departamentos, cómo se protegen los activos informáticos y documentales y cuáles son los riesgos y vulnerabilidades percibidos por el personal, todo dentro del marco de la norma ISO/IEC 27001:2022.

Adicionalmente, el enfoque cualitativo permitió integrar las particularidades de cada departamento, con lo que se aseguró una propuesta de SGSI específica y factible, capaz de determinar el nivel de riesgos y amenazas al que están expuestos los sistemas de información del GAD, y facilitar el diseño de controles, políticas y procesos requeridos para fortalecer la seguridad de la información institucional de forma efectiva y sostenible.

Tipo de investigación

El estudio combinó la investigación documental y la de campo, con el fin de obtener un análisis integral del problema y de sus posibles soluciones. Por un lado, la investigación documental se centra en la revisión de fuentes secundarias, como la norma ISO/IEC 27001:2022, literatura académica sobre sistemas de gestión de seguridad de la información, guías de buenas prácticas y documentos oficiales relacionados con metodologías para la gestión de riesgos tecnológicos (Martínez, 2023). Esta revisión resultó fundamental para comprender los requisitos técnicos y organizacionales que debe cumplir un SGSI, así como para identificar modelos y experiencias previas que sirvan como referencia para determinar el alcance y campo de aplicación de la norma en el contexto municipal.

Por otro lado, la investigación de campo se realizó directamente en el GAD de Píllaro, con lo que se pudo conocer de forma directa las características operativas, organizacionales y tecnológicas de la institución. Se incluyó la aplicación de instrumentos pertinentes al personal clave, la observación de la infraestructura tecnológica y la revisión de documentación interna. Este tipo investigativo permitió identificar de manera específica los activos de información existentes, las políticas y prácticas de seguridad actuales, los procesos administrativos involucrados y las carencias o vulnerabilidades detectadas en el manejo de la información sensible (Martínez, 2023).

Método de investigación

Para el desarrollo de esta investigación se adoptó el método analítico-sintético, que, en palabras de Bernal (2016), combina dos procesos complementarios y esenciales para abordar la complejidad de la gestión de la seguridad de la información en un gobierno local. El análisis consiste en descomponer la realidad institucional en sus elementos constitutivos: identificar los activos de información, los flujos de datos, las amenazas potenciales, las vulnerabilidades actuales, los controles existentes y los procesos críticos de cada departamento involucrado (Bernal, 2016). Esta descomposición permitió conocer con precisión cómo se maneja la información en los departamentos del GAD, e identificar puntos débiles y brechas de seguridad que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos.

La síntesis integra los hallazgos del análisis para formular un diagnóstico completo y coherente, que oriente el diseño de la guía de alcance del SGSI y la elaboración de mapas de procesos que representen de forma clara y estructurada los flujos de información y las interacciones entre sistemas y usuarios (Bernal, 2016). Esta integración implicó describir el estado actual y proponer mejoras basadas en los principios y requisitos de la norma ISO/IEC 27001:2022 para la protección de los activos identificados. La aplicación de este método permitió la construcción de soluciones prácticas y adaptadas al contexto del GAD Píllaro, de manera sólida, factible y contextualizada, de esta forma, se obtuvo un enfoque integral para el fortalecimiento de la gestión de la seguridad de la información.

Técnicas e instrumentos de investigación

Para el desarrollo de esta investigación se emplearon técnicas cualitativas para recolectar información que permita diagnosticar la situación actual y diseñar una guía de alcance y los mapas de procesos del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022. En primer lugar, se utilizó una entrevista semiestructurada dirigida al director del área de Tecnologías de la Información, con preguntas abiertas que posibilitaron explorar de manera profunda los procesos, activos de información, mecanismos de control, políticas de respaldo y recuperación de datos, así como las percepciones sobre vulnerabilidades y necesidades específicas.

Además, se aplicó una encuesta con escala Likert dirigida al personal del área de Tecnologías de la Información y a usuarios clave de cuatro departamentos estratégicos para el SGSI: Departamento Financiero, Avalúos y Catastros, Administrativo y Desarrollo Organizacional, y Administración de Justicia. Esta encuesta fue diseñada para recoger percepciones sobre la gestión de activos, los procedimientos de respaldo, los controles de acceso, los flujos de información y la identificación de riesgos. La inclusión de esta técnica permitió enriquecer el diagnóstico con información proveniente de quienes utilizan y gestionan los sistemas de información en sus tareas diarias.

Aparte de la entrevista y la encuesta, a lo largo del estudio se aplicó la observación directa de los procesos institucionales, sistemas y prácticas cotidianas en el manejo de la información, con lo que se pudo identificar los flujos de información entre departamentos, las condiciones de almacenamiento y seguridad de los datos, y las prácticas de manejo de respaldos, controles de acceso y procedimientos de recuperación. Todo lo mencionado se complementó con la revisión documental de políticas, normativas, inventarios de activos, registros presupuestarios y procedimientos administrativos del GAD, con el fin de comprender el marco que regula la seguridad de la información en el GAD.

Población y muestra

La población objetivo de esta investigación está conformada por el personal del GAD de Santiago de Píllaro involucrado en la gestión, uso y protección de la información institucional. Este grupo incluye al personal técnico del área de Tecnologías de la Información (TI), responsable de los sistemas y la infraestructura tecnológica; y, a funcionarios de los departamentos clave que manejan información sensible y utilizan los sistemas institucionales en sus procesos cotidianos.

Para garantizar un diagnóstico integral y adaptado a la realidad institucional, se utilizó un muestreo intencionado que incluyó dos componentes. El primero, formado por el personal del área de TI, compuesto por el director y dos técnicos, quienes poseen un conocimiento especializado sobre la infraestructura tecnológica, los procedimientos de respaldo y recuperación de datos, y los controles de acceso. El segundo, es una muestra de usuarios clave de cuatro departamentos estratégicos identificados para el alcance del SGSI: Departamento Financiero, Avalúos y Catastros, Administrativo y Desarrollo Organizacional, y Administración de Justicia. Para estos departamentos se consideró la participación de 3 funcionarios por área, quienes interactúan de forma frecuente con los sistemas de información y gestionan datos sensibles. En la Tabla 2 se muestran la estructura de la muestra.

Tabla 2. Muestra de funcionarios para la encuesta

Departamento	Cargo	Participantes	Justificación
Tecnologías de la Información	Director y técnicos	3	Conocimiento especializado en infraestructura, respaldos y controles de acceso
Financiero	Funcionarios y usuarios clave	3	Gestión de información contable y presupuestaria crítica, con acceso a sistemas financieros sensibles
Avalúos y Catastros	Funcionarios y usuarios clave	3	Manejo de bases de datos catastrales, planos y registros prediales con información sensible de contribuyentes
Administrativo y Desarrollo Organizacional	Funcionarios y usuarios clave	3	Administración de expedientes de personal, contratos y comunicaciones oficiales, con datos confidenciales
Administración de Justicia	Funcionarios y usuarios clave	3	Gestión de expedientes legales, resoluciones y actas con información reservada y de alta sensibilidad jurídica
Total:		15	

Fuente: Elaboración propia

Esta estrategia de muestreo integró la visión técnica del área de TI con las percepciones de los usuarios directos de los sistemas, de tal forma que la propuesta de alcance y mapas de procesos del SGSI se fundamenten en las necesidades reales de protección de los activos de información en todos los niveles operativos del GAD de Píllaro. En el Anexo 1 se muestra el formato de entrevista semiestructurada dirigida al Director de TI, mientras que en el Anexo 2 se muestra el formato de encuesta dirigida a los técnicos de TI y al personal de los departamentos clave.

2.3. Diagnóstico de la situación actual de la seguridad de la información en el GAD de Píllaro

Este diagnóstico busca identificar las necesidades específicas relacionadas con la gestión de activos de información, los controles de acceso, los procesos de respaldo y recuperación de datos y la cultura organizacional de seguridad. A partir del diagnóstico se podrá diseñar la propuesta de alcance y los mapas de procesos del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a la norma ISO/IEC 27001:2022, de acuerdo con los flujos de información de los departamentos estratégicos del GAD de Píllaro.

Análisis de la entrevista

La entrevista con el director de TI reveló varias limitaciones estructurales en la gestión de la seguridad de la información, las cuales tienen impacto directo en los procesos operativos y la protección de datos sensibles. En lo que se refiere a los activos de información del GAD, el entrevistado manifestó que los más críticos son las bases de datos de catastros y avalúos, los registros financieros, los datos administrativos, los expedientes legales y los sistemas que procesan pagos y trámites, , contienen información sensible de los ciudadanos y permiten la operatividad institucional diaria; además expresó que el control de activos físicos lo lleva el de Finanzas, pero que no existe un inventario digital para datos o software; Afirmó que se comparten las bases de datos de catastros y los documentos financieros, cuyo acceso está parametrizado por usuario mediante *Active Directory* y grupos por aplicación, sin embargo, no existe una política formal ni controles avanzados como doble autenticación.

Comentó que los procesos y flujos de información, se gestionan a partir de una solicitud de soporte, luego se crean los usuarios y se habilita el acceso al sistema, por otra parte, cada una sube o consulta información de acuerdo con su grado de accesibilidad; sin embargo, no se cuenta con un mapeo formal, políticas, controles documentados de estos flujos, por el contrario, manifestó que el intercambio de datos es informal por lo que se podrían presentar accesos indebidos o uso incorrecto de la información sensible. Para contrarrestar esto, el personal de TI administra accesos por usuario y grupo en servidores y genera respaldos periódicos, aunque faltan procedimientos documentados y mejor control.

En cuanto a la seguridad, el entrevistado dijo que, para conservar los datos, los respaldos diarios se archivan en un computador externo al *DataCenter* y se guardan en la caja fuerte de Tesorería cada mes, pero que no hay procedimientos escritos ni pruebas formales de recuperación. Para la autenticación y control de acceso se utiliza *Active Directory* con usuarios y contraseñas por aplicación, sin control de acceso biométrico o de doble autenticación. Además, mencionó que el GAD tiene tres servidores con Windows Server 2008 de 64 bits, que aún son funcionales, pero ya empiezan a quedar obsoletos, lo cual provoca falta de análisis de riesgos, falta de personal especializado en seguridad, respaldos no documentados y controles de

acceso limitados.

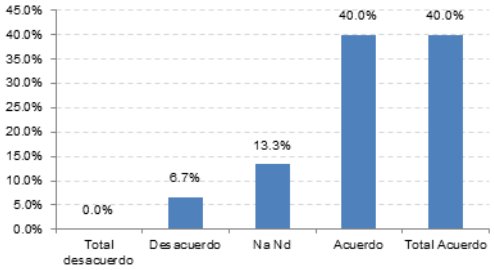
La respuesta ante incidentes de seguridad informática en el GAD es reactiva, , no se cuenta con un plan ni protocolos estandarizados, además, añadió que no se ha realizado un análisis formal de riesgos tecnológicos, lo cual representa una debilidad muy grande, por lo que considera que sería adecuado implementar un SGSI, documentar políticas y procedimientos, actualizar la infraestructura tecnológica, capacitar al personal y crear un inventario de activos de información.

Análisis de las encuestas

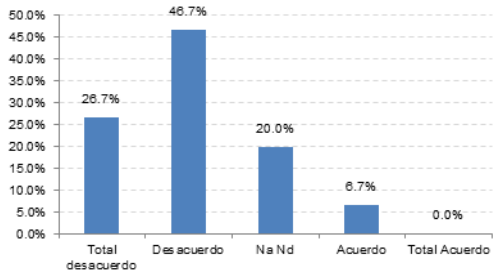
El análisis de la encuesta aplicada al personal del área de TI y usuarios de los departamentos clave del GAD de Píllaro, se realizó con gráficas de frecuencias y porcentajes, los resultados obtenidos permitieron establecer el diagnóstico de la situación actual de la Seguridad de la Información en la institución.

En cuanto a la Gestión de Activos; la identificación y conocimiento de los activos de información (**Figura 4a**) presenta una respuesta positiva general con un 80% de acuerdo o totalmente de acuerdo, especialmente en TI, lo que indica que el personal clave comprende la importancia de la información que maneja. Sin embargo, en la existencia de registros actualizados (**Figura 4b**) y gestión de los activos por sensibilidad (**Figura 4c**), predominan los niveles de desacuerdo, con más del 70%, lo que demuestra una ausencia de inventarios clasificados y actualizados.

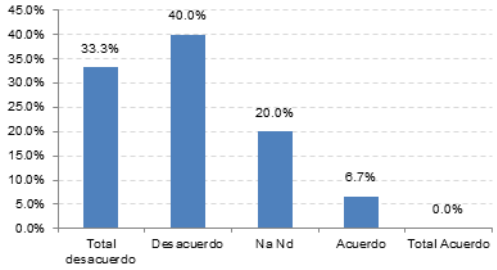
Figura 4. Gestión de Activos de Información



a) Conozco los activos de información con los que trabajo



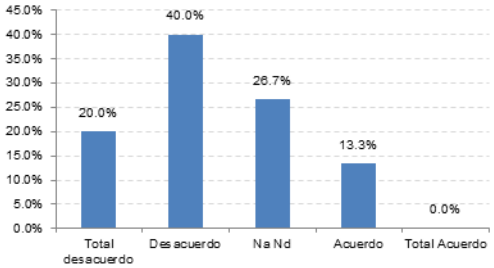
b) Existen registro claro y actualizado de activos de información



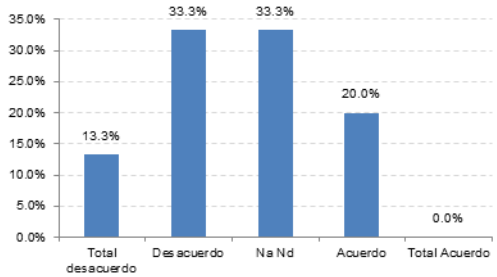
c) Los activos son gestionados por criticidad y sensibilidad

Fuente: Elaboración propia

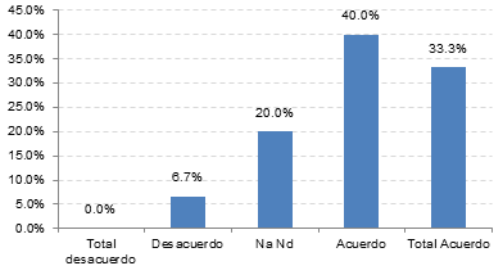
Figura 5. Flujos de información y procesos



a) Los procesos de intercambio están definidos



b) El flujo de información es seguro



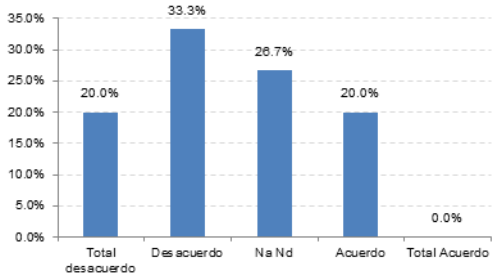
c) Identifico puntos vulnerables al compartir información

Fuente: Elaboración propia

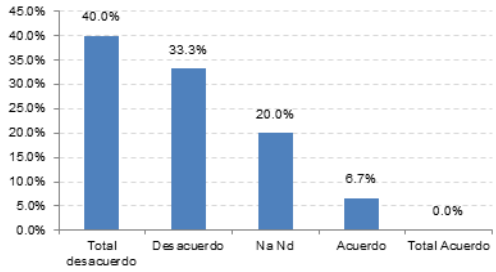
Los procesos de intercambio de información (**Figura 5a**) y la percepción de flujo seguro (**Figura 5b**) muestran niveles de desacuerdo mayores al 60%, con lo que se confirma que los departamentos clave no cuentan con procedimientos y flujos documentados, definidos y estandarizados; y el riesgo de errores, omisiones o accesos no autorizados se incrementa. En contraste, más del 70% de encuestados (**Figura 5c**) está de acuerdo en que la capacidad de identificar puntos vulnerables y riesgos es alta.

Las prácticas de respaldo y recuperación de datos son deficientes, pues la frecuencia de respaldo (**Figura 6a**), la existencia de procedimientos claros de recuperación (**Figura 6b**) y la confianza en la seguridad de los respaldos (**Figura 6c**) muestran más del 60% de desacuerdo, esto evidencia una falta de políticas y estándares para garantizar la disponibilidad y continuidad de la información.

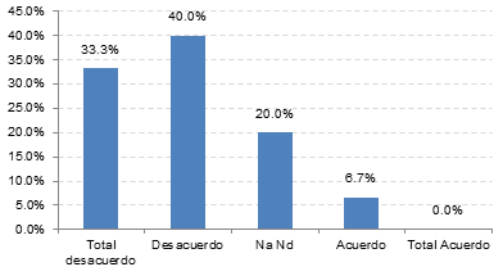
Figura 6. Respaldo y recuperación de datos



a) Se hacen respaldos con la frecuencia necesaria



b) Existen procedimientos claros de recuperación



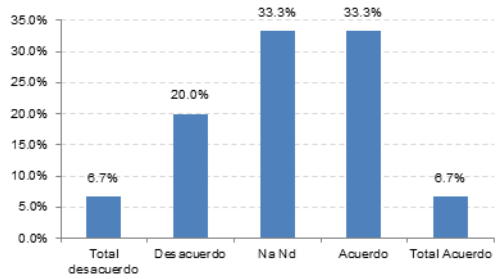
c) Confío en la seguridad del respaldo

Fuente: Elaboración propia

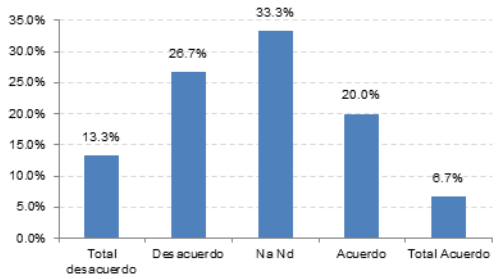
Los controles de acceso (**Figura 7a**) y niveles de privilegio (**Figura 7b**) tienen respuestas con dispersión significativa, pues un tercio de los encuestados no tienen una percepción clara sobre estos aspectos, esto posiblemente refleja diferencias de opinión entre el personal de TI y los usuarios de otros departamentos, lo cual señala

la necesidad de políticas claras y unificadas. Por su parte, el monitoreo de accesos (**Figura 7c**) presenta niveles de desacuerdo superiores al 70%, lo cual refleja un riesgo de vulneración a la seguridad.

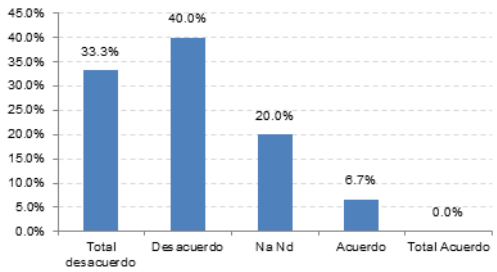
Figura 7. Controles de acceso y autenticación



a) El acceso a los sistemas está bien controlado



b) Se respetan los niveles de privilegio de usuarios

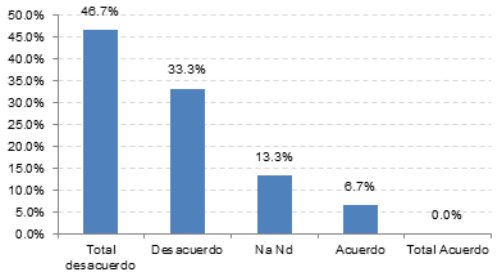


c) Se monitorea accesos a información sensible

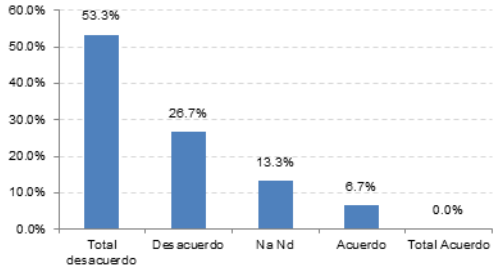
Fuente: Elaboración propia

La capacitación en seguridad (**Figura 8a**) y la evaluación de riesgos (**Figura 8b**) presentan niveles de desacuerdo superiores al 70%, lo que ratifica la necesidad de establecer procedimientos, programas de concienciación y análisis formal de riesgos. Esto se vuelve más evidente con la percepción sobre la necesidad de fortalecer las políticas de seguridad (**Figura 8c**), pues en este punto se registra un 93.3% se acuerdo; y constituye una oportunidad de mejorar la seguridad con el apoyo de los funcionarios del GAD.

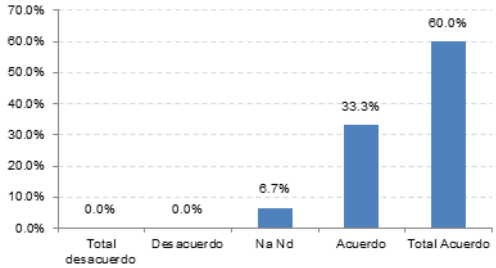
Figura 8. Percepción de riesgos y necesidades



a) Ha recibido capacitación en seguridad de la información



b) Existe una evaluación adecuada de riesgos de seguridad



c) Se debe fortalecer políticas y procedimientos de seguridad

Fuente: Elaboración propia

El diagnóstico de la situación actual de la seguridad de la información en el GAD Santiago de Píllaro muestra que existen limitaciones estructurales y operativas que justifican la necesidad urgente de implementar un SGSI conforme a la norma ISO/IEC 27001:2022. Entre los hallazgos más destacados se pueden mencionar la inexistencia de un inventario digital de activos, la ausencia de procedimientos para respaldos y recuperación, controles de acceso limitados sin autenticación avanzada, monitoreo insuficiente de actividades, obsolescencia tecnológica, carencia de análisis de riesgos formales y flujos de información poco estandarizados, todo esto incrementa la exposición a accesos no autorizados y a vulnerabilidades operativas. Con base en estos resultados, queda claro que es necesario desarrollar una guía de alcance y diseñar mapas de procesos del SGSI, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales y fortalecer la confianza de la ciudadanía en la gestión municipal.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Para desarrollar la guía del alcance, se tomó como base el diagnóstico de la situación actual del GAD; además de los resultados de la entrevista y las encuestas; y, los elementos de la Norma ISO/IEC 27001:2022, los cuales definen los límites del SGSI, los departamentos involucrados, los activos de información a proteger y los controles mínimos requeridos. Por otra parte, los mapas de procesos se diseñaron a partir de los flujos de información y los puntos críticos de riesgo de las áreas estratégicas; con ello se pudieron definir herramientas para planificar, organizar y controlar la gestión de la seguridad de la información en la institución.

3.1. Resultados

Como resultados de esta investigación, se desarrolló una Guía que define el Alcance de un SGSI, con los principios establecidos por la norma ISO/IEC 27001 diseño de un mapa de procesos del alcance de un SGSI, sino que también incluye el diseño de un mapa de procesos que facilita la visualización y el control de flujos de la información dentro de la municipalidad del Cantón Píllaro.

3.2. Evaluación y validación

Pontificia Universidad Católica del Ecuador | Sede Ambato

Matriz de Evaluación de la Guía para el análisis del alcance y campo de aplicación de las normas ISO/IEC 27001:2022

Objetivo:

Validar el contenido de la guía parala posible implementación de un SGSI en el GAD Municipal Santiago de Píllaro, mismo que evaluara la claridad, la estructura, y el aporte en la implementación de la norma ISO/IEC 21001:2022

Instrucciones:

Una vez revisada la guía, evalúe cada uno de los criterios otorgando una calificación del 1 al 5 en la columna correspondiente. Esta valoración permitirá detectar tanto los aspectos positivos como las áreas que requieren mejoras en el contenido.

Escala de valoración:

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

Tabla 1 Matriz de evaluación de la guía.

Criterio	Descripción	Puntuación (1-5)
Alcance	La guía está elaborada conforme a las necesidades y exigencias establecidas por la municipalidad.	5
Coherencia y cohesión de la norma ISO 27001	La guía incorpora los lineamientos y la estructura establecidos por la norma ISO 27001.	4
Aplicabilidad	La guía propone procesos viables y adaptados a la	5

Pontificia Universidad Católica del Ecuador | Sede Ambato

	operatividad del GAD de Píllaro	
Visibilidad	La guía plantea estándares, recursos y herramientas viables, adecuadas al contexto el GAD de Píllaro.	4
Estructura y organización	La guía sigue una estructura clara con índice, introducción, objetivos, procesos, anexos y mapas de procesos.	4
Originalidad y aporte	La guía expone una perspectiva única, funcional y enriquecida para el GAD de Píllaro.	5
Reducción de riesgos	La guía presenta recomendaciones orientadas a alcanzar los objetivos de seguridad y a prevenir riesgos e incidentes.	5
Mejora continua (PDCA)	Se considera explícitamente el ciclo de mejora continua propuesto por la norma ISO/IEC 27001:2022.	4

Ing. Levy Valle

Nombre:

GADM SANTIAGO DE PILLARO

Institución:

JEFE DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN (E)

Cargo:

Firma:

CONCLUSIONES

- En la revisión bibliográfica se analizaron tesis y artículos científicos referentes a la aplicación de la Norma ISO 27001:2022 y se identificó pocas variaciones con respecto a la ISO 27001:2013, además, se documentó la terminología importante dentro del SGSI, conceptos claves que guiaron el desarrollo de la investigación.

- La investigación se desarrolló bajo un enfoque cualitativo utilizando el método analítico-sintético y aplicando técnicas de investigación documental y de campo, que permitieron el diagnóstico para el GAD de Píllaro evidenció la ausencia de un SGSI formalmente estructurado, lo que ha limitado la capacidad institucional para identificar, evaluar y mitigar los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información crítica. En este diagnóstico también se pudo identificar los aspectos a considerar en base a la norma ISO/IEC27001:2022.

- Los datos clave identificados en el diagnóstico principalmente están relacionados a la falta de inventarios de activos, procedimientos documentados de respaldo y recuperación, y controles de acceso formales, y representan una brecha frente a los estándares internacionales definidos por la norma ISO/IEC 27001:2022, lo que llevó a determinar el alcance de la aplicación de la norma ISO/IEC27001:2022.

- Se desarrolló la Guía del Alcance del SGSI la cual permite delimitar de forma clara los departamentos estratégicos que deben incorporarse al sistema, además, ayuda a definir el límite organizacional y tecnológico sobre el cual aplicar controles de seguridad de la información, y los flujos interdepartamentales que gestionan datos sensibles.

- El diseño de los mapas de procesos propuestos permite visualizar de manera estructurada los flujos de información entre áreas críticas del GAD; e, identifican actividades, responsables, decisiones y controles aplicables en cada etapa.

RECOMENDACIONES

- Es de suma importancia comprenderla lo que dice la literatura de la aplicación de la Norma ISO 27001:2022 y a las variaciones con respecto a la ISO 27001:2013, por lo que se sugiere una actualización continua por los cambios que se van dando en las versiones.
- Se recomienda continuar con un análisis profundo de los puntos esenciales establecido en la norma ISO/IEC 27001:2022, con el fin de identificar y adoptar buenas prácticas que fortalezcan la seguridad de la información en el GAD de Píllaro de manera actualizada.
- Implementar un sistema actualizado y controlado para gestionar el inventario de activos, también es importante documentar de manera formal los procedimientos para respaldar y recuperar la información, además, se deben establecer políticas claras y mecanismos para controlar el acceso, estas medidas ayudarán a cerrar las diferencias que hay y a cumplir con lo que pide la norma ISO/IEC 27001:2022.
- Se sugiere aplicar y socializar la Guía del Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) con todos los departamentos clave que participan, esto es importante para que cada uno entienda sus responsabilidades dentro del sistema, los límites de la organización y la tecnología, así como los procesos de información que manejan datos sensibles. De esta manera, se asegura una implementación efectiva y coordinada de las medidas de seguridad.
- Finalmente, se sugiere verificar los mapas de procesos sugeridos en las áreas clave del GAD. Estos mapas ayudan a entender mejor cómo fluye la información, permiten identificar de manera clara las actividades, las personas responsables, las decisiones y los controles, y ayudan a gestionar la información de manera más eficiente y segura.

BIBLIOGRAFÍA

Adedoyin, F., & Christiansen, B. (2023). *Effective Cybersecurity Operations for Enterprise-Wide Systems.* New York: IGI Global.

Alemán, H., & Rodríguez, C. (2015). Metodologías para el análisis de riesgos en los sgsi. *Publicaciones e Investigación, 9*, 73-86.

Angulo Chica, D. (2024). *Análisis de un Sistema de Gestión de Seguridad de la Información para la PUCE-E basado en la Norma ISO 27001*. (PUCESE-Escuela de Ingeniería en Tecnologías de la Información) Obtenido de [Tesis]: https://repositorio.puce.edu.ec/handle/123456789/44532

Bala, E., Costales, A., Yñota, J. M., & Ramirez, E. (2022). CONTRAST: An animated short film about rescue against black hat hackers. *2nd International Conference in Information and Computing Research (iCORE)*, 45-48.

Bernal, C. (2016). *Metodología de la investigación* (4ra. ed.). Bogotá, Colombia: Pearson Educación.

Busto-Perez, E. (2024). *Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa Tradu*. (Universitat Oberta de Catalunya) Obtenido de [Tesis]: https://openaccess.uoc.edu/server/api/core/bitstreams/1dfe6bd9-c3ec-42ed-a082-e21afc55904b/content

Casado Robledo, M. J. (2020). Proteger la información ha sido una constante a lo largo de la historia. *Revista Española de Control Externo, XXII*(64), 90-103.

Cerón, C. (2023). Píllaro: cultura, diablada, ecología e historia. Tungurahua - Ecuador. *Revista Homo Educator, 2*(3), 18-28.

Consultores ISO. (2024). *Introducción a la Norma ISO 27001:2022.* GDS & Consultores ISO, SL.

Duarte, O., & Monges, M. (2018). Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001. *Scienti Americana, 5*(2).

Flores Urgilés, C. H., Flores Urgilés, C. M., Carrillo Centeno, J. A., & Andrade Cárdenas, D. P. (2023). Análisis del nivel de cumplimiento de las Políticas de Seguridad de la Información de los GAD's Cantonales Cañar, El Tambo y Suscal. *Pro Sciences Revista de Producción, Ciencias e Investigación, 7*(49), 120-138.

GAD Santiago de Píllaro. (2022). *Resolución Administrativa No. 037-2022*. Obtenido de https://www.pillaro.gob.ec/wp-content/uploads/2016/05/resnormasectorpublico.pdf

GAD Santiago de Píllaro. (2024). *Directorio completo*. Obtenido de https://www.pillaro.gob.ec/wp-content/uploads/2016/05/b1Ene2024.pdf

GAD Santiago de Píllaro. (s.f.). *Misión/Visión*. Obtenido de https://www.pillaro.gob.ec/mision-vision/

GAD Santiago de Píllaro. (s.f.). *Organigrama estructural*. Obtenido de https://www.pillaro.gob.ec/wp-content/uploads/2018/06/Organigrama.pdf

Haufe, K., Colomo, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management . *International Journal of Information Systems and Project Management, 4*(4), 27-47.

Hernández Sampieri, R. (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta* (7ma ed.). México D.F.: Mc Graw Hill Education.

Lolemi, L. (2024). *Qué es ISO 27001 y cómo obtenerla en tu organización*. (INNEVO) Obtenido de https://innevo.com/blog/certificacion-iso-27001-guia-rapida

Mantilla, A. (2017). Gestión de seguridad de la información con la norma ISO 27001:2013. *Revista Espacios, 39*(18), 5.

Martínez, J. (2023). Tipos de investigación. *Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco, 5*(9), 34-35.

Ministerio de Telecomunicaciones y la Sociedad de la información . (2020). *Guía para la gestión de riesgos de seguridad de la información*. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Mogollón Jiménez, K. (2022). *Importancia del Sistema de Gestión de Seguridad de la Información (SGSI) y su incidencia en materia de control interno*. (Universidad Militar Nueva Granada) Obtenido de [Tesis]: https://repository.umng.edu.co/server/api/core/bitstreams/454622d6-fefa-486f-817d-5a7e92029b01/content

Nieves, A. (2017). *Diseño de un siste,a de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013*. Obtenido de https://alejandria.poligran.edu.co/handle/10823/994

PIRANI. (2024). *ISO 27001: de qué se trata y cómo implementarla*. Obtenido de https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Rajeshwari, K. (2024). *ISO 27001:2022 PDF Free Download – Secure Your Organization's Information*. (ISO Docs) Obtenido de https://iso-docs.com/blogs/iso-27001-isms/iso-27001-2022-pdf-free-download

Ramírez Alba, T. (2023). *La ciberseguridad y su incidencia en la gestión de tecnologías de información en una empresa de seguros*. (Repositorio Institucional UCV) Obtenido de [Tesis]: https://repositorio.ucv.edu.pe/handle/20.500.12692/110828

Ramos, R., Cahuaya, R., & Llanqui, R. (2023). IT policy and information security management based on ISO 27001. *Innovation and Software, 4*(1), 96-106.

Risco Villarreal, E. (2021). *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructura Pérez & Pérez SAC*. (Repositorio Institucional UCV) Obtenido de [Tesis]: https://repositorio.ucv.edu.pe/handle/20.500.12692/63424

Tapia, E., Ruiz, R., & Vega, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Mision Jurídica Revista de Derecho y Ciencias Sociales, 14*(20), 142-158.

Tasa Cantanzaro, M., Maquera Quispe, H., Rojas Bujaico, J., & Delgado Rospigliosi, M. (2022). Análisis de información de la gestión de incidentes de seguridad en organizaciones. *PURIQ Revista de Investigación Científica, 4*(e196).

UNIR. (2019). *¿Qué es la certificación ISO 27001 y para qué sirve?* Obtenido de https://www.unir.net/revista/ingenieria/iso-27001/

Urcuqui, C., García, M., Osorio, J., & Navarro, A. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos.* Cali: Editorial Universidad ICESI.

Yungán, J., & Narváez, C. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias, 8*(3), 1025-1041.

ANEXOS

Anexo 1. Entrevista realizada al Director de TI del GAD de Píllaro

Pontificia Universidad Católica del Ecuador | Sede Ambato

Entrevista para el diagnóstico de seguridad de la información en el GAD Santiago de Píllaro

Tema: Análisis del alcance y campo de aplicación de las normas ISO/IES27001:2022 en el GAD Píllaro

Instrucciones:
Las siguientes preguntas buscan recopilar información sobre la gestión de la seguridad de la información, los activos tecnológicos y documentales, los controles existentes, vulnerabilidades y necesidades específicas para el diseño de una guía de alcance y mapas de procesos del SGSI; y, están diseñadas con base en la Cláusula 6.1 (Evaluación de riesgos) y Anexo A (Controles) de la Norma ISO/IEC 27001:2022.
Los datos que se recojan mediante este cuestionario son exclusivamente para uso académico.

A. ACTIVOS DE INFORMACIÓN
1. ¿Qué activos de información considera más críticos para el funcionamiento del GAD y por qué?
2. ¿Cómo se gestionan actualmente los inventarios de activos tecnológicos y documentales?
3. ¿Existen activos compartidos entre los departamentos? ¿Cómo se controla su acceso?
B. PROCESOS Y FLUJOS DE INFORMACIÓN
4. Describa los principales procesos o flujos de información entre el área de TI y los departamentos Financiero, Avalúos y Catastros, Administrativo y Desarrollo Organizacional, y Administración de Justicia.
5. ¿Cuáles son los puntos más vulnerables o problemáticos en esos flujos?
6. ¿Qué controles existen para garantizar la confidencialidad, integridad y disponibilidad de la información en esos procesos?
C. SEGURIDAD TECNOLÓGICA Y OPERATIVA
7. ¿Cuáles son las políticas o procedimientos existentes para respaldos y recuperación de datos?
8. ¿Qué mecanismos de autenticación y control de acceso se utilizan en los sistemas institucionales?
9. ¿Qué nivel de actualización tienen los servidores y sistemas operativos?
10. ¿Qué riesgos tecnológicos ha identificado en los últimos años?

D. GESTIÓN DE INCIDENTES Y MEJORA CONTINUA
11. ¿Cómo se gestiona actualmente la respuesta ante incidentes de seguridad de la información?
12. ¿Se realiza algún análisis o evaluación de riesgos? ¿Con qué frecuencia?
13. ¿Qué necesidades o mejoras considera prioritarias para fortalecer la seguridad de la información en el GAD?

Muchas gracias por su colaboración

Anexo 2. Encuesta dirigida al personal técnico de TI y usuarios de las áreas clave

Pontificia Universidad Católica del Ecuador | Sede Ambato

Encuesta sobre prácticas de seguridad de la información en el GAD Santiago de Píllaro

Tema: Análisis del alcance y campo de aplicación de las normas ISO/IES27001:2022 en el GAD Píllaro

La aplicación de esta encuesta forma parte de un proyecto académico de investigación cuyo objetivo es obtener la percepción del personal técnico del área de TI y de los usuarios clave de los departamentos estratégicos sobre el manejo de activos, flujos de información, controles de seguridad, respaldo de datos y necesidades de mejora, para fundamentar el diseño de una guía de alcance y mapas de procesos del SGSI conforme a la norma ISO/IEC 27001:2022.
Los datos que se recojan mediante este cuestionario son exclusivamente para uso académico.

INSTRUCCIONES

Lea cada afirmación y seleccione la opción que mejor represente su nivel de acuerdo.

A. GESTIÓN DE ACTIVOS DE INFORMACIÓN

1. Conozco los activos de información con los que trabajo o administro.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

2. Existe un registro claro y actualizado de los activos de información utilizados en mi área.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

3. Los activos de información son gestionados considerando su nivel de criticidad o sensibilidad.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

B. FLUJOS DE INFORMACIÓN Y PROCESOS

4. Los procesos de intercambio de información entre áreas están bien definidos.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

5. El flujo de información en mi área sigue lineamientos claros de seguridad.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

6. Identifico puntos vulnerables o riesgosos en la forma en que se comparte la información.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

C. RESPALDO Y RECUPERACIÓN DE DATOS

7. Los respaldos de información se realizan con la frecuencia necesaria.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

8. Existen procedimientos claros para recuperar datos en caso de incidentes.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

9. Confío en que la información crítica de mi área se respalda de forma segura

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

D. CONTROLES DE ACCESO Y AUTENTICACIÓN

10. El acceso a los sistemas o información está bien controlado mediante credenciales o permisos.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

11. Se respetan los niveles de privilegio establecidos para cada usuario.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

12. Percibo que se monitorean o auditan los accesos a la información sensible

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

E. PERCEPCIÓN DE RIESGOS Y NECESIDADES

13. He recibido capacitación o indicaciones sobre seguridad de la información en el GAD.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

14. Considero que se realiza una adecuada evaluación de riesgos de seguridad.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

15. Es necesario fortalecer las políticas y procedimientos de seguridad de la información en mi área.

Totalmente en desacuerdo ☐
En desacuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
De acuerdo ☐
Totalmente de acuerdo ☐

Muchas gracias por su colaboración

PUCE | AMBATO

GUÍA

ANÁLISIS DEL ALCANCE Y CAMPO DE APLICACIÓN DE LAS NORMAS

ISO/ICE 27001:2022

GAD PILLARO

AUTORA

NADIA CUYAGO

DIRECTORA

MG. LILIANA MENA

CONTENIDO

01

Introducción

La presente Guía del Alcance del Sistema de Gestión de Seguridad de la Información para el Gobierno Autónomo Descentralizado Santiago de Píllaro, se basa en los requisitos establecidos por la norma ISO/IEC 27001:2022. Se busca definir de forma clara y documentada los límites, exclusiones, procesos cubiertos, activos protegidos, departamentos implicados y responsabilidades institucionales que en conjunto permitirán garantizar la confidencialidad, integridad y disponibilidad de la información crítica para el funcionamiento municipal.

Este alcance es el punto de partida para la implantación del SGSI, pues define las áreas, activos y procesos organizativos que estarán sometidos a controles de seguridad, en coherencia con los objetivos estratégicos institucionales y la gestión de riesgos tecnológicos identificados en el diagnóstico previo. Esta guía servirá de referencia para planificar, implementar, operar, monitorear, revisar y mejorar el SGSI de forma sistemática y alineada con estándares internacionales, asegurando la confianza ciudadana y el cumplimiento legal.

02

Objetivo de la guía de alcance

Establecer formalmente el alcance del SGSI del GAD de Píllaro, delimitando con precisión los departamentos involucrados, los procesos críticos, los activos de información que requieren protección y los controles necesarios, así como definir las exclusiones, responsabilidades institucionales y principios rectores para la gestión de la seguridad de la información, conforme a la norma ISO/IEC 27001:2022.

03

Principios rectores y lineamientos normativos

El SGSI abarca tanto los sistemas informáticos como los procesos documentales y físicos asociados, incluyendo actividades internas y flujos de información interdepartamentales. Su aplicación será obligatoria para todo el personal involucrado en el tratamiento de información institucional.

- Inventario y clasificación de activos de información: Identificación, categorización y valoración de datos en función de su criticidad y sensibilidad.
- Gestión de identidades y accesos: Definición de roles, permisos y autenticación, incluyendo controles avanzados como autenticación multifactor.
- Control y monitoreo de accesos: Registro, auditoría y supervisión de actividades de usuarios en sistemas críticos.
- Respaldo y recuperación ante incidentes: Políticas, procedimientos documentados y pruebas periódicas.
- Intercambio de información interdepartamental: Definición de flujos estandarizados y seguros.
- Gestión de incidentes de seguridad: Reporte, análisis, documentación, comunicación y respuesta coordinada.
- Continuidad del negocio: Procedimientos para asegurar la operación ante fallas o desastres.
- Capacitación y concienciación: Formación continua del personal sobre seguridad de la información y buenas prácticas.
- Evaluación y tratamiento de riesgos: Metodología sistemática para identificar amenazas, vulnerabilidades y aplicar controles adecuados.

04

Alcance del SGI

La definición del alcance del SGSI se sustenta en los siguientes principios, inspirados en los controles y buenas prácticas de la norma ISO/IEC 27001:2022:

- Confidencialidad: Garantizar que la información solo sea accesible a personal autorizado, previniendo filtraciones y accesos indebidos.
- Integridad: Proteger la exactitud y completitud de los datos, asegurando que no sean alterados de manera no autorizada o accidental.
- Disponibilidad: Asegurar el acceso oportuno y confiable a la información y los sistemas cuando sea requerido para la prestación de servicios.
- Enfoque basado en riesgos: Identificar, analizar, evaluar y tratar de forma sistemática los riesgos asociados a la seguridad de la información.
- Ciclo de mejora continua: Aplicar la metodología PDCA (Planificar, Hacer, Verificar y Actuar) para mantener y mejorar el SGSI.
- Cumplimiento legal y normativo: Respetar las leyes locales, regulaciones sectoriales y compromisos contractuales aplicables.
- Responsabilidad compartida: Involucrar a todas las áreas institucionales para identificar activos, riesgos y controles específicos.

05

Procesos incluidos

El SGSI abarca tanto los sistemas informáticos como los procesos documentales y físicos asociados, incluyendo actividades internas y flujos de información interdepartamentales. Su aplicación será obligatoria para todo el personal involucrado en el tratamiento de información institucional.

- Inventario y clasificación de activos de información: Identificación, categorización y valoración de datos en función de su criticidad y sensibilidad.
- Gestión de identidades y accesos: Definición de roles, permisos y autenticación, incluyendo controles avanzados como autenticación multifactor.
- Control y monitoreo de accesos: Registro, auditoría y supervisión de actividades de usuarios en sistemas críticos.
- Respaldo y recuperación ante incidentes: Políticas, procedimientos documentados y pruebas periódicas.
- Intercambio de información interdepartamental: Definición de flujos estandarizados y seguros.
- Gestión de incidentes de seguridad: Reporte, análisis, documentación, comunicación y respuesta coordinada.
- Continuidad del negocio: Procedimientos para asegurar la operación ante fallas o desastres.
- Capacitación y concienciación: Formación continua del personal sobre seguridad de la información y buenas prácticas.
- Evaluación y tratamiento de riesgos: Metodología sistemática para identificar amenazas, vulnerabilidades y aplicar controles adecuados.

06

Activos de información cubiertos

- Bases de datos institucionales (financieras, catastrales, administrativas y legales).
- Expedientes físicos y electrónicos (contratos, actas, resoluciones).
- Sistemas informáticos y aplicaciones de gestión municipal.
- Infraestructura tecnológica (servidores, redes, equipos de respaldo).
- Sistemas de almacenamiento físico y digital de respaldos.
- Contraseñas, credenciales, claves criptográficas.
- Documentos de soporte, informes y registros administrativos.

07

Exlusiones

- Información y procesos que sean responsabilidad exclusiva de proveedores externos con sus propios SGSI certificados.
- Datos y servicios de sistemas o plataformas ajenas sin vínculo contractual con el GAD de Píllaro.
- Procesos no relacionados con la gestión municipal o con la prestación de servicios a la ciudadanía.

08

Limitaciones

- Recursos limitados para actualización tecnológica.
- Falta de personal especializado en seguridad de la información.
- Dependencia de software con obsolescencia tecnológica.
- Cultura organizacional incipiente en seguridad de la información.

09

Elementos a definir

- Política de seguridad de la información: Documento aprobado por la Dirección que declare el compromiso institucional, los objetivos y los lineamientos generales.
- Organización de la seguridad: Definición de roles y responsabilidades, creación del Comité de Seguridad de la Información.
- Gestión de activos: Elaboración y mantenimiento de inventarios, clasificación por criticidad y nivel de sensibilidad.
- Seguridad de recursos humanos: Cláusulas de confidencialidad, inducción, formación continua y sensibilización.
- Seguridad física y del entorno: Controles de acceso físico, protección frente a desastres, mantenimiento de infraestructuras.
- Gestión de operaciones y comunicaciones: Procedimientos documentados, control de cambios, monitoreo de servicios.
- Control de accesos: Políticas de gestión de identidades, autenticación multifactor, segregación de funciones.
- Adquisición, desarrollo y mantenimiento de sistemas: Requisitos de seguridad en software, actualizaciones periódicas.
- Gestión de incidentes: Mecanismos de reporte, análisis de causas raíz, acciones correctivas y preventivas.
- Continuidad de operaciones y recuperación ante desastres: Planes documentados y probados para asegurar la operación.
- Conformidad: Cumplimiento legal, auditorías internas y revisiones de la Dirección de TI.

10

Responsables y actores del SGI

- Alta dirección del GAD: Aprobación formal del alcance, asignación de recursos, definición de políticas y liderazgo del cambio.
- Área de Tecnologías de la Información: Implementación de controles técnicos, administración de accesos, realización de respaldos, gestión de incidentes y soporte técnico.
- Departamentos estratégicos: Identificación de activos, definición de procesos sensibles, colaboración en la implementación y mejora de controles.
- Usuarios finales: Cumplimiento de políticas, reporte de incidentes, participación en actividades de concienciación.
- Comité de Seguridad de la Información: Instancia de coordinación, seguimiento y mejora continua del SGSI.

11

Mapas de procesos

La elaboración de mapas de procesos es fundamental para el diseño e implementación de un SGSI, conforme a la norma ISO/IEC 27001:2022. Con ellos, se podrá visualizar de manera estructurada los flujos de información, las actividades, las áreas involucradas, los puntos de interacción y los controles aplicados, además, se podrán identificar los riesgos, estandarizar de procedimientos y mejorar de manera continua la seguridad de la información institucional.

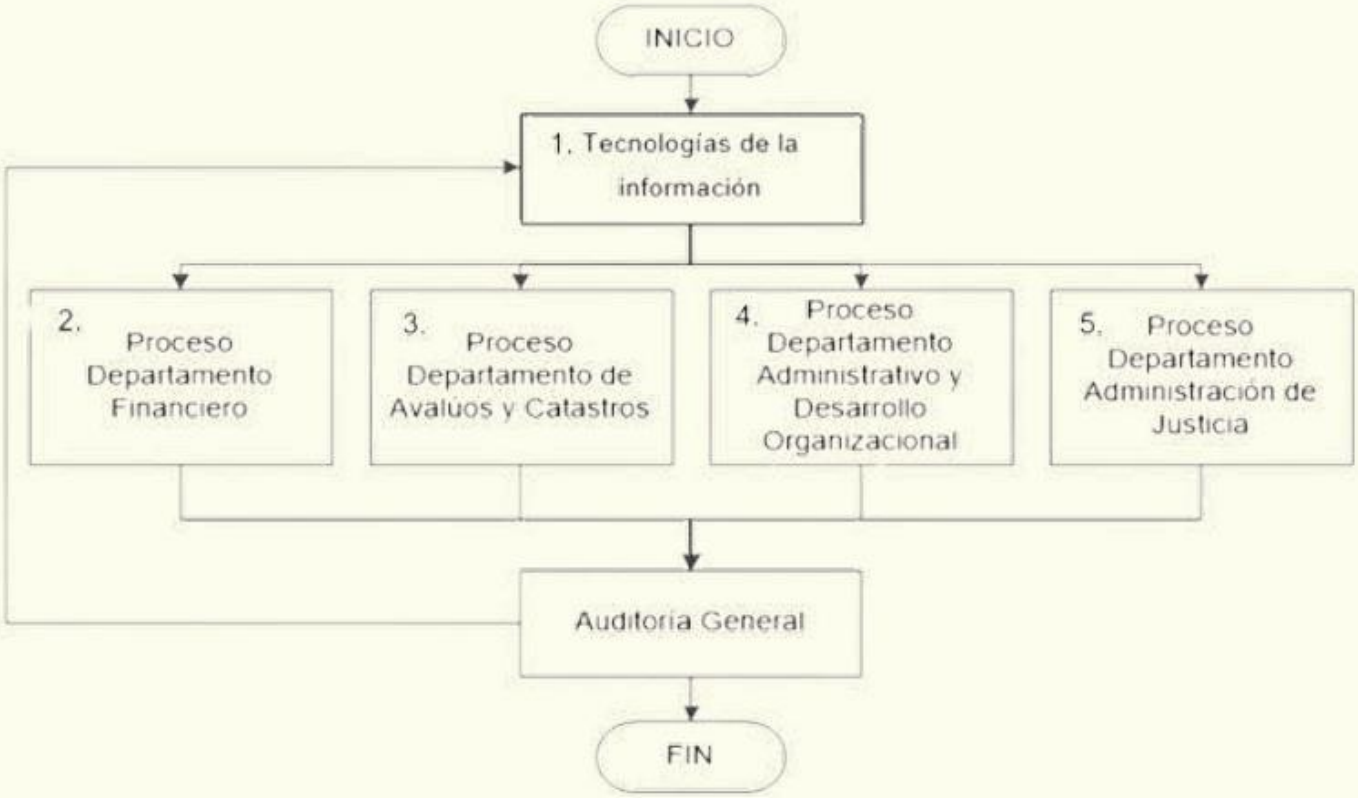


DIAGRAMA DEL MACRO PROCESO DEL SGSI

PROCESO DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN

Etapa del proceso	Descripción	Responsable	Entrada principal	Salida principal	Controles de seguridad aplicados
1. Identificación de activos	Registrar servidores, bases de datos, aplicaciones y respaldos.	Jefe de TI	Listado físico y digital	Inventario actualizado	Control de accesos al inventario, clasificación por nivel de sensibilidad.
2. Gestión de usuarios y accesos	Creación y parametrización de cuentas en Active Directory.	Personal de TI	Solicitud de acceso autorizada	Cuenta de usuario creada/modificada	Autenticación, permisos basados en roles, doble factor (propuesta futura).
3. Respaldo de información	Realización de respaldos diarios y mensuales.	Técnico de TI	Bases de datos y archivos críticos	Archivos de respaldo	Almacenamiento seguro fuera del DataCenter, política de cifrado (propuesta futura).
4. Recuperación de datos	Restauración de datos en caso de fallos o incidentes.	Personal de TI	Solicitud de recuperación	Datos restaurados	Procedimientos documentados, pruebas regulares, registro de incidentes.
5. Monitoreo y auditoría de accesos	Revisión de logs y registros de actividad en servidores y sistemas.	Jefe de TI	Logs del sistema	Reporte de monitoreo	Auditoría interna, alarmas automáticas (propuesta futura), registros inalterables.
6. Gestión de incidentes de seguridad	Registro y análisis de incidentes, comunicación a departamentos.	Área de TI Comité de SGSI	Reporte de incidente	Plan de respuesta ejecutado	Registro formal, análisis de causa raíz, plan de acción correctiva.
7. Actualización de infraestructura	Mantenimiento y renovación de servidores, licencias y sistemas.	Área de TI	Plan de actualización	Infraestructura actualizada	Control de versiones, eliminación de software obsoleto.
8. Capacitación interna	Formación técnica sobre seguridad de la información para el personal de TI.	Área de TI Comité de SGSI	Plan de formación	Personal capacitado	Registro de asistencia, evaluación del aprendizaje.

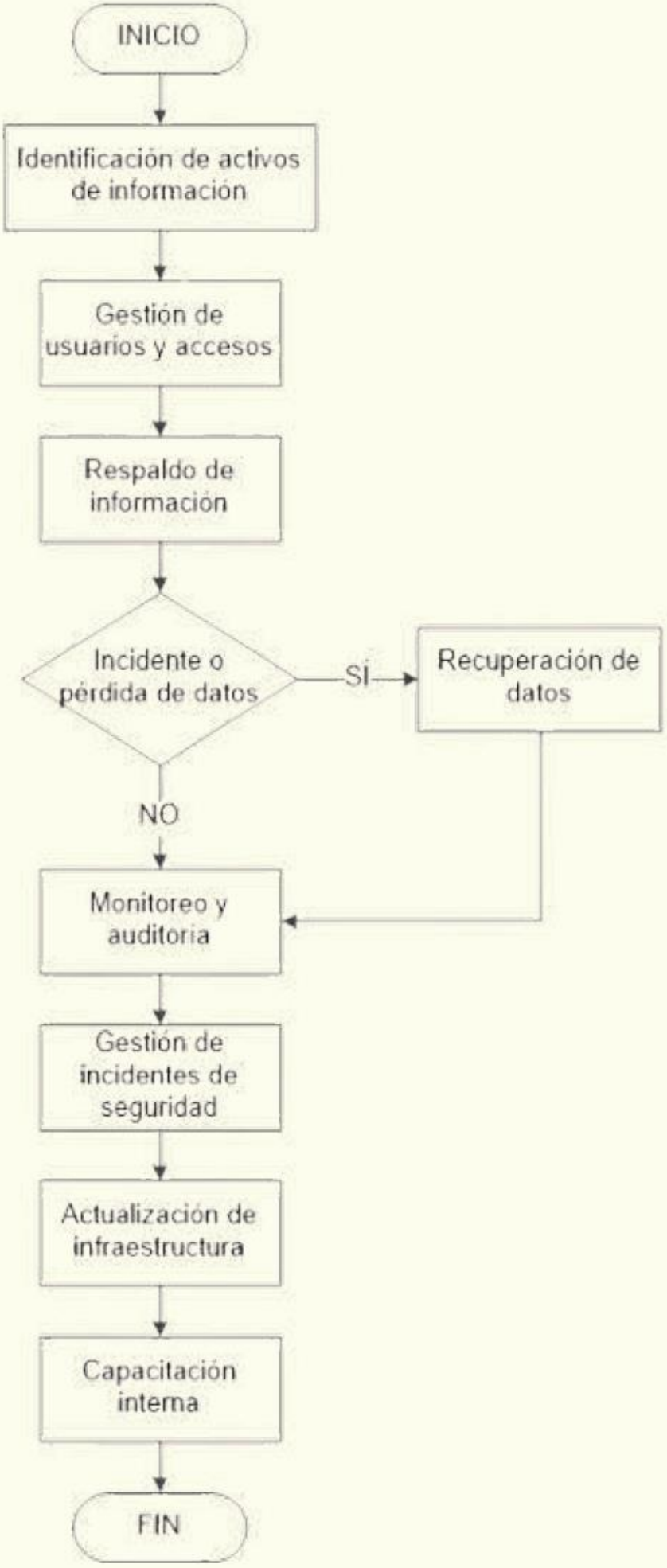


DIAGRAMA DE FLUJO DEL PROCESO DE TECNOLOGÍAS DE LA INFORMACIÓN

PROCESO DEL DEPARTAMENTO FINANCIERO

Etapa del proceso	Descripción breve	Responsable	Entrada principal	Salida principal	Controles de seguridad aplicados
1. Identificación de activos financieros	Bases de datos, presupuestos, informes y respaldos.	Director Financiero	Documentos físicos/digitales	Inventario de activos financieros	Clasificación por criticidad, controles de acceso.
2. Solicitud de creación de usuarios	Solicitudes de alta o modificación de cuentas para sistemas financieros.	Personal Financiero TI	Formulario autorizado	Solicitud procesada	Firma autorizada, verificación de roles.
3. Acceso a sistemas financieros	Aplicaciones contables y presupuestarias con cuentas personalizadas.	Personal Financiero	Credenciales del usuario	Transacciones financieras registradas	Control de accesos basado en roles, autenticación individual.
4. Manejo de datos sensibles	Información tributaria, pagos, presupuestos, informes confidenciales.	Personal Financiero	Datos ciudadanos / proveedores	Procesos contables actualizados	Restricciones de acceso, control de impresiones y exportaciones.
5. Intercambio de información con TI	Comunicación para respaldos, mantenimiento y soporte técnico.	Personal Financiero TI	Solicitud de respaldo o soporte	Respaldo confirmado / incidente resuelto	Canales institucionales seguros, registros de solicitud y cierre.
6. Respaldo de información	Coordinar para respaldos de datos financieros.	Personal Financiero y TI	Archivos contables	Copias de respaldo almacenadas	Procedimiento documentado, almacenamiento seguro.
7. Recuperación de información	Solicitud de restauración de datos en caso de pérdida o incidente.	Personal Financiero TI	Solicitud de recuperación	Datos restaurados	Control de acceso al proceso de restauración, registro del incidente.
8. Monitoreo y auditoría	Verificación periódica de accesos y transacciones en sistema financiero.	Director Financiero TI	Logs del sistema	Informe de auditoría	Análisis de logs, auditorías internas, alarmas de actividad sospechosa.
9. Capacitación y concienciación	Formación del personal financiero en manejo seguro de información y políticas del SGSI.	Dirección Financiera Comité SGSI	Plan de capacitación	Personal sensibilizado	Registro de asistencia, contenido validado, evaluación del aprendizaje.

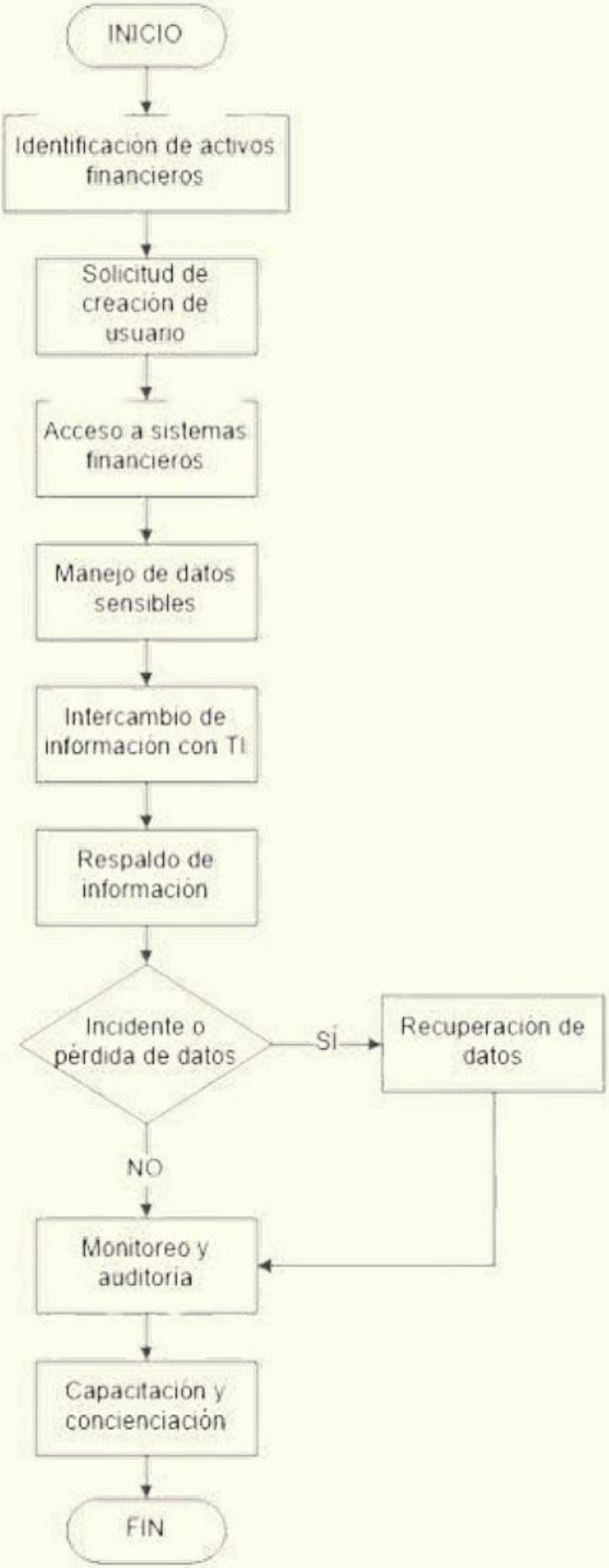


DIAGRAMA DE FLUJO DEL PROCESO DEL DEPARTAMENTO FINANCIERO

MAPA DE PROCESOS DEL DEPARTAMENTO DE AVALÚOS Y CATASTROS

Etapa del proceso	Descripción breve	Responsable	Entrada principal	Salida principal	Controles de seguridad aplicados
1. Identificación de activos catastrales	Registro de bases de datos, planos, expedientes físicos y digitales.	Director de Avalúos y Catastros	Documentos y archivos	Inventario de activos actualizado	Clasificación por criticidad y sensibilidad, control de acceso.
2. Solicitud de creación de usuarios	Gestión de solicitudes para acceso a sistemas de catastros.	Personal de Avalúos / Área de TI	Formulario autorizado	Solicitud procesada	Firma responsable, verificación de roles.
3. Acceso a sistemas catastrales	Uso de aplicaciones para gestión de catastros y avalúos.	Personal de Avalúos	Credenciales del usuario	Actualización de registros catastrales	Control de accesos basado en roles, autenticación individual.
4. Manejo de datos sensibles	Gestión de información territorial, predial y datos de contribuyentes.	Personal de Avalúos	Datos de catastros	Registros actualizados	Restricciones de acceso, control de exportación e impresión.
5. Intercambio de información con TI	Coordinación para respaldos, soporte técnico y mantenimiento.	Personal de Avalúos / Área de TI	Solicitud de respaldo o soporte	Respaldo confirmado / incidente resuelto	Canales institucionales seguros, registro de solicitudes y resolución.
6. Respaldo de información	Coordinación y ejecución de respaldos diarios/mensuales de datos catastrales.	Personal de Avalúos / Área de TI	Archivos y bases de datos catastrales	Copias de respaldo almacenadas	Procedimiento documentado, almacenamiento seguro.
7. Recuperación de información	Solicitud de restauración de datos en caso de incidentes.	Personal de Avalúos / Área de TI	Solicitud de recuperación	Datos restaurados	Control de acceso al proceso de restauración, registro del incidente.
8. Monitoreo y auditoría	Verificación periódica de accesos y modificaciones a registros catastrales.	Director de Avalúos / Área de TI	Logs del sistema	Informe de auditoría	Revisión de logs, alarmas de actividad sospechosa, auditorías internas.
9. Capacitación y concienciación	Formación del personal sobre manejo seguro de información y políticas del SGSI.	Dirección de Avalúos / Comité de SGSI	Plan de capacitación	Personal capacitado	Registro de asistencia, contenido validado, evaluación del aprendizaje.

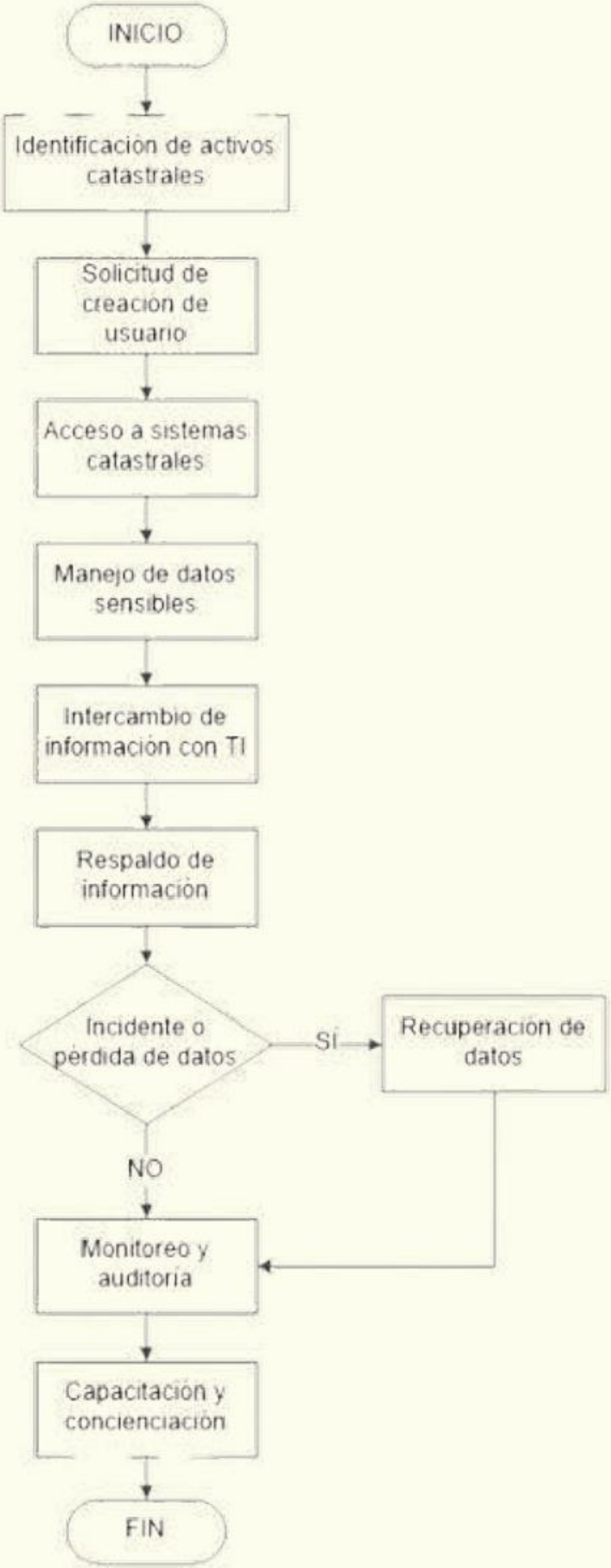


DIAGRAMA DE FLUJO DEL PROCESO DEL DEPARTAMENTO DE AVALUOS Y CATASTROS

PROCESO DEL DEPARTAMENTO ADMINISTRATIVO Y DESARROLLO ORGANIZACIONAL

Etapa del proceso	Descripción breve	Responsable	Entrada principal	Salida principal	Controles de seguridad aplicados
1. Identificación de activos administrativos	Registro de expedientes, datos de personal, comunicaciones oficiales.	Director Administrativo	Documentos y archivos	Inventario de activos actualizado	Clasificación por criticidad y sensibilidad, control de acceso.
2. Solicitud de creación de usuarios	Solicitudes de acceso a sistemas administrativos e institucionales.	Personal Administrativo / Área de TI	Formulario autorizado	Solicitud procesada	Firma responsable, verificación de roles.
3. Acceso a sistemas administrativos	Uso de sistemas para trámites internos, recursos humanos y atención ciudadana.	Personal Administrativo	Credenciales del usuario	Registros administrativos actualizados	Control de accesos basado en roles, autenticación individual.
4. Manejo de datos sensibles	Información de personal, contrataciones, permisos y comunicación institucional.	Personal Administrativo	Datos del personal y de procesos	Actualización de registros	Restricciones de acceso, control de impresión y exportación de datos.
5. Intercambio de información con TI	Coordinación para respaldos, soporte técnico y mantenimiento.	Personal Administrativo / Área de TI	Solicitud de respaldo o soporte	Respaldo confirmado / incidente resuelto	Canales institucionales seguros, registro de solicitudes y resolución.
6. Respaldo de información	Coordinación y ejecución de respaldos de expedientes y archivos administrativos.	Personal Administrativo / Área de TI	Archivos administrativos	Copias de respaldo almacenadas	Procedimiento documentado, almacenamiento seguro.
7. Recuperación de información	Solicitud de restauración de datos en caso de incidente o pérdida.	Personal Administrativo / Área de TI	Solicitud de recuperación	Datos restaurados	Control de acceso al proceso de restauración, registro del incidente.
8. Monitoreo y auditoría	Verificación periódica de accesos y modificaciones a registros administrativos.	Director Administrativo / Área de TI	Logs del sistema	Informe de auditoría	Análisis de logs, alarmas de actividad sospechosa, auditorías internas.
9. Capacitación y concienciación	Formación sobre políticas de seguridad de la información y manejo responsable de datos.	Dirección Administrativa / Comité de SGSI	Plan de capacitación	Personal sensibilizado	Registro de asistencia, contenido validado, evaluación del aprendizaje.

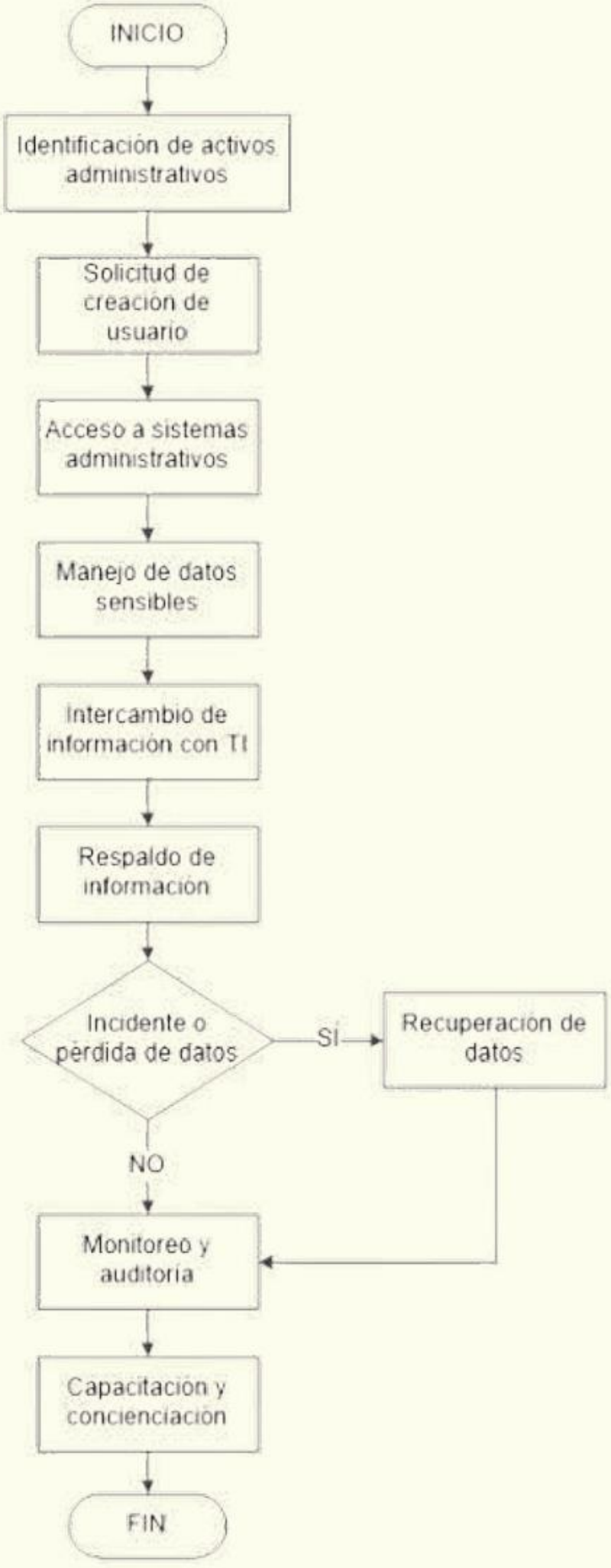


DIAGRAMA DE FLUJO DEL PROCESO DEL DEPARTAMENTO ADMINISTRATIVO

PROCESO DEL DEPARTAMENTO DE ADMINISTRACIÓN DE JUSTICIA

Etapa del proceso	Descripción breve	Responsable	Entrada principal	Salida principal	Controles de seguridad aplicados
1. Identificación de activos jurídicos	Registro de expedientes legales, resoluciones, actas, archivos físicos y digitales.	Jefe de Administración de Justicia	Documentos y archivos	Inventario de activos actualizado	Clasificación por sensibilidad y criticidad, control de acceso.
2. Solicitud de creación de usuario	Solicitudes para acceso a sistemas jurídicos internos.	Personal de Justicia / TI	Formulario autorizado	Solicitud procesada	Firma responsable, verificación de roles.
3. Acceso a sistemas jurídicos	Uso de sistemas para gestión de expedientes y resoluciones.	Personal de Justicia	Credenciales del usuario	Registro judicial actualizados	Control de accesos, autenticación individual.
4. Manejo de datos sensibles	Gestión de información confidencial sobre procesos judiciales y sanciones administrativas.	Personal de Justicia	Expedientes y resoluciones	Actualización de registros jurídicos	Restricciones de acceso, control de exportación, protección de integridad documental.
5. Intercambio de información con TI	Coordinación para respaldos, soporte técnico y mantenimiento.	Personal de Justicia / Área de TI	Solicitud de respaldo o soporte	Respaldo confirmado / incidente resuelto	Canales institucionales seguros, registro de solicitudes y resolución.
6. Respaldo de información	Coordinación y ejecución de respaldos periódicos de expedientes y bases de datos legales.	Personal de Justicia / Área de TI	Archivos jurídicos	Copias de respaldo almacenadas	Procedimiento documentado, almacenamiento seguro, cifrado propuesto.
7. Recuperación de información	Solicitud de restauración de datos en caso de incidente o pérdida.	Personal de Justicia / Área de TI	Solicitud de recuperación	Datos restaurados	Control de acceso al proceso de restauración, registro del incidente.
8. Monitoreo y auditoría	Verificación periódica de accesos y modificaciones en registros jurídicos y sistemas.	Jefe de Justicia / Área de TI	Logs del sistema	Informe de auditoría	Análisis de logs, alarmas de actividad sospechosa, auditorías internas.
9. Capacitación y concienciación	Formación sobre manejo de información y cumplimiento de políticas del SGSI.	Dirección de Justicia / Comité de SGSI	Plan de capacitación	Personal capacitado	Registro de asistencia, contenidos validados, evaluación del aprendizaje.

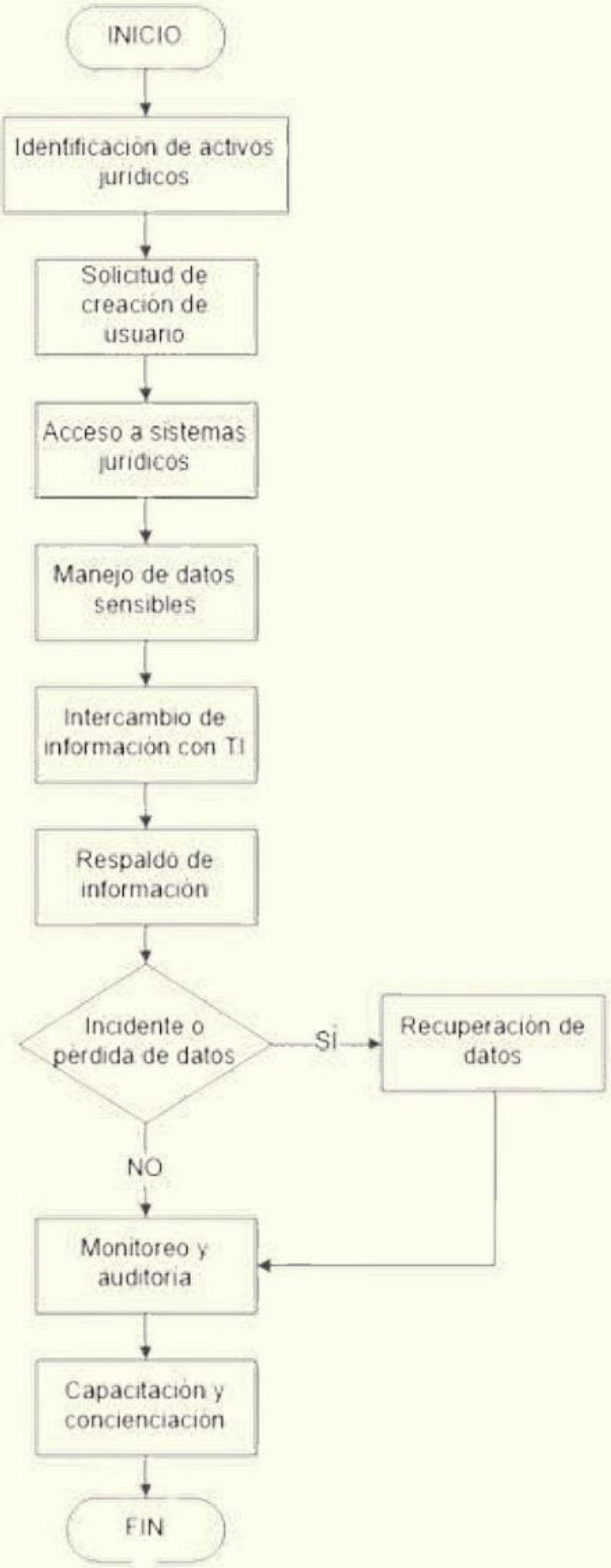


DIAGRAMA DE FLUJO DEL PROCESO DEPARTAMENTO DE ADMINISTRACIÓN DE JUSTICIA

12

Recomendaciones

- Se recomienda establecer liderazgo institucional sólido, garantiza el compromiso visible y sostenido de la alta dirección del GAD, mediante la asignación de recursos adecuados, apoyo a la política de seguridad y respaldo a las iniciativas de mejora continua.

- Implementar un sistema actualizado y controlado para gestionar el inventario de activos, también es importante documentar de manera formal los procedimientos para respaldar y recuperar la información, además, se deben establecer políticas claras y mecanismos para controlar el acceso, estas medidas ayudarán a cerrar las diferencias que hay y a cumplir con lo que pide la norma ISO/IEC 27001:2022.

- Se sugiere aplicar y socializar la Guía del Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) con todos los departamentos clave que participan, esto es importante para que cada uno entienda sus responsabilidades dentro del sistema, los límites de la organización y la tecnología, así como los procesos de información que manejan datos sensibles. De esta manera, se asegura una implementación efectiva y coordinada de las medidas de seguridad.

- De igual manera se recomienda aplicar controles de acceso eficaces ya que permite establecer mecanismos de autenticación robusta, como el uso de contraseñas seguras, autenticación multifactor (MFA) y permisos basados en roles, minimizando el riesgo de accesos no autorizados.

- Finalmente se recomienda realizar respaldos periódicos de los sistemas críticos, probar regularmente los planes de recuperación y almacenar copias de seguridad en ubicaciones seguras y separadas del entorno operativo.

13

Glosario

Activo de información

Cualquier dato, documento, sistema, recurso tecnológico o soporte que tenga valor para la organización y que debe ser protegido.

Autenticación multifactor (MFA)

Mecanismo de seguridad que requiere más de un método de verificación para acceder a un sistema, generalmente combinando algo que el usuario sabe (contraseña), tiene (token) o es (biometría).

Confidencialidad

Principio que garantiza que la información solo sea accesible por personas autorizadas.

Control de accesos

Conjunto de mecanismos que limitan el acceso a recursos informáticos únicamente a usuarios autorizados.

Disponibilidad

Capacidad de la información de estar accesible y utilizable cuando sea requerida.

Gestión de riesgos

Proceso mediante el cual se identifican, analizan, evalúan y tratan los riesgos relacionados con la seguridad de la información.

Incidente de seguridad

Evento que compromete la confidencialidad, integridad o disponibilidad de la información.

Integridad

Propiedad de la información que asegura que los datos no han sido alterados de manera no autorizada.

ISO/IEC 27001:2022

Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).

PDCA (Plan-Do-Check-Act)

Ciclo de mejora continua que guía la implementación y mantenimiento de un SGSI eficaz.

Respaldo

Copia de seguridad de información crítica para su recuperación en caso de pérdida o incidente.

SGSI (Sistema de Gestión de Seguridad de la Información)

Conjunto de políticas, procedimientos y controles que garantizan la protección de la información en una organización.

Vulnerabilidad

Debilidad que puede ser explotada por una amenaza para dañar o comprometer un activo de información.

Comité de Seguridad de la Información

Grupo encargado de coordinar y supervisar la implementación del SGSI y sus mejoras continuas.

Departamento estratégico

Unidad organizacional que maneja procesos o activos clave para la operación institucional, como TI, financiero, administrativo, entre otros

PUCE | AMBATO

AUTORA

NADIA CUYAGO

DIRECTORA

MG. LILIANA MENA