Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.

Fernández Orozco, Gabriela Paulina

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Msc. Pinto Auz, Diego Julián

30 de septiembre del 2021

URKUND

DIEGO JULIAN

Urkund Analysis Result

Analysed Document:	TESIS_GABRIELA FERNÁNDEZ_Versión Final_MGS.pdf (D112176848)
Submitted:	9/7/2021 1:56:00 PM
Submitted By:	biblioteca@espe.edu.ec
Significance:	6 %

Sources included in the report:

1521516145_615__PROYECTO%252BFINAL%252BNORMAS%252BISO%252B27001.pdf (D36730975)
1521427876_149__PROYECTOS%252BJORGE%252BDURAN.docx (D36684044)
TESIS YAN MARZO 2017.pdf (D26148636)
13723-Nuñez Noriega, Diego Adrián.pdf (D46605620)
http://repositorio.unesum.edu.ec/bitstream/53000/2581/1/MAYANQUER%20ANDINO%20JAVIER%20ANIBAL.pdf
https://docplayer.es/87510289-Realizar-un-sistema-de-gestion-de-seguridad-informatica-para-centro-educativo-de-sistemas-uparsistem-de-acuerdo-a-la-normativa-iso-iec.html
https://sig.mineducacion.gov.co/files/mod_documentos/documentos/PM-FT-10/PM-FT-10%20V3.xlsx
https://www.red-tic.unam.mx/content/iso-27001-0
https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27001.pdf
https://dspace.ups.edu.ec/handle/123456789/10372
https://1library.co/title/implementacion-sistema-gestion-iso-proteger-informacion-procesos
https://repository.unad.edu.co/bitstream/handle/10596/23954/%20%2509jearaquei.pdf?sequence=1&isAllowed=y
http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456
https://repositorio.uta.edu.ec/bitstream/123456789/26537/1/Tesis_%20t1318si.pdf
https://digitk.areandina.edu.co/bitstream/handle/areandina/2767/Seguridad%20de%20la%20Informaci%C3%B3n%20en%20una%20empresa%20de%20seguridad%20privada%20de%20Pereira.pdf?sequence=1&isAllowed=y
http://repositorio.utp.edu.pe/bitstream/UTP/2870/1/Liseth%20Cajusol_Trabajo%20de%20Investigacion_Bachiller_2020.pdf
http://polux.unipiloto.edu.co:8080/00003862.pdf
http://repository.ean.edu.co/bitstream/10882/9521/2/FonsecaOmar2019_Anexo.pdf
https://docplayer.es/80491606-Universidad-nacional-del-centro-del-peru-metodologia-para-la-seguridad-de-tecnologias-de-informacion-y-comunicaciones-en-la-clinica-ortega.html
https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12927/1/1065573091.pdf

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí**" fue realizado por la señorita ***Fernández Orozco, Gabriela Paulina*** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 30 de septiembre del 2021

Firma:

Pinto Auz, Diego Julián

Director

C.C.: 1710807072

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo, ***Fernández Orozco, Gabriela Paulina***, con cédula de ciudadanía n° 060445161-7, declaro que el contenido, ideas y criterios del trabajo de titulación: **Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 30 de septiembre del 2021

Firma:

Fernández Orozco, Gabriela Paulina

C.C.: 060445161-7

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo, ***Fernández Orozco, Gabriela Paulina,*** con cédula de ciudadanía n° 060445161-7, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 30 de septiembre del 2021

Firma:

Fernández Orozco, Gabriela Paulina

C.C.: 060445161-7

DEDICATORIA

A mi madre, por su apoyo incondicional a lo largo de mi formación personal y profesional, por siempre ser mi motivación con su ejemplo de respeto, humildad, justicia y perseverancia. Gracias mami por nunca soltarme la mano en los momentos más difíciles, éste logro es para usted.

A mi padre, que desde el cielo sé que me envía sus bendiciones para continuar en la lucha por lograr mis metas.

Gabriela Paulina Fernández Orozco

AGRADECIMIENTO

Gracias a Dios por guiarme en el camino del bien. A la Universidad de las Fuerzas Armadas ESPE por haberme formado como profesional de cuarto nivel, en especial al Ing. Diego Pinto por su tutoría en el desarrollo del presente proyecto. A la Ing. Marcela Riera por su colaboración y predisposición en el levantamiento de información en la unidad de informática de la Municipalidad. A mi gran amiga Suyi, a toda mi familia y a cada una de las personas que de una u otra forma contribuyeron para la finalización de éste trabajo.

Gabriela Paulina Fernández Orozco

INDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El proyecto tiene como objetivo el diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, se aplica a la disminución de riesgos en el almacenamiento de información de la unidad de informática del GAD Municipal del Cantón Pujilí. La norma permite el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, fomenta a que las organizaciones desarrollen una cultura de seguridad, asegurando la continuidad del negocio. La gestión de la seguridad de la información se complementa con las buenas prácticas establecidas en la norma ISO 27002. Para llevar a cabo el estudio se establece el problema, los objetivos, la justificación, importancia y alcance. Se aborda la conceptualización, así como la descripción de la normativa de seguridad de la información en Ecuador. Se describen las principales metodologías de análisis de riesgos. El diseño del sistema de gestión parte estableciendo el alcance, la metodología de análisis de riesgos, el inventario de activos, la identificación de las amenazas y vulnerabilidades, la evaluación de los riesgos, el establecimiento de los controles y la declaración de aplicabilidad. El sistema de gestión diseñado se convierte en una herramienta para mejorar el nivel de madurez en seguridad de la información, ayudando a la organización a disminuir los riesgos a los que se encuentra expuesta, y será un pilar para establecer una cultura orientada a la protección de activos de información.

- Palabras clave:

- **SEGURIDAD DE LA INFORMACIÓN**
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**
- **RIESGO**
- **VULNERABILIDAD**
- **ISO/IEC 27001:2013**

ABSTARCT

The project aims to design an information security management system based on the ISO / IEC 27001: 2013 standard; it is applied to the reduction of risks in the storage of information of the computer unit of the GAD Municipal of the Canton Pujilí. The standard allows the assurance of confidentiality, integrity and availability of information, encourages organizations to develop a culture of security, ensuring business continuity. The management of information security is complemented by the good practices established in the ISO 27002 standard. To carry out the study, the problem, objectives, justification, importance and scope are established. The conceptualization is addressed, as well as the description of the information security regulations in Ecuador. The main risk analysis methodologies are described. The design of the management system starts by establishing the scope, the risk analysis methodology, the inventory of assets, the identification of threats and vulnerabilities, the assessment of risks, the establishment of controls and the statement of applicability. The designed management system becomes a tool to improve the level of maturity in information security, helping the organization to reduce the risks to which it is exposed, and it will be a pillar to establish a culture oriented to the protection of information assets.

- Keywords:

- **SECURITY OF THE INFORMATION**
- **INFORMATION SECURITY MANAGEMENT SYSTEM**
- **RISK**
- **VULNERABILITY**
- **ISO/IEC 27001:2013**

Capítulo I

GENERALIDADES

En el primer capítulo se plantea el problema, el cuál será el motivo de estudio durante el desarrollo del presente proyecto, se definen los objetivos y se determina la justificación, importancia y alcance del mismo.

Antecedentes

Entre las principales competencias que deben cumplir los gobiernos autónomos descentralizados, se determinan: planificar, junto con otras instituciones del sector público, el desarrollo provincial y formular los correspondientes planes de ordenamiento territorial, en el ámbito de sus competencias, de manera articulada con la planificación nacional, regional, cantonal y parroquial, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad, también establece gestionar la cooperación internacional para el cumplimiento de sus competencias (Vargas Arias, 2019).

El GAD Municipal de Pujilí es una entidad de gobierno seccional cuya función es administrar el cantón de manera autónoma frente al gobierno central, el poder ejecutivo está representado por el alcalde, y el poder legislativo formado por los miembros del Concejo Cantonal. Por disposición del artículo 238 de la Constitución de la República de 2008, “Los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera, y se regirán por los principios de solidaridad, subsidiariedad, equidad interterritorial, integración y participación ciudadana. En ningún caso el ejercicio de la autonomía permitirá la secesión del territorio nacional. Constituyen gobiernos autónomos descentralizados las juntas parroquiales rurales, los concejos municipales, los concejos metropolitanos, los consejos provinciales y los consejos regionales.”

La misión del GAD Municipal del cantón Pujilí es planear, implementar y sostener las acciones del desarrollo del gobierno local a fin de dinamizar los proyectos de obras y servicios con calidad, que aseguren el desarrollo social y económico del cantón, con la participación directa y efectiva de los diferentes actores sociales, dentro de un marco de transparencia, ética institucional y el uso óptimo de los recursos humanos capacitados.

Una estrategia de seguridad de la información es definir vínculos entre los planes estratégicos, operativos y de seguridad, caso contrario se corre el riesgo que los mismos no estén alineados y no brinden soluciones para los problemas y necesidades actuales. Se debe lograr un balance total, es decir se debe establecer controles más restrictivos, mitigar o eliminar riesgos.

El objetivo de diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) es que sea sustentable y sostenible, y que esté en sintonía con la misión, estrategias y objetivos de las empresas. Un SGSI es un sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implementar la gestión de la seguridad de la información, también permite minimizar daños, aumentar oportunidades de negocio, retorno de la inversión y continuidad del negocio de las empresas (Satán Cevallos, 2017).

Problema

El GAD Municipal del Cantón Pujilí a pesar de tener autonomía política, administrativa y financiera, en relación a la prevención frente a posibles riesgos es escasa, los procedimientos de seguridad de la información hacen referencia a que no hay control sobre: las políticas de seguridad, la administración de incidentes, gestión de la continuidad del negocio, la seguridad física, la gestión de comunicaciones y operaciones, el control de acceso, etc.

El establecimiento y mantenimiento de un SGSI no sólo concierne al departamento relacionado con tecnología, sino a todos y cada uno de los empleados de la organización. Además, no se cuenta con ningún tipo de restricción para el uso de los recursos informáticos. Según la evaluación que se realizó en base de la norma ISO/IEC27001:2013, se determina que existe un incumplimiento del 66%, con respecto a los 12 dominios.

Objetivo general

Realizar el análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO-IEC 27001:2013, para disminuir los riesgos en el almacenamiento de información de la unidad de informática del GAD Municipal del Cantón Pujilí.

Objetivos específicos

- Realizar un diagnóstico de la situación actual de la seguridad de la información que posee la unidad de informática del GAD Municipal del cantón Pujilí, mediante el levantamiento de información y de acuerdo a las políticas existentes.
- Analizar y evaluar los riesgos del proceso más crítico de la entidad pública, aplicando la metodología de análisis de riesgos y herramientas informáticas.
- Fortalecer las medidas de seguridad de información a través del diseño de un sistema de gestión.
- Entregar documento guía para la implementación de un SGSI acorde a las necesidades del GAD Municipal, que determinen las políticas y procedimientos de seguridad de la información frente a los posibles riesgos.

Justificación, importancia y alcance del proyecto

El presente proyecto, determina los lineamientos a cumplir a través del diseño de un SGSI para que exista un orden de seguridad en cuanto a la información que posee la unidad de informática del GAD Municipal, debido a que ésta no cuenta con alguna norma o procedimiento que garantice la seguridad de su información, lo cual tiene como consecuencia que exista algún tipo de vulnerabilidad para el robo de información.

La importancia que posee este proyecto es garantizar y asegurar la información que se gestiona en la unidad de informática, debido a que por ser publica dentro de ella existe muchos datos registrados de las personas que se acercan a la entidad a realizar cualquier tipo de trámite. Es importante que en la unidad de informática del GAD en mención tome en cuenta aspectos fundamentales como: la disponibilidad de los datos, la confidencialidad de los documentos y la integridad de la información.

El alcance del presente proyecto es que la unidad de informática del GAD Municipal pueda contar con la documentación guía para la implementación de un SGSI acorde a sus necesidades a fin de determinar las políticas y procedimientos de seguridad de la información frente a posibles riesgos. Además, en el futuro la organización podría obtener la certificación de norma ISO/IEC 27001:2013, generando mayor confianza y posicionándola como una entidad confiable.

Hipótesis

- **Pregunta de investigación:** ¿Cómo preservar la confidencialidad, integridad y disponibilidad de la información de una organización?
- **Hipótesis:** El diseño de un SGSI permitirá implementar los controles adecuados para preservar la confidencialidad, integridad y disponibilidad de la información.

Categorización de las variables

- **Variable independiente:** Sistema de gestión de seguridad de la información.

- **Variable dependiente:** Disminución de riesgos.

Trabajos relacionados

- En (Imbaquingo Esparza & Pusdá Chulde, 2015), concluyen que la aplicación de la norma ISO 27001 desempeña un papel importante para identificar el cumplimiento de controles que garanticen la seguridad de la información aplicada a cualquier tipo de organización. En las organizaciones no se da la importancia necesaria a como se debe gestionar la seguridad de la información.
- Según (Solarte Solarte, Enriquez Rosero, & Benavides, 2015), el SGSI tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos.
- En (Garzón Garzón, 2017) , afirma que la ISO/IEC 27001:2013 es una norma internacional, emitida por la Organización Internacional de Normalización ISO. Indica qué requisitos deben conformar un SGSI y describe cómo gestionar la seguridad de la información en una empresa. La ISO/IEC 27001:2013 es actualmente el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organización, tanto por su tamaño como por su actividad.

- Mientras que (Chunga Ramirez, 2017), determina que como parte del ciclo de vida del sistema de gestión de seguridad de la información, es necesario realizar la identificación de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de información e identificar las debilidades en la seguridad de la información que puedan amenazar a los activos de información.
- En (Bayona, Chauca, Lopez, & Maldonado, 2015), presentan los factores críticos para una efectiva implementación de la ISO/IEC 27001. Estos factores fueron categorizados de la siguiente manera:

Alineamiento de negocios: los objetivos y actividades de seguridad de la información deben estar alineados con los objetivos y requisitos de negocio, y dirigido por la gestión empresarial.

Apoyo organizacional: el apoyo de la dirección es considerada crucial para el éxito de seguridad de la información de una organización.

Conciencia organizacional: la estrategia de la seguridad de la información de una organización debería abordar de manera integral los factores humanos, como la conciencia de seguridad y capacitación en seguridad.

Competencia de TI: las competencias de TI se refieren a las capacidades integradas e interrelacionadas de elementos esenciales para el cumplimiento de un objetivo empresarial.

Desarrollo de controles de seguridad: se identifican los siguientes procesos de desarrollo de los controles de seguridad de alta prioridad: gestión de riesgos, la implementación de políticas de seguridad y el cumplimiento de las normas.

Evaluación de desempeño: la evaluación del desempeño de la gestión de sistemas de información se utiliza para monitorear el progreso hacia el logro de objetivos, identificación de las causas de un rendimiento insatisfactorio, y la mejora continua de la gestión.

Capítulo II

FUNDAMENTACIÓN TEÓRICA

En el segundo capítulo se realiza la descripción de las definiciones más importantes que servirán como base para el desarrollo del proyecto, así como la interpretación de la serie de normas ISO/IEC 27000 y la normativa de seguridad de la información ecuatoriana.

Seguridad de la información

La información que posee cualquier tipo de organización constituye uno de los activos más importantes, por lo tanto, dicha organización debe contar con las herramientas y estrategias necesarias para mitigar o eliminar los riesgos a los que podrían estar expuestos y asegurar así la continuidad del negocio. Los objetivos de la seguridad de la información son:

- Gestionar adecuadamente los riesgos.
- Detectar oportunamente posibles amenazas y vulnerabilidades.
- Optimizar los recursos.
- Garantizar la continuidad del negocio.
- Cumplir con el marco legal vigente.

La seguridad de la información según la norma ISO/IEC 27001:2013 se encarga de preservar la confidencialidad, integridad y disponibilidad de los datos que posee una organización, lo que muestra la Figura 1.

Esto se puede lograr con la implementación de políticas o procedimientos en donde se debe considerar un conjunto de reglas que son las encargadas de precisar cómo se maneja, protege y difunde la información.

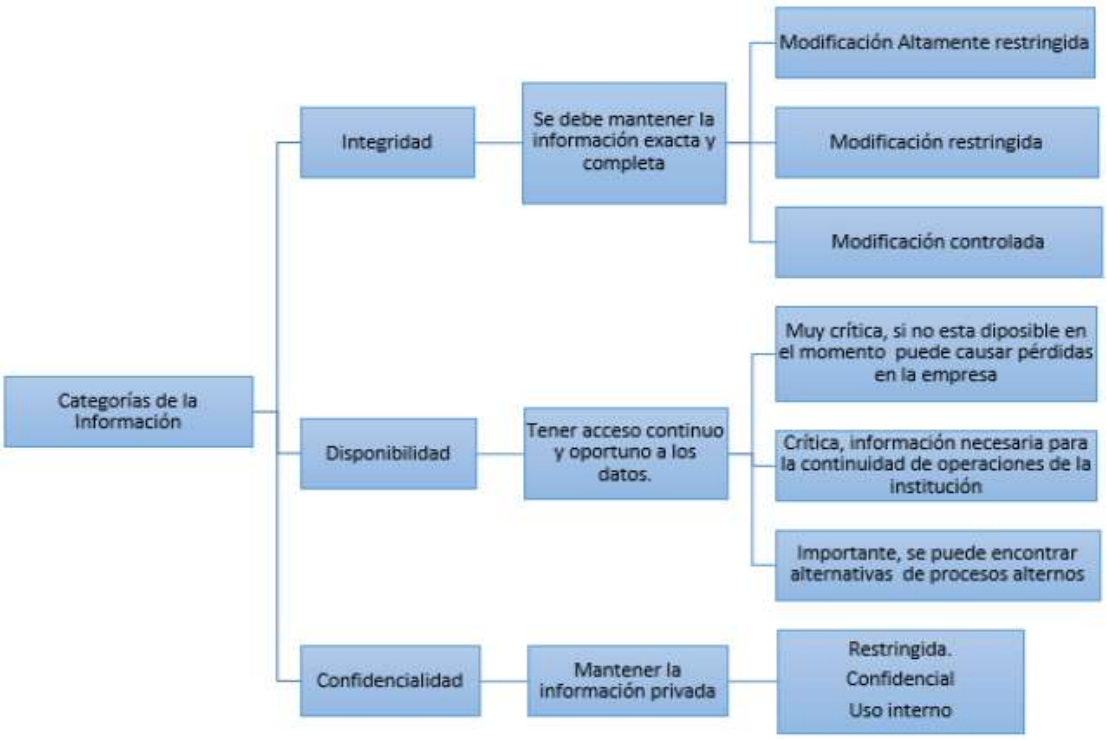
Confidencialidad: la información no se pone a disposición ni se revela a personas no autorizadas. En necesario implementar controles de acceso para la identificación, autenticación y autorización.

Integridad: se debe salvaguardar la totalidad y exactitud de la información que se gestiona, existe casos en el que la información se ha visto alterada por errores humanos, entre ellos se puede ejemplificar el borrado o modificación de archivos, ingreso de datos erróneos, etc.

Disponibilidad: es el acceso y utilización de la información por parte de personas autorizadas en el momento que así lo requieran.

Figura 1.

Categorías de la clasificación de la información



Fuente: (Lara Guijarro, 2019)

Vulnerabilidades, amenazas y riesgos

El internet es el medio de comunicación más usado a nivel mundial, es indispensable en nuestras vidas ya que es la vía de comunicación más práctica y rápida, por lo tanto, puede estar expuesta a ciertas vulnerabilidades que podrían ser explotadas por amenazas en cualquier momento.

La necesidad del aseguramiento de la información, la gestión de los riesgos y el incremento de requerimientos para controlar la información, son elementos clave para las organizaciones. El valor, el riesgo y el control constituyen la esencia del gobierno de TI. Es necesario tener en cuenta las siguientes definiciones:

- **Activo:** es un recurso del sistema de información, necesario para que la organización funcione correctamente y alcance los objetivos establecidos. **Amenaza:** es un evento que puede producir un incidente en la organización, produciendo daños materiales o pérdidas económicas.
- **Impacto:** es la consecuencia de la ejecución de una amenaza.
- **Riesgo:** es la posibilidad de que se ejecute un impacto determinado en un activo o en toda la organización.
- **Vulnerabilidad:** es la posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.
- **Ataque:** es un evento, que puede producirse o no.

La diferencia que existe entre riesgo y vulnerabilidad es que la vulnerabilidad está asociada a una amenaza y el riesgo a un impacto. Los activos de una organización están propensos a amenazas, son aquellas que representan un peligro para los activos o a la seguridad de la información en general. Dentro de estas amenazas se encuentran las descritas en la Tabla 1 (Doria Corcho, 2015):

Tabla 1.

Amenazas a la seguridad de la información

AMENAZAS	TIPOS
Adivinación de contraseñas	Ataques de diccionario, de fuerza bruta.
Aplicación	Desbordamiento de buffer, privilegio de admin.
Código malicioso	Virus, troyanos, gusanos, spyware, adware.
Husmeo	Sniffing.
Denegación de servicio	Envenenamiento DNS, ping de la muerte, inundamiento de SYN.
Reconocimiento	Escaneo de vulnerabilidades y puertos.
Seguridad de aplicaciones web/BD	Inyección SQL, secuencia de comando de sitios cruzados (XSS, cross-site scripting).
Suplantación de identidad	Hombre en el medio, secuestro de sesión, suplantación IP.

Fuente: (Doria Corcho, 2015)

Riesgo informático: se consideran problemas potenciales en donde los sistemas de información se pueden ver afectados si no se cuenta con medidas efectivas para preservar la información, los riesgos se clasifican en: riesgos de acceso, de integridad, de utilidad, de infraestructura y de relación. Los sistemas informáticos y su seguridad dependen de varios principios:

- La concienciación de los altos directivos, es necesario destinar los recursos suficientes a temas de seguridad.
- Los conocimientos y las capacidades de los responsables del sistema informático de la organización.
- La cultura organizacional de todos los empleados de la organización.
- La correcta instalación, configuración, mantenimiento y soporte del hardware, a fin de cubrir brechas de seguridad.
- Alineación de los objetivos con la misión y visión de la organización.

Sistema de gestión de seguridad de la información (SGSI)

El SGSI es el concepto central sobre el que se construye ISO/IEC 27001:2013. Garantizar un nivel de protección total es casi imposible, si no se cuenta con una planificación adecuada, incluso en el caso de disponer de un gran presupuesto.

El principio de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos y gestionados por la organización de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, en el entorno y la tecnología (Neira & Spohr, 2016).

Los resultados se podrán medir y evaluar de acuerdo a la metodología que se diseñe e implemente, esto conlleva a una mejora continua. Para su implementación se utiliza el modelo PDCA, éste modelo está dividido en cuatro fases en el que finalizada la última y analizados sus resultados se vuelve a repetir el ciclo. Las actividades en relación a la continua evaluación del SGSI debe estar documentadas (Mero García, 2016), los tipos de documentación que se representa en la Figura 2.

Figura 2.

Pirámide de documentación del SGSI

Fuente: (Normas ISO, 2020)

Las políticas son las bases de la seguridad, realizando la descripción de los objetivos generales y las implementaciones realizadas en la organización. Su meta es determinar las estrategias necesarias para el cumplimiento de los objetivos sin entrar en detalles técnicos, deben ser conocidas por toda la organización.

Los procedimientos detallan los objetivos definidos en las políticas, en estos se definirán detalles más técnicos y se determina cómo conseguir los objetivos principales. Deben ser conocidos por las personas que así lo requieran.

Las instrucciones conforman el desarrollo de los procedimientos, en ellos se describe los comandos técnicos que se deben realizar para la ejecución de dichos procedimientos.

Los registros determinan el correcto diseño e implementación del SGSI y el cumplimiento de los requisitos. Se debe contar con una serie de métricas de seguridad que permitan evaluar la ejecución de los objetivos de seguridad establecidos.

Un SGSI proporciona seguridad permanente ya que posee un enfoque integral, las organizaciones deben definir una estrategia de seguridad basada en el negocio y no sólo en la tecnología. La confidencialidad, integridad y disponibilidad de la información son importantes para mantener los niveles de competitividad, rentabilidad e imagen institucional necesarios para lograr los objetivos (Oidor González, 2017).

La implementación de un SGSI es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la dirección, en éste caso desde la alcaldía, basándose en objetivos organizacionales. Los beneficios de la implementación de un SGSI son:

- **Aspecto personal:** concientización del personal con respecto a temas de seguridad de la información.
- **Aspecto económico:** menores costos vinculados a incidentes de seguridad.

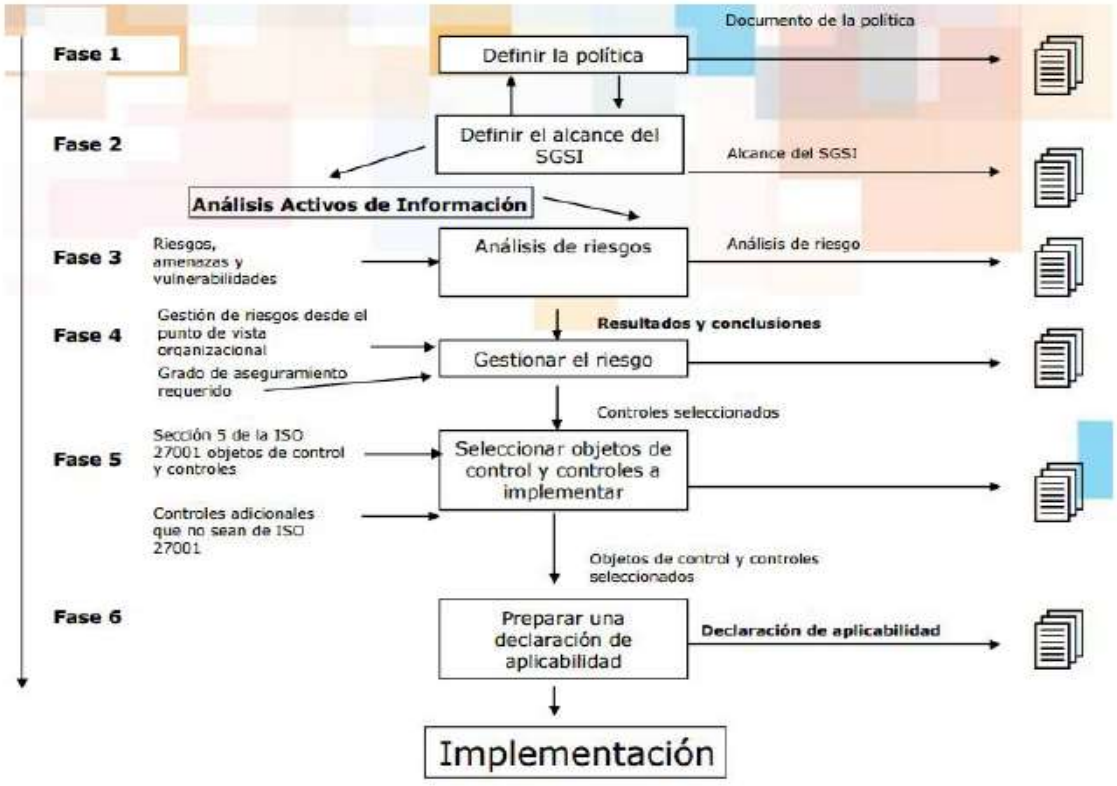
- **Aspecto organizacional:** demuestra que la organización está preparada para afrontar incidentes de seguridad en todo momento.
- **Aspecto funcional:** gestión de los riesgos.
- **Aspecto legal:** cumplimiento con leyes y regulaciones vigentes de cada país.

La norma ISO/IEC 27001:2013 proporciona la metodología para la implementación de la gestión de seguridad de la información en cualquier tipo de organización, sigue una serie de fases.

La Figura 3, muestra los procesos a realizar para la implementación del SGSI.

Figura 3.

Metodología del SGSI según ISO 27001



Fuente: (Oidor González, 2017)

Ciclo de Deming

Para establecer y gestionar un SGSI en base a la norma ISO/IEC 27001:2013, se utiliza el ciclo PDCA. El Ciclo de Deming así llamado por su creador Edwards Deming, también es conocido como ciclo de mejora continua (Quintero Parra, 2015).

El Ciclo Deming tiene cuatro etapas que son cíclicas, como se muestra en la Figura 4, una vez que se culmina la última etapa se debe volver nuevamente a la primera e iniciar el ciclo.

De esta manera se pueden establecer e implementar las mejoras que sean necesarias. La aplicación del ciclo de Deming posee los siguientes aspectos relevantes:

- La mejora de procesos y servicios.
- Mejora permanente de la calidad.
- Reducción de costos.
- Optimización de los niveles de productividad.

La norma ISO/IEC 27001:2013 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. A continuación, se describen los pasos del ciclo Deming (Recalde Caicedo, 2019).

- **Plan (planificar):** se establecen las actividades y procesos necesarios para alcanzar los objetivos establecidos por la organización.
- **Do (hacer):** se implementa el plan establecido en el paso anterior, se ponen en marcha los procesos estudiados.
- **Check (verificar):** se analizan los resultados obtenidos en la fase anterior y los compara con los resultados esperados del “Plan” para analizar diferencias.
- **Act (actuar):** se realizan acciones correctivas necesarias para alcanzar los resultados esperados, en el caso de obtener alguna diferencia con los resultados obtenidos.

Figura 4.

Fases del ciclo deming

Fuente: (Tola Franco & Freire, 2015)

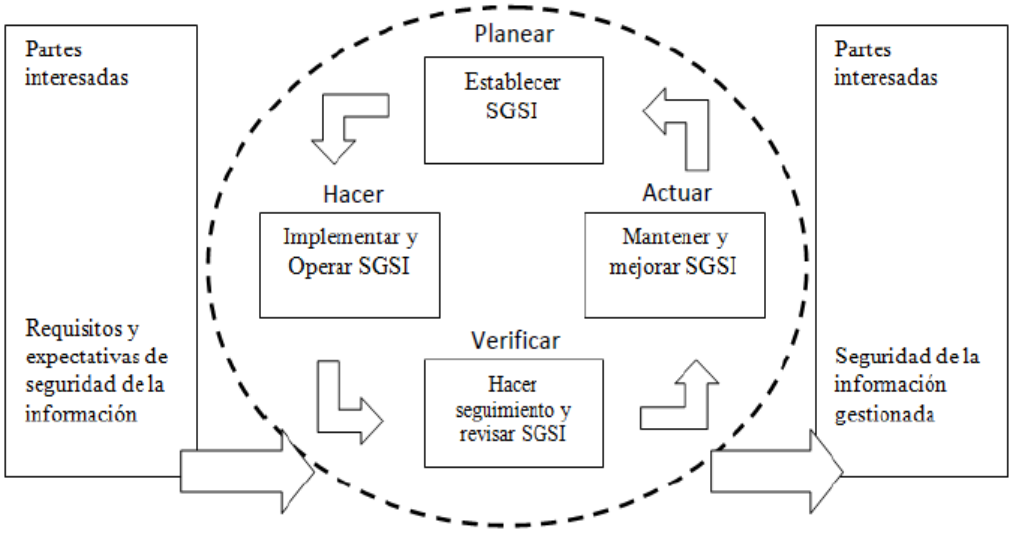
Ciclo deming y los procesos del SGSI

La adopción del ciclo deming refleja los principios establecidos para la seguridad de la información, como se muestra en la Figura 5. Este es un modelo para diseñar e implementar las directrices que controlan la evaluación de riesgos. La gestión de la seguridad de la información hace referencia a que deben interactuar personas, procesos y la tecnología.

El SGSI deberá ser sostenible en el tiempo, debe tener la capacidad de incorporar mejoras continuas, beneficiando a la organización, es necesario tener una metodología definida. La Tabla 2. muestra la descripción de las etapas del ciclo deming, con los procesos del SGSI.

Figura 5.

Ciclo deming y los procesos del SGSI



Fuente: (Aguirre Tobar & Zambrano Ordoñez, 2015)

Análisis y gestión de riesgos

La gestión de riesgos es el proceso de identificación y evaluación del mismo, así como también la toma de medidas para reducirlo a un nivel aceptable para la organización. El riesgo es una función de probabilidad de que una amenaza explote una vulnerabilidad, y el resultante sea un efecto negativo a la organización (Reinoso Córdova, 2017).

Las organizaciones están expuestas a una serie de peligros, que se han incrementado por las nuevas amenazas, por el uso de la tecnología, es por esto que es importante contar con métodos adecuados para determinar, analizar, valorar y clasificar los riesgos, para poder implementar mecanismos que permitan controlarlos y minimizarlos.

Tabla 2.

Ciclo deming y los procesos del SGSI

CICLO DEMING	PROCESOS SGSI
Planificar	Definir alcance del SGSI. Definir política de seguridad. Metodología de evaluación de riesgos. Inventario de activos. Identificar amenazas y vulnerabilidades. Análisis y evaluación de riesgos. Selección de controles.
Hacer	Definir plan de tratamiento de riesgos. Implantar plan de tratamiento de riesgos. Implementar los controles. Formación y concienciación. Operar el SGSI.
Verificar	Revisar el SGSI. Medicar eficacia de los controles. Revisar riesgos residuales. Realizar auditorías internas del SGSI. Realizar acciones y eventos.
Actuar	Implantar mejoras. Acciones correctivas y preventivas. Comprobar eficacia de las acciones.

Fuente: (Vásquez Escalante, 2018) (ISO Tools, 2020)

La gestión de riesgos es una actividad para salvaguardar los activos de información de una organización. Es un proceso que debe ser constante para minimizar los costos operacionales y económicos causados por la interrupción de las actividades, aplicando controles de protección sobre los sistemas de información que dan soporte al correcto funcionamiento de toda la organización (García Balaguera & Ortíz González, 2017).

El proceso de gestión de riesgos involucra cuatro actividades cíclicas, empezando por la identificación de los activos y los riesgos como se puede ver en la Figura 6.

Figura 6.

Actividades de la gestión de riesgos

Fuente: Propia

La gestión de riesgos es la idea base de la norma ISO/IEC 27001:2013, ésta describe cómo gestionar un SGSI diseñando un conjunto de políticas y procedimientos que establecen cómo se maneja la seguridad de la información en una organización. La decisión de la implementación de los controles está basada en los resultados obtenidos en la evaluación del riesgo. En el proceso para la correcta gestión de los riesgos intervienen las siguientes fases:

1. Para poder entender y definir el impacto de los riesgos, es necesario identificar, analizar y evaluar los mismos, debido a que cada organización está expuesta a un sinnúmero de amenazas y vulnerabilidades diferentes que podrían afectar el cumplimiento de sus objetivos.
2. El tratamiento de riesgos es el proceso de selección e implementación de controles para mitigar o eliminar posibles riesgos.
3. El monitoreo y revisión es un proceso para medir la eficiencia y efectividad de los controles establecidos para la gestión del riesgo.

Este proceso asegura que los planes de acción hagan referencia a las amenazas y vulnerabilidades que se puedan presentar en el futuro.

4. La comunicación y concientización con todas las personas que conforman la organización, son actividades necesarias para socializar información en temas del tratamiento de los riesgos.

Evaluación del riesgo

La organización puede elegir cualquiera de las metodologías de gestión de riesgos existentes, para realizar la evaluación de riesgos ISO 27001 requiere combinar activos, amenazas y vulnerabilidades en un mismo modelo de evaluación.

La Figura 7 describe el proceso de la evaluación del riesgo, lo que permite a una organización cumplir con los requerimientos de la norma.

Figura 7.

Proceso de evaluación del riesgo

Fuente: Propia

Identificación de activos

Para realizar una correcta evaluación de riesgos se debe efectuar la valoración de activos de cada organización. Cada activo debe estar identificado y valorado.

La ISO 17799 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera (Recalde Caicedo, 2019):

- **Activos de información:** son las bases de datos y archivos de datos, documentación del sistema, manuales de usuario, procedimientos operativos de apoyo, planes de continuidad.
- **Documentos impresos:** son los documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes.
- **Activos físicos:** son los equipos de comunicación y computación, medios magnéticos.
- **Personas:** es el personal, clientes, proveedores.
- **Imagen y reputación de la compañía.**
- **Servicios:** son los servicios de computación y comunicación.

Tratamiento del riesgo

Identificados y evaluados los riesgos, la organización debe definir el Plan de Tratamiento de Riesgos (PTR), es un documento de vital importancia para el SGSI. El objetivo es determinar de forma clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos se asignarán para la realización de cada una de estas actualizaciones y las prioridades en la ejecución de las actualizaciones. Existen las siguientes estrategias:

Reducción del riesgo: se deben implementar controles apropiados para lograr disminuirlos a niveles aceptables.

Cuando se hayan identificado los controles a ser implantados se deben considerar los requerimientos de seguridad relacionados con el riesgo, así como la identificación de vulnerabilidades y amenazas. Las formas para reducir los riesgos son:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre.
- Reduciendo los costos en caso de que una amenaza se materialice.

Aceptación del riesgo: en ciertas ocasiones, la organización deberá tomar la decisión de aceptar el riesgo, esto se debe a que no se pueden implementar controles y tampoco es viable diseñarlos si el costo de implantación es mayor que las consecuencias.

Transferencia del riesgo: cuando técnica y económicamente es muy difícil implementar los controles para reducir o mitigar el riesgo. Una opción podría ser transferir el riesgo a otra organización. Teniendo en cuenta, que, con las empresas aseguradoras, existirá un riesgo residual.

Evitar el riesgo: la decisión de evitar el riesgo debe ser comparada contra las necesidades financieras y comerciales de la organización. Las formas de evitar el riesgo son:

- Dejar de realizar ciertas actividades.
- Transferir activos de información de un área de riesgo a otra.
- No procesar cierto tipo de información si no se consigue la protección adecuada a cada activo.

Normas ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), como se puede ver en la Figura 8. La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los SGSI (Lanche Capa, 2015).

La ISO y la IEC constituyen un sistema cuya función es crear normalizaciones a nivel mundial, donde los organismos miembros de diferentes países participan en el proceso de desarrollo de las normas. Para el SGSI han establecido la familia de normas o estándares ISO/IEC 27000, que se describen en la Tabla 3.

Tabla 3.

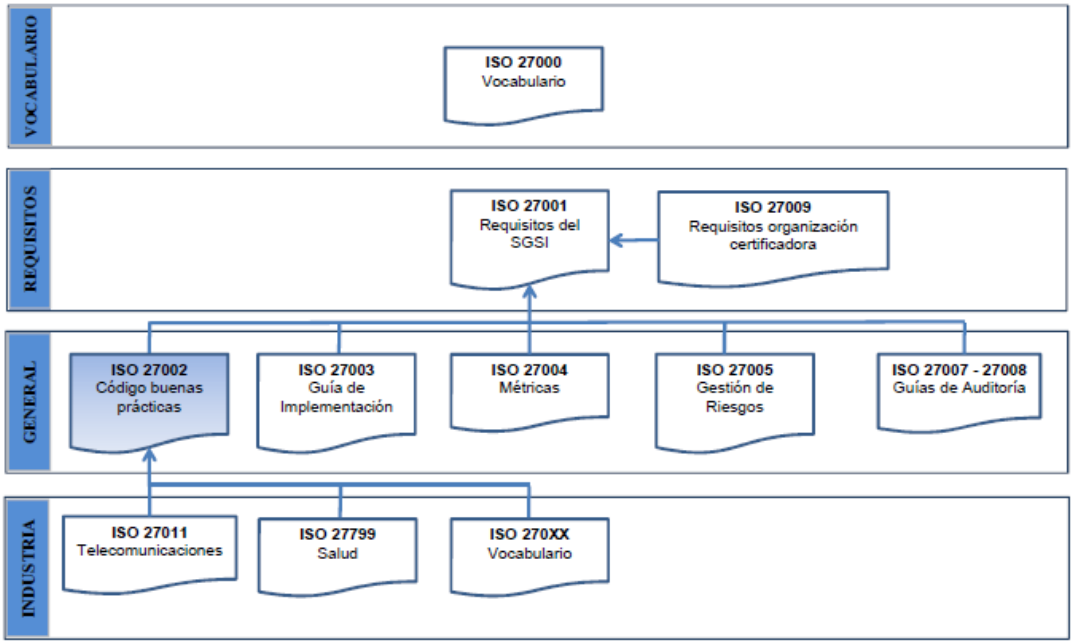
Familia ISO/IEC 27000

NORMA	PUBLICACIÓN	CERTIFICABLE	DESCRIPCIÓN
ISO 27000:2018	Febrero del 2018	No	Proporciona una visión general de las normas que componen la serie 27000, es una introducción a los sistemas de gestión de seguridad de la información, una breve descripción del proceso PDCA y da a conocer los términos y definiciones.
ISO 27001:2013	Octubre del 2013	Si	Es la norma principal de toda la serie ya que incluye los requisitos del SGSI. En el Anexo A se enumeran los objetivos de control para que se puedan implantar en las empresas durante el progreso de sus SGSI. La empresa podrá argumentar el hecho de no aplicar los controles que no se encuentran implementados ya que no es obligatorio.
ISO 27002:2013	Octubre del 2013	No	Es un manual de buenas prácticas en el que se describen los objetivos de control y las recomendables en cuanto a la seguridad de la información. En ella podemos encontrar 14 dominios, 35 objetivos de control y 114 controles.
ISO 27003:2017	Marzo del 2017	No	Es un manual para implementar un SGSI, además brinda la información necesaria para la utilización del modelo PDCA con los requerimientos de sus diferentes fases.

NORMA	PUBLICACIÓN	CERTIFICABLE	DESCRIPCIÓN
ISO 27004:2016	Diciembre del 2016	No	Es una guía para el desarrollo y utilización de métricas y técnica de medida aplicables para determinar la eficacia de un SGSI y de los controles implementados según la ISO/IEC 27001.
ISO 27005:2018	Julio de 2018	No	Establece las directrices para la gestión de los riesgos. Es un apoyo a los conceptos que se especifican en la ISO 27001 y está diseñada para ayudar a aplicar la seguridad de la información en un enfoque de gestión de riesgos.
ISO 27006:2015	Octubre de 2015	No	Especifica los requisitos para lograr la acreditación en las entidades de auditoría y certificación del SGSI. Ayuda a interpretar los criterios de ISO/IEC 17021 cuando se aplican en organismos de certificación de la ISO 27001.
ISO 27007:2016	Diciembre del 2016	No	Es un manual de auditoria de SGSI. Es un estándar que proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.

Figura 8.

Familia de normas de Seguridad de la Información ISO 27000



Fuente: (Lanche Capa, 2015)

Norma ISO/IEC 27001:2013

La ISO 27001 es una norma internacional emitida por la ISO y describe cómo gestionar la seguridad de la información en una organización. La primera revisión se publicó en 1998 y fue un estándar nacional británico certificable BS 7799-2. La versión más actual fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Permite que una empresa sea certificada, esto significa que una entidad de certificación determina que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27014 (Cárdenas Herrera & Higuera, 2016).

La Tabla 4. muestra una comparación entre la norma ISO 27001:2005 y la norma ISO 27001:2013.

El Anexo A de la norma ISO/IEC 27001:2013 muestra los controles que están descritos en la norma ISO/IEC 27002. El detalle de los dominios, objetivos de control y controles se listan en el Anexo 1.

Tabla 4.

Comparación normas ISO 27001

NORMA ISO 27001:2005	NORMA ISO 27001:2013
Manual del SGSI	Políticas de seguridad
Organización de la seguridad	Organización de la seguridad de la información.
Gestión de activos	Seguridad de los RRHH
Seguridad de RRHH	Gestión de activos
Seguridad Física	Control de acceso
Gestión de comunicaciones y operaciones	Criptografía
Control de acceso	Seguridad física y ambiental
Adquisición, desarrollo y mantenimiento de la información.	Operaciones de seguridad
Gestión de incidentes	Seguridad de las comunicaciones
Continuidad del negocio	Sistemas de adquisición, desarrollo y mantenimiento
Cumplimiento	Relaciones con proveedores
-	Gestión de incidentes
-	Seguridad de la información para la continuidad del negocio
-	Cumplimiento

Fuente: (Villacís Espinosa, 2016)

La nueva estructura del Anexo A agrega 3 dominios de control, incluyen un total de 114 controles.

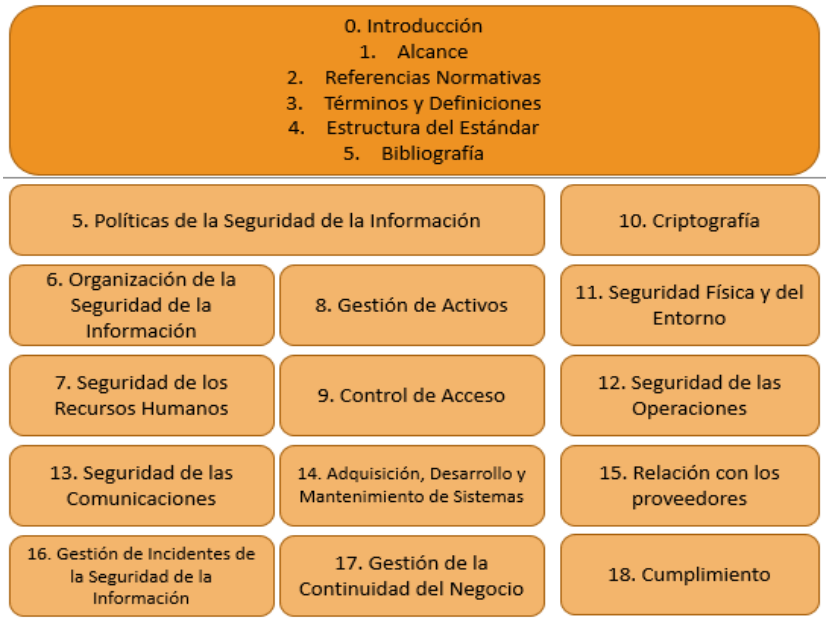
Dentro de los nuevos dominios de control están: criptografía, siendo separada de adquisición, desarrollo y mantenimiento de la información. El segundo dominio de control es: relación con proveedores y el tercero es el resultado de la división del dominio gestión de comunicaciones y operaciones en dos nuevos dominios: operaciones de seguridad y seguridad de las comunicaciones.

La norma ISO/IEC 27002 consta de 14 dominios, 35 objetivos de control y 114 controles. Puede ser aplicada a cualquier organización, de no aplicar cierto control se debe especificar la justificación (Sangoluisa Chamorro, 2015).

Los controles están estructurados como se muestra en la Figura 9. En Ecuador, el Instituto Ecuatoriano de Normalización (INEN) toma como referencia la norma ISO/IEC 27001:2013 para crear la referencia NTE INEN-ISO/IEC 27001:2016, ésta norma contiene una serie de requisitos que son necesarios establecer. Estos requisitos indispensables son los numerales del 4 al 10 que se detallan en la Tabla 5.

Figura 9.

Dominios de Seguridad



Fuente: Elaboración propia. Adaptado de (Jara Pérez, 2017)

La norma ISO 27001 tiene puntos en común con otras normas: la ISO 22301 de continuidad del negocio y la ISO/IEC 20000, de gestión de servicios TI. La ISO 22301 trabaja en temas de la seguridad desde una perspectiva más general, asegurando la continuidad del negocio.

Por otro lado, la ISO 20000 se enfoca en aspectos que van a permitir su sustentabilidad, utilizando elementos y controles que van a evitar las consecuencias de amenazas, y encontrar las causas que motivan el problema, y en conjunto sirven para garantizar un servicio seguro, sin interrupciones y de calidad.

Alcance de la norma ISO/IEC 27001:2013

Esta norma asegura la selección de los controles de seguridad adecuados y asegura la protección de la información de las partes interesadas (Recalde Caicedo, 2019). Incluye los siguiente:

- Formulación de objetivos para la seguridad de la información.
- Gestión adecuada de los riesgos.
- Asegurar el cumplimiento legal vigente en cada país.
- Gestión de controles para asegurar el cumplimiento de los objetivos de seguridad específicos de una organización.
- Identifica los procesos críticos para la gestión de la seguridad de la información en la organización.
- Puede ser una herramienta de ayuda para auditores internos y externos para determinar el grado de cumplimiento de la norma.
- Proporcionar información relevante sobre seguridad de la información a clientes y proveedores.
- Gestión adecuada de los recursos de la organización.

Tabla 5.

Requisitos de la Norma ISO/IEC 27001:2013

NORMA ISO/IEC 27001:2013	DESCRIPCIÓN
4. Contexto de la organización	La organización debe determinar su alcance, límites y capacidad, garantizando la correcta implantación del SGSI, también debe estar consciente de las operaciones internas y externas que podrían influir en los resultados deseados.
5. Liderazgo	La alta gerencia de la organización debe liderar el proceso del SGSI verificando que se cumplan los requerimientos de la norma, garantizando los recursos, documentando las políticas y objetivos de seguridad propuestos y asignando las responsabilidades para cada una de las actividades.
6. Planificación	La organización debe escoger una metodología de clasificación, análisis y evaluación de riesgos, formando criterios para establecer los controles de seguridad y así mantener los niveles de riesgo a un nivel aceptable de acuerdo a las políticas y objetivos de seguridad.
7. Soporte	La organización debe comunicar las políticas de seguridad a todos sus empleados y que éstos se comprometan al mejoramiento continuo del SGSI. También se deben garantizar los recursos y que se cuente con personal capacitado, y generar los documentos que exige la norma.
8. Operación	La organización debe documentar y planear los procesos para llevar a cabo las actividades, incluyendo las valoraciones de riesgos de la seguridad de la información y el plan de tratamiento de riesgos.
9. Evaluación del riesgo	La organización debe velar por el desempeño de la seguridad de la información y medir la eficacia del SGSI, mediante auditorías internas a intervalos planificados, con el fin de verificar si se están cumpliendo con los objetivos y políticas de seguridad.
10 Mejora continua	La organización debe aplicar las acciones correctivas y velar por el mejoramiento continuo.

Fuente: (ISO/IEC 27001, 2013)

Objetivos de la norma ISO/IEC 27001:2013

Entre los objetivos que se pretende cumplir con la Norma ISO/IEC 27001:2013, están:

- Aumentar y mantener la eficacia de un proceso o servicio.
- Potenciar un servicio final, ésta opción supone la implementación de un SGSI.
- Potenciar la gestión interna, el alcance es identificar aquellas partes de la organización en las que la implementación del SGSI, sirva para potenciar y estructurar la gestión interna.
- El control define el enunciado específico para el cumplimiento del objetivo.
- El lineamiento de implementación proporciona información para cumplir con el objetivo de control.

Normativa de Seguridad de la Información en Ecuador

Mediante acuerdos ministeriales publicados en el Registro Oficial No. 804 del 29 de julio de 2011 y No. 837 del 19 de agosto de 2011, la Secretaría Nacional de Administración Pública (SNAP) crea la comisión para la seguridad informática y de las tecnologías de la información y comunicación para el control en las empresas públicas.

Dentro de sus responsabilidades tiene que establecer los lineamientos de seguridad informática. Para las entidades de la Administración Pública Central e Institucional.

En respuesta a esta tarea, la comisión desarrolla el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Norma ISO/IEC 27001. El EGSI establece un conjunto de directrices prioritarias para la gestión de la seguridad de la información e inicia un proceso de mejora continua en las organizaciones de la administración pública ecuatorianas.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la información (Jara Arenas, 2019).

Un estudio realizado por la empresa Deloitte conjuntamente con el MINTEL sobre la seguridad de la información en Ecuador en el que participaron más de 50 empresas nacionales y multinacionales, determinó que: alrededor del 50% tuvo alguna brecha de seguridad, y de esto, el 20 % no pudo determinar el impacto de dicha brecha ya que no contaban con un proceso de gestión de incidentes. Más del 50% citó como una de sus principales dificultades la falta de presupuesto, la falta de visibilidad e influencia y falta de personal competente. Además, alrededor del 75% no midió el retorno de las inversiones y solo 20% estaba preparado para afrontar incidentes de seguridad originados en redes sociales y el 60% no disponía de un SOC (Security Operation Center). El 36% de las empresas evaluadas no contaba con un plan de recuperación de desastres. En cuanto al EGSI, fueron evaluadas 55 entidades, de las cuáles solo el 16.36% obtuvo un resultado bueno en el cumplimiento del EGSI, el 65.45% logró un resultado regular, mientras, que el 7.27% obtuvo una calificación mala y el 10.91%, muy mala (MINTEL, 2018).

Según acuerdo ministerial N° 025-2019, el registro oficial publica la versión 2.0 del EGSI el 10 de enero del 2020, en donde se presentan las mejoras ante la primera versión, es función del Ministerio de telecomunicaciones y de la sociedad de la información (MINTEL) expedir el EGSI, el cual es de implementación obligatoria en las instituciones de la administración pública central.

El artículo 4 determina que se debe mejorar o implementar el EGSI en un plazo de doce meses a partir de la publicación del registro oficial. El MINTEL a través de la subsecretaría del Estado-Gobierno Electrónico, realizará la evaluación del cumplimiento del EGSI.

En cuanto a la evaluación de riesgos y el plan de tratamiento de riesgos para cada institución, se ejecutarán en un plazo de cinco meses, y la actualización o implementación de los controles que determina el EGSI se realizará en un plazo de siete meses. La actualización o implementación, se ejecutará en cada organización de acuerdo al ámbito de acción, estructura orgánica, recursos, nivel de madurez en la gestión de la seguridad de la información (Registro Oficial, 2020).

Norma NTE INEN ISO/IEC 27001

La Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001 es una traducción idéntica de la Norma Internacional ISO/IEC 27001:2013. Esta norma ecuatoriana proporciona los requisitos para planificar, implementar, mantener y mejorar un SGSI. La adopción de un SGSI es una decisión estratégica para una organización.

El diseño e implementación del SGSI están vinculados a las necesidades y objetivos de la organización. El SGSI preserva la confidencialidad, integridad y disponibilidad de la información mediante la adopción de una metodología de gestión de riesgos y como resultado se espera que los riesgos sean gestionados adecuadamente, mediante un plan de tratamiento de riesgos.

Esta norma puede ser utilizada por toda la organización para evaluar la capacidad de cumplir con los requisitos de seguridad de la información en cualquier proceso o servicio.

Capítulo III

METODOLOGÍAS DE RIESGOS

En el presente capítulo se realizará un análisis comparativo de las metodologías de análisis de riesgo. Empezando con la descripción de los principales marcos de referencia y sus características. Luego se seleccionará la metodología que mejor se adapte a la organización con la cual se efectuará el análisis y evaluación del riesgo.

Marco de referencia para la gestión del riesgo

El análisis de riesgos es una parte fundamental en la gestión de la seguridad de la información en cualquier organización, es importante la identificación de los puntos más débiles de la estructura de TI que dan soporte a los procesos o servicios críticos de la organización.

Las metodologías de análisis de riesgo son de gran ayuda para el establecimiento del marco de gestión de riesgos, las mismas garantizan bases para el correcto análisis de los mismos. Para realizar el proceso de evaluación de riesgo existen varias metodologías que se pueden aplicar para establecer el correcto tratamiento de riesgos, según las necesidades de la organización. Los principales marcos de referencia para la evaluación de riesgos se describen a continuación.

OCTAVE

Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation): es una metodología desarrollada por el CERT/CC. Se centra en el estudio de riesgos organizacionales y se focaliza principalmente en los aspectos relacionados con el día a día de las organizaciones (Lopez Rimari, 2020).

La evaluación inicia a partir de la identificación de los activos relacionados con la información, es decir todos los elementos que tienen valor para la organización. OCTAVE estudia la infraestructura de información con el fin de que una organización pueda cumplir su misión, todos los empleados necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos, para ello, es importante que en la evaluación estén directamente involucradas personas de diferentes niveles de la organización.

Esta metodología que es evaluación de amenazas operacionalmente críticas, de activos y vulnerabilidades, se implementa con la conformación de un equipo mixto, compuesto de personas de las áreas de negocio y de TI. Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener. Existen 3 versiones de la metodología OCTAVE: la versión original OCTAVE, OCTAVE-S y OCTAVE-ALLEGRO (Ramos Ruiz, 2021).

ISO / IEC 27005:2018

La norma ISO/IEC 27005:2018 brinda las directrices necesarias para la gestión del riesgo de la seguridad de la información. Proporciona soporte a los conceptos generales que contiene de la norma ISO/IEC 27001. Describe los procesos para la gestión del riesgo en la seguridad de la información y proporciona directrices para seguridad de la información de gestión de riesgos. Puede ser aplicada en todo tipo de organizaciones que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización. (Castillo Palma & Molina Jiménez, 2020).

NIST SP 800-30

Es una guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos. La guía proporciona apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos. La gestión de riesgos tiene un papel crítico en la protección de los activos de la organización, ya que ayuda a identificar todos los activos, las amenazas, las vulnerabilidades frente a las amenazas y calcula el riesgo existente de un posible impacto sobre el activo. Con toda esta información, el responsable de seguridad puede tomar las decisiones pertinentes para implantar medidas de seguridad optimizando el factor riesgo-inversión. (NIST, 2018)

Los resultados son una guía para que la organización pueda tomar decisiones sobre si es necesario implantar nuevos mecanismos de seguridad y qué controles o procesos de seguridad serán los más adecuados, según las necesidades de cada organización.

En ésta metodología se realizan nueve pasos de evaluación de riesgos, éstos pasos deben ser personalizados para cada entidad a fin de identificar correctamente los riesgos, algunos pasos se pueden realizar simultáneamente.

MAGERIT

Magerit es una metodología desarrollada por el Ministerio de Administraciones Públicas de España, está dirigido para la administración pública. Existen diferentes fases para la estimación e impacto de los riesgos que pueden afectar a los sistemas de información, la estimación de los tiempos y los recursos para el tratamiento de los riesgos.

Las fases finales involucran la gestión de riesgos en sí, se seleccionan soluciones a los riesgos detectados y mecanismos o salvaguardas que implementen dichas soluciones (Oidor González, 2017).

Magerit tiene los siguientes objetivos:

- Hacer que todas las personas que conforman la organización sean conscientes de la existencia de riesgos y de la necesidad de tratarlos a tiempo.
- Ofrecer un método holístico para realizar el análisis de los riesgos.
- Apoyar en la planificación e implantación de medidas adecuadas para mitigar o eliminar los riesgos.
- Preparar a las organizaciones en los procesos de evaluación, auditoría o certificación.

MEHARI

Es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (Club Francés de la Seguridad de la Información) en 1995 y se deriva de las metodologías previas Melissa y Marion (Moncada Castillo & Ramírez Gualteros, 2017).

Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una organización mediante un análisis de los principales factores de riesgo, acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la organización mediante el establecimiento de políticas de seguridad y mantenimiento de los riesgos a un nivel aceptable.

El principal objetivo de Mehari es proporcionar un método para la evaluación y gestión de los riesgos, concretamente en el dominio de la seguridad de la información, por medio de un conjunto de herramientas y elementos necesarios para su implementación (Novoa & Rodríguez, 2015).

CRAMM

Cramm es una metodología que fue desarrollada por el Centro de informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido. Su versión inicial data de 1987. El significado del acrónimo proviene de CCTARisk Analysis and Management Method.

Cramm es aplicable a todo tipo de sistemas y redes de información, se puede aplicar en todas las etapas del ciclo de vida del sistema de información, desde la planificación, a través del desarrollo e implementación del mismo. Se puede aplicar de acuerdo a las necesidades. La metodología Cramm está orientada para:

- El análisis y gestión de riesgos.
- Aplicar sus conceptos de una manera formal, disciplinada y estructurada.
- Proteger la confidencialidad, integridad y disponibilidad de sus activos.
- Usar evaluaciones cuantitativas y cualitativas.

Comparación de metodologías de gestión de riesgos

Se realiza un cuadro comparativo entre las metodologías OCTAVE, ISO / IEC 27005:2018, NIST SP 800-30, MAGERIT, MEHARI y CRAMM, cuyas características, ventajas y desventajas se describen en la Tabla 6.

Tabla 6.

Comparación de metodologías de gestión de riesgos

METODOLOGÍA	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
OCTAVE	• Agiliza y optimiza los procesos de evaluación de riesgos • Clasifica a los componentes de la organización en activos y los ordena de acuerdo a su importancia. • Usa el método OCTAVE, Método OCTAVE-S y Método OCTAVE ALLEGRO. • Estudia la infraestructura de información y la manera como dicha infraestructura se usa.	• Es una metodología flexible y auto dirigida. • Involucra como elementos de su modelo de análisis: procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. • Hace partícipe a todo el personal de la organización.	• No especifica claramente la clasificación de los activos de información. • Usa muchos documentos anexos lo que hace complicado su comprensión y aplicación. • No identifica oportunamente los riesgos importantes para la organización.
ISO / IEC 27005:2018	• Es un estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. • Determina las directrices para la gestión de riesgos, apoyando los requisitos del SGSI definidos en ISO 27001. • Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización.	• Es un estándar internacional que es aplicable a cualquier organización sin importar el tipo, tamaño o naturaleza. • Su última versión fue publicada en el 2018. • Está orientada a la gestión de riesgos de la seguridad de la información. • Es considerada con un alcance completo, tanto en el análisis como en la gestión de riesgos.	• No es certificable. • No brinda detalles para la valoración de las amenazas. • No posee herramientas que sirvan de ayuda para su implementación.

METODOLOGÍA	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
NIST SP 800-30	• Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI. • Esta guía provee los fundamentos necesarios para un programa de administración de riesgos.	• Proporciona una guía para la evaluación de riesgos de seguridad en las infraestructuras de TI. • La guía provee herramientas para la valoración y mitigación de los riesgos. • Asegura los sistemas informáticos que almacenan, procesan y transmiten información. • Mejora la administración a partir de los resultados del análisis de riesgos.	• En el modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias. • Se convierte en una limitante para su aplicación en pequeñas empresas con altas limitaciones de recursos humanos.
MAGERIT	• Es una metodología de análisis y gestión de riesgos de la información desarrollada por el consejo superior de administración electrónica. • Tiene el propósito de establecer principios para el uso eficaz, eficiente y aceptable de las TI.	• Ayuda a planificar las medidas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación, auditoría, o certificación. • Tiene un alcance completo, tanto en el análisis como en la gestión de riesgos. • Posee un extenso archivo de inventarios sobre amenazas y tipo de activos.	• No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. • No posee un inventario completo en lo referente a políticas.

METODOLOGÍA	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
MEHARI	• Es un método para la evaluación y gestión de riesgos según requerimientos de ISO/IEC 27005. • Proporciona una metodología consistente, con bases de datos de conocimiento adecuadas para ayudar a los CISO. • Modelo de riesgos cualitativo y cuantitativo. • Capacidad para evaluar y simular los niveles de riesgo derivado de medidas adicionales	• Permite un análisis directo e individual de situaciones de riesgos descritas en los escenarios. • Proporciona un conjunto de herramientas diseñadas para la gestión de la seguridad a corto, mediano y largo plazo. • Complementa y acopla a las necesidades de la norma ISO 27001, 27002 Y 27005 para definir los SGSI y la gestión de riesgos.	• Se enfoca solo en los 3 principios de seguridad olvidando el no repudio. • La recomendación de los controles no incluye dentro del análisis sino dentro de la gestión de los riesgos.
CRAMM	• Es una metodología de análisis de riesgos, desarrollada por el Central Communication and Telecommunication Agency (CCTA) del gobierno del Reino Unido, • Es utilizada, por lo general, en Europa y dirigida a grandes industrias, y organizaciones gubernamentales.	• Brinda confidencialidad, integridad y disponibilidad de los sistemas de información mediante el uso de una evaluación mixta. • Identifica y clasifica los activos de TI. • Identifica y evalúa amenazas y vulnerabilidades, así como los niveles de riesgos.	• No contempla elementos importantes como los procesos y los recursos.

Fuente: Elaboración propia. Adaptado de (Novoa & Rodríguez, 2015) (Mogollón, 2016)

Selección de la metodología

La selección adecuada de una metodología de análisis de riesgos contribuye a que las organizaciones tengan mayor control sobre sus activos, realizar una correcta evaluación de los riesgos y que puedan minimizar las amenazas, siendo determinante el diseño e implementación de medidas de seguridad que garanticen la continuidad del negocio. Se han realizado una comparación entre las fases que involucra cada metodología para el establecimiento del SGSI, ver Tabla 7.

Según el resultado obtenido se determina que la metodología de gestión de riesgos que se usará para el presente proyecto es la Norma ISO/IEC 27005:2018. Dicha norma es aplicable a todo tipo de organización y cumple en su mayoría con las fases de análisis de riesgos.

Tabla 7.

Fases de metodologías de riesgos

FASES	METODOLOGÍAS					
	OCTAVE	ISO/IEC 27005	NIST SP 800-30	MAGERIT	MEHARI	CRAMM
Caracterización del Sistema	X	X	X	X	X	X
Identificar amenazas	X	X	X	X		X
Identificar vulnerabilidades	X	X	X	X		X
Análisis de controles	X	X	X	X	X	
Determinación de la probabilidad			X			

FASES	METODOLOGÍAS					
	OCTAVE	ISO/IEC 27005	NIST SP 800-30	MAGERIT	MEHARI	CRAMM
Análisis de impacto		X	X			
Determinación del riesgo	X	X	X	X	X	X
Recomendaciones de control	X	X	X		X	X
Documentación	X	X	X		X	
Parámetros				X		
Necesidades de Seguridad	X	X				X

Fuente: (Tejena Macías, 2018)

Descripción de la norma ISO/IEC 27005

La norma ISO 27005 fue publicada en el año 2008 y su principal finalidad es la de proporcionar directrices para la gestión de riesgos de seguridad de la información, ésta norma proporciona recomendaciones, usa el condicional, el cual se observa en la Figura 10, por ello no es necesario seguir todos los pasos del método.

La norma ISO/IEC 27005:2011 es aplicable en toda organización y sustituye las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000 de gestión de la información y comunicaciones de tecnología de seguridad.

El 10 de julio del 2018, se publica la nueva versión de ISO/IEC 27005 Information technology - Security techniques - Information security risk management, que ahora es su tercera edición.

Esta norma tiene gran importancia por ser una de las principales normas que se conecta a la norma de requisitos ISO/IEC 27001:2013 y que no había sido actualizada desde el 2011.

La actual edición de la norma ISO/IEC 27005 no presenta cambios radicales o muy detallados, centrándose principalmente en eliminar las referencias que ya no son de utilidad y las modificaciones necesarias para que la redacción sea compatible con los requisitos y fines de la ISO/IC 27001:2013.

Es importante mencionar que esta norma destaca, que para el cumplimiento de los requisitos de ISO/IEC 27001 se puede utilizar distintas metodologías de gestión del riesgo, con lo cual el contenido de esta ISO/IEC 27005 es totalmente aplicable pero no es la única metodología, se pueden utilizar otras formas de cumplir los requisitos de gestión del riesgo dependiendo de las necesidades y recursos de cada empresa.

Entre los principales cambios en la última versión tenemos:

- Se eliminan por completo todas las referencias a la norma internacional ISO/IEC 27001:2005.
- La introducción de la norma contiene información sobre la aplicabilidad de esta norma en el cumplimiento de los requisitos de ISO/IEC 27001.
- Se elimina el anexo G y todas sus referencias.
- Se realizan los cambios editoriales pertinentes para mantener una coherencia en el texto del documento.
- ISO 27001 se ha agregado a la bibliografía
- ISO 27001:2005 se ha eliminado de la Cláusula 2.

Con la publicación de esta norma, en su última versión se completa el conjunto de normas que son base para el apoyo en implementación de un SGSI basado en ISO/IEC 27001:2013.

Además, se complementa con la norma ISO/IEC 27005 (gestión del riesgo), con la ISO/IEC 27002 (código de practica sobre controles), ISO/IEC 27003 (guía sobre los requisitos) y la ISO/IEC 27004 (monitoreo, medición, análisis y evaluación).

ISO/IEC 27005:2018 brinda el enfoque para la gestión de riesgos y dependiendo de la naturaleza del entorno, se establecen los criterios para el análisis. La forma en que se gestionan los riesgos es importante, ya que se deben generar estrategias para dar cumplimiento a los objetivos de la organización.

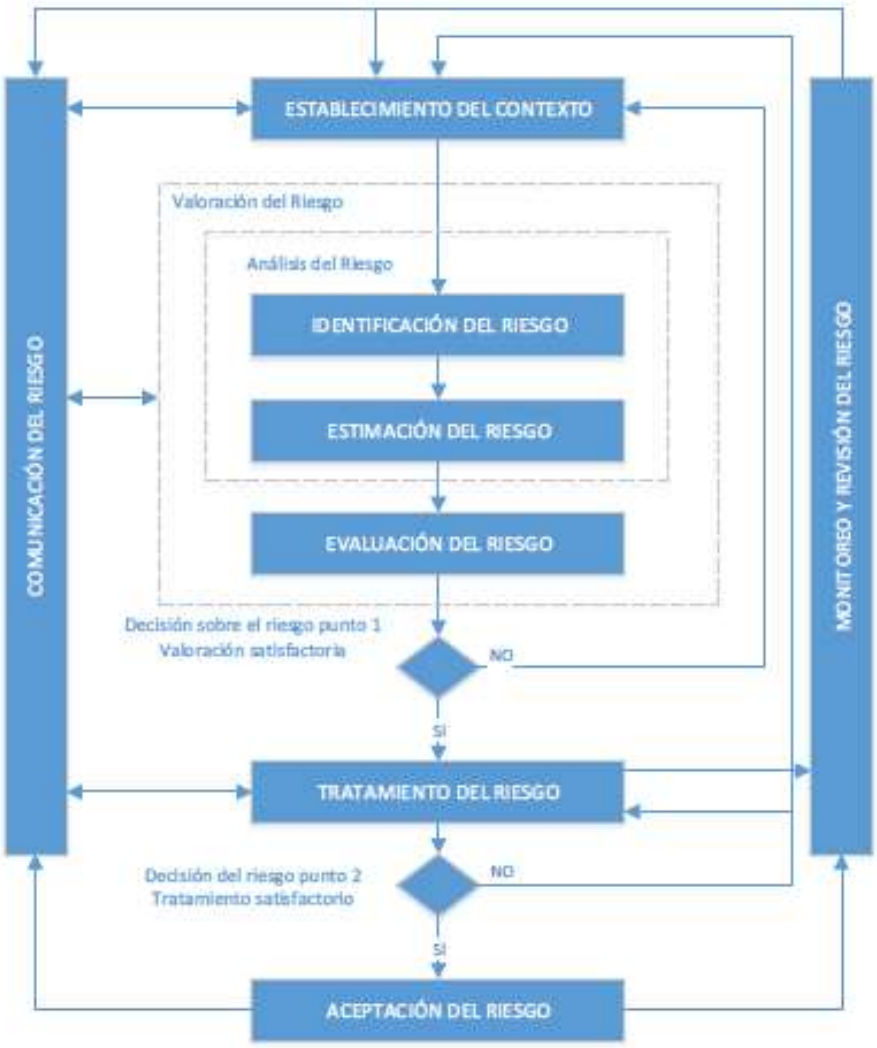
La gestión de riesgos es un proceso continuo el cual nos proporciona las herramientas necesarias para revaluar la gestión realizada y garantizar así el estudio de nuevos riesgos y el establecimiento de nuevos criterios según sea el entono en el que se encuentre.

Las actividades de gestión de riesgos presentadas en la Cláusula 7 a la Cláusula 12 de ésta norma están estructuradas de la siguiente manera:

- **Entrada:** identifica la información requerida para realizar las diferentes actividades en la organización.
- **Acción:** describe la actividad.
- **Guía de implementación**: proporciona una pauta sobre la realización de la acción.
- **Salida:** identifica información originada después de realizar la actividad.

Figura 10.

Gestión del riesgo



Fuente: (Lema Vinlasaca & Donoso Gallo, 2018)

La norma ISO/IEC 27005:2018 describe las actividades y procesos para realizar una correcta gestión del riesgo en cuanto a la seguridad de la información en determinada organización. Para su análisis se determina realizar lo siguiente:

1. **El establecimiento del contexto:** se define los objetivos, el alcance, hasta donde llegará el análisis y representa donde se establecen los criterios necesarios para el análisis de riesgos.
2. **La evaluación del riesgo:** los tres aspectos que se contemplan son:

- La identificación del riesgo: se realiza la clasificación de los activos, se estable el nivel de importancia de cada uno, se identifican las amenazas, las vulnerabilidades y el impacto que se tendría en caso de que una amenaza explote una vulnerabilidad.
- La estimación del riesgo: se define la metodología, los criterios para la valoración de las consecuencias y la valoración de los incidentes.

3. La evaluación del riesgo: se realiza el análisis de los activos relacionándolos con las posibles amenazas, se realiza la construcción de una matriz, cuyo objetivo es hallar el nivel de riesgo de cada uno de los activos de la organización.
4. **El tratamiento del riesgo:** se definen los riesgos encontrados, los controles y las estrategias a implementar para cada uno de ellos.
5. **La aceptación del riesgo:** se determina si los riesgos se aceptan o no, y se definen los controles que deben proporcionarse para cada uno de ellos.
6. **La comunicación y consulta del riesgo:** se debe comunicar a la organización, el tratamiento que se les dé a los riesgos encontrados.
7. **Monitoreo y revisión del riesgo:** en base al tratamiento que se dé a los riesgos encontrados, se debe realizar el respectivo monitoreo y mejora continua.

Capítulo IV

SITUACIÓN ACTUAL DE LA ORGANIZACIÓN

En el presente capítulo se realizará el análisis de la situación actual del GAD Municipal del cantón Pujilí, en cuanto a la seguridad de la información. Se empezará con las generalidades y su estructura organizacional, para luego realizar una evaluación del estado actual frente a la seguridad de la información, y validar el cumplimiento de los dominios de la norma. ISO27001:2013.

Generalidades del GAD Municipal del Cantón Pujilí

Historia

La municipalidad del cantón Pujilí, fue creada mediante decreto de la Honorable Asamblea Constituyente de 22 de septiembre de 1852, publicado por el juzgado primero parroquial de Pujilí, el 14 de octubre del mismo año, durante la presidencia del Gral. José María Urbina, es reconocido como Cantón de la Provincia de León (Cotopaxi). Posteriormente cambio su denominación a Gobierno Autónomo Descentralizado Municipal del Cantón Pujilí (Fuenmayor Pazmiño & Sarzosa Pavón, 2015).

Siendo una entidad de gobierno seccional tiene como función principal administrar el cantón de manera autónoma frente al gobierno central, el poder ejecutivo está representado por el alcalde, y el poder legislativo formado por los miembros del Concejo Cantonal. La Constitución prevé para los gobiernos autónomos descentralizados autonomía tanto política, administrativa y financiera, dando amplitud y legalidad para gobernar bajo sus propias normas y medios de gobierno dentro de sus respectivos límites territoriales.

Misión

La misión que el Departamento de Planificación del GAD Municipal del cantón Pujilí, ha planteado en su administración es la siguiente:

- Plantear, implementar y sostener las acciones del desarrollo del gobierno local.
- Dinamizar los proyectos de obras y servicios con calidad y oportunidad, que asegure el desarrollo social y económico de la población, con la participación directa y efectiva de los actores sociales, dentro de un marco de transparencia, ética, institucional y el uso óptimo de recursos humanos.

Visión

El Gobierno Autónomo Descentralizado Municipal de Pujilí, para los próximos años se constituirá en un ejemplo del desarrollo local y contará con una organización interna, altamente eficiente, que genere productos y servicios compatibles con la demanda de la sociedad, capaz de asumir los nuevos papeles vinculados con el desarrollo, con identidad cultural y de género.

Valores organizacionales

Los valores organizacionales son un conjunto de principios y reglas que regula a la entidad. Estos valores sirven como orientación para la conducta de los servidores del GAD Municipal del cantón Pujilí, los valores más destacados son:

- Equidad
- Imparcialidad
- Respeto
- Honestidad
- Confidencialidad
- Responsabilidad
- Solidaridad
- Justicia

Estructura organizacional del GAD Municipal

De acuerdo a las Reformas del Reglamento Orgánico de Gestión Organizacional, El GAD Municipal del cantón Pujilí, para el cumplimiento de su misión y responsabilidades, define los procesos que se muestran en la Figura 11.

- Los **procesos gobernantes** se encargan de la formulación de políticas y la expedición de normas para poner en funcionamiento a toda la organización.
- Los **procesos habilitantes** están encaminados a generar productos y servicios para los procesos gobernantes, institucionales y para sí mismos, viabilizando la gestión institucional.
- Los procesos **agregadores de valor** generan, administran y controla los productos y servicios destinados a usuarios externos.

Figura 11.

Mapa de procesos GAD Municipal de Pujilí

Fuente: Elaboración propia. Adaptado de (BG Consultores Asociados, 2015)

Análisis FODA

La matriz FODA es una herramienta que sirve para realizar el análisis a ser aplicado a cualquier situación, individuo, o empresa que sea tratado como objeto de estudio.

El objetivo del análisis FODA en el GAD Municipal, se orienta a conformar un cuadro de la realidad actual de la organización, conociendo sus fortalezas, oportunidades, debilidades y amenazas, es decir obtener un diagnóstico preciso que permitirá tomar decisiones de acuerdo a los objetivos y políticas establecidos. La matriz FODA muestra en la Tabla 8.

Tabla 8.

Matriz FODA GAD Municipal

FORTALEZAS	OPORTUNIDADES
• El GAD municipal cumple con todos los reglamentos para la ejecución de trámites. • Cubre las necesidades de la sociedad con un liderazgo efectivo. • Trabajo en equipo. • Soporte y coordinación tecnológico entre áreas.	• Nuevas tecnologías en software y hardware. • Mejorar la imagen institucional. • Optimización, eficiencia y agilidad en los procesos. • Proporcionar información actual y precisa. • Excelencia en la atención al usuario interno y externo. • Información financiera oportuna
DEBILIDADES	**AMENAZAS**
• Incertidumbre, desmotivación e inestabilidad laboral. • Falta de un plan de contingencia informático y de seguridad institucional. • Falta de responsabilidad y compromiso de la institución. • Débil capacitación técnica o actualización de conocimientos • Falta de cultura organizacional.	• Recorte de presupuestos técnicamente establecidos. • Incremento de la cartera vencida. • Fuga de información. • Inestabilidad política. • Inconformidad de la comunidad. • Falta de procedimientos institucionales para la gestión de la información.

Eje político institucional y de participación ciudadana

La municipalidad cuenta con 8 objetivos estratégicos alineados con los objetivos del Buen Vivir, mismos que promueven el desarrollo integral del cantón. Su propósito fundamental es trabajar por los intereses locales, mejorar las zonas tanto urbanas como rurales, buscar soluciones a problemas sociales, ambientales y económicos, considerar las problemáticas y encontrar alternativas.

Dentro del ámbito interno del GAD se plantea capacitar continuamente al personal, desenvolverse en un ambiente ético y transparente. La Tabla 9, muestra el objetivo estratégico, los indicadores por objetivo y las metas por objetivo relacionadas a las actividades que deberían alcanzar la unidad de informática. Las Figura 12 muestra el organigrama institucional actual.

Tabla 9.

Eje político institucional GAD Municipal

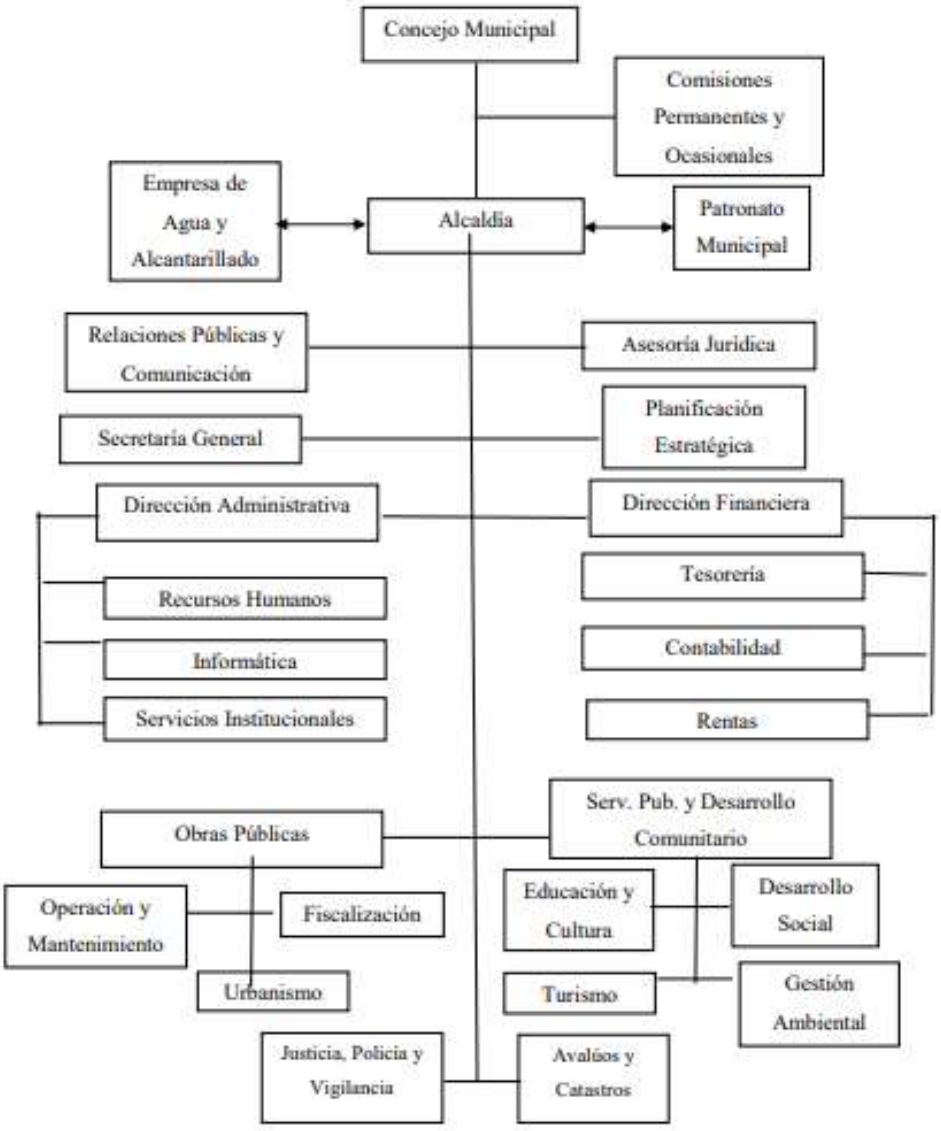
OBJETIVO ESTRATÉGICO	**IMPULSAR EL FORTALECIMIENTO INSTITUCIONAL**
Indicadores por objetivo	• Servidores capacitados. • Procesos Implementados. • Página Web actualizada. • Implementado el sistema cantonal de información. • Redes, protección de equipo informático y otras mejoradas. • Proyecto de Infraestructura de comunicación voz y datos, seguridad y video vigilancia, sistema de control de personal, data center implementado.
Metas por objetivo	• 100% de servidores capacitados. • 100 % de procesos implementados. • 100% Página web Actualizada. • 100% del Mejoramiento de redes, protección de equipo informático. • 100% en la implementación del proyecto de Infraestructura de comunicación voz y datos, seguridad y video vigilancia, sistema de control de personal, data center.

Fuente: Elaboración propia. Adaptado de (BG Consultores Asociados, 2015)

Organigrama institucional

Figura 12.

Organigrama institucional actual



Fuente: (Dirección de Planificación, 2018)

Identificación de los controles existentes

Las organizaciones tratan de proteger sus activos estableciendo controles para así evitar que sus activos se vean afectados por las potenciales amenazas a los que están expuestos diariamente. Para verificar el establecimiento de controles en la organización, se debe realizar la revisión en el lugar donde se efectúa el control y verificar el correcto cumplimiento, es importante realizar un seguimiento a los controles existentes validando la eficacia de los mismos, si no se realiza este proceso, se puede estar expuesto a que las amenazas exploten las vulnerabilidades, para ello se deben tener controles que realicen el tratamiento del riesgo identificado de manera eficaz y eficiente.

Actualmente no se ha realizado el establecimiento de un SGSI en la unidad de informática del GAD Municipal del cantón Pujilí, esto conlleva a realizar una evaluación el estado actual de la seguridad de la información, y validar como se encuentra con respecto al cumplimiento de los 14 dominios de la norma. De éstos 14 dominios, no se aplica el dominio 7 sobre la seguridad de los recursos humanos y el dominio 14 de la adquisición, desarrollo y mantenimiento de sistemas. La Tabla 10, se puede observar los resultados de la validación de controles en la unidad de informática del GAD Municipal, obteniendo el estado actual de seguridad de la información con respecto a la norma ISO/IEC 27001:2013. Se determina lo siguiente:

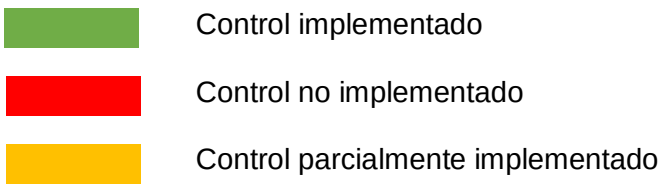


Tabla 10.

Estado actual de la seguridad de la información

A.5 Políticas de seguridad de la información					
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información **Objetivo:** Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.					
A.5.1.1	Políticas para la seguridad de la información.	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	**Implementado** SI / **NO** / PARCIAL		La unidad de informática no cuenta con políticas de seguridad de la información publicadas y comunicadas a los empleados y partes externas pertinentes, que permita conocer las directrices con respecto a la seguridad.
A.5.1.2	Revisión de la política para la seguridad de la información.	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos.	**Implementado** SI / NO / PARCIAL		La unidad de informática al no tener políticas de seguridad de la información publicadas y comunicada a los empleados y partes externas pertinentes, tampoco las revisan.
A.6 Organización de la seguridad de la información					
6.1 Organización interna **Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.					
A.6.1.1	Roles y responsabilidades para la seguridad de información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	**Implementado** SI / NO / PARCIAL		En la unidad de informática no se ha implementado un SGSI, por lo tanto, no se tienen definidas y asignadas las responsabilidades con respecto a la seguridad de la información.

A.6.1.2	Separación de deberes.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional.	**Implementado** SI NO PARCIAL En el GAD Municipal, todo el personal está separado por áreas y funciones y se le concede el acceso necesario a la información y/o activos para realizar su trabajo diariamente.
A.6.1.3	Contacto con las autoridades.	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.	**Implementado** SI NO PARCIAL Las incidencias referentes a la seguridad de la información en la unidad de informática son resueltas internamente por el personal.
A.6.1.4	Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	**Implementado** SI NO PARCIAL No existe vínculos con proveedores de servicios, especializados en seguridad, que guíen a la unidad de informática sobre la seguridad de la información.
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	**Implementado** SI NO PARCIAL En la unidad de informática no se incluye a la seguridad de la información, en la gestión de proyectos realizados.

6.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.6.2.1	Política para dispositivos móviles.	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	**Implementado** SI NO PARCIAL En la unidad de informática no existen políticas y medidas de seguridad, publicada y aprobada, que gestionen el uso de dispositivos móviles.

A.6.2.2	Teletrabajo.	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	**Implementado** SI NO PARCIAL En la unidad de informática no existen políticas y medidas de seguridad, publicada y aprobada, que gestionen el teletrabajo.

A.7 Seguridad de los recursos humanos

7.1 Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio.	**Implementado** SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.
A.7.1.2	Términos y condiciones del empleo.	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	**Implementado** SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.

7.2 Durante la ejecución del empleo

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

A.7.2.1	Responsabilidades de la dirección.	Control: La dirección debe exigir a los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.	**Implementado** SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes.	**Implementado** SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**Implementado** SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.

7.3 Terminación o cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.

A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado.	Implementado SI NO PARCIAL NO APLICA. La contratación del personal es responsabilidad del área de recursos humanos.

A.8 Gestión de activos

8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

A.8.1.1	Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de activos.	**Implementado** SI NO PARCIAL En el GAD Municipal, la unidad informática cuenta con un inventario parcial de los activos de información, el cual se encuentra desactualizado y no se encuentran evaluados de acuerdo a su criticidad e importancia.
A.8.1.2	Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario.	**Implementado** SI NO PARCIAL En el GAD Municipal, la unidad informática cuenta con un inventario parcial de los activos de información, el cual se encuentra desactualizado, y no se determina la tenencia y la legítima custodia de los activos de éste inventario.
A.8.1.3	Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	**Implementado** SI NO PARCIAL Según la unidad informática de la entidad no cuenta con un manual donde no existan reglas para el uso aceptable de los activos asociados con la información y procesamiento de la información.
A.8.1.4	Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	**Implementado** SI NO PARCIAL Al terminar su vínculo laboral de los empleados, existe un proceso de paz y salvo mediante el cual se valida que los empleados registren la devolución de los activos entregados por el GAD Municipal.

8.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

A.8.2.1	Clasificación de la información.	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	**Implementado** SI NO PARCIAL En la unidad informática no se realiza un proceso de clasificación de la información en cuanto a la criticidad, importancia y valor de la misma.
A.8.2.2	Etiquetado de la información.	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado.	**Implementado** SI NO PARCIAL En la unidad informática al no realizarse la clasificación de la información, es evidente que no se realiza un adecuado etiquetado de la misma.
A.8.2.3	Manejo de los activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema adoptado por la organización.	**Implementado** SI NO PARCIAL En la unidad informática no cuenta con un manual de procedimientos en donde se determine el manejo de los activos.

8.3 Manejo de medios

Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

A.8.3.1	Gestión de medios removibles.	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema adoptado por la organización.	**Implementado** SI NO PARCIAL En la unidad informática, no existen procedimientos para la gestión de medios removibles que sean utilizados o empleados dentro de la organización.

A.8.3.2	Disposición de los medios.	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	**Implementado** SI NO PARCIAL Los medios son ubicados en un lugar seguro, sin embargo en la unidad de informática, no existe un procedimiento formal que regule este proceso.
A.8.3.3	Transferencia de medios físicos.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	**Implementado** SI NO PARCIAL Los medios físicos son ubicados en un lugar seguro, sin embargo, éstos medios poseen mínimas condiciones de seguridad para el acceso no autorizado, uso indebido o corrupción durante el transporte.

A.9 Control de acceso

9.1 Requisitos del negocio para control de acceso

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

A.9.1.1	Política de control de acceso.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Implementado SI NO PARCIAL En la unidad informática, no existen controles físicos ni lógicos debido a no contar con una política de control de acceso que defina la visión de la seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Implementado SI NO PARCIAL Aunque en la unidad informática existen controles para el uso de recursos de red, no existe una política establecida y documentada correctamente, que indique los controles con respecto al personal que debería contar con accesos a éstos servicios.

9.2 Gestión de acceso de usuarios

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

A.9.2.1	Registro y cancelación del registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	**Implementado** SI / **NO** / PARCIAL A los servidores de la entidad, no se les asigna un identificador único de usuario dentro de los sistemas informáticos que usan y han usado.
A.9.2.2	Suministro de acceso de usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas.	**Implementado** **SI** / NO / PARCIAL Existe un proceso mediante el cual se asignan o revocan derechos de accesos a los usuarios para todos los sistemas y servicios que presta el área dentro de la institución.
A.9.2.3	Gestión de derechos de acceso privilegiado.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**Implementado** **SI** / NO / PARCIAL A los servidores que son usuarios de los diferentes sistemas se les otorga privilegios, teniendo en cuenta el perfil del cargo y las necesidades diarias en las actividades que realizan
A.9.2.4	Gestión de información de autenticación secreta de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	**Implementado** SI / NO / **PARCIAL** A los servidores se les entrega claves de acceso, sin embargo no existe un proceso formal para controlar el acceso a la información de tipo secreta.
A.9.2.5	Revisión de los derechos de acceso de usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	**Implementado** SI / NO / **PARCIAL** En la unidad informática que son los propietarios de los activos no cuenta con un inventario actualizado de los mismos, por lo que se dificulta realizar el control de derechos de forma periódica.

A.9.2.6	Retiro o ajuste de los derechos de acceso.	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo.	**Implementado** SI NO PARCIAL La unidad informática realiza el retiro de accesos a los servidores que dejan de prestar servicios en la institución, sin embargo no existe un proceso o documentación formal para el retiro de privilegios de acceso.

9.3 Responsabilidades de los usuarios
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

A.9.3.1	Uso de información de autenticación secreta.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	**Implementado** SI NO PARCIAL La unidad informática previamente informa a los usuarios de los diferentes sistemas, que la política institucional es cumplir correctamente con la autenticación secreta para el uso de la información.

9.4 Control de acceso a sistemas y aplicaciones
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1	Restricción de acceso Información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	**Implementado** SI NO PARCIAL Los sistemas informáticos que maneja la entidad poseen controles específicos y exclusivos que restringen el acceso, sin embargo, no se encuentra una política formalizada.
A.9.4.2	Procedimiento de ingreso seguro.	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	**Implementado** SI NO PARCIAL La unidad informática reporta que, si se cumple con los procedimientos de ingreso seguro, en los sistemas informáticos que posee la entidad.

A.9.4.3	Sistema de gestión de contraseñas.	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	**Implementado** SI NO PARCIAL La unidad informática ha implementado los requisitos mínimos para el uso de las contraseñas, sin embargo, no se configura en los sistemas de información, un tiempo de vencimiento de las contraseñas, forzando a los usuarios a cambiarlas periódicamente.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	**Implementado** SI NO PARCIAL La unidad informática ha implementado medianamente los controles para evitar que los servidores puedan instalar herramientas que afectan el normal y correcto funcionamiento de los equipos y de los sistemas de información de la entidad.
A.9.4.5	Control de acceso a códigos fuente de programas.	Control: Se debería restringir el acceso a los códigos fuente de los programas.	**Implementado** SI NO PARCIAL La unidad informática a través de su personal son las personas autorizadas, que por medio de la programación de sus equipos y a los sistemas informáticos restringen la manipulación y modificación del código fuente.

A.10 Criptografía

10.1 Controles criptográficos

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

A.10.1.1	Política sobre el uso de controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Implementado SI NO PARCIAL Actualmente la unidad informática reporta que no existe una política sobre el uso de algoritmos de encriptación para la protección de la información de la entidad.

A.10.1.2	Gestión de llaves.	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.	**Implementado** SI NO PARCIAL Actualmente la unidad informática reporta que no existe política sobre el uso, protección y tiempo de vida de las llaves criptográficas.

A.11 Seguridad física y del entorno

11.1 Áreas seguras

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

A.11.1.1	Perímetro de seguridad física.	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica.	**Implementado** SI NO PARCIAL La unidad informática no cuenta con un perímetro de seguridad definido, tampoco cuenta con las medidas de protección activas y pasivas.
A.11.1.2	Controles de acceso físicos.	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	**Implementado** SI NO PARCIAL En la unidad informática no están implementados controles de acceso biométricos y magnéticos que registren la hora y fecha de acceso, por lo tanto, aumenta el riesgo de daños o hurto de información sensible.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**Implementado** SI NO PARCIAL En la unidad informática no se evidencia que exista dispositivos de seguridad física.
A.11.1.4	Protección contra amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**Implementado** SI NO PARCIAL En el GAD Municipal, así como en la unidad informática no existen medidas de contingencia necesarias para hacer frente a las eventualidades de origen antrópico y natural, y que garanticen la continuidad del negocio.

A.11.1.5	Trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	**Implementado** SI / **NO** / PARCIAL Actualmente la unidad informática no cuenta con las condiciones mínimas de seguridad en la infraestructura que garantice el trabajo y las operaciones que se realizan en éste sitio.
A.11.1.6	Áreas de despacho y carga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**Implementado** **SI** / NO / PARCIAL El GAD municipal y en específico la unidad informática se encuentra de acuerdo a su distribución de ambientes y espacios se encuentra de forma aislada de las área de despacho, carga y alto tráfico de personas.

11.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	**Implementado** SI / **NO** / PARCIAL Los equipos en la unidad informática no se encuentran ubicados correctamente, además no se encuentran protegidos con medidas de seguridad activa y pasiva, así como el resguardo de la seguridad interna y externa de ésta área.
A.11.2.2	Servicios de suministro.	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	**Implementado** SI / NO / **PARCIAL** El GAD Municipal cuenta mínimamente con dispositivos de energía ininterrumpida para los equipos informáticos, pero carece de soporte alterno de fluido eléctrico y de comunicaciones.

A.11.2.3	Seguridad del cableado.	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación o interferencia.	**Implementado** SI / **NO** / PARCIAL La unidad de informática no cuenta con cableado estructurado, no existe una política que exija requerimientos mínimos que se deben cumplir para realizar la instalación de puntos de datos, de acuerdo a los estándares requeridos.
A.11.2.4	Mantenimiento de equipos.	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	**Implementado** SI / NO / PARCIAL La unidad informática realiza mantenimientos realizados por personal autorizado, éstos no son periódicos. sin embargo, se incumple con la disponibilidad e integridad de los mismos.
A.11.2.5	Retiro de activos.	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	**Implementado** **SI** / NO / PARCIAL La unidad informática notifica a sus servidores y usuarios de los sistemas, que el retiro de equipos, información o software se lo realizará previo a autorización.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones.	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera las mismas.	**Implementado** **SI** / NO / PARCIAL El GAD municipal, a través de la unidad informática determina como política que los equipos y activos informáticos, no pueden abandonar las instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado.	**Implementado** SI / NO / PARCIAL La unidad informática para los equipos que han cumplido su vida útil o tiempo de uso, verifica que la información, datos sensibles y software con licencia sea extraído y retirado de forma segura, sin embargo no existe un procedimiento formal para este proceso.

A.11.2.8	Equipos de usuario desatendidos.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les de protección apropiada.	**Implementado** SI NO PARCIAL La unidad informática garantiza medianamente el procedimiento de protección para los equipos desantedidos.
A.11.2.9	Política de escritorio limpio y pantalla limpia.	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	**Implementado** SI **NO** PARCIAL La unidad informática no cuenta con políticas de escritorio limpio y pantalla limpia y medios de almacenamiento removibles para los equipos y activos de la institución, como un proceso de capacitación a los servidores, en donde se especifiquen las mejores prácticas.

A.12 Seguridad de las operaciones

12.1 Procedimientos operacionales y responsabilidades.

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

A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Implementado SI NO PARCIAL La unidad informática no cuenta con los procedimientos operacionales y tampoco se encuentran documentados a fin de salvaguardar los equipos y activos informáticos de la organización.
A.12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Implementado SI NO PARCIAL Actualmente no se cuenta con un proceso establecido o definido que salvaguarde los sistemas de procesamiento de información por cambios en la entidad e instalaciones que puedan verse afectados en la seguridad de estos.

A.12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones.	**Implementado** SI NO PARCIAL En la unidad informática se realiza un control de los recursos y se realiza la proyección para la adquisición anual de nuevo equipamiento, de acuerdo a las necesidades del área en mención
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo informático.

12.2 Protección contra códigos maliciosos

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

A.12.2.1	Controles contra códigos maliciosos.	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**Implementado** SI NO PARCIAL La unidad informática cuenta con un servicio de firewall, mediante el cual se logra identificar y bloquear códigos maliciosos.

12.3 Copias de respaldo

Objetivo: Proteger contra la perdida de datos.

A.12.3.1	Respaldo de la información.	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de respaldo.	Implementado SI NO PARCIAL Se realizan copias de seguridad de los sistemas y aplicaciones más importantes para la continuidad del negocio, sin embargo, no se realizan pruebas periódicas de los mismos por parte de la unidad informática.

12.4 Registro y seguimiento
Objetivo: Registrar eventos y generar evidencia.

A.12.4.1	Registro de eventos.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**Implementado** SI NO PARCIAL La unidad informática mantienen los logs de los eventos ocurridos en los sistemas de información críticos para el negocio como medida de protección.
A.12.4.2	Protección de la información de registro.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	**Implementado** SI NO PARCIAL La unidad de informática cuenta con controles de autenticación en los sistemas de información con el objeto de evitar accesos no autorizados, los mismos que son alertados periódicamente.
A.12.4.3	Registros del administrador y del operador.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar.	**Implementado** SI NO PARCIAL Se registran las actividades de los administradores y de quienes operan los distintos sistemas de información, que posee la organización.
A.12.4.4	Sincronización de relojes.	Control: Los relojes de todos los sistemas de información dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	**Implementado** SI NO PARCIAL Los relojes de los sistemas de información, se encuentran sincronizados de acuerdo a una única zona horaria.

12.5 Control de software operacional
Objetivo: Asegurar la integridad de los sistemas operacionales.

A.12.5.1	Instalación de software en sistemas operativos.	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	**Implementado** SI NO PARCIAL Los usuarios de la organización no cuentan con los permisos necesarios para la instalación de ningún software, para cualquier instalación se debe solicitar autorización a la unidad de informática, no existe un procedimiento formal.

12.6 Gestión de la vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

A.12.6.1	Gestión de las vulnerabilidades técnicas.	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades.	**Implementado** SI NO PARCIAL Actualmente no se realizan evaluaciones continuas sobre las vulnerabilidades técnicas de los sistemas de información que se podrían presentar.
A.12.6.2	Restricciones sobre la instalación de software.	Control: Restricciones sobre la instalación de software.	**Implementado** SI NO PARCIAL La unidad informática posee procedimiento absoluto que restringe a los usuarios de la organización sobre la instalación de ningún software autorizado.

12.7 Consideraciones sobre auditorías de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

A.12.7.1	Controles de auditoría de sistemas de información.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para	Implementado SI NO PARCIAL Existe un área de auditoría interna de la organización, sin embargo, no se planifica ni se estima la realización de procedimientos de auditoría relacionados a la identificación de vulnerabilidades de los sistemas de información y que

		minimizar las interrupciones en los procesos del negocio.	se puedan tomar las acciones necesarias para la disminución de riesgos.

13. Seguridad de las comunicaciones

13.1 Gestión de la seguridad de las redes

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

A.13.1.1	Controles de redes.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	**Implementado** SI / **NO** / PARCIAL El GAD Municipal no cuenta con la implementación de infraestructura de llave pública que garantice la confidencialidad, integridad y disponibilidad de la información.
A.13.1.2	Seguridad de los servicios de red.	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea propios o contratados.	**Implementado** SI / NO / **PARCIAL** La unidad de informática cuenta con acuerdos de niveles de servicio con el ISP, en cuanto a la disponibilidad del servicio con el proveedor contratado.
A.13.1.3	Separación en las redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	**Implementado** SI / **NO** / PARCIAL Los usuarios de los servidores de los diferentes sistemas que posee la organización, no se encuentran separados a través de Vlans.

13.2 Transferencia de información

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

A.13.2.1	Políticas y procedimientos de transferencia de información.	Control: Se debería contar con políticas, procedimientos y controles para proteger la transferencia de información	**Implementado** **SI** / NO / PARCIAL En la unidad de informática cuenta con una política o procedimientos de transferencia de información con un

		mediante el uso de todo tipo de instalaciones de comunicación.	formato establecido sobre la capacidad (envío y recepción) de información.
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio.	**Implementado** SI NO PARCIAL La unidad de informática cuenta con controles criptográficos, así como los protocoles de transferencia segura para garantizar la transferencia segura de información.
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	**Implementado** SI NO PARCIAL La unidad de informática cuenta con un proceso para proteger la información enviada por medio de correo electrónico.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad que reflejen las necesidades de la organización.	**Implementado** SI NO PARCIAL La unidad de informática emite ciertos criterios sobre la confidencialidad y la no divulgación generada perteneciente a la entidad como medio de protección de la misma.

14 Adquisición, desarrollo y mantenimientos de sistemas

14.1 Requisitos de seguridad de los sistemas de información

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

A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, divulgación y modificación no autorizadas.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes y la divulgación no autorizada.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

14.2 Seguridad en los procesos de desarrollo y soporte

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

A.14.2.1	Política de desarrollo seguro.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo informático
A.14.2.2	Procedimientos de control de cambios en sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.2.4	Restricciones en los cambios a los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.2.5	Principios de construcción de sistemas seguros.	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.2.6	Ambiente de desarrollo seguro.	Control: La organización debe establecer y proteger los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, y actualizaciones se deben establecer pruebas y criterios de aceptación.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

14.3 Datos de Prueba

Objetivo: Asegurar la protección de los datos usados para pruebas.

A.14.3.1	Protección de datos de prueba.	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	**Implementado** SI NO PARCIAL NO APLICA. En la unidad de informática no se realiza desarrollo.

15. Relación con los proveedores

15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.	Control: Los requisitos de seguridad de la información para mitigar los riesgos del el acceso de proveedores a los activos, se deberían acordar y documentar.	Implementado SI NO PARCIAL La unidad informática no cuenta con una política que determine los lineamientos de seguridad que limite el acceso de los proveedores, contratistas a los activos que la institución posee referente a la información.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información con cada proveedor.	Implementado SI NO PARCIAL La unidad informática no ha estimado los requisitos de seguridad de la información que deben cumplir los proveedores.

A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información.	**Implementado** SI NO PARCIAL La unidad informática no determina acuerdos con los proveedores con respecto al tratamiento de los riesgos, en los que se ven inmersos la debida custodia, manipulación adecuada y responsabilidad de los activos de información.

15.2 Gestión de la prestación de servicios con los proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	**Implementado** SI NO PARCIAL La unidad informática realiza supervisión y seguimiento a la prestación de servicios de los proveedores, estimados a los procesos contractuales que tiene con ellos.
A.15.2.2	Gestión de cambios en los servicios de proveedores.	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información.	**Implementado** SI NO PARCIAL La unidad informática realiza supervisión y seguimiento a la prestación de servicios que los proveedores brindan a la entidad, los cuales son supervisados y revisados para que se mantenga la seguridad en los activos que poseen información..

16. Gestión de incidentes de seguridad de la información

16.1 Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información.

A.16.1.1	Responsabilidad y procedimientos.	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	**Implementado** SI NO PARCIAL El GAD Municipal no tiene determinadas las responsabilidades y procedimientos de respuesta a los posibles incidentes de seguridad de la información, que permitan dar una respuesta oportuna a cualquier eventualidad.
A.16.1.2	Reporte de eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	**Implementado** SI NO PARCIAL El GAD Municipal no tiene establecidos mecanismos y protocolos de comunicación efectiva sobre las eventualidades que pudieran presentarse referente a los incidentes de seguridad de la información.
A.16.1.3	Reporte de debilidades de seguridad de la información.	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad.	**Implementado** SI NO PARCIAL El GAD Municipal no tiene establecidos mecanismos de detección de las debilidades que podrían presentarse referente a los incidentes de seguridad de la información.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes.	**Implementado** SI NO PARCIAL La unidad informática no cuenta con procedimientos de evaluación que le permita definir las eventualidades que sucedieran, para posteriormente clasificarlo como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	**Implementado** SI NO PARCIAL La unidad informática no cuenta con protocolos de acción plenamente documentados, que le permitan actuar antes posibles incidentes de seguridad de la información.

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	**Implementado** SI NO PARCIAL La unidad informática no se cuenta con un registros de incidentes ocurridos y como han sido solventados, como medida de análisis y hacer frente ante futuros incidentes de seguridad de la información.
A.16.1.7	Recolección de evidencia.	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**Implementado** SI NO PARCIAL La unidad informática no cuenta con la fundamentación de los incidentes de seguridad de la información que se han presentado en eventos previos.

17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

17.1 Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

A.17.1.1	Planificación de la continuidad de la seguridad de la información.	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.	**Implementado** SI NO PARCIAL La unidad informática no estima procedimientos de contingencia definidos para garantizar la seguridad y la gestión de la información con el fin de asegurar la continuidad del negocio, frente a las posibles situaciones adversas.
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido.	**Implementado** SI NO PARCIAL La unidad informática no tiene claro el mecanismo para la implementación de los procedimientos de contingencia definidos para garantizar la seguridad y la gestión de la información.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	**Implementado** SI / **NO** / PARCIAL La unidad informática desde sus inicios no ha planificado, implementado y desarrollado acciones de monitoreo, seguimiento y control para garantizar la seguridad y la gestión de la información así como la operatividad y funcionalidad con el fin de asegurar la continuidad del negocio.

17.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	**Implementado** SI / **NO** / PARCIAL La unidad informática no dispone de redundancia de la información.

18. Cumplimiento

18.1 Cumplimiento de requisitos legales y contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

A.18.1.1	Identificación de la legislación aplicable a de los requisitos contractuales.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar, documentar y mantenerlos actualizados para cada sistema de información.	**Implementado** **SI** / NO / PARCIAL Este proceso es realizado por el área jurídica del GAD Municipal, quien garantiza el cumplimiento de los reglamentos legales aplicables a la organización, en función de cada uno de los sistemas informáticos que posee.

A.18.1.2	Derechos de propiedad intelectual.	Control: Se deberían implementar procedimientos para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	**Implementado** SI NO PARCIAL La unidad informática como usuario general de los sistemas informáticos, ya tienen propiedad intelectual por parte del administrador que se encuentra normado por la legislación de uso y operatividad de estos.
A.18.1.3	Protección de registros.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación contractuales.	**Implementado** SI NO PARCIAL La unidad informática no realiza acciones de protección contra la perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de registros sin base legal determinante.
A.18.1.4	Privacidad y protección de información de datos personales	Se debe asegurar la privacidad y la protección de la información de datos personales como se exige en la legislación.	**Implementado** SI NO PARCIAL Los sistemas informáticos que maneja y usa el GAD Municipal posee características de privacidad y protección de los datos personales de forma efectiva de acuerdo a la legislación vigente nacional sobre este tema.
A.18.1.5	Reglamentación de controles criptográficos.	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	**Implementado** SI NO PARCIAL El GAD Municipal a través de la unidad informática reporta que no se usan controles necesarios que garanticen la transmisión segura de la información.

18.2 Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

A.18.2.1	Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	**Implementado** SI NO PARCIAL El GAD Municipal a través de la unidad informática reporta que no se revisa los objetivos de control, políticas, procesos ni procedimientos documentados para la seguridad de la información por la no existencia de los mismos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas.	**Implementado** SI NO PARCIAL El GAD Municipal a través de la unidad informática reporta que no el cumplimiento como tal de los objetivos de control, políticas, procesos ni procedimientos documentados para la seguridad de la información.
A.18.2.3	Revisión del cumplimiento técnico.	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	**Implementado** SI NO PARCIAL El GAD Municipal a través de la unidad informática reporta que no se programan la revisión y monitoreo de forma periódica normadas y estandarizados a la seguridad de la información.

Fuente: Elaboración propia. Adaptado de (ISO/IEC 27002, 2013) (Maureira Sánchez, 2017) (Oidor González, 2017) (Doria Corcho, 2015)

En la Tabla 11 se muestra los resultados, con los porcentajes de cumplimiento y el total de controles implementados en la organización según la norma ISO/IEC 27001:2013. El porcentaje total de controles implementados es de un 21%, existiendo dominios para los cuales no hay ningún tipo de control, lo que representa riesgos de seguridad de la información manejada por la unidad de informática del GAD Municipal.

Tabla 11.

Porcentajes de cumplimiento.

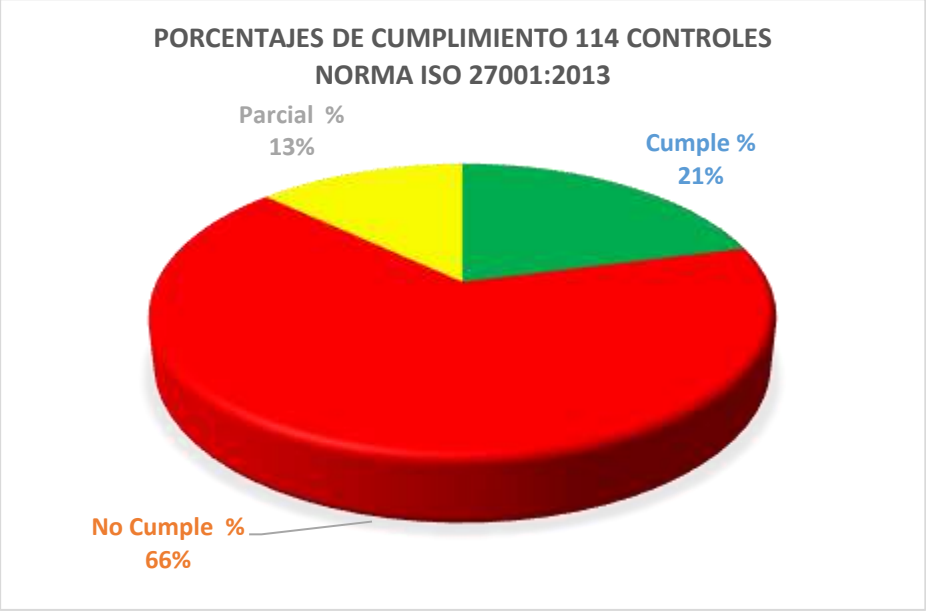
Dom.	Nombre	Total controles	Cumple	Cumple %	No cumple %	Parcial %
A5.	Políticas de la seguridad de la información	2	0	0%	100%	0%
A6.	Organización de la seguridad de la información	7	1	14%	86%	0%
A7.	Seguridad de los recursos Humanos	-	.	-	-	-
A8.	Gestión de activos	10	1	10%	50%	40%
A9.	Control de acceso	14	5	36%	14%	50%
A10.	Criptografía	2	0	0%	100%	0%
A11.	Seguridad física y del Entorno	15	3	20%	53%	27%
A12.	Seguridad de las operaciones	13	7	54%	23%	23%
A13.	Seguridad de las Comunicaciones	7	3	43%	43%	14%
A14.	Adquisición, desarrollo y mantenimiento de sistemas	-	-	-	-	-

Dom.	Nombre	Total controles	Cumple	Cumple %	No cumple %	Parcial %
A15.	Relación con los Proveedores	5	2	40%	60%	0%
A16.	Gestión de incidentes de seguridad de información	7	0	0%	100%	0%
A17.	Continuidad del negocio	4	0	0%	100%	0%
A18.	Cumplimiento	8	3	38%	62%	0%
TOTAL		**94**	**25**	**21%**	**66%**	**13%**

El porcentaje de nivel de cumplimiento general, respecto a los 12 dominios evaluados que se tiene actualmente en la organización se representa en la Figura 13.

Figura 13.

Nivel de cumplimiento



Fuente: Propia

Con los resultados obtenidos, se determina que la unidad de informática del GAD Municipal del cantón Pujilí no cumple con la mayoría de los dominios, objetivos de control y controles de seguridad que corresponden a la norma ISO/IEC 27002:2013, este porcentaje de no cumplimiento se debe a que no se tiene la debida documentación sobre la seguridad de la información, tampoco el empleo de mecanismos de seguridad para preservar la confidencialidad, integridad y disponibilidad de la información.

Por otro lado, las instalaciones físicas no están debidamente protegidas con controles de acceso, es decir, el personal y los activos informáticos de la unidad de informática no están lo suficientemente protegidos ante una eventualidad negativa, y no existen procedimientos de contingencia para garantizar la continuidad del negocio. En el Anexo 3, se puede observar la infraestructura actual de la unidad en mención.

Efectividad de controles-ISO 27001:2013

La gestión de la seguridad de la información debe pasar por varios niveles, cada uno tiene un valor asociado y un contexto de aplicabilidad. Se determina una escala de progresión en lo que ahora determinamos como SGSI basados en la norma ISO 27001.

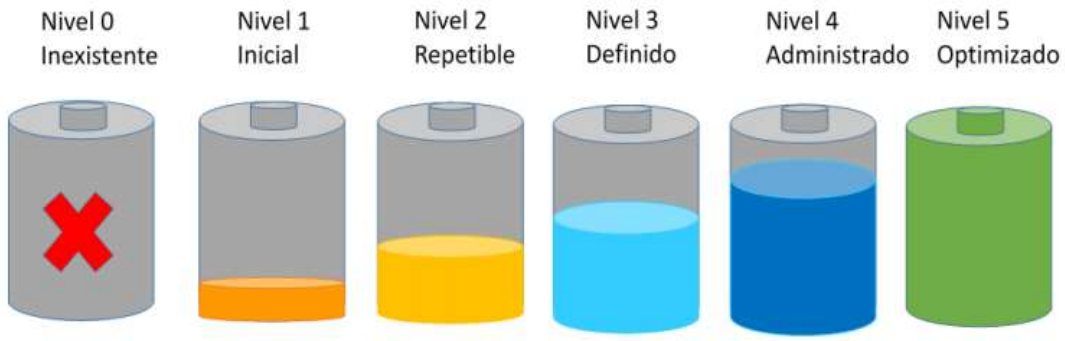
Este esquema identifica el nivel de madurez de la unidad de informática, midiendo la brecha entre el nivel actual y el nivel optimizado. A continuación, en la Figura 14, se muestran los diferentes niveles que conforman el modelo de madurez.

Cabe recalcar que la norma ISO 27001 requiere llevar a cabo las siguientes actividades:

- Definir responsabilidades para la administración de los controles.
- Medir y monitorear oportunamente la efectividad de los controles.
- Implementar acciones correctivas cuando se detecten fallos en los controles.

Figura 14.

Niveles de madurez



Fuente: (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2016)

- **Nivel 0:** Desconocimiento, no se tiene en cuenta el tema de la seguridad de la información.
- **Nivel 1:** Se reconoce que existen problemas de seguridad, que necesitan ser resueltos.
- **Nivel 2:** Se cuenta con procedimientos de seguridad, aunque no son formales para la organización.
- **Nivel 3:** Se realizan las siguientes etapas previas a la implementación.
- **Nivel 4:** Se realizan las fases de evaluación y mejora continua.
- **Nivel 5:** Se determina a la seguridad de la información, como valor agregado.

El esquema muestra los niveles de madurez, pretende establecer los criterios de valoración para determinar el estado actual de la seguridad de la información en la unidad de informática, como se muestra en la Tabla 12. Adicional, se realizó una encuesta a la analista de la unidad, para recopilar información acerca de los posibles riesgos que puedan afectar las actividades desarrolladas, ver el Anexo 2.

El tratamiento de la información es importante para el correcto funcionamiento de la organización, logrando en corto, mediano y largo plazo la ejecución de sus objetivos y garantizar la continuidad del negocio.

Según los resultados de la autoevaluación, en la Figura 15, se observa la brecha actual, así como también la brecha de seguridad a la cual se espera llegar de acuerdo a los plazos establecidos por el comité de seguridad de la información. Según (Campo Martínez, 2019) en la primera implementación del SGSI, el objetivo es llegar al cumplimiento de los dominios en un 60%.

Figura 15.

Brecha ISO27001:2013-Anexo A

Fuente: Propia

Tabla 12.

Evaluación de efectividad de controles

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
N°	DOMINIO	CALIFICACIÓN ACTUAL %	CALIFICACIÓN OBJETIVO %	EVALUACIÓN DE EFECTIVIDAD
A.5	Políticas de seguridad de la información	0%	60%	Inexistente
A.6	Organización de la seguridad de la información	14%	60%	Inicial
A.7	Seguridad de los recursos humanos	-	-	-
A.8	Gestión de activos	10%	60%	Inicial
A.9	Control de acceso	36%	60%	Repetible
A.10	Criptografía	0%	60%	Inexistente
A.11	Seguridad física y del entorno	20%	60%	Inicial
A.12	Seguridad de las operaciones	54%	60%	Efectivo
A.13	Seguridad de las comunicaciones	43%	60%	Efectivo
A.14	Adquisición, desarrollo y mantenimiento de sistemas	-	-	-
A.15	Relaciones con los proveedores	40%	60%	Repetible
A.16	Gestión de incidentes de seguridad de la información	0%	60%	Inexistente
A.17	Aspectos de seguridad de la	0%	60%	Inexistente

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
N°	DOMINIO	CALIFICACIÓN ACTUAL %	CALIFICACIÓN OBJETIVO %	EVALUACIÓN DE EFECTIVIDAD
	información de la gestión de la continuidad del negocio			
A.18	Cumplimiento	38%	60%	Repetible
Promedio evaluación de controles		**21%**	**60%**	**Repetible**

El realizar la evaluación de efectividad de los controles no es algo enfocado solo para conseguir la certificación de la norma internacional ISO 27001:2013, sino que debemos tener en cuenta que un sistema de gestión de la seguridad de la información correctamente implementado en la organización, puede ser la parte más importante para alinear los procesos de TI con los procesos operativos y comerciales de la organización.

La integración de la seguridad de la información en los procesos de la organización nos ayudará principalmente a reducir o mitigar el nivel del riesgo y proteger los activos de información.

La norma ISO 27001:2013 no tiene definidos los puntos de medición concretos para cada área de la organización.

La decisión sobre qué medir exactamente y los factores o procesos críticos de medición deben ser claramente definidos por la empresa y deben ser parte de la alineación del SGSI con las estrategias y los objetivos del negocio.

Análisis de red y vulnerabilidades

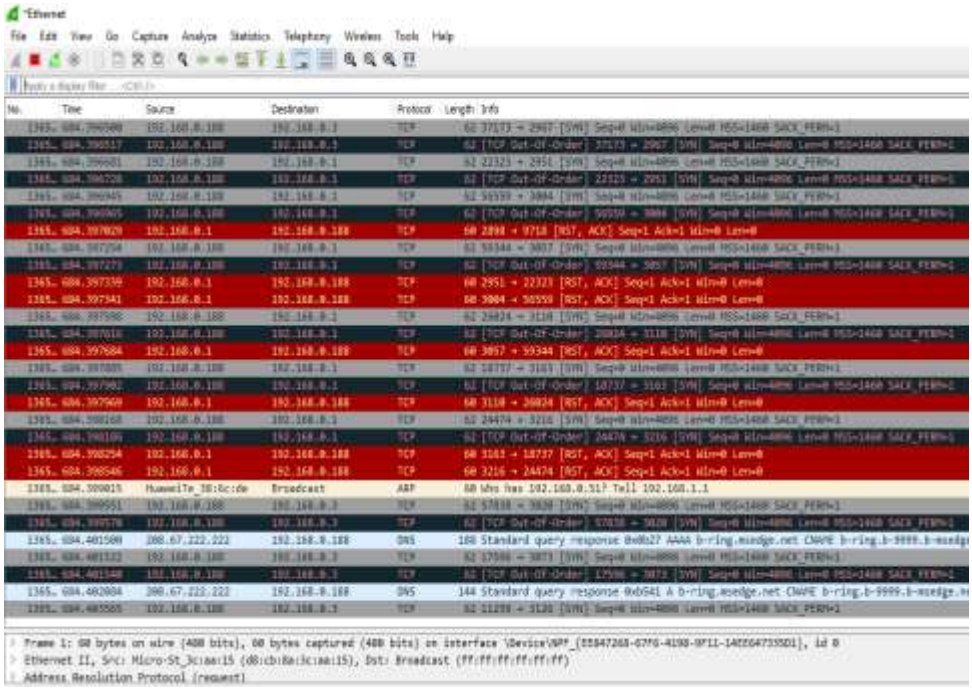
Wireshark es un analizador de protocolos de red. Le permite capturar y navegar interactivamente el tráfico que se ejecuta en una red informática. Tiene un conjunto de características y es la herramienta más popular del mundo en su tipo.

Se ejecuta en la mayoría de las plataformas informáticas, incluidas Windows, macOS, Linux y UNIX. Los profesionales de la red, los expertos en seguridad, los desarrolladores y los educadores lo usan regularmente. Está disponible gratuitamente como código abierto y se publica bajo la GNU General Public License versión 2 (Wireshark, 2021).

Se realizó el análisis en la unidad de informática para capturar los paquetes, y encontrar actividades maliciosas que afecte al desarrollo de las actividades, para ello se definió la interfaz y los paquetes se empiezan a capturar, como muestra la Figura 16.

Figura 16.

Captura de paquetes con Wireshark

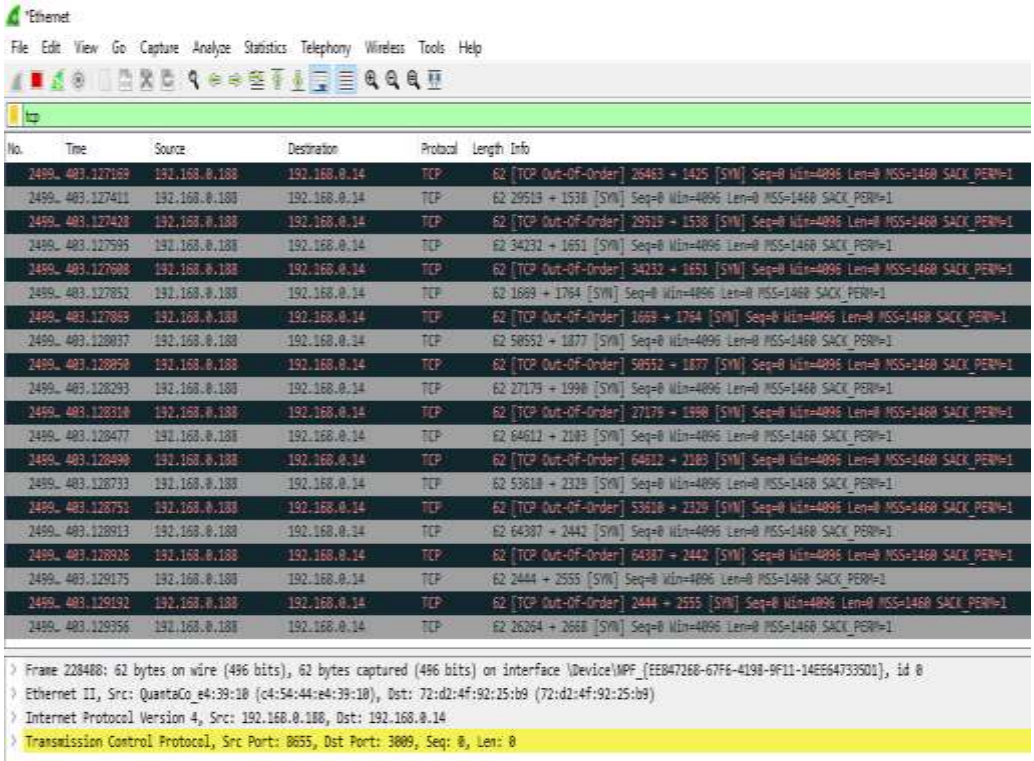


Fuente: Propia

Una de las principales características de Wireshark es el filtrado de paquetes, para obtener información detallada sobre un determinado protocolo. En el panel de captura se puede visualizar el número de secuencia de los paquetes, que no es más que un identificador único para cada uno, también se puede observar la marca del tiempo en el que un paquete fue capturado, las direcciones IP de origen y destino, el protocolo analizado, el tamaño del paquete e información adicional. En la Figura 17, se puede ver el filtrado del protocolo TCP.

Figura 17.

Filtrado protocolo TCP



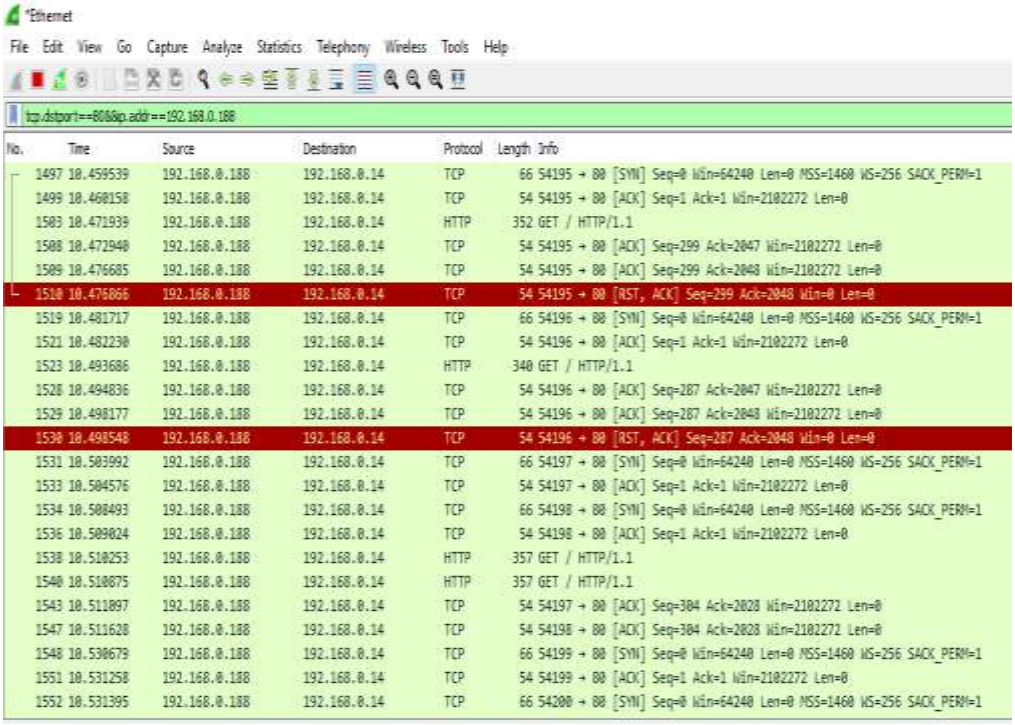
Fuente: Propia

Wireshark es una herramienta de gran utilidad para verificar todas las actividades que se están ejecutando en tiempo real en la red.

También se puede aplicar filtros específicos para el análisis, a continuación, en la Figura 18 se muestra la aplicación de un filtro para el análisis del protocolo TCP y cuya dirección de origen sea la IP 192.168.0.188.

Figura 18.

Filtrado TCP y dirección origen

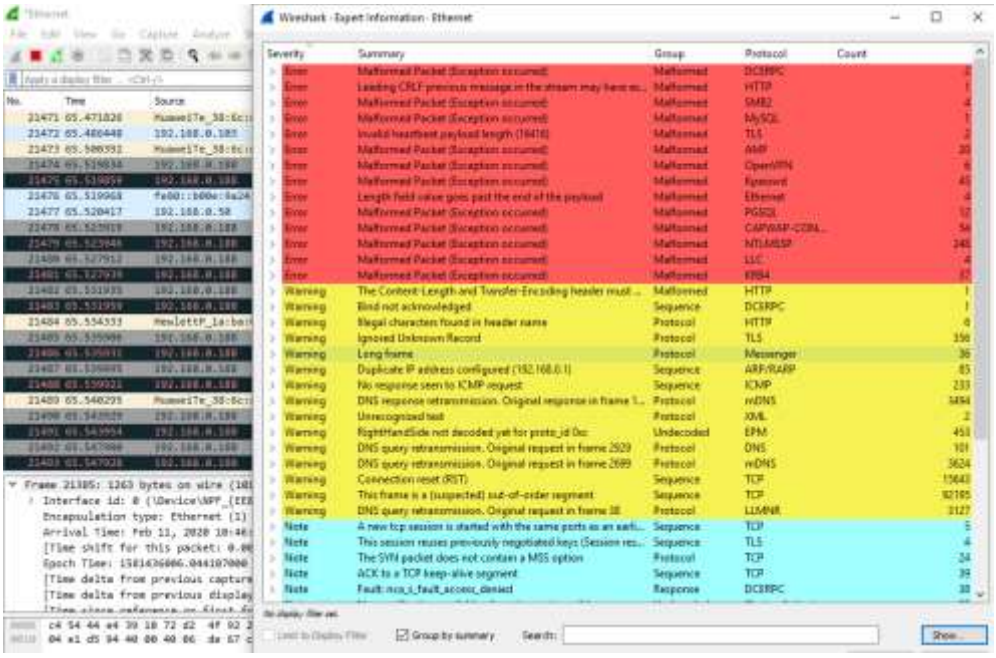


Fuente: Propia

A continuación, en la Figura 19 se muestra la información recopilada en el análisis realizado en la unidad de informática, para mantener un rastro de cualquier anomalía que se generó en la captura de los paquetes. Se encontraron errores, advertencias, notas de información y chat. Para un mejor análisis, la información se agrupa por protocolos, con lo que se obtiene información detallada para su análisis futuro.

Figura 19.

Información experta



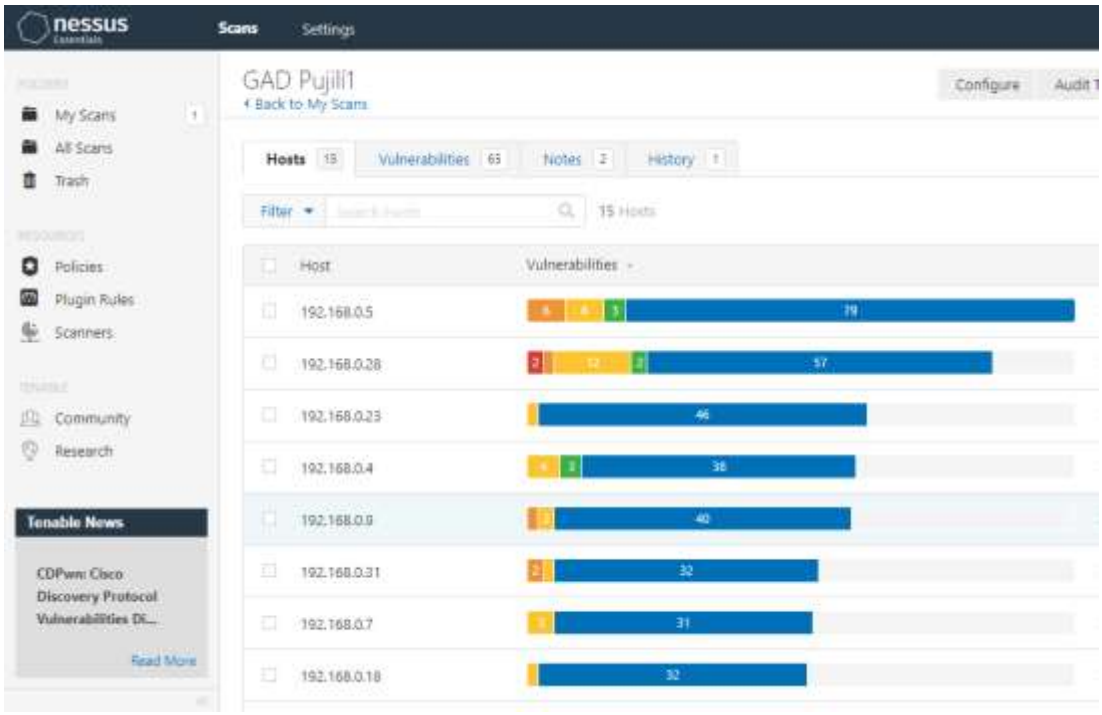
Fuente: Propia

Por otro lado, **Nessus** es una herramienta de escaneo de seguridad remota, que es capaz de escanear una dirección IP y generar una alerta si descubre cualquier vulnerabilidad que los hackers maliciosos podrían usar para acceder a cualquier computadora que se haya conectado a la red. Esto lo realiza ejecutando más de 1200 controles, para comprobar si alguno de estos ataques podría ser utilizado para entrar en el equipo o dañarlo de otro modo (Avilés Guzmán & Silva Uría, 2017).

Las pruebas realizadas en la unidad de informática del GAD Municipal del Cantón Pujilí, se realizaron con la dirección IP 192.168.0.0 para poder verificar el estado de la red, se realizó un escaneo avanzado, cuando finaliza el escaneo, se muestra una lista de todas las IP que están conectadas a la red en ese momento, como se puede ver en la Figura 20.

Figura 20.

Vulnerabilidades



Fuente: Propia

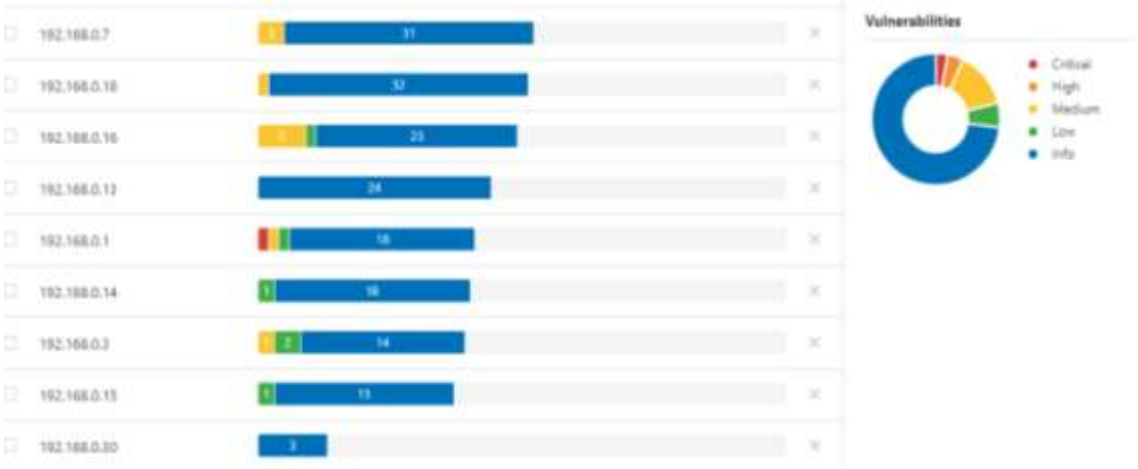
También muestra en un gráfico de anillos, con el total de vulnerabilidades encontradas, las clasifica en vulnerabilidades bajas, medias, altas y críticas con sus respectivos colores, Figura 21.

Al seleccionar las vulnerabilidades, se muestran primero las críticas con sus respectivos nombres, familia y adicional se muestra la cantidad de vulnerabilidades iguales que existen, como se representa en la Figura 22.

Es verdad que las vulnerabilidades son capaces de tirar abajo un sistema completo en cuestión de minutos, por eso para intentar frenarla es indispensable realizar controles de intrusión para así, minimizar los riesgos.

Figura 21.

Gráfico de anillos



Fuente: Propia

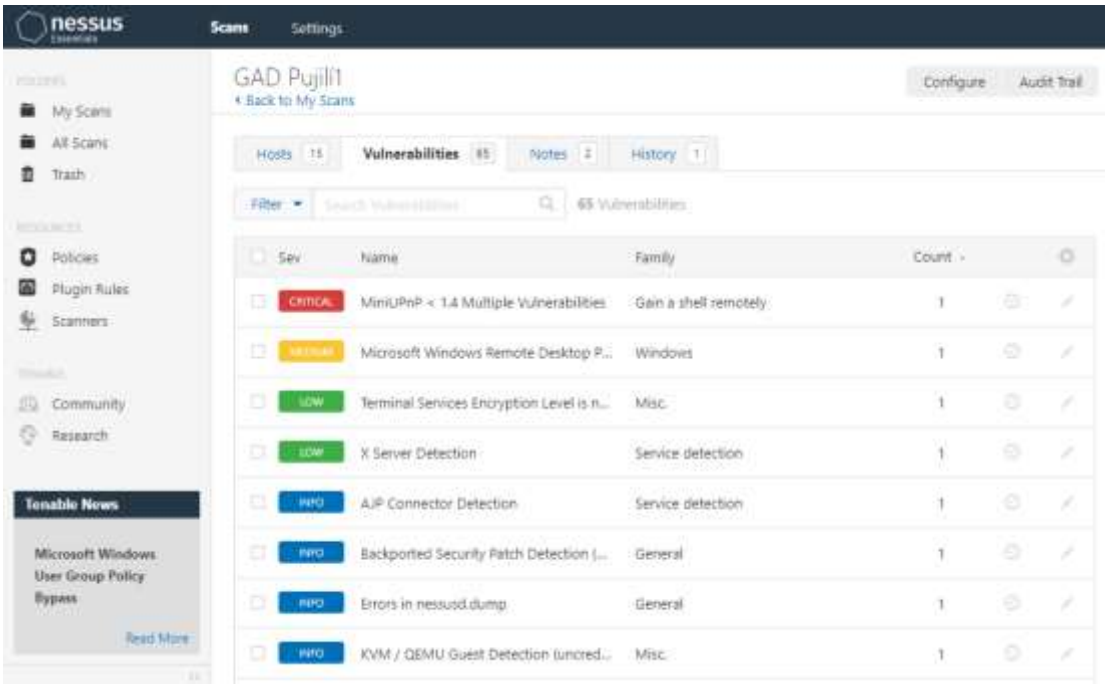
Al realizar el escaneo en la unidad de informática, se visualiza que existe una vulnerabilidad crítica. Se escogió la vulnerabilidad crítica encontrada, la cual muestra la descripción detallada para poderla analizar, la o las direcciones IP de los ordenadores que contienen la misma vulnerabilidad y la solución a aplicar, como muestra la Figura 23.

Se hace referencia a que la versión de MiniUPnP que se ejecuta en el host remoto es inferior a la 1.4, este es un protocolo de comunicación entre dispositivos, dentro de una red privada, cuya función está en abrir puertos de manera automática, sin que el administrador tenga que modificar la configuración del router.

Se debe tener en cuenta que, si la comunicación se inicia en Internet hacia la LAN, se necesita abrir un puerto para redirigir los paquetes correctamente a su destino. Los equipos de la LAN hacen uso de direccionamiento privado que no es enrutable a través de Internet.

Figura 22.

Clasificación de vulnerabilidades



Fuente: Propia

Una de las vulnerabilidades conocidas es: Cross Site Scripting (XSS). Esta es una vulnerabilidad que se presenta en las aplicaciones web, su función es inyectar código VBScript o JavaScript en páginas web a las que más ingresa el usuario.

El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL correcta, pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este lugar, se las está enviando al atacante.

Por otro lado, la denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red.

Figura 23.

Vulnerabilidad crítica

Fuente: Propia

Nessus es una de las herramientas más completa para poder realizar un análisis de vulnerabilidades en una organización, el problema hallado es que su precio es elevado y que la versión de prueba dura únicamente 7 días.

La interfaz gráfica de Nessus presenta los resultados de los análisis en tiempo real, la ventaja es que no se debe esperar a que finalice el análisis. Lo que hace diferente a Nessus de otros programas de escaneo de vulnerabilidades es que no supone que un servicio dado se ejecuta en un puerto fijo, sino que intenta comprobar una vulnerabilidad a través de su explosión.

La Tabla 13 muestra las vulnerabilidades que suelen manifestarse en determinado entorno de red. Por lo general estas vulnerabilidades aparecen debido a la falta de información sobre temas de seguridad de la información en todos los funcionarios de la organización.

Tabla 13.

Vulnerabilidades comunes

Vulnerabilidades	Descripción
Contraseñas, falta de ellas o dejar las predeterminadas del sistema.	Falta de contraseñas administrativas o usar contraseñas predeterminadas establecidas por el proveedor. Suele pasar en hardware tales como routers o switches.
Suplantación de IP	Una máquina remota actúa como un nodo en su red local, encuentra vulnerabilidades con sus servidores e instala un programa trasero para obtener recursos sobre la red.
Vulnerabilidades de servicios	El atacante busca una debilidad en un servicio en la red, compromete todo el sistema y datos que pueda contener.
Vulnerabilidades de aplicaciones	El atacante busca fallas en el escritorio y aplicaciones de trabajo, ejecutan un código arbitrario, implantan caballos de troya para dañar los sistemas.
Ataques de denegación de servicio	El atacante envía paquetes no autorizados al host de destino, para forzar al recurso a convertirse en disponible para usuarios legítimos.

Fuente: (Avilés Guzmán & Silva Uría, 2017)

Capítulo V

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En el presente capítulo se realizará el diseño de un sistema de gestión de seguridad de la información para la unidad de informática del GAD Municipal del cantón Pujilí, dicho sistema de gestión se basa en la norma ISO/IEC 27001:2013, en donde se realiza la identificación de los activos, amenazas y vulnerabilidades, se aplicará una metodología de gestión de riesgos con el fin de salvaguardar los activos.

Necesidad para diseñar e implementar un SGSI

Cada día, profesionales de TI se enfrentan a un mundo lleno de amenazas que ponen en riesgo los activos de su organización, debido a la gran cantidad de información importante que se maneja en la misma. Es por ello que las organizaciones tienen la necesidad de proteger la información que es su activo más valioso, estableciendo controles acordes a sus necesidades.

El establecimiento de un SGSI en una organización se podría tomar como un modelo para crear, implementar, mantener y mejorar la protección de los activos de información. La base del SGSI serán las políticas de seguridad de la información, donde la organización determinará los requisitos de seguridad y las estrategias para el debido cumplimiento de sus objetivos.

El sistema de gestión que se diseñe estará basado en una evaluación continua que permita una gestión eficaz y eficiente de los riesgos, e incluye el apoyo de la alta dirección y en sí de toda la organización. A través de la implementación de un SGSI se garantiza la gestión y protección eficiente de la información, la mejora continua, el monitoreo y las auditorías internas facilitan que los controles estén siempre actualizados y funcionen correctamente.

Selección de la metodología

Para el diseño e implementación del SGSI, la norma ISO/IEC 27001:2013 define que es necesario el cumplimiento de las siguientes fases, como se muestra en la Figura 24. Para el caso de estudio se desarrolla la fase “Plan”, incluyendo el plan de tratamiento de riesgos. Luego de terminar de implementar todas las fases, se vuelve a la primera para evaluar las mejoras necesarias.

Es importante tener en cuenta que la presencia y apoyo de la alta gerencia es primordial para el buen funcionamiento del SGSI en la organización.

Figura 24.

Fases del SGSI

Fuente: (Landázuri Benalcázar, 2017)

FASE I: Contextualización de la organización

La organización

El GAD Municipal cantonal de Pujilí es una institución pública del nivel cantonal con jurisdicción política administrativa, está ubicado en las calles García Moreno 5-00 y José Joaquín Olmedo, como se observa en la Figura 25.

Fue creado el 22 de septiembre de 1852. En la actualidad posee una población total de 69.055 habitantes, de los cuales 36.319 son mujeres y 32.736 son hombres (INEC, 2010).

Sus límites son: al norte: los cantones Sigchos, Saquisilí y Latacunga. Al sur: Pangua, y la provincia del Tungurahua. Al Este: Saquisilí, Latacunga y Salcedo. Al oeste: La Maná y Pangua, como se observa en la Figura 26. Tiene un total de 230 empleados (Unidad de Talento Humano, 2020).

Figura 25.

GAD Municipal del Cantón Pujilí

Fuente: (BG Consultores Asociados, 2015)

El GAD Municipal del Cantón Pujilí representa uno de los edificios más emblemáticos del cantón, por la estructura de su edificio antiguo, siendo así, uno de los municipios reconocidos a nivel nacional, gracias al esfuerzo y sacrificio de todos los habitantes y de sus autoridades (González Pástor, 2017).

Figura 26.

Cantón Pujilí

Fuente: (INEC, 2010)

Competencias del GAD Municipal

La Constitución de la República del Ecuador, establece que las competencias establecidas, requieren que las estructuras organizacionales de los GADs permitan asumir nuevos retos que podrán mejorar el manejo en el territorio.

La función del GAD municipal es trabajar para el bien de su cantón y brindar un servicio equitativo y de calidad. A continuación, se detalla los aspectos más relevantes en los que debe trabajar un Gobierno Autónomo Descentralizado (González Pástor, 2017).

- Ejercer el control sobre el uso y ocupación del suelo en el cantón.
- Planificar, construir y mantener la vialidad urbana.
- Planificar, construir y mantener la infraestructura física y los equipamientos de salud y educación, así como los espacios públicos destinados al desarrollo social, cultural y deportivo, de acuerdo con la ley.
- Elaborar y administrar los catastros inmobiliarios urbanos y rurales del cantón Pujilí.
- Gestionar los servicios de prevención, protección, socorro y extinción de incendios.
- Gestionar la cooperación internacional para el cumplimiento de sus competencias.

A continuación, en la Tabla 14 se detalla los servidores municipales.

Tabla 14.

Detalle de los servidores municipales

Personal del GAD Municipal del cantón Pujilí	**Número**
Procesos gobernantes	
Alcalde	1
Vicealcalde	1
Concejales	7
Secretaria Ejecutiva	1
-Gestión de procuraduría síndica	3
-Gestión de comunicación	4
Procesos habilitantes	
-Gestión de secretaria general	
Secretaria general	14
Unidad de prosecretaria – archivo	3
-Gestión administrativa	
Dirección administrativa	3
Unidad de talento humano	9
Unidad de compras públicas	6

Personal del GAD Municipal del cantón Pujilí	**Número**
Unidad de servicios administrativos	7
Unidad de informática	2
-Gestión financiera	
Dirección financiera	7
Unidad de presupuesto	1
Unidad de contabilidad	5
Unidad de tesorería	8
Unidad de rentas	3
Procesos agregadores de valor	
-Gestión de planificación	
Dirección de planificación	2
Unidad de avalúos y catastros	5
Unidad de planificación territorial e institucional	3
Unidad de diseño urbano y arquitectónico	4
Unidad de gestión urbana	6
-Gestión de obras públicas	
Dirección de obras públicas	2
Unidad de construcción y mantenimiento	57
Unidad de fiscalización	5
-Gestión de registro de la propiedad	
Registro de la propiedad	12
-Gestión ambiental	
Dirección de gestión ambiental	2
Unidad de control ambiental y desechos sólidos	4
Unidad de servicios públicos	5
Unidad de seguridad ciudadana y gestión de riesgos	5
-Gestión de desarrollo social	
Desarrollo social	3
Unidad de servicio social	5
Unidad de cultura	11
Unidad de deporte recreativo	3
Unidad de turismo	4
Unidad de junta cantonal de protección de derechos	3
Unidad de proyectos asociativos y comunitarios	4

Fuente: (Unidad de Talento Humano, 2020)

Estado actual frente a la seguridad

La unidad informática del GAD, tiene un alto porcentaje de incumplimiento con respecto a los controles que determina la norma ISO/IEC 27001:2013, entre los puntos más destacados, se resume a continuación los siguientes:

- No cuenta con un sistema de gestión de seguridad de la información diseñado.
- No cuenta con políticas de seguridad de la información publicadas.
- No existe un área específica que se encargue de gestionar los temas relacionados a la seguridad de la información.
- No se gestionan los activos de información de acuerdo a su criticidad.
- No hay claridad, con respecto a los responsables de cada activo de información.
- No existen controles físicos ni lógicos.

Algunas de las actividades implementadas de manera informal son:

- Existe un proceso mediante el cual se asignan o revocan derechos de accesos a los usuarios para todos los sistemas y servicios que presta el área.
- Se ha realizado el levantamiento inicial de un inventario de activos de información.
- Implementación de un firewall para garantizar la seguridad de la información.
- Actualmente la unidad de informática dispone de una red de comunicaciones en cascada, que es una forma fácil de añadir más puertos a una red existente. ver el Anexo 4.

Roles y responsabilidades

La estructura de la organización se conforma por personas que poseen conocimiento de todas las actividades de la organización y del entorno en el cual se desenvuelven.

Es así que la estructura organizacional actual deberá ser redefinida y acoplada a los roles y responsabilidades necesarios para el diseño, implementación y operación del SGSI. Según la norma ISO/IEC 27003 se establecen los roles que se muestran en la Tabla 15.

FASE II: Definición del alcance y objetivos del SGSI

De acuerdo a las necesidades de la organización, en éste caso de la unidad de informática de la municipalidad, se deberá determinar el alcance y la aplicabilidad sobre el sistema de gestión de seguridad de la información.

Alcance del SGSI

El presente proyecto proporciona el diseño de un SGSI en el almacenamiento de información de la unidad informática del GAD Municipal del cantón Pujilí, determina un conjunto de políticas y controles para proteger los activos de información de dicha unidad, ya que los servicios brindados son de vital importancia para el correcto desempeño de las actividades, servicios y procesos en la organización.

Tabla 15.

Roles y responsabilidades del SGSI

ROLES	RESPONSABILIDADES
Alta Dirección	Toma de decisiones estratégicas. Incluye al Director General de Operaciones, Director Ejecutivo, Director de Seguridad y Director Financiero.
Gerentes de línea	Responsabilidad superior de las funciones organizacionales.
Director de seguridad de la Información	Responsabilidad y dirección total de la seguridad de la información asegurando el manejo correcto de los activos de información.
Miembro del comité de seguridad de la información	Manejo de los activos de información y el rol de liderazgo para el SGSI en la organización.
Equipo de planificación de la Seguridad de la Información	Durante la implementación del SGSI, el equipo trabaja con los departamentos y resuelve los conflictos hasta que el SGSI sea establecido.

ROLES	RESPONSABILIDADES
Parte interesada	Personas u organizaciones que tienen interés directo sobre la organización.
Administrador de Sistemas	Administrador responsable de un sistema de TI
Gerente de TI	Gestión de los recursos de TI.
Seguridad física	Persona responsable de la seguridad física.
Gestión de Riesgos	Persona/s responsable del marco referencial de gestión del riego.

Fuente: (Lema Vinlasaca & Donoso Gallo, 2018)

Se hace énfasis en la primera fase del ciclo de Deming, ya que según la norma ISO/IEC 27001:2013, los sistemas de gestión de seguridad de la información deben ser periódicamente mejorados.

El desarrollo del proyecto se basa en la primera fase, no abarca las fases de hacer, verificar y actuar que corresponden a la implementación, mantenimiento y revisión del SGSI, sin embargo, en la primera fase se realizará el diseño del plan de tratamiento de riesgos.

Objetivos del SGSI

- **Ob1:** salvaguardar los activos de información que intervienen en el almacenamiento de información de la unidad de informática del GAD Municipal del cantón Pujilí.
- **Ob2**: definir controles de seguridad sobre los activos de información, preservando así la confidencialidad, integridad y disponibilidad de los mismos
- **Ob3:** ayudar al logro de la misión y de los objetivos principales de la organización, con la correcta gestión de los riesgos de seguridad de la información.

FASE III: Identificación de activos

El inventario de activos de información es una parte fundamental para el diseño y posterior implementación del SGSI. Permite clasificar los activos a los que se debe brindar mayor protección de acuerdo a la importancia de cada uno de ellos.

Los activos de información requieren la protección necesaria para evitar consecuencias negativas que pueden afectar al cumplimiento de la misión y objetivos organizacionales.

Elección de la metodología

Según la norma ISO27005, el primer paso para la elaboración del inventario de activos es la identificación de los activos primarios y de soporte. Los activos primarios son los procesos y la información central de las actividades y los activos de soporte son los elementos de procesamiento de información que pueden ser vulnerados, y afectar a los activos primarios. En base a éstos grupos, se establecieron los siguientes activos:

1. **Dato**: es toda información que se gestiona dentro de la organización.
2. **Aplicación:** es el software que se utiliza para apalancar los procesos.
3. **Personal:** son las personas que participan en el manejo de los activos.
4. **Servicio:** son los servicios que brinda la organización.
5. **Tecnología:** es el hardware donde se gestiona la información.
6. **Instalación:** es el lugar donde se encuentran los activos de información.

Etiquetado de los activos

De acuerdo a cada tipo de activo identificado en la unidad de informática de la organización, se etiquetarán de la siguiente manera, ver la Tabla 16.

Tabla 16.

Etiquetado de activos

Tipo	Identificación
Dato	INFO
Aplicación	SW
Tecnología	HW
Servicio	SERV
Instalación	INS
Personal	PER

Inventario de activos

El inventario de los activos para el almacenamiento de información de la unidad de informática se muestra en la Tabla 17, el cual es el resultado del trabajo de campo a través de la observación y levantamiento de información “in situ” en específico en la mencionada dependencia municipal, por intermedio de la analista del área quien ha proporcionado la información necesaria, a continuación, se realiza una descripción sobre la información de cada activo.

- **ID:** código para la identificación para cada activo de información.
- **Activo:** nombre definido para la identificación del activo.
- **Tipo:** clasificación de acuerdo con las características del activo.
- **Responsable:** persona o área encargada del activo de información

Tabla 17.

Inventario de activos

N°	ID	Activo	Descripcion	Tipo	Responsable
1	INFO-001	Base de Datos	SQL Progress	Dato	Unidad de informática
2	INFO-002	Archivos de Datos	Carpetas de almacenamiento	Dato	Unidad de informática
3	INFO-003	Documentación impresa	Contratos, Oficios Renovación licencias Manual del usuario Documentación del sistema	Dato	Unidad de informática
4	SW-001	Sistemas operativos	Windows Linux	Aplicación	Unidad de informática
5	SW-002	Antivirus	Clawing	Aplicación	Unidad de informática
6	SW-003	Navegadores	Mozilla Opera Chrome	Aplicación	Unidad de informática
7	SW-004	Motor de base de datos	SQL Progress	Aplicación	Unidad de informática
8	SW-005	Licencias	Aplicativos Sistemas operativos	Aplicación	Unidad de informática
9	SW-006	Aplicativos	2010, 2016	Aplicación	Unidad de informática

N°	ID	Activo	Descripcion	Tipo	Responsable
10	HW-001	Servidores	Correo institucional (HP Proliant-DL160-Gen 9) Sistema AME (HP Proliant-DL380-Gen 8) Sistema Sinat (Dell-edge R530) Sistema de construcciones (HP Proliant-ML37005)	Tecnología	Unidad de informática
11	HW-002	Computadores de Escritorio	5 computadores	Tecnología	Unidad de informática
12	HW-003	Equipo multifuncional	Impresora/Escáner	Tecnología	Unidad de informática
13	HW-004	Routers	ISP-CNT	Tecnología	Unidad de informática
14	HW-005	Firewall	Servidores/Cisco Meraki Red interna/Sophos	Tecnología	Unidad de informática
15	HW-006	Teléfono	Uso unidad informática	Tecnología	Unidad de informática
16	HW-007	Dispositivos almacenamiento	Memorias USB CDs/DVDs Discos portables Medios magnéticos	Tecnología	Unidad de informática
17	HW-008	Fluido eléctrico	UPS smart online	Tecnología	Unidad de informática
18	SERV-001	Acceso a internet	Red interna	Servicio	Unidad de informática
19	SERV-002	Correo electrónico	Toda la organización	Servicio	Unidad de informática

N°	ID	Activo	Descripcion	Tipo	Responsable
20	SERV-003	Soporte a usuarios	Toda la organización	Servicio	Unidad de informática
21	SERV-004	Mantenimiento de equipos	Toda la organización	Servicio	Unidad de informática
22	SERV-005	Soporte a la red	Toda la organización	Servicio	Unidad de informática
23	SERV-006	Soporte a los sistemas informáticos	Toda la organización	Servicio	Unidad de informática
24	INS-001	Unidad de informática	Infraestructura o espacio físico	Instalación	Unidad de informática
25	INS-002	Instalación de red de Datos	ISP CNT	Instalación	Unidad de informática
26	PER-001	Técnico a cargo	Analista	Personal	Unidad de informática
27	PER-002	Responsable de la unidad	Lider	Personal	Unidad de informática

Valoración de los activos

Luego de realizar la identificación de los activos, se debe realizar la valoración de los mismos, estableciendo la importancia de cada uno y tomando en consideración los criterios de disponibilidad, integridad y confidencialidad.

Para determinar la importancia que tiene cada activo de información identificado en la unidad de informática, se determina la escala cualitativa que se muestra en la Tabla 18.

La tabla en mención muestra cuáles son los criterios usados para realizar la valoración de los activos, los valores que se tendrán en cuenta para clasificarlos y su descripción.

- Según la norma ISO 27000, el principio de confidencialidad se refiere a la propiedad de la información, que pretende garantizar el acceso a la misma, únicamente de las personas o sistemas autorizados.
- La integridad es un atributo de la información importante, ya que sin este no sería posible la comunicación y la toma de decisiones para la organización Por esto es necesario mantener la integridad del activo en todo momento (Caicedo Carrillo & Rojas Suárez, 2017).
- Según (Bermúdez Molina, 2015) la disponibilidad es tener la certeza de que la información va a estar disponible en el momento que requiera ser accedida, por las personas que tienen la autorización.

En la Tabla 19, se muestran los valores que se pueden obtener como resultado, relacionados a un nivel de criticidad. Para poder determinar el valor final de cada activo, se sumará los valores de los criterios. Esta suma estará en el rango de 3 a 9, en donde cada valor representará un nivel de criticidad. Mientras más alto sea el número obtenido, más alta será su criticidad.

Tabla 18.

Criterio de valoración de los activos

Criterio	Valor	Descripción
Confidencialidad	0	No es relevante
	1	El acceso a la información del activo no afecta a las actividades diarias de la unidad de informática
	2	El acceso a la información del activo afecta medianamente a las actividades diarias de la unidad de informática
	3	El acceso a la información del activo afecta altamente a las actividades diarias de la unidad de informática.
Integridad	0	No es relevante
	1	La modificación del activo no afecta a las actividades diarias de la unidad de informática.
	2	La modificación del activo afecta medianamente a las actividades diarias de la unidad de informática.
	3	La modificación del activo afecta altamente a las actividades diarias de la unidad de informática.
Disponibilidad	0	No es relevante
	1	La ausencia del activo no afecta a las actividades diarias de la unidad de informática.
	2	La ausencia del activo afecta medianamente a las actividades diarias de la unidad de informática.
	3	La ausencia del activo afecta altamente a las actividades diarias de la unidad de informática.

Tabla 19.

Niveles de criticidad

Valor	Criticidad
0	No aplica
1	Baja
2	Baja
3	Baja
1	Media
2	Media
3	Media
1	Alta
2	Alta
3	Alta

En la Tabla 20 se muestra la valoración de cada activo de la unidad de informática, de acuerdo al criterio de valoración de las siguientes dimensiones que están representadas por:

C = Confidencialidad

I = Integridad

D = Disponibilidad

Realizada la valorización de los activos existentes en la unidad de informática, se obtuvo una lista de 13 activos con criticidad “Alta”, los cuáles se muestran en la Tabla 21. Por ello, la organización debería orientar los suficientes recursos, con el fin de salvaguardar los mismos, manteniendo un nivel de riesgo aceptable y evitando afectar las actividades del negocio.

Tabla 20.

Valoración de activos

ID	ACTIVO	[C]	[I]	[D]	NIVEL	VALORACIÓN
INFO-001	Base de Datos	3	3	3	9	Alta
INFO-002	Archivos de Datos	2	2	3	7	Alta
INFO-003	Documentación impresa	2	2	2	6	Media
SW-001	Sistema operativo	2	2	2	6	Media
SW-002	Antivirus	0	0	2	2	Baja
SW-003	Navegadores	0	0	2	2	Baja
SW-004	Motor de base de datos	3	3	3	9	Alta
SW-005	Licencias	2	2	2	6	Media
SW-006	Aplicativos	2	2	3	7	Alta
HW-001	Servidores	3	3	3	9	Alta
HW-002	Computadores de Escritorio	1	2	3	6	Media
HW-003	Equipo multifuncional	0	0	2	2	Baja
HW-004	Routers	2	3	3	8	Alta
HW-005	Firewall	2	3	2	7	Alta
HW-006	Teléfono	0	0	1	1	Baja
HW-007	Dispositivos almacenamiento	2	2	2	6	Media
HW-008	Fluido Eléctrico	3	3	3	9	Alta
SERV-001	Internet	2	2	3	7	Alta
SERV-002	Correo electrónico	2	2	2	6	Media
SERV-003	Soporte a usuarios	1	2	3	6	Media
SERV-004	Mantenimiento equipos	1	2	3	6	Media

ID	ACTIVO	[C]	[I]	[D]	NIVEL	VALORACIÓN
SERV-005	Soporte a la red	2	3	3	8	Alta
SERV-006	Soporte a los sistemas informáticos	1	3	3	7	Alta
INS-001	Unidad de informática	3	3	3	9	Alta
INS-002	Instalación de red de Datos	3	3	3	9	Alta
PER-001	Analista	2	2	2	6	Media
PER-002	Lider	2	2	2	6	Media

Tabla 21.

Activos con criticidad alta

N°	ID	ACTIVO
1	INFO-001	Bases de Datos
2	INFO-002	Archivos de Datos
3	SW-004	Motor de bases de datos
4	SW-006	Aplicativos
5	HW-001	Servidores
6	HW-004	Routers
7	HW-005	Firewall
8	HW-008	Fluido Eléctrico
9	SERV-001	Internet
10	SERV-005	Soporte a la red
11	SERV-006	Soporte a los sistemas informáticos
12	INS-001	Unidad de informática
13	INS-002	Instalación de red de Datos

FASE IV: Gestión de riesgos

Identificación de amenazas

Las organizaciones están expuestas a varios tipos de amenazas. Se las debe identificar, analizar y determinar la probabilidad de materialización.

Para la identificación, los propietarios de los activos definen antecedentes en los que se hayan visto afectadas la confidencialidad, integridad y disponibilidad de los activos. Las amenazas se pueden clasificar como se muestra en la Tabla 22.

La detección oportuna, prevención y control de condiciones peligrosas (principalmente en equipos y procedimientos), que se determinen como amenazas, es la primera estrategia orientada a la gestión de los riesgos. El riesgo depende de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto en los activos de información de una organización. El producto de estos factores representa el riesgo.

Tabla 22.

Tipo de amenaza

Tipo de amenaza	Identificación	Definición
Deliberada	D	Se usa para todas las acciones deliberadas que tienen como objetivo los activos de la información.
Accidental	A	Se usa para las acciones humanas que pueden dañar accidentalmente los activos de la información de la organización.
Ambiental	E	Se usa para todos los incidentes que no se basa en acciones humanas.

Fuente: (Recalde Caicedo, 2019) (ISO/IEC 27005, 2018)

De acuerdo a la norma ISO/IEC 27005 y su Anexo C, se realizó la identificación de las amenazas, para cada activo de información, las categorías de amenazas se pueden clasificar como se muestra en la Tabla 23.

Tabla 23.

Identificación de amenazas

Inciso	Amenaza
A	Daño físico
B	Eventos Naturales
C	Pérdida de servicios esenciales
D	Perturbación por radiación
E	Compromiso de la información
F	Fallas técnicas
G	Acciones no autorizadas
H	Compromiso de las funciones
I	Errores humanos
J	Fallas en la gestión y la operación del servicio

Fuente: (Chunga Ramirez, 2017) (ISO/IEC 27005, 2018)

Identificación de vulnerabilidades

Ahora se procede con la identificación de las vulnerabilidades que pueden ser explotadas, y su posterior impacto para los activos de información definidos en el SGSI. En caso de que una vulnerabilidad, pueda ser explotada por una amenaza, se determinará un impacto ya sea alto, mediano o bajo, generando condiciones negativas en las actividades diarias, perdida de la continuidad del negocio y el incumplimiento de los objetivos y de la misión de la organización.

La Tabla 24 muestra las vulnerabilidades a las que pueden estar expuestos los activos encontrados y su relación con las amenazas.

Tabla 24.

Amenazas y vulnerabilidades

ID	Activo	Amenaza	Vulnerabilidad
INFO-001 INFO-002	Base de Datos, Archivos de Datos	Hurto de información	Información disponible para personas no autorizadas Almacenamiento sin protección Falta de backups de información
		Ingreso de datos falsos	Desconocimiento de la aplicación Mala digitación para el ingreso de datos No existen formatos para ingresar datos
		Acceso forzado al sistema	Almacenamiento sin protección
		Saturación del sistema	Falta de mantenimiento regular
		Divulgación de la información	Mala seguridad de las contraseñas
INFO-003	Documentación impresa	Hurto de información	Información disponible para personas no autorizadas Almacenamiento sin protección
		Recuperación de medios reciclados o desechados	Reutilización de los medios de almacenamiento sin borrado adecuado
		Destrucción de la documentación	Susceptible a la húmedas, polvo Falta de reemplazo regular No existe un procedimiento para la eliminación de documentación impresa
SW-001 SW-002 SW-003 SW-004 SW-005 SW-006	Sistemas operativos, Antivirus, Navegadores, Motor de bases de datos, Licencias, Aplicativos	Uso de software falso o copiado	Desconocimiento de licenciamiento Costos elevados
		Mal funcionamiento del software	Falta de control eficaz del cambio Software no garantizado Falta de actualización del software
		Infección con software malicioso	Falta de medidas de detección y prevención contra códigos maliciosos
		Ataques contra el sistema	Falta de mecanismos de seguridad

ID	Activo	Amenaza	Vulnerabilidad
HW-001	Servidores,	Daño por fuego	Falta de mecanismo contra incendios
HW-002	Computadores de	Falla del equipo	Instalación fallida de los medios de
HW-003	Escritorio,		almacenamiento.
HW-004	Equipo multifuncional,	Fluctuaciones de energía eléctrica	Equipos sensibles a variaciones de
HW-005	Routers,		voltaje
HW-006	Firewall,	Manipulación con software	Uso no controlado del software
HW-007	Teléfono,	Pérdida del suministro de energía	Falta de dispositivos de
HW-008	Dispositivos de		almacenamiento de energía (UPS)
	almacenamiento,		Falta de esquemas de reemplazo
	Fluido eléctrico		periódico.
			Red energética inestable
		Polvo, corrosión, golpes	Falta de mantenimiento preventivo y
			correctivo
		Hurto del equipo	Falta de protección física y controles de
			puertas y ventanas
		Divulgación de la información	Mala seguridad de contraseñas
SERV-002	Internet,	Manipulación de información	Falta de privilegios en los permisos
SERV-003	Correo electrónico,	Abuso de derechos	Mala gestión de contraseñas
SERV-004	Soporte a usuarios,	Saturación en los sistemas de	Gestión inadecuada de la red
SERV-005	Mantenimiento de	información	
SERV-006	equipos,	Ataques informáticos	Falta de proceso de la gestión de
	Soporte a la red,		vulnerabilidades técnicas
	Soporte a los sistemas		
INS-001	Unidad de informática	Pérdida del suministro de energía	Falta de sistema para el suministro de
			energía ininterrumpida
		Daño por fuego	Falta de mecanismo contra incendios
		Falta de mantenimiento	Indisponibilidad de personal
		Inundaciones	Falta de proceso para asegurar la
			continuidad del negocio
		Terremoto	Falta de proceso para asegurar la
			continuidad del negocio

ID	Activo	Amenaza	Vulnerabilidad
		Polvo, corrosión, golpes	Falta de mantenimiento preventivo y correctivo
		Desastres naturales	Falta de proceso para asegurar la continuidad del negocio en caso de erupción del volcán
INS-002	Instalación de red de Datos	Falla en los equipos de Red	Cableado desprotegido
		Arquitectura de red insegura	Espionaje remoto
		Saturación de los sistemas de información	Gestión inadecuada de la red
		Uso no autorizado de los equipos de red	Conexiones de red desprotegidas
PER-001	Analista, Líder	Suplantación de identidad	Sesiones de usuario habilitadas
PER-002			Almacenamiento sin protección
		Hurto de información	Información disponible para personas no autorizadas
			Almacenamiento sin protección
		Error en el uso de sistemas de información	Falta de proceso de control de cambios en los sistemas
		Abuso de privilegios	Falta de controles para el uso de derechos de accesos privilegiados.
		Ataques de ingeniería social	Falta de concienciación y capacitación en seguridad de la información.
		Divulgación de la información	Falta de controles en la salida de la información

Probabilidad e impacto

La probabilidad de un incidente refleja la posibilidad de que una amenaza se materialice, y explote una vulnerabilidad, se puede verificar revisando los eventos previos y sustentando dicha información con los usuarios y administradores la frecuencia de ocurrencia de dichos eventos (Caicedo Carrillo & Rojas Suárez, 2017).

Para el presente proyecto, se determinaron 5 niveles cualitativos de probabilidad, como se ve en la Tabla 25, basándose en la ocurrencia en actividades anteriores, obtenida de la información proporcionada por del analista de sistemas de la unidad de informática.

Tabla 25.

Niveles de probabilidad

Probabilidad	Descripción
Muy baja	No es probable que la amenaza explote una vulnerabilidad.
Baja	No ha ocurrido, es poco probable que la amenaza explote una vulnerabilidad.
Media	Ha ocurrido una vez al año, existe la probabilidad que la amenaza explote una vulnerabilidad.
Alta	Ha ocurrido una vez al mes, es probable que la amenaza explote una vulnerabilidad
Muy alta	Ha ocurrido una vez a la semana, la amenaza explotará una vulnerabilidad.

Ahora se determina el impacto que se daría, cuando una vulnerabilidad llega a ser explotada por una amenaza, teniendo en cuenta los valores de criticidad asignados anteriormente a cada uno de los activos.

Para el presente proyecto se clasificó el impacto, en 5 niveles cualitativos, ver la Tabla 26.

Tabla 26.

Niveles de impacto

Impacto	Descripción
Muy bajo	El incidente no tiene ninguna afectación.
Bajo	Existe afectación en las actividades de la unidad, por lo menos 2 horas.
Medio	Existe afectación en las actividades de la unidad, por lo menos 8 horas.
Alto	Existe afectación en las actividades de la unidad, por lo menos 1 día.
Muy alto	Existe afectación total en las actividades de la organización.

Mapa de riesgos

Cuando las vulnerabilidades y amenazas que puedan afectar a los activos de la unidad de informática has sido analizadas y evaluadas, se procede a realizar la valoración de los riesgos, usando como referencia la norma ISO/IEC 27005, la cual tiene como criterios la probabilidad que una amenaza explote una vulnerabilidad y el impacto que tendría al materializarse. La Tabla 27 muestra la matriz de calor.

El nivel del riesgo es la relación que existe entre la probabilidad de ocurrencia de un incidente y el impacto resultante del mismo. Los tipos son:

- **Muy bajo:** la materialización de una amenaza podría ser insignificante
- **Bajo:** la materialización de una amenaza podría tener consecuencias mínimas.
- **Medio:** la materialización de una amenaza puede tener como consecuencia la afectación en las actividades de la unidad, por un periodo de tiempo no mayor a 4 horas.

- **Alto:** la materialización de una amenaza puede tener como consecuencia la afectación en las actividades de la unidad, por un periodo de tiempo no mayor a 10 horas.
- **Muy alto:** la materialización de una amenaza puede tener como consecuencia la afectación total en las actividades de la unidad.

Tabla 27.

Mapa de calor

		IMPACTO				
		Muy baja	Baja	Media	Alta	Muy alta
PROBABILIDAD	Muy alto	Tolerable	Tolerable	Moderado	Inaceptable	Inaceptable
	Alto	Aceptable	Tolerable	Moderado	Inaceptable	Inaceptable
	Medio	Aceptable	Tolerable	Tolerable	Moderado	Moderado
	Bajo	Aceptable	Aceptable	Tolerable	Tolerable	Tolerable
	Muy bajo	Aceptable	Aceptable	Aceptable	Aceptable	Tolerable

Fuente: (Lema Vinlasaca & Donoso Gallo, 2018)

Evaluación del riesgo

En base al concepto sobre la explotación del riesgo en cuanto a las pérdidas materiales, económicas o de continuidad, es necesario definir el riesgo, comprendiendo su naturaleza y la afectación que podrían tener los activos de información y a los diferentes procesos o servicios.

Se debe usar la evaluación de riesgos, asignando valores de probabilidad, impacto e identificando los valores más altos para poder darles el tratamiento respectivo y así lograr la reducción o eliminación de los mismos.

A continuación, en la Tabla 28 se determina el nivel de riesgo según el impacto que provocaría en la organización, y la probabilidad de que una amenaza se materialice. El contenido de la tabla se describe a continuación.

- **ID:** es un código alfanumérico, asignado a cada activo de información.
- **Activo:** es el nombre del activo de información.
- **ID Riesgo:** es un código alfanumérico, asignado a cada riesgo identificado.
- **Amenaza:** es la causa del riesgo, para cada activo de información.
- **Probabilidad:** es un valor cualitativo asignado a la posibilidad de que se materialice una amenaza.
- **Impacto:** es un valor cualitativo que determina la afectación que tendrían los activos, si llegase a ocurrir un incidente.
- **Riesgo:** es la relación entre la probabilidad y el impacto.

En la tabla 28, siguiendo la relación entre la probabilidad de ocurrencia y el impacto, se muestra que 10 de los riesgos identificados fueron definidos como “Inaceptables”, Estos riesgos deben ser priorizados para su tratamiento, con la finalidad de reducirlos a un valor aceptable.

El proceso de evaluación de riesgos debe ser realizado periódicamente para validar la clasificación asignada a los mismos, para verificar que a los riesgos se les haya dado el respectivo tratamiento y sean reducidos a niveles mínimos. Finalmente se obtendrá una retroalimentación, para la toma de decisiones y estrategias para nuevas acciones, que permitan reducir el riesgo. La Tabla 29 muestra la clasificación de los riesgos.

Tabla 28.

Evaluación del riesgo

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
INFO-001	Bases de datos	R001	Hurto de información	Media	Muy alto	Moderado
		R002	Ingreso de datos falsos	Baja	Alto	Tolerable
		R003	Acceso forzado al sistema	Baja	Alto	Tolerable
		R004	Saturación del sistema	Alta	Muy alto	Inaceptable
		R005	Divulgación de la información	Media	Medio	Tolerable
INFO-002	Archivos de Datos	R006	Hurto de información	Media	Medio	Tolerable
		R007	Ingreso de datos falsos	Baja	Bajo	Aceptable
		R008	Acceso forzado al sistema	Baja	Medio	Tolerable
		R009	Saturación del sistema	Media	Alto	Moderado
		R010	Divulgación de la información	Media	Alto	Tolerable
INFO-003	Documentación impresa	R011	Hurto de información	Alta	Medio	Moderado
		R012	Recuperación de medios reciclados o desechados	Alta	Medio	Moderado
		R013	Destrucción de la documentación.	Media	Medio	Tolerable
SW-001	Sistemas operativos	R014	Uso de software falso o copiado	Alta	Bajo	Tolerable
		R015	Mal funcionamiento del software	Media	Medio	Tolerable
		R016	Infección con software malicioso	Alta	Medio	Moderado
		R017	Ataques contra el sistema	Baja	Medio	Tolerable
SW-002	Antivirus	R018	Uso de software falso o copiado	Alta	Alto	Inaceptable

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
		R019	Mal funcionamiento del software	Media	Medio	Tolerable
		R020	Infección con software malicioso	Media	Alto	Moderado
		R021	Ataques contra el sistema	Muy baja	Medio	Aceptable
SW-003	Navegador	R022	Uso de software falso o copiado	Baja	Bajo	Aceptable
		R023	Mal funcionamiento del software	Baja	Bajo	Aceptable
		R024	Infección con software malicioso	Baja	Bajo	Aceptable
SW-004	Motor de bases de datos	R025	Uso de software falso o copiado	Baja	Medio	Tolerable
		R026	Mal funcionamiento del software	Alta	Alto	Inaceptable
		R027	Infección con software malicioso	Media	Alto	Moderado
		R028	Ataques contra el sistema	Baja	Alto	Tolerable
SW-005	Licencias	R029	Uso de software falso o copiado	Alta	Alto	Inaceptable
		R030	Mal funcionamiento del software	Media	Muy alto	Moderado
		R031	Infección con software malicioso	Media	Alto	Moderado
		R032	Ataques contra el sistema	Baja	Alto	Tolerable
SW-006	Aplicativos	R033	Uso de software falso o copiado	Alta	Alto	Inaceptable
		R034	Mal funcionamiento del software	Alta	Alto	Inaceptable
		R035	Infección con software malicioso	Media	Alto	Moderado

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
		R036	Ataques contra el sistema	Baja	Medio	Tolerable
HW-001	Servidores	R037	Daño por fuego	Alto	Muy alto	Inaceptable
		R038	Falla del equipo	Alto	Muy alto	Inaceptable
		R039	Fluctuación de energía eléctrica	Media	Muy alto	Moderado
		R040	Manipulación con software	Baja	Alto	Tolerable
		R041	Pérdida del suministro de energía	Media	Alto	Moderado
		R042	Polvo, corrosión, golpes	Media	Medio	Tolerable
		R043	Hurto del equipo	Baja	Muy alto	Tolerable
		R044	Divulgación de la información.	Media	Muy alto	Moderado
HW-002	Computadores de Escritorio	R045	Daño por fuego	Baja	Medio	Tolerable
		R046	Falla del equipo	Media	Medio	Tolerable
		R047	Fluctuación de energía eléctrica	Media	Medio	Tolerable
		R048	Manipulación con software	Baja	Medio	Tolerable
		R049	Pérdida del suministro de energía	Media	Medio	Tolerable
		R050	Polvo, corrosión, golpes	Media	Bajo	Tolerable
		R051	Hurto del equipo	Media	Alto	Moderado
		R052	Divulgación de la información.	Media	Alto	Moderado
HW-003	Equipo multifuncional	R053	Daño por fuego	Media	Bajo	Aceptable
		R054	Falla del equipo	Baja	Medio	Tolerable
		R055	Fluctuación de energía eléctrica	Media	Medio	Tolerable
		R056	Pérdida del suministro de energía	Baja	Medio	Tolerable
		R057	Polvo, corrosión, golpes	Baja	Bajo	Aceptable
		R058	Hurto del equipo	Media	Bajo	Tolerable

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
HW-004	Routers	R059	Daño por fuego	Media	Muy alto	Moderado
		R060	Falla del equipo	Media	Muy alto	Moderado
		R061	Fluctuación de energía eléctrica	Media	Muy alto	Moderado
		R062	Manipulación con software	Baja	Alto	Tolerable
		R063	Pérdida del suministro de energía	Media	Muy alto	Moderado
		R064	Polvo, corrosión, golpes	Media	Bajo	Tolerable
		R065	Hurto del equipo	Media	Muy alto	Moderado
		R066	Divulgación de la información.	Media	Muy alto	Moderado
HW-005	Firewall	R067	Daño por fuego	Media	Alto	Moderado
		R068	Falla del equipo	Media	Muy alto	Moderado
		R069	Fluctuación de energía eléctrica	Media	Alto	Moderado
		R070	Manipulación con software	Baja	Medio	Tolerable
		R071	Pérdida del suministro de energía	Media	Alto	Moderado
		R072	Polvo, corrosión, golpes	Media	Medio	Tolerable
		R073	Hurto del equipo	Media	Muy alto	Moderado
HW-006	Teléfono	R074	Daño por fuego	Baja	Bajo	Aceptable
		R075	Falla del equipo	Muy baja	Bajo	Aceptable
		R076	Fluctuación de energía eléctrica	Baja	Bajo	Aceptable
		R077	Pérdida del suministro de energía	Media	Bajo	Tolerable
		R078	Polvo, corrosión, golpes	Baja	Muy bajo	Aceptable
		R079	Hurto del equipo	Media	Bajo	Tolerable
HW-007	Dispositivos almacenamiento	R080	Daño por fuego	Baja	Medio	Tolerable
		R081	Fluctuación de energía eléctrica	Baja	Bajo	Aceptable
		R082	Manipulación con software	Baja	Bajo	Aceptable

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
		R083	Polvo, corrosión, golpes	Baja	Muy bajo	Aceptable
		R084	Hurto del equipo	Media	Medio	Tolerable
		R085	Divulgación de la información.	Media	Alto	Moderado
HW-008	Fluido Eléctrico	R086	Daño por fuego	Media	Muy alto	Moderado
		R087	Falla del equipo	Baja	Muy alto	Tolerable
		R088	Fluctuación de energía eléctrica	Media	Alto	Moderado
		R089	Polvo, corrosión, golpes	Baja	Bajo	Aceptable
		R090	Hurto del equipo	Media	Muy alto	Moderado
SERV-001	Internet	R091	Manipulación de información	Baja	Alto	Tolerable
		R092	Abuso de privilegios	Baja	Alto	Tolerable
		R093	Saturación del sistema de información	Media	Muy alto	Moderado
		R094	Ataques informáticos	Media	Muy alto	Moderado
		R095	Falla de los equipos de red	Media	Muy alto	Moderado
SERV-002	Correo electrónico	R096	Manipulación de información	Media	Medio	Tolerable
		R097	Abuso de privilegios	Baja	Medio	Tolerable
		R098	Saturación de los sistemas de información	Baja	Medio	Tolerable
		R099	Ataques informáticos	Baja	Medio	Tolerable
SERV-003	Soporte a usuarios	R100	Manipulación de información	Baja	Medio	Tolerable
		R101	Abuso de privilegios	Baja	Bajo	Aceptable
		R102	Saturación de los sistemas de información	Media	Medio	Tolerable
		R103	Ataques informáticos	Media	Medio	Tolerable

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
SERV-004	Mantenimiento de equipos	R104	Manipulación de información	Baja	Medio	Tolerable
		R105	Abuso de privilegios	Baja	Medio	Tolerable
		R106	Saturación de los sistemas de información	Media	Alto	Moderado
		R107	Ataques informáticos	Media	Medio	Tolerable
SERV-005	Soporte a la red	R108	Manipulación de información	Baja	Alto	Tolerable
		R109	Abuso de privilegios	Baja	Alto	Tolerable
		R110	Saturación de los sistemas de información	Media	Muy alto	Moderado
		R111	Ataques informáticos	Media	Alto	Moderado
SERV-006	Soporte a los sistemas informáticos	R112	Manipulación de información	Baja	Alto	Tolerable
		R113	Abuso de privilegios	Media	Medio	Tolerable
		R114	Saturación de los sistemas de información	Media	Alto	Moderado
		R115	Ataques informáticos	Media	Alto	Moderado
INS-001	Unidad de informática	R116	Polvo, corrosión	Baja	Bajo	Aceptable
		R117	Daño por fuego	Media	Muy alto	Moderado
		R118	Perdida de suministro de energía	Media	Alto	Moderado
		R119	Falta de mantenimiento	Media	Medio	Tolerable
		R120	Inundaciones	Baja	Muy alto	Tolerable
		R121	Terremotos	Media	Muy alto	Moderado
		R122	Desastres naturales	Alta	Muy alto	Inaceptable
INS-002	Instalación de red de Datos	R123	Falla en los equipos de red	Media	Muy alto	Moderado
		R124	Arquitectura de red insegura	Alta	Muy alto	Inaceptable
		R125	Saturación de los sistemas de información	Media	Muy alto	Moderado

ID	Activo	ID Riesgo	Amenazas	Probabilidad	Impacto	Riesgo
		R126	Uso no autorizado de los equipos de red	Baja	Alto	Tolerable
PER-001	Analista	R127	Suplantación de identidad	Media	Alto	Moderado
		R128	Hurto de información	Media	Alto	Moderado
		R129	Error en el uso de sistemas de información	Baja	Alto	Tolerable
		R130	Abuso de privilegios	Baja	Alto	Tolerable
		R131	Divulgación de la información.	Media	Alto	Moderado
PER-002	Lider	R132	Suplantación de identidad	Media	Alto	Moderado
		R133	Hurto de información	Media	Alto	Moderado
		R134	Error en el uso de sistemas de información	Baja	Alto	Tolerable
		R135	Abuso de privilegios	Baja	Alto	Tolerable
		R136	Divulgación de la información.	Media	Alto	Moderado

Tabla 29.

Clasificación de los riesgos

PROBABILIDAD	IMPACTO				
	Muy baja	**Baja**	**Media**	**Alta**	**Muy alta**
Muy alto					
Alto		R014	R011, R012, R016	R018, R026, R029, R033, R034	R004, R037, R038, R122, R124
Medio		R050, R053, R058, R064, R077, R079	R005, R006, R013, R015, R019, R042, R046, R047, R049, R055, R072, R084, R096, R102, R103, R107, R113, R119	R009, R010, R020, R027, R031, R035, R041, R051, R052, R067, R069, R071, R085, R088, R106, R111, R114, R115, R118, R128, R131, R132, R133, R136	R001, R030, R039, R044, R059, R060, R061, R063, R065, R066, R068, R073, R086, R090, R093, R094, R095, R110, R117, R121, R123, R125,
Bajo	R078, R083	R007, R022, R023, R024, R057, R074, R076, R081, R082, R089, R101, R116	R008, R017, R025, R036, R045, R048, R054, R056, R070, R080, R097, R098, R099, R100, R104, R105	R002, R003, R028, R032, R040, R062, R091, R092, R108, R109, R112, R126, R129, R130, R134, R135	R043, R087, R120
Muy bajo		R075	R021		

Plan de tratamiento de riesgos

El proceso para realizar el plan de tratamiento de riesgos consiste en seleccionar y aplicar las medidas adecuadas para modificar el riesgo, y así evitar daños a los activos de información.

Luego de haber definido los niveles de riesgos respecto a las amenazas de cada activo de información, se establecen los criterios de aceptación del riesgo el cual se enfoca en determinar el tipo de riesgo y si se necesita aplicar algún control. La Tabla 30 muestra las acciones a tomar.

Tabla 30.

Aceptación del riesgo

Zona	Acción a tomar
Aceptable	Aceptar
Tolerable	Transferir
Moderada	Reducir
Inaceptable	Evitar

Fuente: (ISO/IEC 27005, 2018)

Es importante para la organización mantener monitoreo periódico sobre los riesgos identificados, para lograr seleccionar los factores que los provocan, ya que la organización debe asignar los recursos necesarios al tratamiento de los riesgos.

Criterio para el tratamiento del riesgo

En la Tabla 31 se muestran los criterios para el tratamiento de los riesgos identificados y evaluados anteriormente.

Se determina las acciones a tomar según el nivel de riesgo adquirido de acuerdo al análisis de probabilidad e impacto de cada uno de los activos de información.

- **Aceptar:** el nivel de exposición es adecuado, por lo tanto, se acepta.

- **Transferir:** Se puede permitir gestionar, es decir se entrega el riesgo a otra entidad o área, la cual se encuentra en plena capacidad de gestionarlo.
- **Reducir:** Se debe fortalecer los controles existentes y/o agregar nuevos controles, de tal manera que el riesgo sea aceptable.
- **Evitar:** Se requiere acciones inmediatas que permitan reducir la probabilidad de materialización.

Tabla 31.

Criterio para el tratamiento del riesgo

		Impacto				
		Muy bajo	Bajo	Medio	Alto	Muy alto
Probabilidad	Muy alta	Transferir	Transferir	Reducir	Evitar	Evitar
	Alta	Aceptar	Transferir	Reducir	Evitar	Evitar
	Media	Aceptar	Transferir	Transferir	Reducir	Reducir
	Baja	Aceptar	Aceptar	Transferir	Transferir	Transferir
	Muy baja	Aceptar	Aceptar	Aceptar	Aceptar	Transferir

Fuente: (ISO/IEC 27005, 2018)

Plan de tratamiento de riesgos.

En la Tabla 32 se muestra el plan de tratamiento correspondiente a los riesgos identificados y evaluados anteriormente, para la construcción de dicha tabla se toman en cuenta los criterios de tratamiento definidos. Cualquier sistema de tratamiento de riesgos debe garantizar como mínimo:

- Funcionamiento efectivo y eficiente de la organización.
- Controles internos adecuados y continuidad del negocio.
- Conformidad con las leyes y reglamentos vigentes.

La principal medida que se puede adoptar con el fin de minimizar los efectos de la ejecución del riesgo, son los planes de contingencia. Un plan de contingencia define

los procedimientos y procesos alternativos que se han de aplicar a una organización cuando un riesgo ya se ha ejecutado.

Tabla 32.

Plan de tratamiento de riesgos

Amenaza	Activos	Nivel de riesgo	Tratamiento
Acceso forzado al sistema	Bases de datos	Tolerable	Transferir
	Archivos de datos	Tolerable	Transferir
	Motor de bases de datos	Tolerable	Transferir
Ingreso de datos falsos	Bases de datos	Tolerable	Transferir
	Archivos de datos	Aceptable	Aceptar
Fluctuaciones de energía eléctrica	Servidores	Moderado	Reducir
	Computadores de escritorio	Tolerable	Transferir
	Equipo multifuncional	Tolerable	Transferir
	Routers	Moderado	Reducir
	Firewall	Moderado	Reducir
	Teléfono	Aceptable	Aceptar
	Dispositivos de almacenamiento	Aceptable	Aceptar
Daño por fuego	Servidores	Inaceptable	Evitar
	Computadores de escritorio	Tolerable	Transferir
	Equipo multifuncional	Aceptable	Aceptar
	Routers	Moderado	Reducir
	Firewall	Moderado	Reducir
	Dispositivos de almacenamiento	Tolerable	Transferir
	Teléfono	Aceptable	Aceptar
	Fluido eléctrico	Moderado	Reducir
	Unidad de informática	Moderado	Reducir
Hurto del equipo	Servidores	Tolerable	Transferir
	Computadores de escritorio	Moderado	Reducir
	Equipo multifuncional	Tolerable	Transferir
	Routers	Moderado	Reducir
	Firewall	Moderado	Reducir
	Dispositivos de almacenamiento	Tolerable	Transferir

Amenaza	Activos	Nivel de riesgo	Tratamiento
	Teléfono	Tolerable	Transferir
	Fluido eléctrico	Moderado	Reducir
Pérdida del suministro de energía	Servidores	Moderado	Reducir
	Computadores de escritorio	Tolerable	Transferir
	Equipo multifuncional	Tolerable	Transferir
	Routers	Moderado	Reducir
	Firewall	Moderado	Reducir
	Teléfono	Tolerable	Transferir
	Unidad de informática	Moderado	Reducir
Polvo, corrosión, golpes	Servidores	Tolerable	Transferir
	Computadores de escritorio	Tolerable	Transferir
	Equipo multifuncional	Aceptable	Aceptar
	Routers	Tolerable	Transferir
	Firewall	Tolerable	Transferir
	Dispositivos de almacenamiento	Aceptable	Aceptar
	Teléfono	Aceptable	Aceptar
	Fluido eléctrico	Aceptable	Aceptar
	Unidad de informática	Aceptable	Aceptar
Saturación del sistema	Bases de datos	Inaceptable	Evitar
	Archivos de datos	Moderado	Reducir
	Instalación de red de datos	Moderado	Reducir
	Internet	Moderado	Reducir
	Correo electrónico	Tolerable	Transferir
	Soporte a usuarios	Tolerable	Transferir
	Mantenimiento a equipos	Moderado	Reducir
	Soporte a la red	Moderado	Reducir
	Soporte a los sistemas informáticos	Moderado	Reducir
Hurto de información	Bases de datos	Moderado	Reducir
	Archivos de datos	Tolerable	Transferir
	Documentación impresa	Moderado	Reducir
	Analista	Moderado	Reducir
	Lider	Moderado	Reducir
Mal funcionamiento del software	Sistemas operativos	Tolerable	Transferir
	Antivirus	Tolerable	Transferir

Amenaza	Activos	Nivel de riesgo	Tratamiento
	Navegadores	Aceptable	Aceptar
	Motor de bases de datos	Inaceptable	Evitar
	Licencias	Moderado	Reducir
	Aplicativos	Inaceptable	Evitar
Ataques contra el sistema	Sistemas operativos	Tolerable	Transferir
	Antivirus	Aceptable	Aceptar
	Motor de bases de datos	Tolerable	Transferir
	Licencias	Tolerable	Transferir
	Aplicativos	Tolerable	Transferir
Falta de mantenimiento	Unidad de informática	Tolerable	Transferir
Inundaciones	Unidad de informática	Tolerable	Transferir
Falla en los equipos de red	Internet	Moderado	Reducir
Terremoto	Unidad de informática	Moderado	Reducir
Desastres naturales	Unidad de informática	Inaceptable	Evitar
Ataques informáticos	Internet	Moderado	Reducir
	Correo electrónico	Tolerable	Transferir
	Soporte a usuarios	Tolerable	Transferir
	Mantenimiento de equipos	Tolerable	Transferir
	Soporte a la red	Moderado	Reducir
	Soporte a los sistemas informáticos	Moderado	Reducir
Recuperación de medios reciclados o desechados	Documentación impresa	Moderado	Reducir
Destrucción de la documentación	Documentación impresa	Tolerable	Transferir
Uso de software falso o copiado	Sistemas operativos	Tolerable	Transferir
	Antivirus	Inaceptable	Evitar

Amenaza	Activos	Nivel de riesgo	Tratamiento
	Navegadores	Aceptable	Aceptar
	Motor de bases de datos	Tolerable	Transferir
	Licencias	Inaceptable	Evitar
	Aplicativos	Inaceptable	Evitar
Infección con software malicioso	Sistemas operativos	Moderado	Reducir
	Antivirus	Moderado	Reducir
	Navegadores	Aceptable	Aceptar
	Motor de bases de datos	Moderado	Reducir
	Licencias	Moderado	Reducir
	Aplicativos	Moderado	Reducir
Falla del equipo	Servidores	Inaceptable	Evitar
	Computadores de Escritorio	Tolerable	Transferir
	Equipo multifuncional	Tolerable	Transferir
	Routers	Moderado	Reducir
	Firewall	Moderado	Reducir
	Teléfono	Aceptable	Aceptar
	Fluido eléctrico	Tolerable	Transferir
Manipulación con software	Servidores	Tolerable	Transferir
	Computadores de Escritorio	Tolerable	Transferir
	Equipo multifuncional	Tolerable	Transferir
	Routers	Tolerable	Transferir
	Firewall	Tolerable	Transferir
	Dispositivos de almacenamiento	Aceptable	Aceptar
Divulgación de información	Servidores	Moderado	Reducir
	Computadores de Escritorio	Moderado	Reducir
	Routers	Moderado	Reducir
	Dispositivos de almacenamiento	Moderado	Reducir
	Base de Datos	Tolerable	Transferir
	Archivos de Datos	Tolerable	Transferir
	Analista	Moderado	Reducir
	Lider	Moderado	Reducir
Falla en los equipos de red	Instalación de red de Datos	Moderado	Reducir

Amenaza	Activos	Nivel de riesgo	Tratamiento
Arquitectura de red insegura	Instalación de red de Datos	Inaceptable	Evitar
Uso no autorizado de los equipos de red	Instalación de red de Datos	Tolerable	Transferir
Suplantación de identidad	Analista	Moderado	Reducir
	Lider	Moderado	Reducir
Error en el uso de sistemas de información	Analista	Tolerable	Transferir
	Lider	Tolerable	Transferir
Abuso de privilegios	Analista	Tolerable	Transferir
	Lider	Tolerable	Transferir
	Internet	Tolerable	Transferir
	Correo electrónico	Tolerable	Transferir
	Soporte a usuarios	Aceptable	Aceptar
	Mantenimiento de equipos	Tolerable	Transferir
	Soporte a la red	Tolerable	Transferir
	Soporte a los sistemas informáticos	Tolerable	Transferir
Manipulación de información	Internet	Tolerable	Transferir
	Correo electrónico	Tolerable	Transferir
	Soporte a usuarios	Tolerable	Transferir
	Mantenimiento de equipos	Tolerable	Transferir
	Soporte a la red	Tolerable	Transferir
	Soporte a los sistemas informáticos	Tolerable	Transferir

FASE V: Definición de políticas y procedimientos

De acuerdo con al análisis realizado sobre los activos de información, sus amenazas, vulnerabilidades, probabilidad e impacto, se ha establecido que el nivel de riesgo al que están expuestos dichos activos es elevado. Por lo tanto, es importante determinar un conjunto de políticas de seguridad de la información, que sean establecidas y aprobadas por la máxima autoridad, conjuntamente con el comité de gestión de seguridad de la información y socializadas a toda la organización. A continuación, se especifican las políticas y controles de seguridad de la información. Se consideró como base los dominios, objetivos de control y controles del anexo A, de la norma ISO 27001:2013. La guía de implementación para en GAD Municipal, se puede ver en el Anexo 5 y la confirmación de recepción de dicho documento en el Anexo 6.

Políticas de seguridad de la información

- Se fundamenta en el Dominio 5 del anexo A de la norma ISO 27001.
- Las políticas de seguridad de la información que se proponen, están enfocadas en las necesidades de la unidad de informática de la municipalidad, permitirán prevenir, reducir y eliminar en el mejor de los escenarios los riesgos.
- Se deben establecer acciones necesarias para que los activos de información que intervienen en el almacenamiento de información de la unidad de informática sean administrados correctamente, así como los mecanismos empleados para la implementación de dichas acciones, frente a posibles amenazas.
- Todos los funcionarios y proveedores se deben comprometer a mantener la información de la organización de forma confidencial, es decir que se prohíbe la divulgación de cualquier tipo de información, sin la debida autorización del área correspondiente.

Objetivos

- Preservar la confidencialidad, integridad y disponibilidad de los activos de información de la unidad de informática, reduciendo la probabilidad de ocurrencia de las amenazas y que puedan afectar a las actividades diarias de la unidad en mención.
- Promover una cultura de seguridad de la información en toda la organización, realizando campañas de concienciación y aplicando las respectivas sanciones de ser el caso.

Alcance

La política de seguridad de la información diseñada para la unidad de informática del GAD Municipal del Cantón Pujilí, se aplica a todos los funcionarios y proveedores, con el propósito de minimizar los riesgos, que puedan tener efectos negativos en la organización.

Organización de la seguridad de la información

Se fundamenta en el dominio 6 del anexo A de la norma ISO 27001.

Roles y responsabilidades

La unidad de informática, será la encargada de capacitar al resto de la organización sobre todo lo que concierne a la seguridad de la información, para su apoyo se establecerá una comisión para la gestión de la seguridad de la información cuya misión será realizar reuniones regulares con el fin de analizar o mejorar las políticas establecidas.

El oficial de seguridad de la información no pertenecerá a la unidad de informática, la comisión estará conformada por:

- Alcalde
- Oficial de seguridad de la información

- Responsable del área administrativa
- Responsable del área financiera
- Responsable del área jurídica
- Responsable de talento humano
- Responsable de auditoría interna

Responsabilidades del comité de seguridad de la información

- Gestionar la aprobación de la política y normas sobre la seguridad de la información.
- Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas.
- Mantener el monitoreo de los incidentes con nivel de impacto alto.
- Controlar la implementación de los controles para nuevos sistemas o servicios.
- Promover la difusión de la seguridad de la información dentro de la organización.
- El comité deberá reunirse cada dos meses o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.
- Crear y mantener actualizado el registro de las nuevas amenazas y vulnerabilidades.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la organización frente a incidentes imprevistos.
- Consolidar el contacto con grupos de interés, especializados en el campo de la seguridad de la información (EGSI, 2020).

Políticas de gestión de activos

Se fundamenta en el dominio 8 del anexo A de la norma ISO 27001.

Responsabilidad por los activos

Objetivo: proteger los activos de información de la unidad de informática, mitigando o eliminando riesgos potenciales que pueden ser accidentales o intencionados.

Controles

- Es responsabilidad de la unidad de informática el mantener un inventario de activos de información debidamente actualizado.
- Cada activo de información deberá tener un propietario, quien será la persona responsable de la protección del mismo, donde se deberá definir qué usuario o grupo de usuarios podrán acceder al activo.
- Para el uso aceptable de los activos de información se deberán determinar políticas documentadas y revisadas periódicamente, teniendo en cuenta que los activos de información asignados a un funcionario son de uso exclusivo para propósitos laborales.
- Para la asignación de los activos de información, es recomendable realizar un acta de entrega-recepción, para establecer el uso responsable de los mismos, a la finalización del empleo, todos los activos de información asignados se deberán devolver con la firma en el acta antes mencionada.
- En el caso de que se verifique el deterioro del activo de información asignado, según sea el caso, se deberán aplicar las respectivas sanciones.

Clasificación de la información

Objetivo: garantizar que la información posea un nivel de protección de acuerdo su confidencialidad, integridad y disponibilidad.

Controles

- Establecida la propiedad de la información, ésta debe ser clasificada, de acuerdo a los niveles de importancia.

- De acuerdo a las directrices de etiquetado que haya asumido la unidad, la información se deberá etiquetar de acuerdo a los formatos físicos y electrónicos que se dispongan.
- La manipulación de la información se realizará de acuerdo a su clasificación y a la propiedad de la misma, teniendo en cuenta la preservación de la confidencialidad de la información crítica o sensible para la unidad.

Manejo de medios

Objetivo: asegurar la confidencialidad de la información almacenada en medios removibles.

Controles

- La gestión de los medios removibles se realizará de acuerdo con el modelo de clasificación adoptado por la unidad de informática.
- Se debe definir un procedimiento para cuando los medios removibles deban ser desechados, y que sea de forma segura.
- Los medios removibles que contienen información exclusiva de la organización, deberán estar protegidos contra el acceso no autorizado, divulgación o mal uso durante el transporte de los mismos.

Políticas de control de acceso

Se fundamenta en el dominio 9 del anexo A de la norma ISO 27001.

Objetivo: garantizar que el acceso a los activos de información sea exclusivo para los usuarios autorizados por la unidad de informática.

Controles

- La unidad de informática deberá definir reglas para el control de acceso y restricciones de ser el caso, éstas reglas deberán estar documentadas revisadas

y aprobadas conjuntamente con el comité de gestión de la seguridad de la información.

- De acuerdo a las actividades que desempeñen, a los funcionarios y proveedores, se les proporcionará acceso a la red y a los servicios de red a los cuales han sido autorizados.
- Se debe contar con un proceso formal para el registro y cancelación de derechos de acceso de los usuarios a los sistemas de información que sean de uso exclusivo de la organización.
- La asignación y utilización de derechos de acceso privilegiados estarán restringidos y controladas mediante la autenticación. Se debe considerar aspectos para el teletrabajo.
- De acuerdo a la clasificación y propiedad de los activos de información, se deberán revisar los derechos de acceso de los usuarios periódicamente.
- Los derechos de acceso deberán ser retirados después de la finalización del empleo, o cuando exista un cambio de funciones dentro de la organización.
- Todos los usuarios de los sistemas de información de la organización tienen la obligación de acatar las mejores prácticas y políticas que se han definido en cuanto al uso de la información.
- Con la finalidad de restringir el acceso a personas no autorizadas a los sistemas información y aplicativos, se deberá contar con un sistema de gestión de contraseñas. Algunas recomendaciones para la generación y uso de las contraseñas son:

- No deben ser palabras comunes, ni tener información personal.
- Debe tener mínimo 8 caracteres alfanuméricos.
- Deber ser cambiada obligatoriamente la primera vez que se ingrese al sistema de información.

- Se debe forzar a cambiar al menos cada 30 días o cuando la unidad de informática disponga.
- No deben ser compartidas o mantenerlas a la vista.
- Evitar el uso de las mismas contraseñas para fines personales y asuntos de trabajo.

• En caso de que algún funcionario o proveedor necesite acceso a los sistemas de información o aplicativos, deberá realizar una solicitud a la unidad de informática.
• La unidad de informática será la responsable del control del acceso a los códigos fuente de los programas.
• Los proveedores pueden utilizar sus dispositivos móviles personales en el ambiente de trabajo, pero no pueden acceder a la información de la organización.

Políticas de criptografía

Se fundamenta en el dominio 10 del anexo A de la norma ISO 27001.

Objetivo: hacer uso adecuado de herramientas criptográficas para garantizar la confidencialidad, integridad, disponibilidad de la información de la organización.

Controles

• La unidad de informática debe definir y usar principios sobre el uso de controles criptográficos para el resguardo de la información.
• La unidad de informática debe definir y usar procesos para el uso, protección y duración de las claves criptográficas.

Políticas de seguridad física y del entorno

Se fundamenta en el dominio 11 del anexo A de la norma ISO 27001.

Objetivo: evitar el acceso físico no autorizado, el daño o mal uso de la información en la unidad de informática, a fin de disminuir daños a los activos de información.

Controles

- Es indispensable que la unidad de informática use perímetros de seguridad, con el principal objetivo de salvaguardar la infraestructura de procesamiento y almacenamiento de información.
- Se deben implementar controles de acceso físico a la unidad que permitirán validar la identidad del personal autorizado, éstos controles físicos pueden ser cerraduras electrónicas, cerraduras biométricas, cerraduras con combinación, etc.
- Todos los funcionarios de la organización deben contar con una identificación que les permitirá el acceso seguro, en caso de personas externas, se les asignará una identificación provisional. Es importante disponer de un registro con la fecha y hora de ingreso.
- Se debe contar con protección física para las amenazas que puedan ser causadas por fuego, agua, terremoto, explosión u otras formas de desastres naturales o causadas por el hombre.
- La unidad informática debe tener condiciones mínimas de seguridad en la infraestructura, que garantice el trabajo y las operaciones que se realizan.
- De ser necesario el retiro o traslado de equipos, se deberá contar con la respectiva autorización del líder de la unidad de informática.
- La unidad de informática debe disponer de cableado estructurado que garantice la protección de los equipos, realizando las conexiones adecuadas, separando el cableado eléctrico de la red de datos para evitar posibles interferencias, y como protección contra la intercepción.

- Se deben realizar mantenimientos programados en los equipos de la unidad de informática y realizar pruebas al sistema de energía ininterrumpida, se deberá adquirir un sistema de detección y supresión de incendios y un sistema de aire acondicionado.
- Todos los usuarios deberán conservar sus equipos de cómputo con contraseña y protectores de pantalla cuando no estén en su lugar de trabajo.
- Los puestos de trabajo se deberán mantener limpios de cualquier tipo de papel y medios de almacenamiento extraíbles.

Políticas de seguridad de las operaciones

Se fundamenta en el dominio 12 del anexo A de la norma ISO 27001.

Objetivo: establecer los lineamientos para mantener seguras las operaciones y las instalaciones del procesamiento de información, salvaguardando la integridad de los datos.

Controles

- Mantener los procedimientos de las operaciones debidamente documentados y disponibles para cuando sea necesario usarlos o actualizarlos.
- De acuerdo a la clasificación de los activos, es preciso que el comité de gestión de seguridad de la información realice reuniones regulares para estudiar y aprobar las solicitudes de cambios sobre los activos mencionados.
- Los relojes de todos los sistemas de información de la organización deberán estar sincronizados a una sola fuente de tiempo de referencia.
- La unidad de informática debe realizar un análisis sobre el uso y la capacidad de los sistemas de información, con los que cuenta actualmente y lo que se necesitará en el futuro, con el fin de optimizar el desempeño de dichos sistemas y alcanzar los objetivos organizacionales.

- La unidad de informática proporcionará los controles necesarios para la prevención y detección de software malicioso y las medidas necesarias para el restablecimiento ante un incidente.
- Es obligatorio realizar copias de respaldo de información sensible o crítica, el comité de gestión de seguridad de la información analizará y asignará la persona responsable para realizar los backups, el lugar para el almacenamiento y la validación del buen funcionamiento.
- Los logs de las actividades que realicen los administradores y los usuarios de los sistemas de información se deben registrar y almacenar adecuadamente, para su posterior revisión.
- La unidad de informática es la autorizada para la instalación de software, no está permitido ningún tipo de software ajeno a la organización.
- La unidad de informática debe realizar pruebas de pentest ethical hacking para mantener el control sobre las vulnerabilidades técnicas de los sistemas de información.

Políticas de seguridad en las comunicaciones

Se fundamenta en el dominio 13 del anexo A de la norma ISO 27001.

Objetivo: garantizar la seguridad de la información transmitida en las redes de comunicaciones y su infraestructura.

Controles

- La unidad de informática debe implementar protocolos de seguridad y de transmisión segura para la transferencia de información a través de la red, ya sean servicios propios o contratados.
- Se debe diseñar e implementar el uso de vlans, para la correcta separación de redes, de acuerdo a las áreas o unidades de trabajo dentro de la organización.

- Es recomendable hacer uso de firewall, IPS, IDS, los mismos que deben contar con un registro de incidentes, para llevar un control de eventualidades y comportamiento de la red.
- Si no se cuenta con la respectiva autorización del área de informática, ningún funcionario o proveedor puede conectar a la red ningún dispositivo.
- Se deben establecer e implementar controles para la transferencia de información segura, usando métodos de encriptación o protocolos seguros, que impidan modificaciones, interceptaciones o eliminación de información.
- La configuración que se realice en los equipos, ya sean routers, switches, firewall, etc., debe ser debidamente documentada.
- Los servicios externos deberán contar con cláusulas definidas sobre la transferencia de información segura.
- La información transmitida en mensajería electrónica deberá estar protegida adecuadamente. Los usuarios no deben abrir mensajes, que contengas archivos adjuntos de correos electrónicos desconocidos, para ello es importante contar con un antivirus legal.
- El tamaño máximo permitido para los archivos adjuntos lo determinará la unidad de informática, se debe realizar mantenimiento periódico de las cuentas de correo electrónico.
- Toda información que sea transmitida por la red interna de la organización, puede ser auditada cuando la unidad de informática así lo determine.

Políticas de relación con los proveedores

Se fundamenta en el dominio 15 del anexo A de la norma ISO 27001.

Objetivo: mantener un nivel de seguridad de la información adecuado en la prestación de servicios por parte de proveedores.

Controles

- Los acuerdos para el acceso, manejo o modificación de la información de igual manera se acordarán con los proveedores.
- La unidad de informática conjuntamente con los proveedores, debe definir y documentar las políticas de seguridad de la información para lograr minimizar los riesgos que tengan que ver con el acceso del proveedor a los activos de la unidad en mención.
- La prestación de servicios que proporcionan los proveedores debe ser controlada y auditada periódicamente por el área de informática.

Políticas para la gestión de incidentes de seguridad de información

Se fundamenta en el dominio 16 del anexo A de la norma ISO 27001.

Objetivo: gestionar eficaz y eficientemente los incidentes que comprometan la seguridad de la información en la unidad de informática.

Controles

- El comité de gestión de seguridad de la información debe establecer las responsabilidades y procedimientos con la intensión de generar una respuesta eficaz y eficiente a los incidentes de seguridad de la información.
- Se deberá llevar un registro de los incidentes relacionados a la seguridad de la información reportados a la unidad de informática, para su posterior revisión.
- Los incidentes de seguridad de la información deben tener una respuesta de acuerdo al nivel de criticidad de los mismos.
- Fortalecer las lecciones obtenidas acerca de los incidentes de seguridad de la información que ocurrieron y sobre las acciones tomadas, para evitar incidentes futuros.

Políticas para la continuidad del negocio

Se fundamenta en el dominio 17 del anexo A de la norma ISO 27001.

Objetivo: garantizar la continuidad del negocio, ejecutando controles para contrarrestar las interrupciones que se generen en la unidad de informática de la organización.

Controles

- La unidad de informática deberá identificar los requisitos normativos y contractuales para la seguridad de la información, estos deberán estar definidos y documentados, con el fin de evitar sanciones a la organización o a los funcionarios como resultado de incumplimientos.
- Se deben realizar revisiones periódicas de los controles, políticas o procedimientos que la unidad de informática haya definido en torno a la seguridad dela información.
- La unidad de informática deberá establecer los requisitos para la seguridad de la información y las medidas a tomar durante situaciones desfavorables.
- Para proteger la información se la debe almacenar en el lugar seguro, las instalaciones de procesamiento de información deberán tener la respectiva redundancia para cumplir con los requisitos de disponibilidad.

Políticas de cumplimiento

Se fundamenta en el dominio 18 del anexo A de la norma ISO 27001.

Objetivo: asegurar el cumplimiento de las obligaciones legales, reglamentarias o contractuales en cuanto a la seguridad de la información.

Controles

- La unidad de informática deberá definir, documentar y mantener actualizados todos los requisitos legales, normativos y contractuales para cada sistema de información.
- En cuanto a los derechos de propiedad intelectual y el uso de productos de software propietario, la unidad de informática debe definir e implementar procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, normativos y contractuales de los mismos.
- Los registros se deben salvaguardar ante hurto, destrucción, modificación, acceso no autorizado o divulgación.
- Se debe asegurar la privacidad y la protección de datos personales, según lo que determina la legislación y las normativas aplicables.
- Los responsables de la unidad de informática deben revisar ordinariamente el cumplimiento de las políticas en torno a la seguridad de la información.

FASE VI: Declaración de aplicabilidad.

La norma ISO 27001:2013 tiene dentro de su documentación la declaración de aplicabilidad, ésta declaración corresponde a la relación entre la evaluación del riesgo y el respectivo tratamiento que se dé a los riesgos, a fin de mitigar o eliminar los mismos.

La declaración de aplicabilidad para el presente proyecto, está diseñada para la unidad de informática del GAD Municipal del cantón Pujilí, como se muestra en la Tabla 33.

Tabla 33.

Declaración de aplicabilidad

Dominio	**A.5 Políticas de seguridad de la información.**		
Objetivo de control	**A.5.1 Orientación de la dirección para la gestión de la seguridad de la información.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.5.1.1	Políticas para la seguridad de la información.	SI	Se deben definir un conjunto de políticas de seguridad de la información acordes a los objetivos de seguridad de la unidad de informática. Este documento debe ser probado por el alcalde y se debe comunicar a todos los empleados y público en general.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	SI	Las políticas para seguridad de la información se deben revisar constantemente, o cuando exista algún cambio importante para asegurar su eficacia y eficiencia.
Dominio	A.6 Organización de la seguridad de la información.		
Objetivo de control	**A.6.1 Organización interna.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	SI	Se deben definir claramente los roles y responsabilidades para poder asegurar que se tenga el panorama claro respecto a la ejecución de las actividades definidas en la seguridad de la información.
A.6.1.2	Segregación de deberes.	SI	En el GAD Municipal, todo el personal está separado por áreas y funciones y se les concede el acceso necesario a la información y/o activos para realizar su trabajo diariamente.

A.6.1.3	Contacto con las autoridades	SI	Se debe mantener el contacto oportuno con las autoridades, con el fin de dar soluciones a incidentes o problemas relacionados a la seguridad de la información que así lo requieran.
A.6.1.4	Contacto con grupos de interés especial	SI	Se debe consolidar el contacto con los grupos de interés, especializados en el campo de la seguridad de la información, que puedan contribuir con soluciones para la mitigación de posibles amenazas o vulnerabilidades.
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	Se debe diseñar una política, para realizar el análisis y evaluación de los posibles riesgos, con respecto a la seguridad de la información en los proyectos que se desarrollan en la unidad de informática.
Objetivo de control	**A.6.2 Dispositivos móviles y teletrabajo**		
A.6.2.1	Políticas para dispositivos móviles.	SI	Se debe generar una política de seguridad para gestionar los riesgos en el uso de los dispositivos móviles.
A.6.2.2	Teletrabajo.	SI	La organización deberá generar políticas se seguridad para el teletrabajo.
Dominio	**A.7 Seguridad de los recursos humanos**		
Objetivo de control	**A.7.1 Antes de asumir el empleo**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.7.1.1	Selección.	NO	La contratación del personal es responsabilidad del área de recursos humanos.
A.7.1.2	Términos y condiciones del empleo.	NO	La contratación del personal es responsabilidad del área de recursos humanos.

Objetivo de control	**A.7.2 Durante la ejecución del empleo**		
A.7.2.1	Responsabilidades de la dirección.	NO	La contratación del personal es responsabilidad del área de recursos humanos.
A.7.2.2	Toma de conciencia, educación y formación.	NO	La contratación del personal es responsabilidad del área de recursos humanos.
A.7.2.3	Proceso disciplinario.	NO	La contratación del personal es responsabilidad del área de recursos humanos.
Objetivo de control	**A.7.3 Terminación o cambio de empleo**		
A.7.3.1	Terminación o cambio de responsabilidades de empleo.	NO	La contratación del personal es responsabilidad del área de recursos humanos.
Dominio	**A.8 Gestión de activos.**		
Objetivo de control	**A.8.1 Responsabilidad por los activos**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.8.1.1	Inventario de activos.	SI	La unidad de informática debe realizar y mantener actualizado el inventario de activos de información, ya que es parte esencial para el establecimiento del SGSI.
A.8.1.2	Propiedad de los activos.	SI	De acuerdo al inventario de los activos actualizado que se tenga en la unidad, se debe asignar un responsable a cada uno de ellos, asegurando un control permanente de los mismos.

A.8.1.3	Uso aceptable de los activos.	SI	De acuerdo a las políticas establecidas sobre la seguridad de la información, los usuarios de los sistemas de información se deben comprometer al uso eficaz y eficiente de los activos.
A.8.1.4	Devolución de activos.	SI	Al terminar su vínculo laboral de los empleados, existe un proceso de paz y salvo mediante el cual se valida que los empleados registren la devolución de los activos entregados por el GAD Municipal.
Objetivo de control	**A.8.2 Clasificación de la información.**		
A.8.2.1	Clasificación de la información.	SI	En la unidad de informática se deben establecer niveles de seguridad que permitan priorizar correctamente los riesgos, para ello es importante realizar la clasificación de la información para cada uno de los activos.
A.8.2.2	Etiquetado de la información.	SI	Cada uno de los activos que constan en el inventario, deben estar etiquetados con la clasificación de la información asociada, de acuerdo con los niveles de criticidad establecidos.
A.8.2.3	Manejo de los activos.	SI	Se debe definir un procedimiento que posibilite el manejo de los activos de información, de acuerdo con el nivel de criticidad establecido para cada uno de ellos.
Objetivo de control	**A.8.3 Manejo de medios**		
A.8.3.1	Gestión de medios removibles.	SI	La unidad de informática debe definir un procedimiento para la gestión de los medios removibles, y así disminuir el riesgo de infección con software malicioso.
A.8.3.2	Disposición de los medios.	SI	La unidad de informática debe definir un procedimiento para la disposición de medios removibles al terminar su vida útil.
A.8.3.3	Transferencia de medios físicos.	SI	La unidad de informática debe implementar controles que permitan proteger los medios físicos, de accesos indebidos.

Dominio	A.9 Control de acceso		
Objetivo de control	**A.9.1 Requisitos de negocio para control de acceso.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.9.1.1	Política de control de acceso.	SI	Se debe ser la encargada de generar un procedimiento para el control de acceso con el fin de disminuir los riesgos por hurto de los activos de información.
A.9.1.2	Acceso a redes y a servicios en red.	SI	Se debe generar un procedimiento que garantice el uso de la red y que permita disminuir el riesgo de saturación de los sistemas, divulgación de información crítica o accesos no autorizados.
Objetivo de control	**A.9.2 Gestión de acceso de usuarios**		
A.9.2.1	Registro y cancelación de registro de usuarios.	SI	Se debe generar un procedimiento para facilitar la asignación de derechos de acceso a los usuarios, así como la cancelación del registro.
A.9.2.2	Suministro de acceso de usuarios.	SI	Existe un proceso mediante el cual se asignan o revocan derechos de accesos a los usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	A los servidores que son usuarios de los diferentes sistemas se les otorga privilegios, según el perfil del cargo y las necesidades diarias en las actividades que realizan.
A.9.2.4	Gestión de información de autenticación secreta de usuarios.	SI	Se debe generar un procedimiento para la entrega de claves de acceso a los usuarios de los sistemas de información con la finalidad proteger la información de tipo secreta.
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	SI	La unidad informática debe generar un procedimiento que permita la revisión de los derechos de usuario de forma periódica.

A.9.2.6	Retiro o ajuste de los derechos de acceso.	SI	Se debe generar un procedimiento para el retiro de privilegios de acceso de los usuarios que ya no laboren en la organización o que se les haya cambiado de área, con la finalidad de mitigar riesgos de abuso de privilegios y accesos no autorizados.
Objetivo de control	**A.9.3 Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta.	SI	La unidad informática previamente informa a los usuarios de los diferentes sistemas, que la política institucional es cumplir correctamente con la autenticación secreta para el uso de la información.
Objetivo de control	**A.9.4 Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción de acceso a la información.	SI	Se debe generar una política de controles específicos y exclusivos que restringen el acceso a los sistemas de información, con el cual se logre disminuir riesgos de accesos no autorizados y divulgación de la información.
A.9.4.2	Procedimientos de ingreso seguro.	SI	La unidad informática reporta que, se cumple con los procedimientos de ingreso seguro, en los sistemas informáticos que posee la organización.
A.9.4.3	Sistema de gestión de contraseñas.	SI	La unidad informática ha implementado los requisitos mínimos para el uso de las contraseñas, sin embargo, se debe determinar un tiempo de vencimiento de las contraseñas, forzando a los usuarios a cambiarlas periódicamente.
A.9.4.4	Uso de programas utilitarios privilegiados.	SI	Se encuentran definidos y aplicados controles para evitar que los usuarios puedan instalar herramientas que puedan afectar el funcionamiento de los sistemas de información.
A.9.4.5	Control de acceso a códigos fuente de los programas.	SI	La unidad informática a través de su personal son las personas autorizadas, para controlar y restringir la manipulación y modificación del código fuente.

Dominio	**A.10 Criptografía.**		
Objetivo de control	**A.10.1 Controles criptográficos.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.10.1.1	Política sobre el uso de controles criptográficos.	SI	Se debe generar una política para el uso de controles criptográficos, que permitan disminuir riesgos en la pérdida de información sensible para la organización.
A.10.1.2	Gestión de llaves.	SI	Se debe generar una política de uso, protección y tiempo de vida de las llaves criptográficas.

Dominio	**A.11 Seguridad física y del entorno.**		
Objetivo de control	**A.11.1 Áreas seguras.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.11.1	Perímetro de seguridad física.	SI	La unidad de informática debe contar con un perímetro de seguridad definido y con las medidas de protección activas y pasivas.
A.11.2	Controles de acceso físicos.	SI	La unidad de informática debe implementar controles de acceso biométricos y magnéticos que registren la hora y fecha de acceso, para disminuir riesgos de daños en los equipos o hurto de información sensible.
A.11.3	Seguridad de oficinas, recintos e instalaciones.	SI	Se deben implementar controles físicos de acceso a la unidad de informática, para garantizar la seguridad física.
A.11.4	Protección contra las amenazas externas y ambientales.	SI	Tanto el GAD Municipal, como la unidad de informática deben implementar controles necesarios para hacer frente a las eventualidades de origen antrópico y natural, y que garanticen la continuidad del negocio.

A.11.5	El trabajo en áreas seguras.	SI	La unidad informática debe tener las condiciones mínimas de seguridad en la infraestructura que garantice el trabajo y las operaciones que se realizan en éste sitio.
A.11.6	Áreas de despacho y carga.	SI	La unidad informática se encuentra de acuerdo a su distribución de ambientes y espacios se encuentra de forma aislada de las áreas de despacho, carga y alto tráfico de personas.
Objetivo de control	**A.11.2 Equipos.**		
A.11.2.1	Ubicación y protección de los equipos.	SI	Se debe generar una política que garantice la protección de los equipos con medidas de seguridad activa y pasiva, así como el resguardo de la seguridad interna y externa de ésta área.
A.11.2.2	Servicio de suministro.	SI	La unidad de informática cuenta mínimamente con dispositivos de energía ininterrumpida para los equipos informáticos, se debe proporcionar un soporte alterno de fluido eléctrico y de comunicaciones.
A.11.2.3	Seguridad del cableado.	SI	Se debe generar una política que determine los requerimientos mínimos que se deben cumplir para realizar la instalación de puntos de datos, de acuerdo a los estándares requeridos.
A.11.2.4	Mantenimiento de los equipos.	SI	La unidad informática debe contar con cronograma de mantenimientos periódicos de los equipos para garantizar la disponibilidad e integridad de los mismos.
A.11.2.5	Retiro de activos.	SI	La unidad informática notifica a sus servidores y usuarios de los sistemas, que el retiro de equipos, información o software se lo realizará previo a autorización.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones.	SI	El GAD municipal, a través de la unidad informática determina como política que los equipos y activos informáticos, no pueden abandonar las instalaciones.

A.11.2.7	Disposición segura o reutilización de equipos.	SI	Se debe generar una política para los equipos que han cumplido su vida útil o tiempo de uso, se debe verificar que la información, datos sensibles y software con licencia sea extraído y retirado de forma segura
A.11.2.8	Equipo de usuario desatendido.	SI	La unidad informática garantiza medianamente el procedimiento de protección para los equipos desantedidos.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	SI	Se debe generar una política de escritorio y pantalla limpia en los activos, como un proceso de capacitación a los servidores, en donde se especifiquen las mejores prácticas.

Dominio	**A.12 Seguridad de las operaciones.**		
Objetivo de control	**A.12.1 Procedimientos operacionales y responsabilidades.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.12.1.1	Procedimientos de operación documentados.	SI	La unidad de informática debe documentar y poner a disposición de los usuarios los procedimientos generados y aprobados, para garantizar la seguridad de la información de los activos.
A.12.1.2	Gestión de cambios.	SI	La unidad de informática debe diseñar un procedimiento para la gestión de cambios, con el fin de asegurar el correcto uso de sistemas de información.
A.12.2.3	Gestión de capacidad.	SI	En la unidad informática se realiza un control de los recursos y se realiza la proyección para la adquisición anual de nuevo equipamiento, de acuerdo a las necesidades del área en mención
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operación.	NO	En la unidad de informática no se realiza desarrollo informático.
Objetivo de control	**A.12.2 Protección contra códigos maliciosos.**		

A.12.2.1	Controles contra códigos maliciosos.	SI	La unidad de informática cuenta con un servicio de firewall, mediante el cual se logra identificar y bloquear códigos maliciosos.
Objetivo de control	**A.12.3 Copias de respaldo.**		
A.12.3.1	Respaldo de la información.	SI	Se debe establecer una política que permita realizar copias de seguridad de toda la información a intervalos establecidos por la unidad de informática.
Objetivo de control	**A.12.4 Registro y seguimiento.**		
A.12.4.1	Registro de eventos.	SI	La unidad de informática mantiene los logs de los eventos ocurridos en los sistemas de información críticos para el negocio como medida de protección.
A.12.4.2	Protección de la información de registro.	SI	La unidad de informática cuenta con controles de autenticación en los sistemas de información con el objeto de evitar accesos no autorizados, los mismos que son alertados periódicamente.
A.12.4.3	Registros del administrador y del operador.	SI	Se registran las actividades de los administradores y de quienes operan los distintos sistemas de información, que posee la organización.
A.12.4.4	Sincronización de relojes.	SI	Los relojes de los sistemas de información, se encuentran sincronizados de acuerdo a una única zona horaria.
Objetivo de control	**A.12.5 Control de software operacional.**		

A.12.5.1	Instalación de software en los sistemas operativos.	SI	Se debe generar un procedimiento formal para controlar que los usuarios de la organización no cuenten con los permisos necesarios para la instalación de ningún software, para cualquier instalación se debe solicitar autorización al área respectiva.
Objetivo de control	**A.12.6 Gestión de la vulnerabilidad técnica.**		
A.12.6.1	Gestión de las vulnerabilidades técnicas.	SI	Se debe realizar una evaluación sobre las vulnerabilidades técnicas, el cual debe ser ejecutado de manera periódica, con la finalidad de disminuir los riesgos de seguridad para los sistemas de información.
A.12.6.2	Restricciones sobre la instalación de software.	SI	La unidad informática posee un procedimiento que restringe a los usuarios de la organización sobre la instalación de ningún software autorizado.
Objetivo de control	**A.12.7 Consideraciones sobre auditorías de sistemas de información.**		
A.12.7.1	Controles de auditoría de los sistemas de información.	SI	Se debe planificar la realización de auditorías relacionadas a la identificación de vulnerabilidades de los sistemas de información y que se puedan tomar las acciones necesarias para la disminución de riesgos.
Dominio	**A.13 Seguridad en las comunicaciones.**		
Objetivo de control	**A.13.1 Gestión de la seguridad de las redes.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.13.1.1	Controles de redes.	SI	Se debe implementar una infraestructura de llave pública con algoritmos fuertes de cifrado, para garantizar la confidencialidad e integridad de la información que se transmite a través de la red.

A.13.1.2	Seguridad de los servicios de red.	SI	La unidad de informática cuenta con acuerdos de niveles de servicio con el ISP, en cuanto a la disponibilidad del servicio con el proveedor contratado.
A.13.1.3	Separación en las redes.	SI	Las redes deben estar segmentadas mediante VLANs.
Objetivo de control	**A.13.2 Transferencia de información.**		
A.13.2.1	Políticas y procedimientos de transferencia de información.	SI	La unidad de informática cuenta con una política o procedimientos de transferencia de información con un formato establecido sobre la capacidad (envío y recepción) de información.
A.13.2.2	Acuerdos sobre transferencia de información.	SI	La unidad de informática cuenta con controles criptográficos, así como los protocoles de transferencia segura para garantizar la transferencia segura de información.
A.13.2.3	Mensajería electrónica.	SI	La unidad de informática debe implementar controles para proteger la información enviada por medio de correo electrónico.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	SI	Se debe implementar controles que permitan la identificación, revisión y documentación, regular de los requisitos para los acuerdos de confidencialidad
Dominio	**A.14 Adquisición, desarrollo y mantenimiento de sistemas.**		
Objetivo de control	**A.14.1 Requisitos de seguridad de los sistemas de información.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información.	NO	En la unidad de informática no se realiza desarrollo informático.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones.	NO	En la unidad de informática no se realiza desarrollo informático.
Objetivo de control	**A.14.2 Seguridad en los procesos de desarrollo y soporte.**		
A.14.2.1	Política de desarrollo seguro.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.2	Procedimientos de control de cambios en los sistemas.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.4	Restricciones en los cambios a los paquetes de software.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.5	Principios de construcción de los sistemas seguros.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.6	Ambiente de desarrollo seguro.	NO	En la unidad de informática no se realiza desarrollo informático.

A.14.2.7	Desarrollo contratado externamente.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.8	Pruebas de seguridad de sistemas.	NO	En la unidad de informática no se realiza desarrollo informático.
A.14.2.9	Pruebas de aceptación de sistemas.	NO	En la unidad de informática no se realiza desarrollo informático.
Objetivo de control	**A.14.3 Datos de prueba.**		
A.14.3.1	Protección de datos de prueba.	NO	En la unidad de informática no se realiza desarrollo informático.

Dominio	**A.15 Relaciones con los proveedores.**		
Objetivo de control	**A.15.1 Seguridad de la información en las relaciones con suministradores.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.	SI	Se debe definir una política que determine los lineamientos de seguridad que limite el acceso de los proveedores, contratistas a los activos que la institución posee referente a la información.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	SI	La unidad de informática debe establecer los requisitos de seguridad de la información que deben cumplir los proveedores y los riesgos asociados.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	SI	La unidad de informática debe establecer acuerdos con los proveedores con respecto al tratamiento de los riesgos, en los que se ven inmersos la debida custodia, manipulación adecuada y responsabilidad de los activos de información.

Objetivo de control	**A.15.2 Gestión de la prestación de servicios de proveedores.**		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	SI	La unidad de informática realiza supervisión y seguimiento a la prestación de servicios de los proveedores, estimados a los procesos contractuales que tiene con ellos.
A.15.2.2	Gestión de cambios en los servicios de los proveedores.	SI	La unidad de informática realiza supervisión y seguimiento a la prestación de servicios que los proveedores brindan a la entidad, los cuales son supervisados y revisados para que se mantenga la seguridad en los activos que poseen información.
Dominio	**A.16 Gestión de incidentes de seguridad de la información.**		
Objetivo de control	**A.16.1 Gestión de incidentes y mejoras de la seguridad de la información.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.16.1.1	Responsabilidades y procedimientos.	SI	Se debe definir un procedimiento para determinar las responsabilidades y criterios de respuesta a los posibles incidentes de seguridad de la información, que permitan dar soluciones oportunas a cualquier eventualidad.
A.16.1.2	Reporte de eventos de seguridad de la información.	SI	Se deben establecer mecanismos y protocolos de comunicación efectiva sobre las eventualidades que pudieran presentarse referente a los incidentes de seguridad de la información.
A.16.1.3	Reporte de debilidades de seguridad de la información.	SI	La unidad de informática debe contar con mecanismos de detección de las debilidades que podrían presentarse referente a los incidentes de seguridad de la información.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	SI	Se debe disponer de un formato que permita definir las eventualidades que sucedieran, para posteriormente clasificarlo como incidentes de seguridad de la información.

A.16.1.5	Respuesta a incidentes de seguridad de la información.	SI	Se deben definir protocolos de acción plenamente documentados, que le permitan actuar antes posibles incidentes de seguridad de la información.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	SI	Se debe mantener registros de incidentes ocurridos y como han sido solventados, como medida de análisis y hacer frente ante futuros incidentes de seguridad de la información.
A.16.1.7	Recolección de evidencias.	SI	Se debe documentar eficientemente los incidentes de seguridad de la información que se han presentado en eventos previos.

Dominio	**A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.**		
Objetivo de control	**A.17.1 Continuidad de seguridad de la información.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	La unidad informática debe definir los requisitos para garantizar la seguridad y la gestión de la información con el fin de asegurar la continuidad del negocio, frente a las posibles situaciones adversas.
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	SI	La unidad informática debe implementar procedimientos de contingencia definidos para garantizar la seguridad y la gestión de la información con el fin de asegurar la continuidad del negocio, frente a las posibles situaciones adversas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	La unidad informática debe verificar, revisar y evaluar procedimientos de contingencia definidos para garantizar la seguridad y la gestión de la información con el fin de asegurar la continuidad del negocio.

Objetivo de control	**A.17.2 Redundancias.**		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de la información.	SI	Se debe definir un procedimiento para la respuesta a incidentes de seguridad de la información, de tal forma que se pueda mitigar el impacto y que no afecte a la continuidad del negocio.
Dominio	**A.18 Cumplimiento.**		
Objetivo de control	**A.18.1 Cumplimiento de los requisitos legales y contractuales.**		
ID	**Control**	**Aplicable (SI/NO)**	**Justificación**
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	SI	Este proceso es realizado por el área jurídica del GAD Municipal, quien garantiza el cumplimiento de los reglamentos legales aplicables a la organización, en función de cada uno de los sistemas informáticos que posee.
A.18.1.2	Derechos de propiedad intelectual.	SI	La unidad informática como usuario general de los sistemas informáticos, ya tienen propiedad intelectual por parte del administrador que se encuentra normado por la legislación de uso y operatividad de estos.
A.18.1.3	Protección de registros.	SI	Se deben realizar acciones de protección contra la perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de registros sin base legal determinante.
A.18.1.4	Privacidad y protección de información de datos personales.	SI	Los sistemas informáticos que maneja y usa la unidad de informática posee características de privacidad y protección de los datos personales de forma efectiva de acuerdo a la legislación vigente nacional sobre este tema.
A.18.1.5	Reglamentación de controles criptográficos.	SI	Se deben usar controles necesarios que garanticen la transmisión segura de la información.

Objetivo de control	A.18.2 Revisiones de seguridad de la información.		
A.18.2.1	Revisión independiente de la seguridad de la información.	SI	La unidad informática debe usar controles necesarios que garanticen la transmisión segura de la información, realizando revisiones periódicas acerca de éste tema.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad.	SI	Se deben establecer controles necesarios que garanticen la transmisión segura de la información.
A.18.2.3	Revisión del cumplimiento técnico.	SI	Se deben programar las revisiones y monitoreo de forma periódica normadas y estandarizados a la seguridad de la información.

Fuente: Elaboración propia. Adaptado de (Doria Corcho, 2015) (Tola Franco & Freire, 2015) (Maureira Sánchez, 2017)

Capítulo VI

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Según el análisis inicial con relación al cumplimiento de los controles que especifica el Anexo A de la norma ISO/IEC 27001, se concluye que dicha unidad se encuentra en un nivel de madurez repetible, debido a que no se cuenta con una política o conjunto de políticas que gestionen de manera adecuada los temas de seguridad de la información en dicha unidad, existiendo dominios para los cuales no existen controles debidamente documentados y conocidos por toda la organización, lo que implica estar expuestos a un sin número de amenazas que pueden ser explotadas en cualquier momento.
- A partir del análisis efectuado, se determina que un riesgo es un suceso incierto, que, si se ejecuta, causaría daños o efectos negativos a la organización, dicho riesgo está asociado a la probabilidad de ocurrencia y al impacto que tendría si se materializa. En consecuencia, la correcta identificación de los riesgos comprende una serie de actividades como el reconocimiento de los activos, amenazas, vulnerabilidades y controles implementados. Dichas actividades se ejecutan en pro de salvaguardar los activos de información en las empresas. Así se concluye que la correcta gestión de los riesgos determina aplicar medidas preventivas para poder garantizar la confidencialidad, integridad y disponibilidad de la información y, por ende, la continuidad del negocio.
- De acuerdo al avance de la tecnología, las organizaciones originan mayor preocupación para proteger su información de cualquier tipo de amenaza existente. Es por ello que es de gran utilidad el diseño e implementación de un

sistema de gestión de seguridad de la información, cuya función principal es gestionar la seguridad de la información en las organizaciones, estableciendo un conjunto de políticas, métodos o técnicas para salvaguardar la información. En base a lo descrito, se concluye que la adopción de un SGSI, contribuye un mejoramiento continuo, lo que produce un análisis continuo de la situación actual y provee la detección de posibles incidentes de seguridad a tiempo.

- Se concluye que, el poseer un inventario de activos actualizado, facilita su clasificación según el nivel de riesgo, lo que conlleva a tener una mayor protección de los mismos Para la valoración de los activos se establece la importancia de cada uno de ellos, tomando en consideración los criterios de disponibilidad, integridad y confidencialidad. En la unidad de informática del GAD en mención se encontraron un total de 13 activos cuya criticidad fue alta, los cuales se tomaron en cuenta para el desarrollo del SGSI.
- La norma ISO/IEC 27005, es una metodología para realizar la gestión de los riesgos de seguridad de la información en las organizaciones, constituye una norma de apoyo a la ISO/IEC 27001 y por ende al SGSI. El análisis recomendado de ésta metodología comprende actividades como: evaluación, tratamiento, aceptación, comunicación y revisión del riesgo. De éste modo, se puede concluir que las amenazas se deben mitigar a través del establecimiento de un plan de tratamiento de riesgos, con la finalidad de reducirlos a un valor aceptable para la unidad de informática y por ende para la organización.
- Se concluye que, la razón principal de disponer de un conjunto de políticas de la seguridad de la información es concienciar a los empleados sobre los riesgos de seguridad y proporcionar las herramientas necesarias para el correcto tratamiento de la información.

RECOMENDACIONES

- El logro de los objetivos organizacionales, el oportuno descubrimiento de las causas de un rendimiento insuficiente y la mejora continua son las pautas claves de las empresas para realizar la evaluación del desempeño en las mismas, todo esto con el principal apoyo de la alta gerencia, liderando los proyectos o temas de seguridad dela información, y apoyado de todas y cada una de las áreas de la organización. Con lo expuesto, se recomienda implementar el sistema de gestión de seguridad de la información propuesto en el presente proyecto, en la unidad de informática del GAD Municipal del Cantón Pujilí.
- Para la implementación del SGSI propuesto en el presente proyecto se recomienda crear el comité de gestión de seguridad de la información, para poder definir los roles y responsabilidades con respecto a la ejecución de las actividades definidas para la protección de la información, dicho comité deberá reunirse cada dos o tres meses o cuando las circunstancias lo ameriten para poder coordinar todas las actividades relacionadas a la seguridad de la información.
- Se recomienda planificar y ejecutar capacitaciones periódicas a todos y cada uno de los empleados del GAD Municipal y proveedores, para la socialización, de temas de la seguridad de la información, con el propósito de generar cultura, orientadas a minimizar y mitigar posibles riesgos a los que se puedan enfrentar.
- Se recomienda implementar mayor seguridad física y electrónica en la unidad de informática, de igual manera planificar e implementar mantenimientos preventivos y correctivos regulares en todos los equipos de dicha unidad para poder evitar posibles fallos y garantizar la continuidad del negocio.

- Establecer un plan de respuesta a incidentes y minimizar los riesgos, son actividades indispensables para garantizar la continuidad del negocio en las organizaciones, teniendo en cuenta que algunos incidentes de seguridad pueden ser provocados voluntaria e involuntariamente por el personal de TI, se recomienda establecer procedimientos para determinar las responsabilidades y criterios de respuesta a los posibles incidentes de seguridad de la información, que permitan dar soluciones oportunas a cualquier eventualidad negativa.

REFERENCIAS

Aguirre Tobar, R. A., & Zambrano Ordoñez, A. F. (2015). Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001. UNAD.

Avilés Guzmán, R. G., & Silva Uría, M. A. (2017). Implementación de un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético, en la empresa Blenastor. Ecuador.

Bayona, S., Chauca, W., Lopez, M., & Maldonado, C. (2015). *ISO/IEC 27001 implementation in public organizations: A case study.* Obtenido de https://ieeexplore.ieee.org/

Bermúdez Molina, K. G. (2015). Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. Ecuador.

BG Consultores Asociados. (2015). DIAGNÓSTICO PDOT Gobierno Autónomo Decentralizado del Cantón Pujilí.

Caicedo Carrillo, J. H., & Rojas Suárez, J. J. (2017). Diseño de un sistema de gestión de seguridad de la información para el área de infraestructura tecnológica de Alfragres SA: basado en la norma ISO/IEC 27001: 2013. Colombia.

Campo Martínez, Y. A. (2019). Procedimientos de seguridad del modelo de seguridad y privacidad de la información para la Gobernación del Cauca. Universidad del Cauca.

Cárdenas Herrera, C., & Higuera, D. (2016). Diseño de un sistema integrado de gestión basado en las normas ISO 9001: 2015 e ISO 27001: 2013 para la empresa La Casa del Ingeniero LCI.

Castillo Palma, M. A., & Molina Jiménez, J. K. (2020). Análisis de riesgos al proceso de fiscalización de proyectos de ingeniería para una empresa que brinda servicios de ingeniería bajo la norma ISO/IEC 27005. Ecuador.

Chunga Ramirez, K. (2017). Análisis de Riesgos de los activos de Información del proceso de Contratación de Personal Docente en la Dirección Regional de Educación basado en las directrices de la ISO/IEC 27005. Perú.

Dirección de Planificación. (2018). Organigrama Institucional. Ecuador.

Doria Corcho, A. F. (2015). Diseño de un sistema de gestión de la seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001: 2013 en la oficina de sistemas y telecomunicaciones de la Universidad de Córdoba.

Fuenmayor Pazmiño, M. Y., & Sarzosa Pavón, L. M. (2015). Análisis de la gestión administrativa y financiera del gobierno autónomo descentralizado Municipal del Cantón Pujilí período 2012–2015. Ecuador.

García Balaguera, V. A., & Ortíz González, J. J. (2017). Análisis de riesgos según la norma ISO 27001: 2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. UNAD.

Garzón Garzón, M. (2017). DISEÑAR LOS CONTROLES DE ACCESO APLICABLES A LA EMPRESA SPYTECH S.A.S PARA SU POSTERIOR IMPLEMENTACIÓN, DE ACUERDO CON EL DOMINIO A9 DE LA NORMA ISO 27001:2013. Bogotá, Cundinamarca, Colombia.

González Pástor, M. A. (2017). Propuesta de plan de comunicación interna para el Gobierno Autónomo Descentralizado del cantón Pujilí. Ecuador.

Imbaquingo Esparza, D. E., & Pusdá Chulde, M. R. (2015). Evaluación de amenazas y vulnerabilidades del módulo de gestión académica-sistema informático integrado universitario de la Universidad Técnica del Norte, aplicando ISO 27000. Universidad de las Fuerzas Armadas ESPE.

INEC. (2010). *Población Cantón Pujilí*. Obtenido de https://www.ecuadorencifras.gob.ec/estadisticas/

ISO Tools. (2020). Norma ISO 37001. Aspectos clave de su diseño e implantación.

ISO/IEC 27001. (2013). *International Organization for Standardization.* Obtenido de ISO: https://www.iso.org/search.html?q=27001

ISO/IEC 27002. (2013). *International Organization for Standardization*. Obtenido de https://www.iso.org/search.html?q=27002

ISO/IEC 27005. (2018). *International Organization for Standardization.* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

Jara Arenas, J. A. (2019). FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT. Perú.

Jara Pérez, D. F. (2017). Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesosincluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. Bogotá, Colombia.

Lanche Capa, D. S. (2015). Diseño de un sistema de seguridad de la información para la Compañía Acotecnic Cía. Ltda. basado en la norma NTE INEN ISO/IEC 27002. Cuenca, Ecuador: Universidad de Cuenca.

Landázuri Benalcázar, M. C. (2017). Formulación de una propuesta para un modelo de sistema de gestión de seguridad de la información para empresas de la industria bancaria en el sector privado.

Lara Guijarro, E. G. (2019). Diseño de un modelo de seguridad de la información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de educación: caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán.

Lema Vinlasaca, R. C., & Donoso Gallo, D. F. (2018). Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001: 2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS SA. Ecuador.

Lopez Rimari, R. P. (2020). Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura. Perú.

Maureira Sánchez, D. (2017). Norma ISO/IEC 27001 aplicada a una carrera universitaria. Santiago de Chile.

MINTEL. (2018). Libro blanco de la sociedad de la información y del conocimiento. Ecuador.

Mogollón, A. (2016). Análisis Comparativo: Metodologías de análisis de Riesgos. Universidad Centroccidental Lisandro Alvarado.

Moncada Castillo, A. A., & Ramírez Gualteros, F. (2017). Estudio de viabilidad para el desarrollo de una metodología que mitigue los factores de riesgo en los proyectos de implementación de software ERP SAP. Bogotá, Colombia.

Neira, A. L., & Spohr, J. R. (2016). *El portal de ISO 27001 en Español.* Obtenido de www. iso27000. es

NIST. (2018). *Seguridad Cibernética*. Obtenido de https://www.nist.gov/topics/cybersecurity

Normas ISO, 2. (2020). *Niveles de documentación ISO 27001*. Obtenido de https://normaiso27001.es/fase-5-documentacion-del-sgsi/

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

Oidor González, J. C. (2017). Diseño de un Sistema de Gestión de Seguridad de la Información - SGSI bajo la norma ISO/IEC 27001:2013 para la empresa “en Línea Financiera” de la ciudad de Cali – Colombia.

Quintero Parra, L. E. (2015). Diseño de un sistema de gestión de seguridad de la información (SGSI) para el departamento de informática de la Superintendencia de Notariado y Registro. UNAD.

Ramos Ruiz, K. P. (2021). AUDITORÍA INFORMÁTICA, PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO PRODVISIÓN, DE LA PROVINCIA DE TUNGURAHUA, CANTÓN PELILEO. Ambato, Tungurahua, Ecuador.

Recalde Caicedo, J. P. (2019). PLAN DE IMPLEMENTACIÓN DE UN SGSI Y APLICACIÓN DE CONTROLES CRÍTICOS EN EL CENTRO DE OPERACIONES DE SEGURIDAD DE LA EMPRESA GMS. Ecuador.

Registro Oficial. (2020). Esquema Gubernamental de Seguridad de la Información. Ecuador.

Reinoso Córdova, A. R. (2017). Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local. Aplicación a un caso de estudio. Quito, Ecuador: EPN.

Sangoluisa Chamorro, D. P. (2015). Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000. Quito, Ecuador.

Satán Cevallos, D. G. (2017). PLANTEAMIENTO DE ALMACENAMIENTO Y GESTIÓN DE LOGS PARA FORTALECER LA SEGURIDAD INFORMÁTICA DE UNA EMPRESA TELEFÓNICA. Guayaquil, Ecuador.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. d. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5).* Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Tejena Macías, M. (2018). Análisis de riesgos en seguridad de la información. Polo del conocimiento, 3(4), 230-244.

Tola Franco, D., & Freire, L. (2015). Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. Ecuador: ESPOL.

Unidad de Talento Humano. (2020). Servidores Municipales.

Vargas Arias, L. H. (2019). Límites a la autonomía de los Gobiernos Autónomos Descentralizados Estudio de los GAD parroquiales rurales. Quito, Pichincha, Ecuador.

Vásquez Escalante, J. F. (2018). Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. Lima, Perú.

Villacís Espinosa, M. L. (2016). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red corporativa de la empresa Ecuatronix. Quito, Pichincha, Ecuador.

Wireshark. (2021). *Wireshark*. Obtenido de https://www.wireshark.org/faq.html#q1.1

ANEXOS

ANEXO 1

NORMA ISO/IEC 27002

ANEXO 2

ENCUESTA UNIDAD DE INFORMÁTICA

ANEXO 3

INFRAESTRUCTURA UNIDAD DE INFORMÁTICA

ANEXO 4

RED INTERNA GAD

ANEXO 5

GUÍA DE IMPLEMETACIÓN GAD MUNICIPAL

ANEXO 6

RECEPCIÓN DOCUMENTACIÓN GAD MUNICIPAL