2021

FACULTAD DE POSGRADOS

# DISEÑO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN PÚBLICA


AUTOR

Pablo Bryan Almeida Guaigua


AÑO

2021

FACULTAD DE POSGRADOS

# DISEÑO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN PÚBLICA

_____

Autor

Pablo Bryan Almeida Guaigua

Año

2021

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

# DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN PÚBLICA

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de MAGÍSTER EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

_____

Autor

Pablo Bryan Almeida Guaigua

Año

2021

**AGRADECIMIENTOS**

Agradezco a familia, a mis padres y a mi abuelo por toda la ayuda y la guía que me han sabido brindar para seguir adelante con sueños y objetivos.

**DEDICATORIA**

Este trabajo es dedicado a mi familia por su apoyo y ejemplo de superación que cada día me motiva para seguir adelante con mi crecimiento profesional y personal con gran determinación y profesionalismo.

## RESUMEN

Un sistema de gestión de seguridad de la información cuenta con un enfoque estructurado y sistemático para la gestión de la información que es aplicable a organizaciones, empresas privadas y públicas en el país, proporcionando un marco para la gestión de la seguridad, los riesgos relacionados con las tecnologías de la información y los controles de amplio alcance para salvaguardar la información de diversas amenazas a la seguridad.

Cuenta con políticas, procedimientos, procesos y flujos de trabajo que permiten proteger la seguridad de la información, además utilizan procesos de gestión de riesgos que comprende estructuras organizativas, personas, políticas, procesos y sistemas informáticos.

Los objetivos de una organización o empresa determinan la implantación del SGSI, el tamaño y la estructura de los requisitos de seguridad y los procedimientos empleados. Es una práctica común documentar los procedimientos y las políticas para la administración del SGSI por procesos, para promover el desarrollo y mejora continua del sistema.

Con el aumento global de las violaciones de datos, se ha provocado una mayor preocupación por la seguridad de la información. Teniendo en cuenta los importantes daños financieros y legales que causan las violaciones a la información, todas las empresas y organizaciones con información valiosa deberán considerar la implantación de un sistema de gestión de la seguridad de la información.

## ABSTRACT

An information security management system has a structured and systematic approach to information management that is applicable to organizations, private and public companies in the country, providing a framework for managing security, risks related to information technologies and wide-ranging controls to safeguard information from various security threats.

It has policies, procedures, processes, and workflows to protect information security, and uses risk management processes comprising organizational structures, people, policies, processes, and IT systems.

The objectives of an organization or company determine the implementation of the ISMS, the size and structure of the security requirements and the procedures used. It is common practice to document procedures and policies for the management of the ISMS by process, to promote the development and continuous improvement of the system.

With the global increase in data breaches, there has been an increased concern for information security. Considering the significant financial and legal damage caused by data breaches, all companies and organizations with valuable information should consider implementing an information security management system.

# ÍNDICE

Contenido

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# 1. INTRODUCCIÓN

La información es un valor importante para las organizaciones y empresas, por lo cual dichas empresas y organizaciones poseen la necesidad de proteger la información de forma adecuada y precisa. La mayor parte de la información actual se crea, almacena, transmite y procesa usando tecnologías de la información.

Hoy en día en ninguna industria se discute la necesidad de proteger la información y su entorno, los incidentes de seguridad pueden tener repercusiones de gran alcance que pueden dañar el negocio o interferir con el desempeño de las actividades, en otras palabras, afectar la continuidad de negocio y generar costos adicionales.

La experiencia práctica ha demostrado que la optimización de la gestión de la seguridad de la información suele mejorar la seguridad de la información de forma más eficaz y duradera que la inversión en tecnología de seguridad. Sin embargo, las medidas aplicadas originalmente para mejorar la seguridad de la información también pueden tener un efecto positivo fuera del contexto de la seguridad y pueden resultar rentables.

En muchos casos, las inversiones en seguridad de la información pueden incluso contribuir a ahorrar costes a mediano o largo plazo. Los efectos secundarios positivos que cabe esperar son una mayor calidad del trabajo, un aumento de la confianza de los clientes, la optimización del panorama informático y de los procesos organizativos, así como el aprovechamiento de los efectos de sinergia mediante una mejor integración de la gestión de la seguridad de la información en las estructuras existentes.

# 2. MARCO TEÓRICO

## 2.1 Sistema de gestión de seguridad de la información

Un sistema de gestión de seguridad de la información (SGSI) es un conjunto de políticas y procedimientos para gestionar sistemáticamente los datos confidenciales de una organización. El objetivo de un SGSI es minimizar el riesgo y garantizar la continuidad del negocio limitando proactivamente el impacto de una brecha de seguridad.

Un SGSI generalmente aborda el comportamiento y los procesos de los empleados, así como los datos y la tecnología. Puede estar dirigido a un tipo particular de datos, como los datos de los clientes, o puede implementarse de una manera integral que se convierta en parte de la cultura de la empresa (TechTarget, 2021).

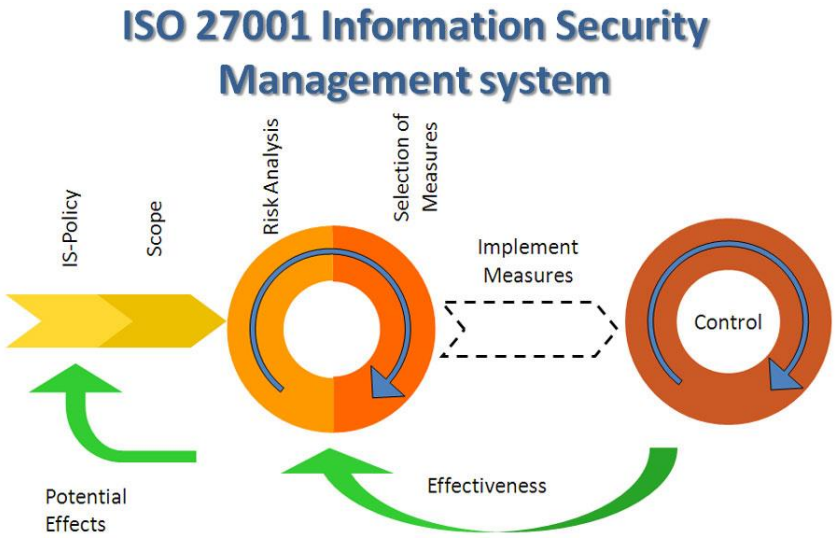


*Figura 1*. Sistema de Gestión de Seguridad de la Información

Tomado de (Infoassureltd, 2021).

## 2.2 ISO/IEC 27001:2013

ISO/IEC 27001: 2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza (ISO/IEC 27001:2013, 2021).


*Figura 2*. ISO/IEC 27001:2013

Tomado de (ISO/IEC 27001:2013, 2021).

## 2.3 ISO/IEC 27002:2013

ISO / IEC 27002: 2013 proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización.

Está diseñado para ser utilizado por organizaciones que pretenden:

- ✓ Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001.
- ✓ Implementar controles de seguridad de la información comúnmente aceptados.
- ✓ Desarrollar sus propias pautas de gestión de seguridad de la información.

(ISO/IEC 27002:2013, 2021).

## 2.4 ISO/IEC 27005:2009

Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información 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. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria (PMG SSI, 2021).

## 2.5 Magerit

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

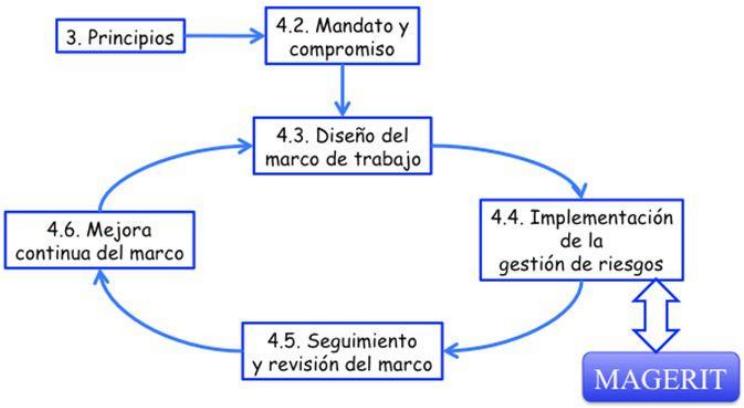


*Figura 3*. Magerit

Tomado de (Portal Administración Electrónica, 2021).

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista (Portal Administración Electrónica, 2021).

## 2.6 NIST

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a los

negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario.


*Figura 4*. NIST Cybersecurity Framework

Tomado de (NIST, 2021).

Brinda a empresas y organizaciones una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su capital en cuestiones de protección de ciberseguridad (Federal Trade Commission, 2021).

# 3. DESARROLLO DEL PROYECTO DE TITULACIÓN

## 3.1 Caso de Negocio

### 3.1.1 Resumen Ejecutivo

En este proyecto se implementará un Diseño del Programa de Sistema de Gestión de la Seguridad de la Información, que proporcionará una mejor estrategia corporativa, calidad de servicio, asesoramiento, coordinación y manejo de la información para los servicios que ofrece la entidad pública.

El desarrollo del sistema de gestión de la seguridad de la información beneficiara a la institución, con la identificación de activos de información, identificación de amenazas y vulnerabilidades, seguridad de la información, gestión de riesgos, definición de políticas y controles de seguridad de la información. Lo cual será llevado a cabo con base en normas y mejores prácticas nacionales e internacionales.

### 3.1.2 Introducción

La Asociación de Municipalidades Ecuatorianas de conformidad a lo dispuesto por el Artículo 313 del Código Orgánico de Organización Territorial, Autonomía y Descentralización – COOTAD es un organismo con autonomía administrativa, financiera y patrimonio propio, de derecho público, con personería jurídica, de representación y asistencia técnica dirigido a los Gobiernos Municipales,

Que promueve la construcción de un modelo de gestión local descentralizado y autónomo, con base en la planificación articulada y la gestión participativa del territorio, a través del ejercicio de la representación institucional, asistencia técnica de calidad y la coordinación con otros niveles de gobierno y organismos del Estado (AME, 2018).

### 3.1.3 Misión

La Asociación de Municipalidades Ecuatorianas es una instancia asociativa de GADs municipales y metropolitanos que promueve la construcción de un modelo de gestión local descentralizado y autónomo, con base en la planificación articulada y la gestión participativa del territorio, a través del ejercicio de la representación institucional, asistencia técnica de calidad y la coordinación con otros niveles de gobierno y organismos del Estado (AME, 2021).

### 3.1.4 Visión

La Asociación de Municipalidades Ecuatorianas es el referente nacional e internacional en desarrollo local a través de la construcción de modelos de gestión territorial equitativos, participativos y solidarios, articulados a políticas nacionales, para la consolidación de gobiernos autónomos descentralizados municipales y metropolitanos que promueven el buen vivir (AME, 2021).

### 3.1.5 Objetivo del programa

Desarrollar un Sistema de Gestión de la Seguridad de la Información (SGSI).

### 3.1.6 Alcance

El alcance del sistema de gestión de seguridad de la información para la institución pública se define dentro del área de sistemas. Además, de definirse los requerimientos, las condiciones y las actividades a desarrollarse dentro de esta.

### 3.1.7 Identificación y Descripción del problema

La organización no cuenta con un Sistema de Gestión de Seguridad de la Información. Que permita realizar un manejo idóneo de la información para que se garantice la confidencialidad, la integridad, la disponibilidad y la privacidad que se maneja.

Tomando en cuenta los servicios y la asistencia técnica que brinda a los diferentes GADs. Para proteger la información de amenazas y riesgos, es necesario el desarrollo y la implementación de un Sistema de Gestión de la Seguridad de la Información, una herramienta que permite establecer políticas, controles y procedimientos para disminuir los riesgos de la organización.

### 3.1.8 Justificación (Razones)

Reducción de los riesgos debido a la definición y seguimiento de controles pertinentes de la seguridad de la información, para reducir amenazas hasta niveles aceptables los cuales sean establecidos por la organización y se garantice la continuidad del negocio.

Ahorro de costos derivados de una racionalización de recursos, se eliminan las inversiones innecesarias e ineficientes como las que se producen por sobre estimar o desestimar los riesgos.

Análisis basado en la gestión y seguridad, que toma como prioridad un clico de vida metódico y controlado en donde participa toda la organización.

Cumplimiento de la normativa legal con el fin de evitar riesgos y costos innecesarios, además de evitar cualquier infracción.

Mejorar la competitividad dentro del mercado, para mejorar la imagen y la confianza de la organización.

### 3.1.9 Descripción de oportunidad

Al no contar con SGSI, el desarrollo de este sistema permitirá la identificación de activos, amenazas y vulnerabilidades, para realizar el tratamiento de riesgos y la definición de políticas de seguridad de la información.

### 3.1.10 Identificación de la solución

De acuerdo con ISO/IEC 27001:2013, para el diseño de un Sistema de Gestión de Seguridad de la Información, se definen los siguientes pasos:

1) Evaluación de los requisitos de la norma ISO 27001.
2) Evaluación de los objetivos de control y controles (Anexo A) de la norma ISO27001.
3) Análisis del contexto organizacional.
4) Identificación y clasificación de activos.
5) Identificación de amenazas y vulnerabilidades.
6) Gestión de riesgos de seguridad de la información.
7) Definición de políticas y controles de seguridad de la información.

### 3.1.11 Cronograma

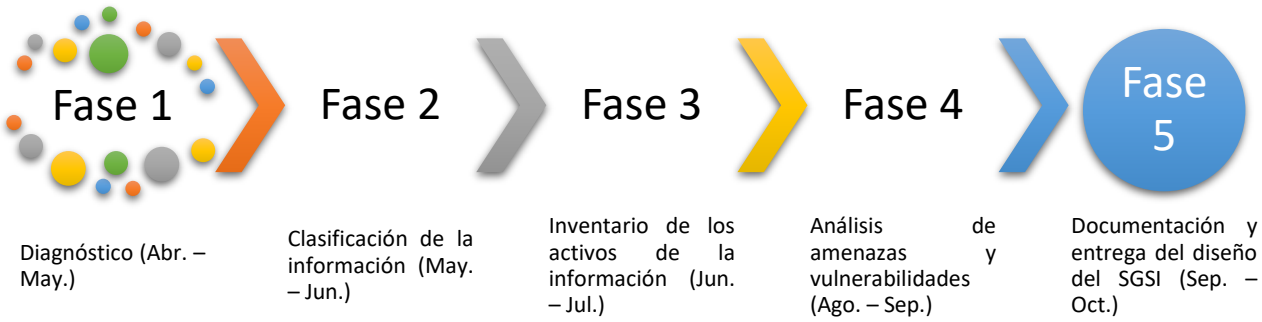


*Figura 5*. Cronograma

## 3.2 Diagnóstico

### 3.2.1 ISO 27001:2013

La norma internacional ISO/IEC 27001:2013 determina los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información tomando en cuenta el contexto de la organización. Esta incluye los requisitos para la evaluación y tratamiento de riesgos de seguridad de la información que se adapten a las necesidades de la organización.

Los requisitos de la norma son genéricos y son aplicables a cualquier organización, sin importar su tipo, tamaño o naturaleza. Cualquier organización debe cumplir con la conformidad de esta norma, tomando en cuenta de manera obligatoria los requisitos especificados en los apartados del 4 al 10 (INTECO, 2021).

Los requisitos del apartado 4 al 10 de la norma internacional se muestran en la Figura 2, los cuales son los siguientes:

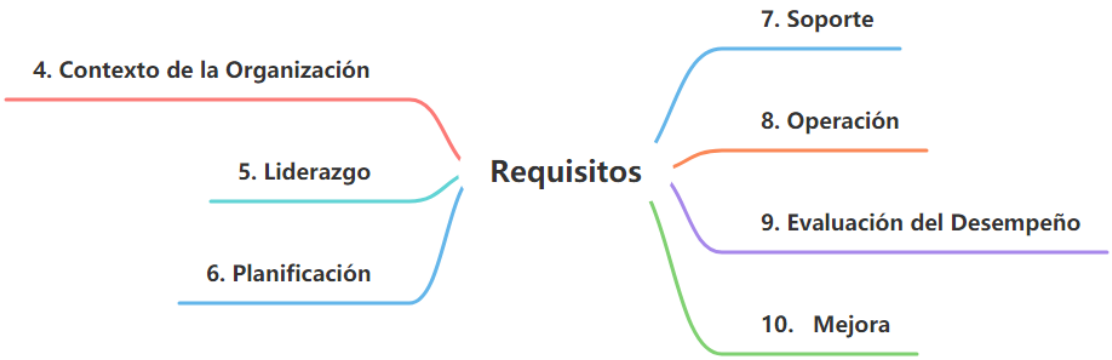


*Figura 6*. Requisitos de la norma ISO/IEC 27001:2013

### 3.2.2 ISO/IEC 27001:2013 Anexo A

El Anexo A de la ISO/IEC 27001:2013 existen 114 controles de seguridad, los cuales se encuentran divididos en 14 categorías, estos controles permiten conocer de manera adecuada como se encuentra una organización.

En la figura 3, se muestra las categorías del Anexo A, las cuales son las siguientes:


*Figura 7*. ISO/IEC 27001:2013 Anexo A

Una vez llevado a cabo la revisión de los controles, existen diferentes pautas que se deben tomar en cuenta y efectuarlas:

- ✓ Definir las responsabilidades para la administración y supervisión de los controles.

- ✓ Revisión de controles.
- ✓ Monitorear y medir la efectividad de los controles.
- ✓ Establecer e implementar acciones correctivas.
- ✓ Mejora continua.

### 3.2.3 Estado inicial del SGSI

Para la definición del estado inicial del sistema de seguridad de la información, se establece una tabla de valoración con su nivel de efectividad, valor, significado y descripción, como se muestra en la Tabla 1.

Esta tabla se adapta del Modelo de Madurez de Capacidades, la cual define niveles de madurez los cuales permiten evaluar los procesos actuales de la institución y conocer el contexto de la institución (ISO/IEC 21827:2008, 2021).

Tabla 1.

Modelo Madurez Capacidad.

| Efectividad | Valor | Significado | Descripción |
|---|---|---|---|
| 0% | L0 | Inexistente | Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver |
| 10% | L1 | Inicial | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo. |
| 50% | L2 | Reproducible pero intuitivo | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo, depende del grado de conocimiento de cada individuo. |
| 75% | L3 | Proceso definido | La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| 90% | L4 | Gestionable y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |
| 100% | L5 | Optimizado | Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las |

| | | | |
|---|---|---|---|
| | | | desviaciones más comunes y se optimizan los procesos. |

Adaptado de (ISO/IEC 21827:2008, 2021)

Una vez establecidos los niveles de madurez para la institución, se procede con la evaluación correspondiente de los controles de la norma.

Tabla 2.

Estado inicial y Proyección a futuro.

| Valor | Estado Inicial | Proyección a Futuro |
|---|---|---|
| L0 | 63% | 0% |
| L1 | 37% | 0% |
| L2 | 0% | 19% |
| L3 | 0% | 81% |
| L4 | 0% | 0% |
| L5 | 0% | 0% |

En la Tabla 2, se muestra el porcentaje del estado inicial, así como la proyección a futuro que la institución deberá tener una vez se desarrolle políticas y procedimientos de alto nivel.

Tabla 3.

Estado inicial y Proyección a futuro del SGSI

| SGSI | Estado Inicial | Proyección a Futuro |
|---|---|---|
| **4. Contexto de la Organización** | L0 | L3 |
| **5. Liderazgo** | L1 | L3 |
| **6. Planificación** | L0 | L3 |
| **7. Soporte** | L1 | L3 |
| **8. Operación** | L0 | L3 |
| **9. Evaluación del Desempeño** | L0 | L2 |
| **10. Mejora** | L0 | L2 |

Adaptado de (ISO/IEC 27001:2013, 2021).

En la Tabla 3, se observa el estado inicial y de proyección a futuro de cada punto de la norma ISO/IEC 27001:2013 de forma general, la cual se ha calificado de acuerdo con la tabla del modelo de madurez de capacidad mencionado en el punto 3.3.3.

Al no contar la institución con un sistema de gestión de seguridad de la organización, se espera que el cumplimiento de la norma se lleva a cabo a un porcentaje igual o mayor del 75%.

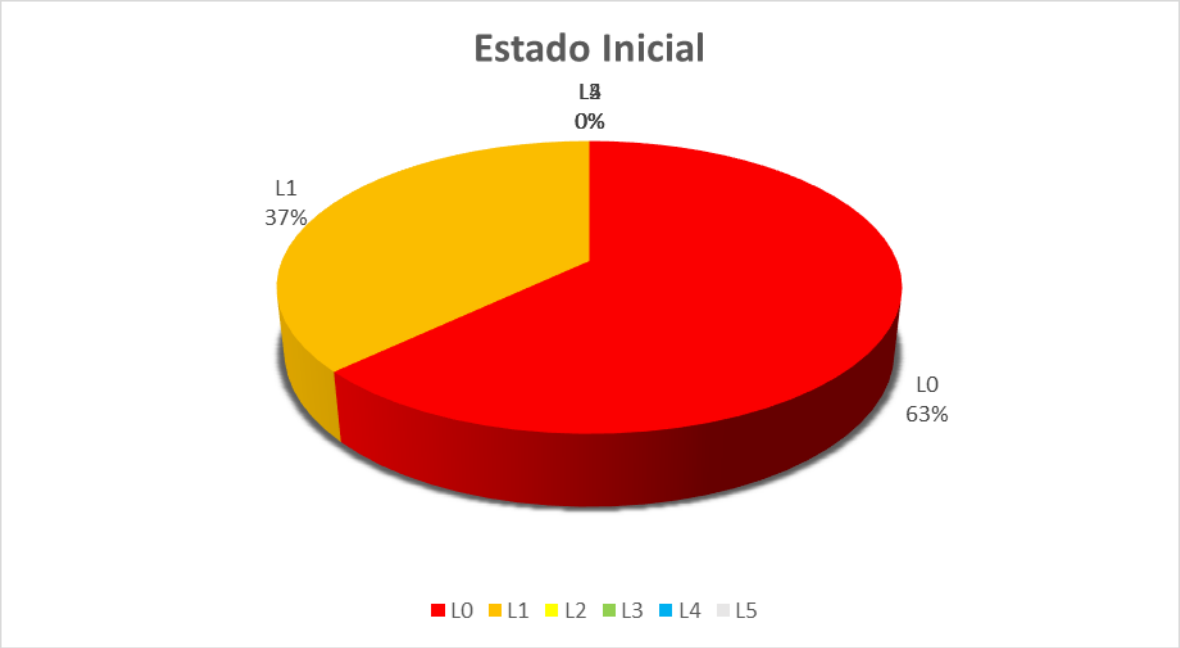


Figura 8. Estado Inicial del sistema de gestión de seguridad de la información

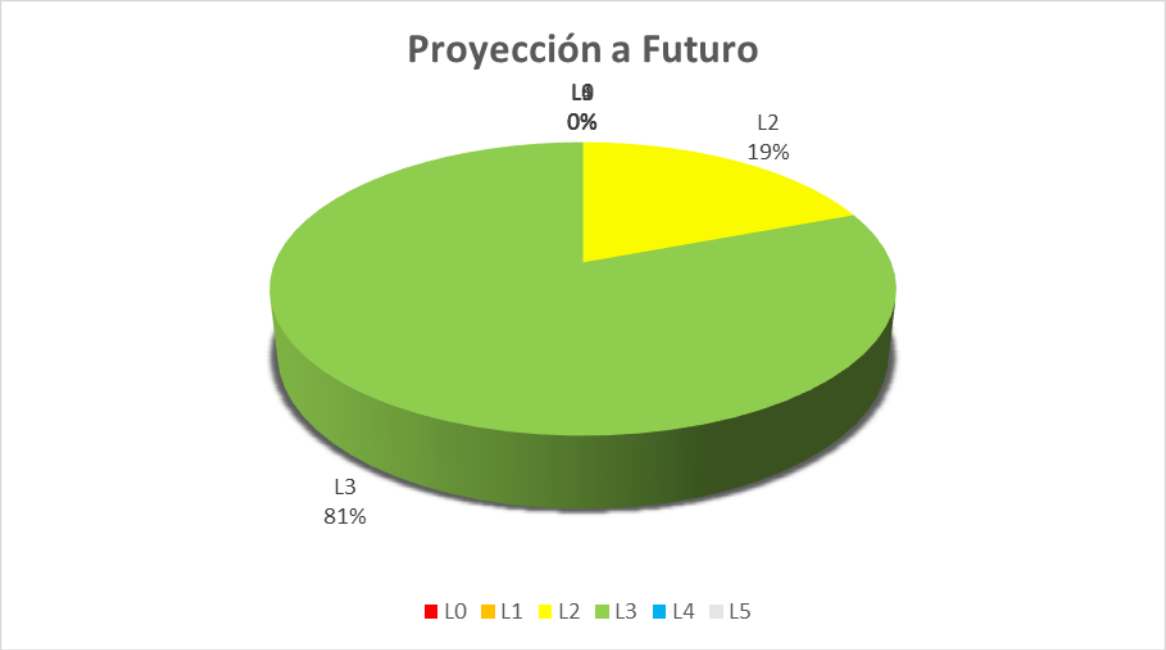

*Figura 9*. Proyección a futuro del sistema de gestión de seguridad de la información

### 3.2.4 Objetivos de control y controles de referencia

Los objetivos de control y controles de referencia (Anexo A) son evaluados de acuerdo con la situación actual de la institución. Los resultados de la evaluación mostrados en porcentajes se visualizan en la Tabla 3.

Tabla 4.

Objetivos de Control y Controles de Referencia

| Objetivos de Control y Controles de Referencia (Anexo A) | Actual |
|---|---|
| **A.5 Políticas de seguridad de la información** | 0,00% |
| **A.6 Organización de la seguridad de la información** | 14,29% |
| **A.7 Seguridad relativa a los recursos humanos** | 50,00% |
| **A.8 Gestión de activos** | 40,00% |
| **A.9 Control de acceso** | 35,71% |
| **A.10 Criptografía** | 0,00% |
| **A.11 Seguridad física y del entorno** | 80,00% |
| **A.12 Seguridad de las operaciones** | 57,14% |
| **A.13 Seguridad de las comunicaciones** | 85,71% |
| **A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información** | 61,54% |
| **A.15 Relación con proveedores** | 0,00% |
| **A.16 Gestión de incidentes de seguridad de la información** | 28,57% |
| **A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio** | 0,00% |
| **A.18 Cumplimiento** | 62,50% |

Adaptado de (ISO/IEC 27001:2013, 2021).

Como se visualiza en la Tabla 3, los puntos A.5, A.6, A.8, A.9, A.10, A.15, A.16, A.17 son los controles que obtienen porcentaje por debajo del 50%.

El punto “A.5 Políticas de seguridad de la información” posee dicho porcentaje, debido a que la institución no cuenta con políticas de seguridad de la información, las cuales puedan cumplir con una revisión y mejora correspondiente.

El punto “A.6 Organización de la seguridad de la información” posee dicho porcentaje debido a que la institución no cuenta con roles y responsabilidades en seguridad de la información.

El punto “A.8 Gestión de activos” posee dicho porcentaje debido a que la institución no posee políticas para la clasificación, etiquetado, manipulación de la información y gestión de soportes.

El punto “A.9 Control de acceso” posee dicho porcentaje debido a que la institución, no cuenta con políticas de gestión de acceso, gestión de privilegios, revisión y reasignación de derechos.

El punto “A.10 Criptografía posee dicho porcentaje debido a que la institución, no cuenta con políticas sobre el uso de los controles criptográficos para proteger la información.

El punto “A.15 Relación con proveedores” posee dicho porcentaje debido a que la institución, no cuenta con políticas y requisitos de seguridad de la información en las relaciones con los proveedores, controles, revisiones y auditoria de los servicios que ofrecen los proveedores.

El punto “A.16 Gestión de incidentes de seguridad de la información” posee dicho porcentaje debido a que la institución, no cuentan con procedimientos y responsabilidades para responder ante incidentes de seguridad, ni con la evaluación, decisión, aprendizaje y respuesta a incidentes de seguridad de la información.

El punto “A.17 Aspectos de seguridad de la información” para la gestión de la continuidad de negocio posee dicho porcentaje debido a que la institución, no cuenta con un plan de continuidad de la seguridad de la información.

Tabla 5.

Objetivos de Control y Controles de Referencia, Anexo A

| Objetivos de Control y Controles de Referencia (Anexo A) | Actual | Objetivo |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | 0,00% | L3 |
| **A.6 Organización de la seguridad de la información** | 14,29% | L3 |

| | | |
|---|---|---|
| **A.7 Seguridad relativa a los recursos humanos** | 50,00% | L3 |
| **A.8 Gestión de activos** | 40,00% | L3 |
| **A.9 Control de acceso** | 35,71% | L3 |
| **A.10 Criptografía** | 0,00% | L3 |
| **A.11 Seguridad física y del entorno** | 80,00% | L4 |
| **A.12 Seguridad de las operaciones** | 57,14% | L3 |
| **A.13 Seguridad de las comunicaciones** | 85,71% | L4 |
| **A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información** | 61,54% | L3 |
| **A.15 Relación con proveedores** | 0,00% | L3 |
| **A.16 Gestión de incidentes de seguridad de la información** | 28,57% | L3 |
| **A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio** | 0,00% | L3 |
| **A.18 Cumplimiento** | 62,50% | L3 |

Adaptado de (ISO/IEC 27001:2013, 2021).

Esta evaluación realizada, la cual visualiza en la Tabla 5, muestra una situación similar al punto 3.3.3 del documento. Esto se debe porque la institución pública no cuenta con un sistema de gestión de seguridad de la información.

Los puntos del Anexo A mencionados anteriormente hacen énfasis con la gestión de activos, control de accesos, gestión de incidentes, políticas y procesos de la seguridad de la información.

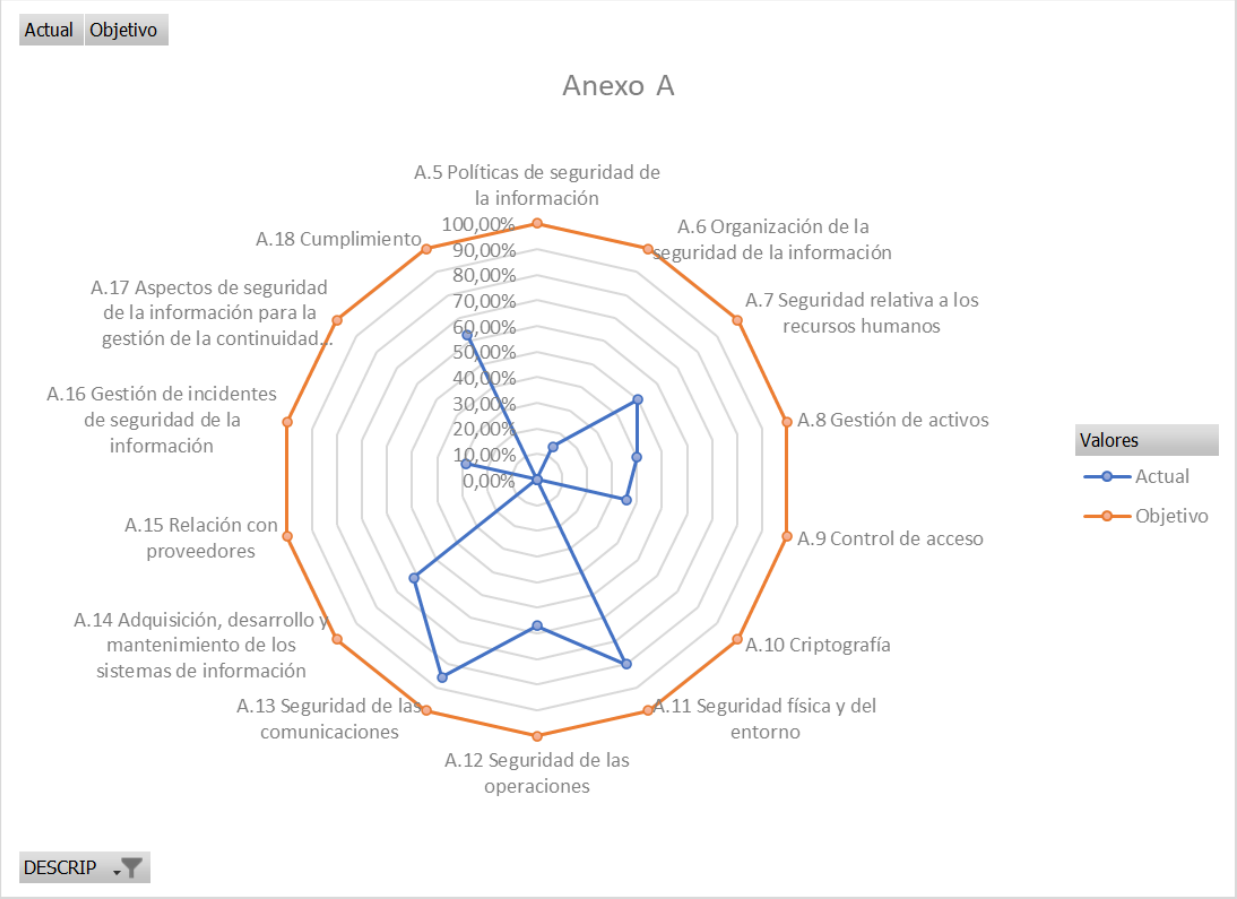


*Figura 10*. ISO/IEC 27001:2013 Anexo A

En la Figura 6, se observa el cumplimento los objetivos de control y controles de referencia de manera gráfica.

### 3.2.5 Planes de acción de mejora

Los planes de acción de mejora son aquellos que permiten a una organización o empresa alcanzar el cumplimiento del programa del sistema de gestión de seguridad de la información. En la Tabla 6, se muestra los planes de acción de mejora en base al análisis del cumplimiento del Anexo A.

Tabla 6.

Planes de acción de mejora

| **A.5 Políticas de seguridad de la información** |
|---|

| |
|---|
| **A.5.1 Directrices de gestión de la seguridad de la información** |
| **A.6 Organización de la seguridad de la información** |
| **A.6.1 Organización interna** |
| **A.6.2 Los dispositivos móviles y el teletrabajo** |
| **A.7 Seguridad relativa a los recursos humanos** |
| **A.7.2 Durante el empleo** |
| **A.8 Gestión de activos** |
| **A.8.2 Clasificación de la información** |
| **A.8.3 Manipulación de los soportes** |
| **A.9 Control de acceso** |
| **A.9.1 Requisitos de negocio para el control de acceso** |
| **A.9.2 Gestión de acceso de usuario** |
| **A.9.3 Responsabilidades del usuario** |
| **A.9.4 Control de acceso a sistemas y aplicaciones** |
| **A.10 Criptografía** |
| **A.10.1 Controles criptográficos** |
| **A.11 Seguridad física y del entorno** |
| **A.11.1 Áreas seguras** |
| **A.11.2 Seguridad de los equipos** |
| **A.12 Seguridad de las operaciones** |
| **A.12.1 Procedimientos y responsabilidades operacionales** |
| **A.12.4 Registros y supervisión** |
| **A.12.5 Control del software en explotación** |
| **A.12.6 Gestión de la vulnerabilidad técnica** |
| **A.13 Seguridad de las comunicaciones** |
| **A.13.2 Intercambio de información** |
| **A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información** |
| **A.14.1 Requisitos de seguridad en los sistemas de información** |
| **A.14.2 Seguridad en el desarrollo y en los procesos de soporte** |
| **A.15 Relación con proveedores** |
| **A.15.1 Seguridad en las relaciones con proveedores** |
| **A.15.2 Gestión de la provisión de servicios del proveedor** |
| **A.16 Gestión de incidentes de seguridad de la información** |
| **A.16.1 Gestión de incidentes de seguridad de la información y mejoras** |
| **A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio** |
| **A.17.1 Continuidad de la seguridad de la información** |
| **A.17.2 Redundancias** |
| **A.18 Cumplimiento** |
| **A.18.2 Revisiones de la seguridad de la información** |

Adaptado de (ISO/IEC 27001:2013, 2021).

## 3.3 Clasificación de la información

### 3.3.1 Tipología de impacto

La tipología de impacto es la cual define la cantidad de riesgo que la institución está dispuesta a aceptar en su búsqueda de valor, esto se realiza en base al apetito del riesgo. Este puede ser modificado en cuanto a los cambios que se presenten dentro de la institución. En la Tabla 7, se muestra la tipología de impacto definido para la institución. Adicionalmente, se define el modulador para la institución pública, el cual se muestra en la Tabla 8.

Tabla 7.

Tipología de impacto

| Tipología de impacto | Aversión | Neutral | Agresivo |
|---|---|---|---|
| **Pérdidas financieras** | | x | |
| **Interrupción de operaciones parciales y/o totales** | x | | |
| **Pérdida / Degradación de la Imagen institucional** | | x | x |
| **Demandas judiciales, afectación Legal** | x | x | |
| **Afectación al clima laboral** | | | x |

Tabla 8.

Modulador

| Tipología de Impacto | INSIGNIFICANTE | MENOR | MODERADO | MAYOR | CATASTRÓFICO |
|---|---|---|---|---|---|
| **Pérdidas financieras** | No pierde | No pierde | No pierde | Entre 10,000 a 50,000 | Más de 50.000 |
| **Interrupción de operaciones parciales y/o totales** | Entre 0 a 1 hora | Entre 1 a 2 horas | Entre 2 a 5 horas | Entre 5 a 12 horas | Más de 12 horas |
| **Pérdida / Degradación de la Imagen institucional** | N/A | N/A | Pérdida de confianza | Pérdida de confianza | Pérdida de confianza |

| | | | | | |
|---|---|---|---|---|---|
| **Demandas judiciales, Afectación legal** | N/A | N/A | Pueden existir reclamos por la no disponibilidad de los servicios. | Sanciones que generan conflictos legales por la no disponibilidad del servicio. | Sanciones que generan conflictos legales por la no disponibilidad del servicio. |
| **Afectación al clima laboral** | N/A | N/A | N/A | Poca evidencia de conflictos laborales que afectan a la organización. | Mediana evidencia de conflictos laborales que afectan a la organización. |

La institución pública no cobra a los GADs por el uso de sus servicios y/o sistemas. Adicionalmente, no pierde porque no lucra, además no recibe bonificación por parte del uso de sus sistemas.

### 3.3.2 Sujetos y Tipos de información

En la institución pública, se han identificado dos puntos importantes. Los sujetos y tipos de información correspondientes. Los sujetos de información se definen como aquellos sobre los cuales se produce la información. Y los tipos de información es donde se clasifica la información en base a los sujetos de la información.

Tabla 9.

Sujetos y Tipos de información

| Nombre de la Entidad | Nombre del Tipo de Información | Definición del Tipo de Información |
|---|---|---|
| Empleados | Info. del empleado | Información del empleado, numero telefónico, correo, contacto. |
| | Descripción laboral | Descripción del empleo que se ejerce el empleado, funciones. |
| | Seguro Social | Afiliación, servicios, tramites, certificados, beneficios (IEES). |
| | Salud | Estado de salud, exámenes, certificados, cobertura. |
| | Financiero | Información bancaria, certificados. |
| | Ingresos | Sueldos, beneficios, bonos, comisiones, horas extras. |
| | Normativa Legal | Contrato, código del trabajo, artículos, leyes nacionales. |
| | Formación (educación, experiencia) | Experiencia laboral, formación académica, pregrado, posgrados, certificados. |
| GADs (Clientes) | Info. del cliente | Información del cliente, numero telefónico, correo, razón social, ruc, contacto. |
| | Financiero | Información financiera del cliente, remuneración, banca, cuentas. |
| | Estrategia Comercial | Definición de nicho, beneficios, promoción, seguimiento. |
| | Servicios | Acceso a la información, automatización, mejora continua de procesos |
| | Normativa Legal | Contrato, clausulas, artículos, leyes nacionales. |
| Facturación Electrónica (Sistema para Autorización de Comprobantes Electrónicos) | Información del servicio | Información, descripción del servicio que ofrece la organización, carga, firma, archivos comprobantes electrónicos, gestión de las autorizaciones SRI, entrega de RIDE autorizado a los contribuyentes vía correo electrónico. |
| | Documentación del servicio | Documentación necesaria para utilizar el servicio (gestión municipal, información técnica, comprobantes electrónicos, instructivos de uso). |
| | Infraestructura tecnológica | Infraestructura tecnológica que se utiliza para dar el servicio y gestionar la información (BDD, sistemas de computo, componentes de hardware y software, sistemas de información del negocio, entre otros). |
| | Normativa Legal | Normativas, reglamentos, contrato, clausulas, artículos, leyes nacionales. |
| | Solicitud servicio | Documentación, formatos, información para el sistema, encuestas, espacio de trabajo, generación de convenios. |
| | Financiero | Información bancaria, certificados, contratos, clausulas, normas. (insumo SIGAME), notas de debito, crédito, retención, facturas. |
| Sistema Nacional de Información Municipal (SNIM) | Información del servicio | Información, descripción del servicio que ofrece la organización, creacion y levantamiento de fichas, analisis e integracion de informacion (GAD). |
| | Documentación del servicio | Documentación necesaria para utilizar el servicio, información técnica, reglamentos y normas de entes reguladores, fichas de levantamiento de informacion y malla de validacion, requerimientos. |
| | Infraestructura tecnológica | Infraestructura tecnológica que se utiliza para dar el servicio y gestionar la información (BDD, sistemas de computo, componentes de hardware y software, sistemas de información del negocio, entre otros). |
| | Ingreso de información | Comunicacion sobre la habilitacion del ingreso de informacion de AME hacia los diferentes GAD. |
| | Indicadores de información | Reportes del sistema SNIM de las diferentes competencias para la toma de decisiones. |
| | Normativa Legal | Contrato, clausulas, artículos, leyes nacionales. |

En la Tabla 9, se muestra los sujetos de información con sus respectivos tipos de información que han sido identificados, para cada tipo de la información, le acompaña su respectiva descripción.

Para un sistema de gestión de seguridad de la información, la confidencialidad la integridad y la disponibilidad representan los criterios de la seguridad de la información a ser evaluados, además, la privacidad también debe ser considerado para el sistema de gestión de seguridad de la información.

Los criterios de seguridad de la información son los siguientes:

- ✓ Confidencialidad: la información sea solo accesible a las personas autorizadas.
- ✓ Integridad: la información no deba ser alterada.
- ✓ Disponibilidad: la información esté disponible cuando sea necesario
- ✓ Privacidad: orientado a la información personal.

Las sujetos y tipos de información son evaluados con base en los criterios de seguridad de la información mencionado anteriormente.

La evaluación de la confidencialidad, integridad, disponibilidad y privacidad se lo realiza con base a los niveles de impacto. La evaluación de los criterios de la información se realiza mediante la siguiente tabla.

Tabla 10.

Niveles de impacto

| | |
|---|---|
| 1 | **INSIGNIFICANTE** |
| 2 | **MENOR** |
| 3 | **MODERADO** |
| 4 | **MAYOR** |
| 5 | **CATASTRÓFICO** |

En la Tabla 10, se muestra los niveles de impacto los cuales han sido definidos y utilizados en la evaluación de los sujetos y tipos de información.

Tabla 11.

Tipos de información

| Nombre de la Entidad | Nombre del Tipo de Información | Definición del Tipo de Información | Confidencialidad | Integridad | Disponibilidad | Privacidad |
|---|---|---|---|---|---|---|
| Empleados | Info. del empleado | Información del empleado, numero telefónico, correo, contacto. | MENOR | MENOR | MENOR | MENOR |
| | Descripción laboral | Descripción del empleo que se ejerce el empleado, funciones. | MENOR | MENOR | MENOR | MENOR |
| | Seguro Social | Afiliación, servicios, tramites, certificados, beneficios (IEES). | MAYOR | MAYOR | MAYOR | MODERADO |
| | Salud | Estado de salud, exámenes, certificados, cobertura. | MODERADO | MODERADO | MODERADO | MODERADO |
| | Financiero | Información bancaria, certificados. | MAYOR | MAYOR | MAYOR | MAYOR |
| | Ingresos | Sueldos, beneficios, bonos, comisiones, horas extras. | MODERADO | MODERADO | MODERADO | MODERADO |
| | Normativa Legal | Contrato, código del trabajo, artículos, leyes nacionales. | MAYOR | MAYOR | MAYOR | MAYOR |
| | Formación (educación, experiencia) | Experiencia laboral, formación académica, pregrado, posgrados, certificados. | MENOR | MENOR | MENOR | MENOR |
| GADs (Clientes) | Info. del cliente | Información del cliente, numero telefónico, correo, razón social, ruc, contacto. | MENOR | MENOR | MENOR | MENOR |
| | Financiero | Información financiera del cliente, remuneración, banca, cuentas. | MAYOR | MAYOR | MAYOR | MAYOR |
| | Estrategia Comercial | Definición de nicho, beneficios, promoción, seguimiento. | MODERADO | MODERADO | MODERADO | MODERADO |
| | Servicios | Acceso a la información, automatización, mejora continua de procesos | MODERADO | MODERADO | MODERADO | MODERADO |
| | Normativa Legal | Contrato, clausulas, artículos, leyes nacionales. | MAYOR | MAYOR | MAYOR | MAYOR |
| Facturación Electrónica (Sistema para Autorización de Comprobantes Electrónicos) | Información del servicio | Información, descripción del servicio que ofrece la organización, carga, firma, archivos comprobantes electrónicos, gestión de las autorizaciones SRI, entrega de RIDE autorizado a los contribuyentes via correo electrónico. | MODERADO | MODERADO | MODERADO | MODERADO |
| | Documentación del servicio | Documentación necesaria para utilizar el servicio (gestión municipal, información técnica, comprobantes electrónicos, instructivos de uso). | CATASTRÓFICO | CATASTRÓFICO | CATASTRÓFICO | MAYOR |
| | Infraestructura tecnológica | Infraestructura tecnológica que se utiliza para dar el servicio y gestionar la información (BDD, sistemas de computo, componentes de hardware y software, sistemas de información del negocio, entre otros). | MAYOR | MAYOR | MAYOR | MAYOR |
| | Normativa Legal | Normativas, reglamentos, contrato, clausulas, artículos, leyes nacionales. | MAYOR | MAYOR | MAYOR | MAYOR |
| | Solicitud servicio | Documentación, formatos, información para el sistema, encuestas, espacio de trabajo, generación de convenios. | CATASTRÓFICO | CATASTRÓFICO | CATASTRÓFICO | MAYOR |
| | Financiero | Información bancaria, certificados, contratos, clausulas, normas. (insumo SIGAME), notas de debito, crédito, retención, facturas. | MAYOR | MAYOR | MAYOR | MAYOR |
| Sistema Nacional de Información Municipal (SNIM) | Información del servicio | Información, descripción del servicio que ofrece la organización, creacion y levantamiento de fichas, analisis e integracion de informacion (GAD). | MENOR | MENOR | MENOR | MENOR |
| | Documentación del servicio | Documentación necesaria para utilizar el servicio, información técnica, reglamentos y normas de entes reguladores, fichas de levantamiento de informacion y malla de validacion, requerimientos. | CATASTRÓFICO | CATASTRÓFICO | CATASTRÓFICO | MAYOR |
| | Infraestructura tecnológica | Infraestructura tecnológica que se utiliza para dar el servicio y gestionar la información (BDD, sistemas de computo, componentes de hardware y software, sistemas de información del negocio, entre otros). | MAYOR | MAYOR | MAYOR | MAYOR |
| | Ingreso de información | Comunicacion sobre la habilitacion del ingreso de informacion de AME hacia los diferentes GAD. | CATASTRÓFICO | CATASTRÓFICO | CATASTRÓFICO | MAYOR |
| | Indicadores de información | Reportes del sistema SNIM de las diferentes competencias para la toma de decisiones. | MODERADO | MODERADO | MODERADO | MODERADO |
| | Normativa Legal | Contrato, clausulas, artículos, leyes nacionales. | MAYOR | MAYOR | MAYOR | MAYOR |

En la Tabla 11, se muestra la evaluación de las sujetos y tipos de la información referente a la confidencialidad, integridad, disponibilidad y privacidad con base a los niveles de impacto.

En base al análisis realizado, la entidad de “facturación electrónica” con los tipos de información “documentación del servicio” y “solicitud del servicio” obtienen un nivel de impacto de catastrófico. De la misma manera, la entidad de “sistema nacional de información municipal” con los tipos de información “documentación

del servicio” e “ingreso de información” obtienen un nivel de impacto de catastrófico.

## 3.4 Inventario de activos de la información

El inventario de los activos de la información se define con base a los sujetos y tipos de información los cuales han sido definidos en el punto 3.3.2.

La categorización de estos activos se lo realiza por su nombre, formato, tipo de activo, propietario y clasificación.

En la Tabla 12, se muestra los activos de información, los cuales han sido definidos en conjunto con la institución, los activos mencionados se relacionan con las sujetos y tipos de información, donde la clasificación se obtiene con la valoración de la Tabla 10.

Tabla 12.

Activos de información

| Entidad | Tipo de Información | Nombre del Activo | Formato | Tipo de Activo | Propietario | Clasificación del Activo |
|---|---|---|---|---|---|---|
| Facturación Electrónica (Sistema para Autorización de Comprobantes Electrónicos) | Documentacion del servicio/Solicitud servicio | Portal Web | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Sistema perfil usuarios institucionales | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Administración de virtualización | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Servidor BDD | Digital | Software | Analista Desarrollo/Admin. Sistema | CATASTRÓFICO |
| | | Servidor aplicativos | Digital | Software | Analista Desarrollo/Admin. Sistema | CATASTRÓFICO |
| | | Servidor archivos | Digital | Software | Analista Desarrollo/Admin. Sistema | CATASTRÓFICO |
| | | Servidores | Físico | Hardware | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Servidor Web APP Apache 2.4.6 | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Servidor Aplicaciones WiFLy 8.2 | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Servidor Postgres 9.3 | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Proxmox Virtualizador | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Administrador del sistema | Físico | Personas | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Desarrollador del sistema | Físico | Personas | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Equipos de computo (administración y desarrollo) | Físico | Hardware | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Documentación técnica control de cambios | Digital | Información | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Documentos habilitantes | Digital | Información | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Registro de entidades registradas | Digital | Información | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Registro de usuarios institucionales registrados | Digital | Información | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Servidor de desarrollo | Digital | Software | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Resolución SRI | Digital | Información | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Sistema mesa de ayuda AME | Digital | Software | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Sistema de correo electrónico (buzón) | Digital | Software | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Sistema salida comprobantes (correo electronico) | Digital | Software | Analista Desarrollo/Admin. Sistema | MAYOR |
| | | Documentación reportes institucional | Digital | Información | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Documentación reportes ejecutivos | Digital | Información | Analista Desarrollo/Admin. Sistema | MODERADO |
| | | Documentación reportes carga de archivos | Digital | Información | Analista Desarrollo/Admin. Sistema | MODERADO |
| Sistema Nacional de Información Municipal (SNIM) | Documentacion del servicio/Ingreso de informacion | Portal Web | Digital | Software | Analista Desarrollo | MENOR |
| | | Sistema perfil usuarios institucionales | Físico | Personas | Analista Desarrollo | MENOR |
| | | Administración de virtualización | Digital | Software | Analista Desarrollo | MAYOR |
| | | Servidor BDD | Digital | Software | Analista Desarrollo | CATASTRÓFICO |
| | | Servidor Web APP Apache | Digital | Software | Analista Desarrollo | CATASTRÓFICO |
| | | Proxmox Virtualizador | Digital | Software | Analista Desarrollo | MAYOR |
| | | Equipos de computo (administración y desarrollo) | Digital | Hardware | Analista Desarrollo | MENOR |
| | | Administrador del sistema | Físico | Personas | Analista Desarrollo | MAYOR |
| | | Desarrollador del sistema | Físico | Personas | Analista Desarrollo | MAYOR |
| | | Ficha competencia anual | Digital | Información | Analista Desarrollo | MAYOR |
| | | Malla validación | Digital | Información | Analista Desarrollo | MAYOR |
| | | Servidor de desarrollo | Físico | Hardware | Analista Desarrollo | MAYOR |
| | | Backup | Digital | Información | Analista Desarrollo | MENOR |
| | | Documentación información respaldo ficha por competencia | Digital | Información | Analista Desarrollo | MENOR |
| | | Documentación reporte anual | Digital | Información | Analista Desarrollo | MENOR |
| | | Documentación reportes institucional | Digital | Información | Analista Desarrollo | MENOR |
| Datacenter | | IBM Servidor Xseries 336 [2] | Físico | Hardware | Coordinador TI | CATASTRÓFICO |
| | | IBM Servidor Xseries 346 | Físico | Hardware | Coordinador TI | CATASTRÓFICO |
| | | IBM Servidor Xseries 3650 [3] | Físico | Hardware | Coordinador TI | CATASTRÓFICO |
| | | SAN IBM DS3512 | Físico | Hardware | Coordinador TI | MAYOR |
| | | Switch Core Cisco 4507R+E | Físico | Hardware | Coordinador TI | CATASTRÓFICO |
| | | Switch Acceso Cisco Catalyst 2960 | Físico | Hardware | Coordinador TI | MAYOR |
| | | Access Points Unifi AP-Pro [15] | Físico | Hardware | Coordinador TI | MAYOR |
| | | Huawei Servidor CH121 V3 | Físico | Hardware | Coordinador TI | CATASTRÓFICO |
| | | Firewall Mikrotik RouterOS | Físico | Hardware | Coordinador TI | CATASTRÓFICO |

En base al análisis realizado, los activos de información críticos son los servidores, el switch core y el firewall. De estos activos, el análisis de amenazas y vulnerabilidades se lo realiza al activo de información de “Huawei Servidor CH121 V3”, debido que este activo contiene la información crítica de los tipos de información mencionados en el punto 3.3.2.

## 3.5 Análisis de amenazas y vulnerabilidades

### 3.5.1 Amenazas

Una amenaza se define como una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

De origen natural. - Hay accidentes naturales (terremotos, inundaciones, ...) ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial). - Hay desastres industriales (contaminación, fallos eléctricos, etc) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones. - Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o simplemente vulnerabilidades.

Causadas por las personas de forma accidental. - Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada. - Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios (MAGERIT – versión 3.0. Libro I, 2021).

### 3.5.2 Vulnerabilidades

Una vulnerabilidad se denomina a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Las vulnerabilidades son todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza (MAGERIT – versión 3.0. Libro I, 2021).

### 3.5.3 Análisis del Riesgo

La seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que compro metan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles (MAGERIT – versión 3.0. Libro I, 2021).

Hay que tener en cuenta las siguientes dimensiones de seguridad:

Confidencialidad. - la información solo debe llegar y ser accesible a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos (MAGERIT – versión 3.0. Libro I, 2021).

Integridad. - también conocido como el mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede

aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización (MAGERIT – versión 3.0. Libro I, 2021).

Disponibilidad. – también conocido como la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones (MAGERIT – versión 3.0. Libro I, 2021).

Para el análisis de amenazas y vulnerabilidades del activo de información referente al punto 3.4, se utiliza métodos de análisis llevado a cabo mediante tablas donde se muestra la importancia relativa para la calificación del valor de activo, la magnitud del impacto y la magnitud del riesgo (MAGERIT – versión 3.0. Libro III, 2021). En la Tabla 13, se muestra la escala de calificación.

Tabla 13.

Escala de calificación

| **Escalas** | |
|---|---|
| **MB** | muy bajo |
| **B** | bajo |
| **M** | medio |
| **A** | alto |
| **MA** | muy alto |

Adaptado de (MAGERIT – versión 3.0. Libro III, 2021).

En la Tabla 14, se muestra la estimación de riesgos.

Tabla 14.

Estimación de riesgos

| **Escalas** | | |
|---|---|---|
| **Impacto** | **Probabilidad** | **Riesgo** |
| **MA:** muy alto | **MA:** prácticamente seguro | **MA:** crítico |
| **A:** alto | **A:** probable | **A:** importante |
| **M:** medio | **M:** posible | **M:** apreciable |

| | | |
|---|---|---|
| **B:** bajo | **B:** poco probable | **B:** bajo |
| **MB:** muy bajo | **MB:** muy raro | **MB:** despreciable |

Adaptado de (MAGERIT – versión 3.0. Libro III - Guía de Técnicas, p.7).

En la Tabla 15, se muestra la tabla de la relación entre el riesgo, impacto y probabilidad.

Tabla 15.

Riesgo, impacto y probabilidad

| ***Riesgo*** | | ***Probabilidad*** | | | | |
|---|---|---|---|---|---|---|
| | | MB | B | M | A | MA |
| ***Impacto*** | MA | A | MA | MA | MA | MA |
| | A | M | A | A | MA | MA |
| | M | B | M | M | A | A |
| | B | MB | B | B | M | M |
| | MB | MB | MB | MB | B | B |

Adaptado de (MAGERIT – versión 3.0. Libro III - Guía de Técnicas, p.7).

En el análisis de riesgos, las amenazas se pueden obtener del marco de referencia de MAGERIT e ISO/IEC 27005:2009, así como las vulnerabilidades se pueden obtener del marco de referencia mencionado anteriormente.

En la Tabla 16, se muestra el análisis de riesgos realizado al activo de información. La calificación del impacto y la probabilidad se lo ha realizado en conjunto con la institución.

Tabla 16.

Análisis del riesgo

| Activo | Componentes | Amenazas | Vulnerabilidades | Impacto | Probabilidad | Riesgo | Controles | Controles a implementar | Dimensiones | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Confidencialidad | Integridad | Disponibilidad |
| Huawei Servidor CH121 V3 | [N] Desastres naturales | [N.3] Desastres naturales: Fenómeno climático | Red energética inestable | M | M | M | Fuente de alimentación de energía alterna especidad operativa autónoma | Implementar un plan de contingencia para una fuente de alimentación de energía alterna autónoma | | | D |
| | | [N.4] Desastres naturales: Fenómeno sísmico | Ubicación en un área susceptible de eventos sísmicos | A | M | A | Monitorización con alarmas y notificaciones sobre eventos sísmicos | Implementar un plan de contingencia ante eventos sísmicos | | | D |
| | [I] De origen industrial | [I.3] Contaminación mecánica: vibraciones, polvo, suciedad | Susceptibilidad a la humedad, el polvo y la suciedad | MB | MB | MB | Desinfección y limpieza de los equipos | Definir procedimientos de desinfección y limpieza de los equipos | | | D |
| | | [I.5] Avería de origen físico o lógico: Falla de funcionamiento del hardware | Configuración incorrecta de parámetros | B | M | B | Mantenimiento y actualización de los equipos | Definir procedimientos de mantenimiento y actualización de los equipos | | | D |
| | | [I.6] Corte del suministro eléctrico: Pérdida de suministro de energía | Susceptibilidad a las variaciones de voltaje | B | B | B | Fuente de alimentación de energía de emergencia | Implementar un plan de contingencia para una fuente de alimentación de energía de emergencia | | | D |
| | | [I.8] Fallo de servicios de comunicaciones: Pérdida de los medios de telecomunicación | Gestión inadecuada de la red | B | MB | MB | Protección de la integridad del intercambio de la información | Establecer un plan de gestión y monitoreo de la red y recursos | | | D |
| | | [I.10] Degradación de los soportes de almacenamiento de la información: Avería del hardware | Mantenimiento insuficiente/instalación fallida de los soportes de almacenamiento. | M | B | M | Protección y mantenimiento de los soportes de información | Establecer un plan de mantenimiento y protección de hardware | | | D |
| | [E] Errores y fallos no intencionados | [E.1] Errores de los usuarios: Error de uso | Uso incorrecto de software y hardware | B | B | B | Gestión de cuentas de usuarios sin privilegios | Implementar una gestión de cuentas de usuarios con privilegios y sin privilegios | C | I | D |
| | | [E.2] Errores del administrador: Error de uso | Uso incorrecto de software y hardware | M | B | M | Gestión de cuentas de usuarios con privilegios | Implementar una gestión de cuentas de usuarios con privilegios y sin privilegios | C | I | D |
| | | [E.4] Errores de configuración: Introducción de datos de configuración erróneos | Ausencia de un eficiente control de cambios en la configuración | M | B | M | Monitoreo y control de cambios de configuraciones | Establecer una gestión de configuración y control de cambios del software | | I | |
| | | [E.8] Difusión de software dañino: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Ausencia de mecanismos de monitoreo establecidos para las brechas de la seguridad | A | A | MA | Controles y herramientas de ciberseguridad | Elaborar e implementar políticas y controles de seguridad de la información (analisis y vulnerabilidades del hardware critico) | C | I | D |
| | | [E.9] Errores de re-encaminamiento: Envío de información de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleva la información a donde o por donde no es debido | Errores en la configuración de encaminamiento (información) | B | B | B | Segregación de las redes en diferentes dominios. | Verificar los procesos de encaminamiento de la información dentro de la organización | C | | |
| | | [E.15] Alteración accidental de la información | Ausencia de controles de procesos de modificación de la información | M | B | M | Protección contra modificaciones de información no autorizadas y copia de seguridad | Establecer controles para la modificación adecuada de la información | | I | |
| | | [E.19] Fugas de información: Robo o revelación de información | Ausencia de controles para evitar la fuga de información | A | M | A | Políticas y procedimientos para brechas de la seguridad de la información | Elaborar e implementar políticas y controles de seguridad de la información | C | | |
| | | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | Ausencia en los procedimientos o controles de actualización de los equipos | M | M | M | Mantenimiento, controles y actualización de los equipos | Establecer procedimientos para el mantenimiento, controles y actualización de equipos | | | D |
| | [A] Ataques intencionados | [A.3] Manipulación de los registros de actividad (log) | Ausencia de registros en las bitácoras (logs) de administrador y usuarios | M | B | M | Revisión, análisis e informes de registros de logs | Establecer la revisión correspondiente registros de logs de usuarios y administradores y de informes | | I | |
| | | [A.4] Manipulación de la configuración: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. | Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso | M | B | M | Gestión dinámica y revisión de los privilegios de los usuarios | Establecer proceso para la revisión y supervisión de los derechos de acceso | C | I | D |
| | | [A.5] Suplantación de la identidad del usuario: Usurpación de derecho | Inadecuada gestión y protección de contraseñas | A | B | A | Gestión y protección de contraseñas y credenciales | Definir una gestión y protección de contraseñas y credenciales | C | I | D |
| | | [A.6] Abuso de privilegios de acceso: Abuso de derecho | Asignación errada de los derechos de acceso | A | B | A | Supervisión, control y revisión de accesos | Supervisar la asignación de derechos de acceso así como la revisión de estos | C | I | D |
| | | [A.7] Uso no previsto: utilización de los recursos del sistema para fines no previstos | Ausencia de procedimiento de monitoreo de la utilización de recursos | A | M | A | Gestión de cuentas, monitoreo de cuentas para uso adecuado | Establecer controles para el uso adecuado de los recursos de los sistemas | C | I | D |
| | | [A.8] Difusión de software dañino: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad | A | M | A | Políticas y procedimientos para brechas de la seguridad de la información | Elaborar e implementar controles para la ciberdefensa | C | I | D |
| | | [A.10] Alteración de secuencia: Alteración del orden de los mensajes transmitidos) | Ausencia de sincronización de la información | A | B | A | Protección de las Comunicaciones | Verificar si existe la protección adecuada para las comunicaciones en la organización | | I | |
| | | [A.11] Acceso no autorizado: Uso ilícito del hardware | Asignación errada de los derechos de acceso a los equipos | M | B | M | Control y prohibición del uso de hardware al personal no autorizado | Establecer y verificar de forma periódica los derechos de acceso para el uso de los equipos | C | I | |
| | | [A.14] Interceptación de información (escucha): Escucha pasiva | Tráfico sensible de la información sin protección | A | B | A | Protección de la información de mediante cifrado | Elaborar e implementar políticas y controles de seguridad de la información | C | | |
| | | [A.15] Modificación deliberada de la información: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. | Ausencia de controles en la desvinculación del personal | A | B | A | Gestión, eliminación y retención de información de accesos y privilegios | Verificar, reasignar o eliminar los accesos y privilegios de personal desvinculado | | I | |
| | | [A.18] Destrucción de información: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. | Ausencia de controles de los procesos de eliminación de información | A | B | A | Autorización para la modificación o eliminación de la información | Definir procesos autorizados para la modificación o eliminación de información | | | D |
| | | [A.19] Divulgación de información: revelación de información | Ausencia de controles para la no revelación de la información | A | M | A | Controles de cifrado y de protección para la información | Establecer controles de cifrado para la protección de la información | C | | |
| | | [A.23] Manipulación de los equipos: Sabotaje del hardware | Ausencia de seguimiento y revisión técnica de los programas y aplicaciones | A | B | A | Protección de los equipos informáticos | Definir revisiones técnicas de forma periódica para garantizar la integridad de programas y aplicaciones | C | | D |
| | | [A.24] Denegación de servicio: Saturación del sistema informático | Saturación de los recursos tecnológicos | A | M | A | Plan de contingencia y recuperación | Elaborar e implementar controles para la ciberdefensa | | | D |
| | | [A.26] Ataque destructivo: Destrucción de hardware o de soportes | Ausencia de esquemas de reemplazo periódico | MA | M | MA | Aseguramiento de disponibilidad y protección del hardware | Definir esquemas de reemplazo periódico y mantenimiento para hardware | | | D |
| | | [A.30] Ingeniería social: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. | Ausencia de políticas de seguridad de la información | A | A | MA | Políticas de seguridad de la información y programa de concienciación sobre amenazas | Elaborar e implementar políticas y controles de seguridad de la información | C | I | D |

Adaptado de (MAGERIT – versión 3.0. Libro II & III, 2021).

La calificación del riesgo, es decir el resultado entre el impacto y la probabilidad, se obtiene mediante el cálculo que brinda Tabla 15. Con la calificación del riesgo, se procede a definir controles a implementar los cuales permiten mitigar el riesgo.

## 3.7 Programa del sistema de gestión de seguridad de la información

Los planes de acción de mejora son un mecanismo que permite llevar una mejora continua, los planes se basan en la documentación que posee el objetivo de recopilar la totalidad de las acciones implicadas para la mejora continua del sistema de gestión de seguridad de la información y sus respectivos procesos.

Para cada plan de acción, se establece el análisis de estos y el seguimiento de sus procesos mediante un periodo de tiempo predefinido. Los planes de acción de mejora se encuentran constituidas de la siguiente manera: código, fuente, descripción, costo, responsable, métricas, tiempo y estado.

En la Tabla 17, se muestra los planes de acción de mejora.

Tabla 17.

Programa del SGSI

| Código | Fuente | Planes de acción de mejora | Priorización | Costo | Responsable | Métricas | 2022 | | | | Estado |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | 1er Tri. | 2do Tri. | 3er Tri. | 4to Tri. | |
| PAM.1 | ISO/IEC 27001:2013 Anexo A | Elaborar, implementar y comunicar las políticas de seguridad de la información, realizada para la organización, la cual debe ser aprobada por la alta dirección. [A.5] | MA | Tiempo/jornada laboral | Coordinador de TI | Porcentaje de cobertura de las políticas, grado de despliegue y adopción de las políticas en la organización | | | | | TBD |
| PAM.2 | ISO/IEC 27001:2013 Anexo A | Garantizar la vigencia de las políticas de seguridad de la información a través de la revisión anual o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros. Con la respectiva revisión y documentación pertinente. [A.5.1] | MA | Tiempo/jornada laboral | Coordinador de TI | Frecuencia de actualizaciones de las políticas de seguridad de la información | | | | | TBD |
| PAM.9 | ISO/IEC 27001:2013 Anexo A | La clasificación de la información se debe realizar en relación de su valor, normativa legal vigente, sensibilidad y criticidad para la institución y el estado ante la revelación o modificación no autorizada. [A.8.2] | MA | Tiempo/jornada laboral | Coordinador de TI | Porcentaje de activos de información en cada fase del proceso de clasificación | | | | | TBD |
| PAM.11 | ISO/IEC 27001:2013 Anexo A | Elaborar, implementar y comunicar las políticas de control de acceso a los sistemas de información, de acuerdo con la necesidad institucional y considerando la seguridad de la información. [A.9] | MA | Tiempo/jornada laboral | Coordinador de TI | Porcentaje de cobertura de las políticas de control de acceso, grado de despliegue y adopción de las políticas en la organización | | | | | TBD |
| PAM.15 | ISO/IEC 27001:2013 Anexo A | Restringir el acceso de los usuarios a la información y funciones de los sistemas y aplicaciones, con relación a la política de control de accesos. [A.9.4] | MA | Tiempo/jornada laboral | Coordinador de TI | Porcentaje de revisiones de identidades y accesos | | | | | TBD |
| PAM.34 | ISO/IEC 27001:2013 Anexo A | Establecer los procedimientos y responsabilidades para asegurar una respuesta rápida, efectiva y acorde a los incidentes de seguridad de la información que pueden ocurrir en la organización. [A.16] | MA | Tiempo/jornada laboral | Coordinador de TI | Porcentaje de incidentes que requieren cambios de configuración o procedimientos para su recuperación | | | | | TBD |
| PAM.70 | Análisis de Riesgos | Definir esquemas de reemplazo periódico y mantenimiento para hardware | MA | Tiempo/jornada laboral | Técnico de Infraestructura Tecnológica | Frecuencia de reemplazo y mantenimiento del hardware | | | | | TBD |

Adaptado de (ISO/IEC 27001:2013, 2021).

La alta dirección de la institución es el encargado de aprobar los planes de acción de mejora. Estos planes se deben ir completando a medida que vaya apareciendo nuevas necesidades o sea necesario realizar una mejora dentro de dichos planos (ISOTools, 2021).

## 3.8 Modelo Operacional

El desarrollo de un modelo operacional permite medir y supervisar el desempeño del sistema, alinear los objetivos de la institución con el sistema, el enfoque, el estado inicial, la evaluación de riesgos y los planes de acción para implementar mejores prácticas de gestión.

El marco de referencia utilizado para el modelo operacional es el NIST, el cual es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la información (TI), sistemas de control industrial (ICS), sistemas ciber físicos (CPS) o dispositivos conectados en general, incluido el Internet de las Cosas (IoT).

La aplicabilidad del marco está orientada a organizaciones que dependen de la tecnología, no importa si su enfoque está centrado en las tecnologías de la información, cuenta con sistemas de control industrial, sistemas, ciber físicos o conexiones de varios dispositivos de forma general, incluyendo al internet de las cosas.

El marco cuenta con un conjunto de funciones y actividades de seguridad cibernética, resultados esperados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica (Soluciones GlobalSUITE, 2021).

En la Tabla 18, se muestra el modelo operacional basado en el marco de referencia NIST.

Tabla 18.

Modelo Operacional

| Identificador único de función | Función | Categoría | Métricas |
|---|---|---|---|
| ID | Identificar | Gestión de activos | Porcentaje de activos de información en cada fase del proceso de clasificación<br>Número de activos no autorizados identificados, de activos no documentados descubiertos a través de escaneos de seguridad rutinarios<br>Frecuencia de las revisiones de los requisitos de seguridad de la información |
| | | Gobernanza | Porcentaje de cobertura de las políticas, de grado de despliegue, de adopción de las políticas en la organización<br>Frecuencia de actualizaciones de las políticas de seguridad de la información |
| | | Evaluación de riesgos | Porcentaje de incidentes de seguridad que han pasado los umbrales definidos |
| PR | Proteger | Gestión de identidad y control de acceso | Porcentaje de cobertura de las políticas de control de acceso, grado de despliegue y adopción de las políticas en la organización<br>Porcentaje de titulares de acceso con privilegios a los sistemas<br>Porcentaje de revisiones de identidades y accesos |
| | | Conciencia y capacitación | Evaluaciones de aprendizaje y mejora de procesos |
| | | Procesos y procedimientos de protección de la información | Porcentaje de sistemas y aplicaciones que contienen información sensible |
| DE | Detectar | Anomalías y eventos | Porcentaje de incidentes de seguridad de la información |
| | | Vigilancia continua de seguridad | Porcentaje de eventos descubiertos durante la supervisión y monitoreo de la seguridad de la información |
| | | Procesos de detección | Porcentaje de prácticas correctivas o de seguridad de la información para la detección de eventos anómalos |
| RS | Responder | Planificación de respuesta | Porcentaje de eventos descubiertos durante monitoreos de la seguridad de la información y relacionados con el incumplimiento de terceros con políticas, estándares y requisitos de seguridad |
| | | Mitigación | Porcentaje de problemas críticos relacionados con la seguridad de la información resueltos |
| | | Mejoras | Porcentaje de riesgo de I&T mitigado |
| RC | Recuperar | Planificación de recuperación | Porcentaje de incidentes que requieren cambios de configuración o procedimientos para su recuperación |
| | | Mejoras | Número de problemas críticos relacionados con la seguridad de la información resueltos o por resolver |
| | | Comunicaciones | Número de actividades de recuperación comunicadas dentro a las partes interesadas internas (organización) |

Adaptado de (Framework for Improving. Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology, 2018)

Este marco cuenta con cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Cuando se consideran juntas, estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la seguridad de la información (Soluciones GlobalSUITE, 2021).

En conjunto con el NIST, se define las métricas basadas en COBIT para las cinco funciones que se mencionan anteriormente, las cuales permiten establecer que

el sistema de gestión de seguridad de la información se ejecute de manera eficiente.

## 3.9 Políticas de Alto Nivel

Las políticas de alto nivel permiten a la institución pública realizar la ejecución correcta del sistema de gestión de seguridad de información, los cuales han sido planteado en el documento.

Estas políticas, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

En la Tabla 19, se muestra las políticas de alto nivel.

Tabla 19.

Políticas de Alto Nivel

| Código | Políticas de Alto Nivel | Descripción | Responsable | Alcance |
|---|---|---|---|---|
| POL.01 | Desarrollar e implementar políticas de seguridad de la información | Desarrollar e implementar políticas de seguridad de la información que al menos contengan los siguientes aspectos: compromiso de la alta dirección, utilización adecuada de los servicios, utilización de dispositivos móviles, aspectos de protección de datos, dimensiones de seguridad, entre otros | Coordinador de TI | AME |
| POL.02 | Efectuar un plan de concienciación referente a la seguridad de la información | Llevar a cabo sesiones de formación y concienciación que cubran al personal como a la alta dirección. | Coordinador de TI | AME |
| POL.03 | Desarrollar un plan de continuidad de TI | Llevar a cabo sesiones técnicas para la segmentación de la red institucional y posteriormente implantar sistemas de detección de intrusos. | Coordinador de TI | AME |
| POL.04 | Mejora en la gestion de incidentes | Desarrollar, documentar e implementar procesos para la gestion de los incidentes de seguridad de la informacion | Coordinador de TI | AME |
| POL.05 | Mejoras en la seguridad de la red coporativa | Mejorar la capacidad de respuesta de la organizacion para hacer frente a incidentes y/o contingecias de TI. | Coordinador de TI | AME |
| POL.06 | Clasificacion de la informacion | Definir un sistema de clasificacion de la informacion que contemple al menos tres niveles, publico, privado y confidencial. Ademas, contemplar aspectos de cifrado, destruccion, etiquetado, entre otros. | Coordinador de TI | AME |
| POL.07 | Regulacion de los servicios de TI prestado por terceros | Revisar y normalizar los contratos establecidos con los proveedores de TI externos con el fin de garantizar que sean adecuados a las encesidades de la organizacion. Adicionalmente, establecer acuerdos de nivel de servicio. | Coordinador de TI | AME |

# 4. CONCLUSIONES Y RECOMENDACIONES

## 4.1 Conclusiones

La evaluación del estado actual realizado muestra que la institución no cuenta con políticas de seguridad de la información, por ende, el sistema de gestión de seguridad de la información se encuentra en un estado inicial.

Por medio de la evaluación de los objetivos de control y controles de referencia (Anexo A), la seguridad física del entorno y la seguridad en las comunicaciones obtienen los porcentajes más alto. Por otro lado, las políticas de seguridad de información, la gestión de activos, control de acceso y criptografía son los cuales obtienen los valores más bajos.

La evaluación del impacto, probabilidad y riesgo al activo crítico mencionado en el documento demuestra la necesidad de implementar políticas de seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de los servicios que brinda la institución a sus clientes.

El diseño del programa del sistema de gestión de seguridad de la información para la institución pública se ha definido en el área de sistemas puesto que en el área se maneja los sistemas de gran importancia para la institución.

El programa del sistema de gestión de seguridad de la información, se estima su implementación se lo realice a lo largo del año 2022 donde se hace hincapié en los planes de acción de mejora, los cuales abarcan las políticas de seguridad de la información, de gestión de activos, de control de acceso, la capacitación del personal para la respuesta ante incidentes de seguridad y el mantenimiento de los activos donde se almacena la información.

A través de los análisis y las evaluaciones realizadas con base a la norma ISO/IEC 27001:2013 se ratifica que la institución pública no tiene la capacidad de garantizar la seguridad de la información que manejan entre los servicios que ofrece la institución pública, ni de responder ante incidentes de seguridad de la información.

Las políticas de seguridad de la información a ser implementadas posteriormente deben mantener un esquema de mantenimiento y actualización, generalmente una vez al año, además deben cumplir con la normativa legal, por mencionar la nueva ley (LOPD) Ley Orgánica de Protección de Datos Personales de Ecuador.

## 4.2 Recomendaciones

La alta dirección de la institución debe comprometerse a continuar con el programa del sistema de gestión de seguridad de la información brindado los recursos necesarios para su implementación y su mejora correspondiente.

La aplicación de la norma ISO/IEC 27001:2013 permite a la institución crear, actualizar y formalizar sus políticas y procedimientos de la seguridad de la información, a través de la revisión y el cumplimiento de los controles que brinda la norma.

Cualquier institución o empresa, sea pública o privada, debe tomar en cuenta y establecer un sistema de gestión de seguridad de la información, independientemente de su línea de negocio, para garantizar su información en las tres dimensiones de confidencialidad, integridad y disponibilidad.

# REFERENCIAS

AME. (2018). ASOCIACIÓN DE MUNICIPALES ECUATORIANAS. Recuperado el 31 de agosto de 2021 de: https://plataformamunicipal.ame.gob.ec/QuienesSomos.html

AME. (2021). Misión y Visión. Recuperado el 31 de agosto de 2021 de: https://ame.gob.ec/instiicion/mision-y-vision/

Federal Trade Commission. (2021). Qué es y cómo funciona EL MARCO DE CIBERSEGURIDAD DEL NIST. Recuperado el 24 de agosto de 2021 de: https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

Framework for Improving. Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. April 16, 2018.

Infoassureltd. (2021). Information Security Management Systems (ISO 27001). Recuperado el 21 de agosto de 2021: https://infoassureltd.com/information-security-management-system/

INTECO. (2021). INTE/ISO/IEC 27001:2014. Recuperado el 21 de agosto de 2021 de: https://www.inteco.org/shop/inte-iso-iec-27001-2014-tecnologia-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-la-seguridad-de-la-informacion-requisitos-206#attr=

ISO/IEC 21827:2008, Information technology. Security techniques. Systems Security Engineering, Capability Maturity Model.

ISO/IEC 27001:2013, Information technology. Security Techniques. Code of practice for information security control.

ISO/IEC 27002:2013, Information technology. Security Techniques. Code of practice for information security control.

ISO/IEC 27005:2009, Information technology. Security techniques. Information security risk management

ISOTools. (2021). ISO 27001: Mejora del Sistema de Gestión de Seguridad de la Información. Recuperado el 14 de septiembre del 2021 de: https://www.isotools.org/2014/12/29/iso-27001-mejora-del-sistema-de-gestion-de-seguridad-de-la-informacion/

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.

NIST. (2021). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. Recuperado el 24 de agosto de 2021 de: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

PMG SSI. (2021). ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. Recuperado el 24 de agosto de 2021 de: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

Portal Administración Electrónica. (2021). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 24 de agosto de 2021 de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Soluciones GlobalSUITE. (2021). Qué es NIST Cibersecurity Framework. Recuperado el 14 de septiembre de 2021 de:

https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

TechTarget. (2021). information security management system (ISMS). Recuperado el 24 de agosto de 2021 de: https://whatis.techtarget.com/definition/information-security-management-system-ISMS

# ANEXOS