UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR, MODALIDAD PRESENCIAL

TEMA:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA EL GADIP DEL MUNICIPIO DE CAYAMBE"

Trabajo de titulación previo a la obtención del título de *Ingeniero en Electrónica y Redes de Comunicación*

Línea de investigación: Gestión, producción, productividad, innovación y desarrollo socioeconómico

AUTOR:

LENIN JULIAN JAMI LEMA

DIRECTOR:

MSC. CARLOS ALBERTO VÁSQUEZ AYALA

Ibarra, julio 2024

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1723258511		
APELLIDOS Y NOMBRES:	Jami Lema Lenin Julian		
DIRECCIÓN:	Cayambe, Calle Segundo Durán y Guaranda N2		
EMAIL:	ljjami@utn.edu.ec/leninjami23@gmail.com		
TELÉFONO FIJO:	022-138-375	**TELÉFONO MÓVIL:**	0997834026

DATOS DE LA OBRA	
TÍTULO:	"Diseño de un sistema de gestión de seguridad de la información basado en la ISO 27001 para el GADIP del Municipio de Cayambe."
AUTOR (ES):	Jami Lema Lenin Julian
FECHA: DD/MM/AAAA	29-07-2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **GRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Carlos Alberto Vásquez Ayala, MSc.

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 30 días del mes de julio de 2024

EL AUTOR:

Lenin Julian Jami Lema

Escaneado con CamScanner

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 30 de julio de 2024

CARLOS VÁSQUEZ
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

CARLOS ALBERTO VÁSQUEZ AYALA
C.C.: 100242498-2

Escaneado con CamScanner

DEDICATORIA

Este proyecto de titulación va dedicado a toda mi familia y en especial a mi madre, quien ha sido el pilar principal en mi vida, gracias a todo su esfuerzo y apoyo incondicional que me ha brindado, a pesar de los tropiezos que he tenido en el camino, sé que siempre podré contar con su ayuda.

A mi querida UTN, docentes y mis amigos que he conseguido a lo largo de mis estudios universitarios, a mis compañeros de lucha diaria con el cual compartimos muchos momentos buenos y malos, valió todo ese esfuerzo con el fin de poder llegar a la meta

AGRADECIMIENTO

El agradecimiento va a Dios, por darme fuerza para seguir adelante a pesar de que se presentaron varios obstáculos, él me levantó, cuando todo parecía perdido, nunca me abandonó y solo él sabe que todo lo que he vivido para crecer como persona, como hijo, amigo, gracias a todos esos buenos y malos momentos, ahora soy una persona de bien, gracias por todo el apoyo de mis padres: Cristóbal y Mercedes, en especial a mi madre por su lucha constante y darme la mejor herencia que es el estudio, gracias por todo el esfuerzo que realizó, el sueño de todo padre es ver a su hijo con una profesión, gracias por todo su ayuda incondicional, por los ánimos que me brindaba a diario y por los consejos que fueron de gran ayuda para lograr llegar aquí.

1 INDICE DE CONTENIDOS

1 CAPÍTULO I: ANTECEDENTES 15
1.1 Tema 15
1.2 Problema 15
1.3 Objetivos 16
1.3.1 Objetivo General 16
1.3.2 Objetivos específicos 17
1.4 Alcance 17
1.5 Justificación 18
1.6 Contexto 19
2 CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA 21
2.1 Definición de términos básicos. 21
2.1.1 Seguridad de la información 21
2.1.2 Confidencialidad 22
2.1.3 Integridad 22
2.1.4 Disponibilidad 23
2.1.5 Activo de seguridad de la información 23
2.1.6 Administración. 23
2.1.7 Sistema de Gestión. 24
2.1.8 Política de seguridad. 24
2.1.9 Seguridad perimetral 24
2.1.10 Riesgo 25
2.1.11 Amenaza 26
2.1.12 Vulnerabilidad 26
2.1.13 Impacto 27
2.1.14 Ataques 28
2.2 Norma ISO 27000. 28
2.2.1 Alcance 29
2.2.2 Propósito. 29
2.3 ISO/IEC 27001 29
2.3.1 Propósito 30
2.4 Fases de una SGSI 27001 30
2.4.1 Definir políticas 31
2.4.2 Definir el alcance del SGSI 32
2.4.3 Análisis de Riesgos 33
2.4.4 Gestión de riesgos 35
2.4.5 Selección de controles a implementar. 37

2.4.6 Declaración de aplicabilidad. 37
2.4.7 Revisión del sistema. 37
2.5 Modelo PDCA 38
2.5.1 Planear (PLAN) 39
2.5.2 Hacer (DO) 39
2.5.3 Revisar (CHECK) 39
2.5.4 Actuar (ACT) 40
2.6 Política de seguridad dentro de una SGSI 40
2.7 Elaboración del cuerpo documental 40
2.8 Formación y concienciación 41
2.9 Mejora continua 42
2.9.1 Propósito 43
2.10 Sectores interesados en la implementación del SGSI 43
2.10.1 Sector público. 43
2.11 Metodología de Análisis de Riesgos 44
2.11.1 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) 45
2.12 Empresas que han implementado el SGSI a nivel del Nacional 47
2.13 Leyes, normas y reglamentos nacionales 48
2.13.1 Esquema gubernamental de seguridad de la información (EGSI) 48
2.13.2 Constitución de la República del Ecuador 48
2.13.3 Código orgánico integral penal 49
3 CAPÍTULO III: LEVANTAMIENTO DE INFORMACIÓN Y ESTADO ACTUAL DEL GADIP DEL MUNICIPIO DE CAYAMBE 51
3.1 Estructura organizacional del GADIPMC 52
3.1.1 Departamentos que posee el GADIPMC 53
3.1.2 Departamento de Tecnologías de la Información 54
3.1.3 Principales servicios que brinda el GADIPMC 56
3.2 Topología física de la red del GADIPMC 57
3.3 Direccionamiento IP 58
3.4 El Proveedor de Servicios de Internet 60
3.5 Data Center del GADIPMC (subsistemas) 61
3.6 Sistema de alimentación ininterrumpido (UPS) 70
3.7 Cámaras de video vigilancia 72
3.8 Sistema de Aire acondicionado 73
4 CAPÍTULO IV: ANÁLISIS Y GESTIÓN DE RIESGOS 75
4.1 Análisis de Riesgos 75
4.1.1 Activos 76

4.2 Valoración de los Activos 77
4.3 Desastres naturales 83
4.4 Amenaza Industrial 83
4.5 Errores y fallos no intencionados 85
4.6 Ataques Intencionados 86
4.7 Correlación entre errores y ataques 87
4.8 Determinación del impacto 90
4.9 Degradación 90
4.10 Cálculo de Riesgo 92
4.11 Nivel de madurez 95
4.12 Salvaguardas propuestas 96
5 CAPÍTULO V: DISEÑO DEL SGSI 99
5.1 Declaración de Aplicabilidad (SoA) del Municipio de Cayambe 99
5.2 Desarrollo del Documento de políticas 104
5.3 Manual de políticas 111
5.4 Socialización del SGSI 185
5.5 Conclusiones 189
5.6 Recomendaciones 190
5.7 Referencias 190

INDICE DE TABLAS

Tabla 1 Características de seguridad de la información 22
Tabla 2 Cometidos de la Seguridad Perimetral 25
Tabla 3 Clasificación de la gravedad de vulnerabilidades 27
Tabla 4 Principales impactos 27
Tabla 5 Tipos de ataques 28
Tabla 6 Requisitos para definir las políticas 31
Tabla 7 Al identificar el alcance del SGSI se obtiene 32
Tabla 8 Tareas definidas para el análisis de riesgos 34
Tabla 9 Acciones a ejecutar sobre el riesgo 35
Tabla 10 Tareas definidas para la gestión de riesgos 36
Tabla 11 Requisitos que debe contener una declaración de aplicabilidad 37
Tabla 12 Ciclo de mejora continua del modelo PDCA 38
Tabla 13 Estructura básica de todo cuerpo documental 41
Tabla 14 Algunos beneficios que brinda la ISO/IEC 27001 en el sector público 44
Tabla 15 Objetivos de MAGERIT V3 45
Tabla 16 Departamentos del GADIPMC 53
Tabla 17 Atribuciones y Responsabilidades del Departamento de Tecnologías de la Información 54
Tabla 18 Servicios que Brinda el GADIPMC 57
Tabla 19 Distributivo de Direcciones IP 59
Tabla 20 Hilos de Fibra Óptica que Provee ISP CNT-EP 60

Tabla 21 Subsistemas del Data Center del GADIPMC 61
Tabla 22 Elementos del Data Center del GADIPMC 65
Tabla 23 Switchs que Posee el GADIPMC 66
Tabla 24 Principales Servidores del GADIPMC 68
Tabla 25 UPS que Posee el GADIPMC 71
Tabla 26 Tipos de Activos 77
Tabla 27 Criterio de Valoración de Activos 78
Tabla 28 Criterio de valoración con Respecto a la Confidencialidad 78
Tabla 29 Criterio de Valoración con Respecto a la Integridad 79
Tabla 30 Criterio de Valoración con Respecto a la Disponibilidad 80
Tabla 31 Valoración de los Activos Referentes a CID (Confidencialidad, Integridad y Disponibilidad 82
Tabla 32 Criterio de Valoración con Respecto a Desastres Naturales 83
Tabla 33 Criterio de Valoración con Respecto a Amenaza Industrial 84
Tabla 34 Criterio de Valoración a Fallos no Intencionados 85
Tabla 35 Criterio de Valoración a Ataques Intencionados 86
Tabla 36 Clasificación de la gravedad de las vulnerabilidades 88
Tabla 37 Escala cualitativa y cuantitativa de la Magnitud de Impacto y Riesgo 90
Tabla 38 Tabla para Determinar Estimación del impacto 91
Tabla 39 Escalas cualitativas y cualitativa para un análisis entre Impacto, Probabilidad y el Riesgo 91
Tabla 40 El cálculo para encontrar el Riesgo mediante la combinación del impacto y la probabilidad. 92
Tabla 41 Nivel de Tolerancia 93
Tabla 42 Nivel no Tolerancias de los Activos del GADIPMC 94
Tabla 43 Niveles de Madurez 95
Tabla 44 Salvaguardas propuestas para el GADIPMC 96
Tabla 45 Tabla de Declaración de aplicabilidad para el GADIPMC 100

INDICE DE FIGURAS

Figura 1 Amenazas 26
Figura 2 Familia SGSI 29
Figura 3 Elementos o fases para la implementación de un SGSI 31
Figura 4 Relación entre riesgos amenazas y vulnerabilidades 34
Figura 5 Estructura que conlleva la Gestión de riesgos 36
Figura 6 Relación entre riesgos amenazas y vulnerabilidades 43
Figura 7 Determinar el Riesgo 46
Figura 8 Proceso de Gestión de Riesgos 47
Figura 9 Organigrama del GADIPMC 52
Figura 10 Estructura Organizacional del Departamento de Tecnologías de la Información 53
Figura 11 Topología de la Red GADIPMC 58
Figura 12 Puerta del Data Center 63
Figura 13 Piso Falso Acorde a la Normativa de Un Data Center 63
Figura 14 Techo Falso Acorde a Normativa de un Data Center 64
Figura 15 Biométrico para acceso al Data Center 64
Figura 16 Señalética Adecuada que Indica la Salida del Data Center 65

Figura 17 Tablero de distribución de energía del GADIPMC 70
Figura 18 Cámaras de video vigilancia 73
Figura 19 Cámaras de video vigilancia 73
Figura 20 Sistema de aire acondicionado marca LG 74
Figura 21 Esquema para determinar los riesgos según MAGERIT 76
Figura 22 Metodología para el GADIPMC 99
Figura 23 Entrega y socialización del SGSI para el GADIPMC 186
Figura 24 Recepción de certificado de entrega y socialización del SGSI al Departamento de Tecnologías de la información 186

RESUMEN

En un mundo cada vez más digital, la seguridad de la información es crucial para proteger los datos sensiblemente, especialmente en instituciones públicas. El Gobierno Autónomo Descentralizado Intercultural y Plurinacional del Municipio de Cayambe enfrenta retos significativos en la gestión adecuada de su información, lo que puede resultar en riesgos de seguridad, pérdida de datos y falta de confianza por parte de la ciudadanía. El presente proyecto de tesis muestra un diseño de un Sistema de Gestión de Seguridad de la Información, conforme a la norma ISO 27001, adaptado a las necesidades y particularidades del municipio de Cayambe, para así garantizar la confidencialidad, integridad y disponibilidad de la información pública. Se empleó la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que permite identificar, evaluar y tratar los riesgos asociados a la seguridad de la información. La metodología involucra etapas de diagnóstico actual del sistema de información del municipio, análisis de riesgos a través de la evaluación de amenazas y vulnerabilidades, y la formulación de medidas de seguridad pertinentes en cumplimiento con la norma ISO 27001. El resultado de esta investigación ha sido el diseño de un Sistema de Gestión de Seguridad de la Información robusto que incluye la identificación de 11 activos con riesgos críticos relacionados con la información del municipio. Se han establecido controles específicos en línea con la ISO 27001, priorizando la capacitación del personal, la implementación de políticas de seguridad claras y la realización de auditorías periódicas. Además, se propone la creación de un Comité de Seguridad de la Información que supervise la implementación y el mantenimiento del sistema, garantizando así su eficacia y adaptación a cambios futuros. La implementación de un Sistema de gestión de seguridad de la información permitirá al Municipio de Cayambe gestionar de manera eficaz la seguridad de la información, disminuir los riesgos

identificados y mejorar la confianza de los ciudadanos en la gestión pública, contribuyendo a una administración más segura y transparente.

Palabras clave: Seguridad de la información, Norma ISO 27001, Metodología Magerit, Instituciones públicas, Riesgos de Seguridad, Políticas de Seguridad.

ABSTRACT

In an increasingly digital world, information security is crucial to protect data sensitively, especially in public institutions. The Decentralized Intercultural and Plurinational Autonomous Government of the Municipality of Cayambe faces significant challenges in the proper management of its information, which can result in security risks, loss of data, and lack of trust on the part of citizens. This thesis project shows a design of an Information Security Management System, in accordance with the ISO 27001 standard, adapted to the needs and particularities of the municipality of Cayambe, in order to guarantee the confidentiality, integrity and availability of public information. The Magerit methodology (Methodology for Risk Analysis and Management of Information Systems) was used, which allows identifying, evaluating and treating the risks associated with information security. The methodology involves stages of current diagnosis of the municipality's information system, risk analysis through the evaluation of threats and vulnerabilities, and the formulation of relevant security measures in compliance with the ISO 27001 standard. The result of this research has been the design of a robust Information Security Management System that includes the identification of 11 assets with critical risks related to the municipality's information. Specific controls have been established in line with ISO 27001, prioritizing staff training, implementing clear security policies, and conducting regular audits. In addition, the creation of an Information Security Committee is proposed to supervise the implementation and maintenance of the system, thus guaranteeing its effectiveness and adaptation to future changes. The implementation of an Information Security Management System will allow the Municipality of Cayambe to effectively manage information security, reduce identified risks and improve citizens' confidence in public management, contributing to a more secure and transparent administration.

Keywords: Information security, ISO 27001 Standard, Magerit Methodology, Public Institutions, Security Risks, Security Policie.

1 CAPÍTULO I: ANTECEDENTES

En este capítulo se detallan los antecedentes para el desarrollo de esta tesis para demostrar la importancia de emprender este proyecto.

1.1 Tema

Diseño de un sistema de gestión de seguridad de la información basado en la ISO 27001 para el GADIP del Municipio de Cayambe.

1.2 Problema

El GADIP del municipio de Cayambe, institución que lidera un modelo de gestión intercultural y plurinacional con una activa participación ciudadana y comunitaria atendiendo las necesidades individuales y colectivas de manera corresponsable con los actores sociales y demás niveles de gobierno construyendo una sociedad intercultural (GADIPMC, 2022)

Esta entidad pública tiene como una de sus funciones prioritarias administrar la información relevante de las actividades realizada por los ciudadanos, al acceder a los diferentes servicios que brinda el GADIPMC, datos que están en servidores para mantener el respaldo de acciones realizadas, los servidores BBDD permanecen dentro del data center, el cual cuenta con medidas de seguridad y un entorno apropiado, logrando que la condición de trabajo de los equipos sea la adecuada. El acceso a los equipos es llevado a cabo únicamente por administradores de la Red, sin embargo, el municipio no cuenta con procesos de mejora para mantener la seguridad de la información, no existe una guía de ejecución de procesos sistematizados, documentados que sea una herramienta de ayuda al presentarse posibles actividades malintencionadas con fines negativos que atente en contra la integridad, manipulación, pérdida de información o plagio del mismo. Es necesario que se implemente un SGSI el cual este regida por la ISO 27001 y está cubra con las necesidades del GADIP del municipio de Cayambe, mejorando el tratamiento de

la información con la finalidad de establecer políticas, procesos, necesarios para que la preservación de la información sea la adecuada.

El Municipio de Cayambe tiene como uno de sus objetivos fortalecer la participación ciudadana intercultural las potencialidades socioculturales, económico productivas, el desarrollo del intercultural, el manejo sostenible de los recursos naturales, mediante la implementación de infraestructura física, la provisión de bienes y servicios el ordenamiento y regulación territorial urbano y rural a fin de alcanzar una sociedad solidaria encaminada al Sumak Kawsay. Con propósito de dar mejoras en el servicio que brinda a la ciudadanía, es necesario que se implementen procesos para mejorar la seguridad de la información, generando el aumento de la confianza entre el usuario hacia el GADIP del municipio de Cayambe, evitando dañar la imagen institucional que tiene un Municipio frente a la ciudadanía.(GADIPMC, 2022)

El proceso de diseño e implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001, desde su establecimiento incluye un servicio posterior de monitorización y seguimiento permanentes que aseguren el mantenimiento continuo del sistema, dentro de una organización sea pública o privada. Brinda muchos beneficios que facilitan el tratamiento y análisis de datos, con la implementación de este proceso dentro del GADIP del municipio de Cayambe se busca aplicar procesos técnicos para el monitoreo de la Red y evitar la manipulación de datos, logrando establecer indicadores para medir la eficacia de concienciación de la seguridad, formando buenas prácticas y capacitando al personal que conforma el municipio.

1.3 Objetivos

1.3.1 Objetivo General

Diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 en la red de datos del GADIP del municipio de Cayambe.

1.3.2 Objetivos específicos

- Análisis de la norma ISO 27001, enmarcada en instituciones públicas
- Realizar el levantamiento de información, de la situación actual de la Red de datos del GADIP del municipio de Cayambe.
- Efectuar un análisis y gestión de riesgos en la dirección de tecnología de la información.
- Diseñar la metodología adecuada de un sistema de gestión de seguridad de la información, basado en las normas ISO/IEC 27001, para el GADIP del municipio de Cayambe.
- Socializar el "SGSI" con el personal del GADIP del municipio de Cayambe.

1.4 Alcance

Para iniciar con este proyecto, se hará el estudio de la norma ISO 27001 y todo lo referente a esta normativa para establecer una "SGSI", el estudio contará con información de instituciones en las cuales ya se haya implementado este sistema y cuyos resultados sean satisfactorios.

El levantamiento de información se enfocará en la parte de activos que se encuentran asociados a las instalaciones de la entidad pública, el cual ayudará a determinar el estado actual de la Red de datos para determinar y clasificar el tipo de información, este análisis dará un gran aporte a la investigación que se desarrolle.

Realizar el uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), el cual se basa en la identificación de amenazas y vulnerabilidades que pueden ser utilizadas para actos con fines maliciosos, al identificar

los activos más relevantes del GADIPMC, esta técnica permitirá establecer medidas preventivas, correctivas y a su vez estimar el impacto del daño que podría sufrir. El análisis y gestión de riesgo se llevará a cabo dentro de la Dirección de tecnología de la información debido a que dentro de esta área organizacional se realiza la administración de la Red.

Siguiendo el proceso PDCA que establece la ISO 27001 se diseñará la metodología adecuada para la institución y se complementará usando los controles de la norma ISO 27002, ya que enmarca un listado de buenas prácticas en relación con el tratamiento de riesgos. Se establecerán las políticas acordes a cada uno de los riesgos y se contará con un manual de procedimientos que ayudará a dar seguimiento a una amenaza.

Culminado el proceso de diseño de la SGSI se hará una socialización al personal que conforma el Departamento de Tecnologías de la Información del GADIP del Municipio de Cayambe, con el uso de material físico y digital.

El Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso continuo, sistemático, documentado y conocido por toda la organización; aunque proporcionar un sistema completamente seguro es imposible, el propósito del SGSI es que los riesgos sean conocidos, asumidos, gestionados y minimizados por la misma organización. (NQA, 2024)

1.5 Justificación

El GADIP del municipio de Cayambe entidad pública al servicio de la ciudadanía, conformada por toda la planta administrativa, realiza tareas diarias rigiéndose a los lineamientos propios de la institución, brindando varios servicios como: el recaudar fondos del consumo de agua potable, pagos y/o consulta impuestos, matriculación vehicular, y varios trámites, todos esos cobros se lo realiza de forma personal en una

ventanilla dentro del área de recaudaciones, a través de su página web se puede realizar consultas sobre de pagos de impuestos, solicitar turnos para realizar la revisión vehicular entre otros, cabe recalcar que la institución aún no cuenta con el servicio de pago de a través de la internet.

El municipio posee información importante acerca de las transacciones realizadas por los ciudadanos como datos de uso delicado, en la actualidad el robo de información o pérdida de integridad de la misma afectaría gravemente el prestigio del GADIP del municipio de Cayambe, generando incertidumbre y desconfianza en la institución, es necesario que exista un SGSI el cual minimice la probabilidad de que los datos se vean afectados por factores externos no intencionales o de forma malintencionada por terceras personas.

Este proyecto trata de mitigar ciertos factores de riesgo y dar seguimiento a procesos adecuados dependiendo el tipo de amenaza que presente la Red, demostrando así los conocimientos adquiridos durante toda la carrera de Electrónica y Redes de Comunicación, la finalidad del tema impartido es diseñar un SGSI basado en la ISO 27001, tomando en cuenta los beneficios que presenta la metodología de implantación que ayudan a seguir un proceso ordenado en el diseño de un sistema de seguridad, basándose en criterios humanísticos y haciendo uso de la investigación sobre la temática para tomarla como herramienta principal.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir

1.6 Contexto

“Metodología del SGSI según la norma ISO/IEC 27001 para El gobierno autónomo descentralizado de San Miguel de Urcuqui”: autor Henry Geovany Valencia Fernández.

El trabajo realizado por el señor Henry Geovany Valencia Fernández fue diseñar e implementar un sistema de seguridad para la red de datos del GADMU, siguiendo las especificaciones del administrador de la red, se implementó un modelo de seguridad para proteger los servidores de bases de datos y registro de la propiedad, haciendo uso de un firewall cisco y basado en la Metodología del SGSI según la norma ISO/IEC 27001.

CYNTIA MARIBEL INUCA GONZA. (2015) “Administración y gestión de la red de área local del Gobierno Autónomo Descentralizado Municipal del Cantón Cayambe, basado en el modelo funcional de gestión de red ISO/OSI con el protocolo SNMP y uso de herramientas de software libre” (TESIS DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN)

El tema que ya se ha propuesto, en la tesis (04 RED 075 TESIS.pdf) tuvo como objetivo de ayudar a mejorar la disponibilidad de la red de área local, del GADIP Municipio de Cayambe, a través del modelo funcional de gestión de red ISO/OSI, y sus áreas de gestión; configuración, seguridad, fallos, rendimiento, y contabilidad, la cual permite administrar la red de forma organizada, e indica las funciones que se debe gestionar.

2 CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

Para el desarrollo de este proyecto se ha tomado ciertos puntos clave que están descritos dentro de este capítulo, partiendo como base los términos, metodologías, fases y procesos que conlleva a el diseño e implementación de una SGSI.

2.1 Definición de términos básicos.

Palabras o conceptos usados para la formulación del problema

2.1.1 Seguridad de la información

La seguridad de la información abarca tres principios fundamentales: confiabilidad, integridad y disponibilidad de los datos importantes para la organización indistintamente del tipo de formato que tenga. Para llevar a cabo esos principios es necesario realizar un análisis y gestión de la información, considerando la amplia gama de amenazas y riesgos existentes, en la actualidad es importante dar buen resguardo de la información con el objetivo de garantizar el éxito comercial, siguiendo la continuidad de la organización cuya finalidad es reducir al mínimo las consecuencias de incidentes de seguridad de la información (Areitio Javier, 2008)

La seguridad de la información se logra mediante la aplicación de los controles previamente seleccionados a través del proceso de gestión del riesgo elegido y gestionado a través de un SGSI, el cual incluye las políticas de seguridad, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de la información identificados, para asegurar que se cumplen los objetivos específicos de la organización se espera que los controles de seguridad de la información sean de interés para integrarse a la perfección con los procesos de negocio de una organización (ISO-IEC, 2018). Se ha considerado como las principales características de la seguridad de la información como muestra en la Tabla 1.

Tabla 1

Características de seguridad de la información

Características	Descripción
Autenticidad	Asegurar el origen de la información, la identidad de todos los usuarios debe ser validada al momento de realizar petición de acceso, de modo que se puede demostrar que es quien dice ser.
No repudio	Incapacidad de negación ante terceros de realizar un envió y/o recepción por parte del emisor y/o receptor de la información. Debido a que hay pruebas que indican que el mensaje fue enviado y recibido.
Trazabilidad	Es el conjunto de acciones, procedimientos que permiten verificar y registrar toda la trayectoria de la información, realizado desde un usuario origen hasta un usuario destino es decir logra autenticar la acción del no repudio.

Nota. Adaptada de (Carrasco Alejandro, 2014)

2.1.2 Confidencialidad

Se refiere a que los datos pueden ser legibles y modificados sólo por las partes autorizadas, tanto el acceso a datos almacenados como también durante la transferencia de la información, esta debe realizarse de manera segura, eludiendo un acceso no autorizado a terceras partes.(Vega Edgar, 2021)

2.1.3 Integridad

Es la certeza de que los datos están completos y no han sido alterados por personas no autorizadas, se deben tomar las medidas necesarias para asegurar la integridad de la información, en la actualidad la protección de datos se ha visto como requisito legal que deben cumplir entidades públicas y privadas. (Vega Edgar, 2021)

2.1.4 Disponibilidad

El acceso a los datos debe ser garantizado en el momento necesario, para que una aplicación o servicio esté siempre disponible, el funcionamiento de los equipos debe ser continuo, hay que evitar fallos en el sistema y proveer el acceso a la información. (Vega Edgar, 2021)

2.1.5 Activo de seguridad de la información

Las organizaciones poseen información útil que deben ser protegidos ante cualquier riesgo o amenaza que atente al correcto funcionamiento del objetivo del negocio, ese tipo de información es esencial para las empresas y se las ha denominado activos de seguridad de la información, por lo tanto, necesita ser protegido de forma adecuada. Esta puede ser almacenada en muchas formas como: digital, material, etc. La información puede ser transmitida por varios medios, incluyendo: mensajería, comunicación electrónica o verbal. Toda información tomará forma por el medio el cual se transmite, que siempre necesita una protección adecuada, además depende de la tecnología de información y las comunicaciones. Tecnología que viene a ser un elemento esencial en la organización cuya finalidad es facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información(ISO-IEC, 2018)

2.1.6 Administración.

La administración involucra actividades para dirigir, controlar y mejorar continuamente la organización dentro de las estructuras apropiadas. Las actividades de manejo incluyen el acto, forma, o la práctica de la organización, manejo, dirigir y controlar los recursos. Las estructuras de gestión se extienden de una persona en una

organización pequeña a las jerarquías de administración compuesto por muchas personas en las grandes organizaciones (ISO-IEC, 2018).

En términos de un SGSI, la gestión implica la supervisión y toma de decisiones para alcanzar los objetivos de negocio a través de la protección de los activos de información de la organización, la gestión de seguridad de la información se expresa a través de la formulación y aplicación de políticas de seguridad de información, procedimientos y directrices, que luego se aplican en toda la organización por todas las personas asociadas con la organización (ISO-IEC, 2018)

2.1.7 Sistema de Gestión.

Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos (ISO/IEC, 2018).la Tabla 2 indica los acometidos a cumplir de la seguridad

2.1.8 Política de seguridad.

Es la información documentada en la que se reflejan, en términos generales, los objetivos de la organización en materia de seguridad de la información y las principales líneas de acción que permitan proteger su información frente a pérdida de confidencialidad, integridad y disponibilidad, tener en cuenta los requisitos del negocio, así como los contractuales, legales y estatutarios, los cuales quedarán reflejados en la misma. (José González Rus et al., 2007)

2.1.9 Seguridad perimetral

La seguridad perimetral cumple un papel muy importante, dentro de la seguridad de una Red. Esta establece los recursos y elementos para la protección de diferentes perímetros físicos de la Red, a distintos niveles, dentro de estos recursos pueden ser tanto

mecánicos o electrónicos, los usos de estos recursos tienen como fin ayudar a definir los diferentes niveles de confianza en la Red, permitiendo y restringiendo el acceso a ciertos servicios a usuarios internos y externos (Vega Edgar, 2021)

La seguridad perimetral no es un componente aislado: es una estrategia para proteger los recursos de una organización conectada a la Red, es la realización práctica de la política de seguridad de una organización. Sin una política de seguridad, la seguridad perimetral no sirve de nada. (UNIR FP, 2023)como muestra la Tabla 2 los cometidos de una seguridad perimetral.

Tabla 2

Cometidos de la Seguridad Perimetral

Tareas	Descripción
Rechazar	Alguna conexión ilegítima a los servicios
Permitir	Solo ciertos tipos de tráfico de entrada/salida o entre ciertos nodos
Proporcionar	Un único punto de interconexión con el exterior.
Redirigir	El tráfico entrante a los sistemas adecuados, dentro de la red interna
Ocultar	Ciertos sistemas o servicios vulnerables que son fáciles de proteger
Auditar	El tráfico entre el exterior y el interior
Ocultar información	Nombres de sistemas o servicios vulnerables que son fáciles de proteger

Nota. Adaptada de (Carrasco Alejandro, 2014)

2.1.10 Riesgo

Es la probabilidad de ocurrencia de producir un incidente, es la materialización de una amenaza para explotar una vulnerabilidad existente, generando así un impacto que afecte a un activo.

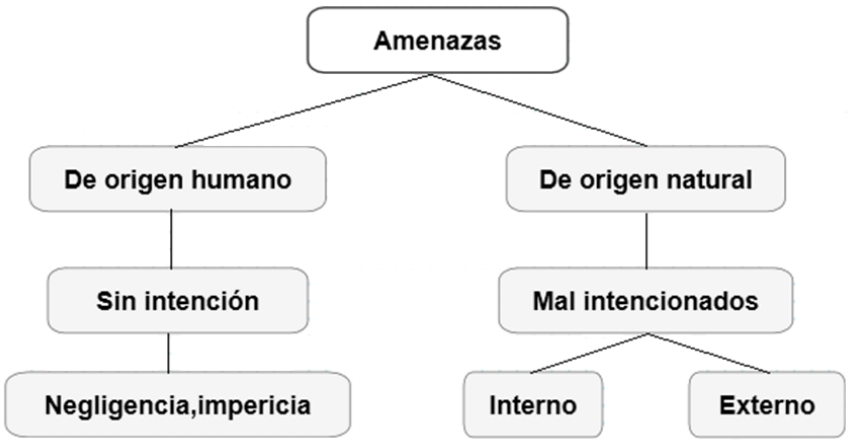
$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

2.1.11 Amenaza

Una amenaza es la acción de la que se vale una vulnerabilidad para atentar contra la seguridad de un sistema de un activo de información. A continuación, la Figura 1 muestra los tipos de amenazas.

Figura 1

Amenazas



Nota. Adaptada de (ISO/IEC, 2018)

2.1.12 Vulnerabilidad

La vulnerabilidad en un sistema es precisamente una apertura para que sea posible realizar un ataque, ningún sistema está completamente a salvo y cualquier descuido puede ser aprovechado, a continuación, en la Tabla 3 muestra la clasificación de las vulnerabilidades.

Tabla 3

Clasificación de la gravedad de vulnerabilidades

Clasificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que debe poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento
Moderada	El impacto de puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo

Nota. Adaptada de (Arribas, 2018)

2.1.13 Impacto

El impacto indica el tamaño de las consecuencias que tiene para el negocio u organización el hecho de que uno o varios de sus activos se hayan visto comprometidos, su confidencialidad integridad y disponibilidad. El nivel de impacto será considerado al activo afectado. La Tabla 4 indica los principales impactos que puede ocasionar dentro de una organización.

Tabla 4

Principales impactos

Impactos
Sanción por violación de la legislación
Perdida de dinero
Violación de confianza

Pérdida de imagen / reputación
Pérdida de eficiencia / desempeño operativo
Interrupción de actividades del negocio

Nota. Adaptada de (Bejarano Forero, 2017)

2.1.14 Ataques

El ataque dentro de redes de datos consiste en aprovechar alguna vulnerabilidad dentro de la red, explotarla todo con el fin de causar daño, los ataques son más numerosos y a su vez son más sofisticados.

"Se pude definir ataques como todas aquellas acciones que supongan una violación de la seguridad de nuestro sistema (autenticidad, confidencialidad, integridad o disponibilidad)" (Carrasco Alejandro, 2014). La Tabla 5 muestra los ataques su objetivo.

Tabla 5

Tipos de ataques

Ataques	**Objetivo**
Confidencialidad	Obtener información privilegiada
Integridad	Modificar o alterar el contenido de la información
Disponibilidad	Alterar el funcionamiento de los servicios, es decir que no estén disponibles.

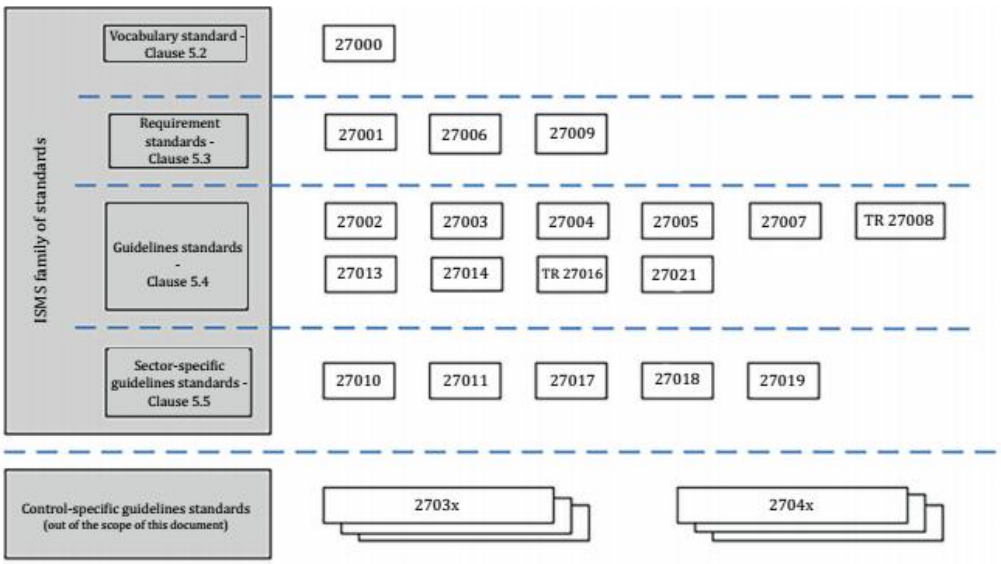
Nota. Adaptada de (Carrasco Alejandro, 2014)

2.2 Norma ISO 27000.

La serie 27000 como muestra la Figura 2, es un conjunto de normas interrelacionadas publicadas y cada una de ellas describe los lineamientos y exigencias para un SGSI ISO/IEC 27001 y los procesos para obtener una certificación.

Figura 2

Familia SGSI



Nota. Fuente (ISO/IEC, 2018)

2.2.1 Alcance

ISO 27000 describe una visión general, la terminología y definiciones que son utilizadas dentro del SGSI, aplicados a cualquier tipo y tamaño de organización.

- Datos generales de la familia 27000
- Introducción a un SGSI
- Términos usados dentro de toda la familia que abarca las normas de SGSI

2.2.2 Propósito.

Describir las bases fundamentales de un SGSI, la familia de normas y definir los términos relacionados.

2.3 ISO/IEC 27001

Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) formalizados en el contexto de los riesgos de negocio globales de la organización. Especifica los requisitos para la aplicación de los controles de seguridad de la información a medida de las necesidades de las organizaciones individuales o partes de los mismos. Este documento puede ser utilizado por todas las organizaciones, independientemente del tipo, tamaño y naturaleza (ISO-IEC, 2018).

2.3.1 Propósito

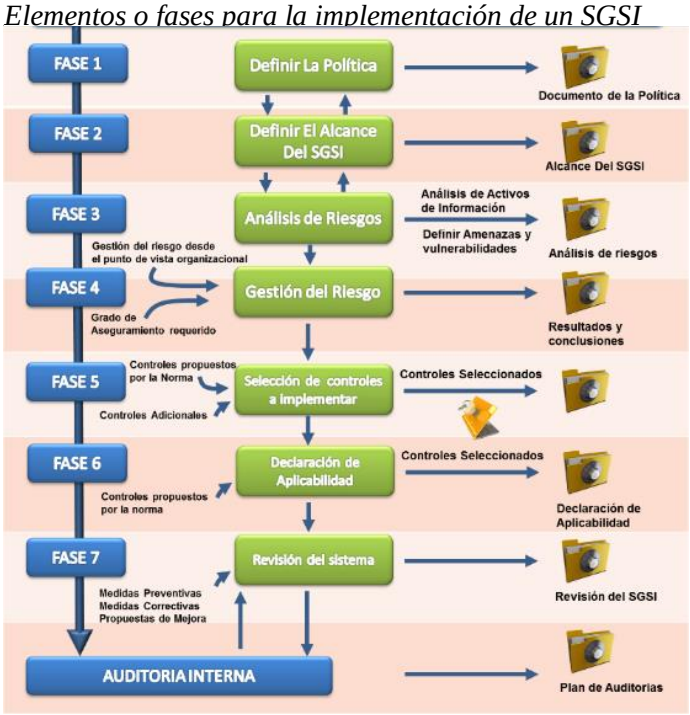
ISO / IEC 27001 proporciona requisitos normativos para el desarrollo y el funcionamiento de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados a los activos de información que la organización trata de proteger al operar su SGSI. Las organizaciones que gestionan un SGSI pueden tener su conformidad auditada y certificado. Los objetivos de control y controles de ISO / IEC 27001: 2022, (véase Anexo 1) se seleccionarán como parte de este proceso SGSI como adecuado para cubrir los requisitos identificados(NQA, 2024).

2.4 Fases de una SGSI 27001

Para realizar la implantación de un SGSI debe desarrollarse siguiendo una serie de fases como indica la Figura 3 muestra cómo se desarrolla cada una de estas actividades.

Figura 3

Elementos o fases para la implementación de un SGSI



Nota. Fuente(INTERCER, 2013)

2.4.1 Definir políticas

Una política dentro de una organización tiene como propósito proteger los activos de información. Para eso se debe cumplir ciertos requisitos como muestra la Tabla 6.

Tabla 6

Requisitos para definir las políticas

Requisitos
Debe incluir un marco general y los objetivos de seguridad de la información.
Debe considerar los requerimientos legales y contractuales relativos a la seguridad de la información.
Debe estar alineada con el contexto estratégico de gestión de riesgos de la organización.
Debe establecer los criterios con los que se va a evaluar el riesgo

Debe ser aprobado por la Dirección.
Cada una de las políticas debe ser cumplida por todos los empleados de la empresa siguiendo los procedimientos establecidos.

Nota. Fuente adaptada de (Olano et al., 2016)

2.4.2 Definir el alcance del SGSI

Para que se ejecute el proyecto con éxito, es necesario saber delimitar un alcance adecuado. La elección de un alcance no apropiado para la organización puede considerar un aumento de tiempo en implementar el SGSI, aumento de recursos humanos y económicos, provocando que la ejecución del proyecto fracase (Merino Bada & Cañizares Sales, 2012).

El alcance puede abarcar a toda o sólo una parte de la organización en función de la estrategia a seguir que adopte la empresa, se puede implementar un SGSI cuyo alcance comprenda un único proceso, una unidad de negocio, un tipo de servicio, o un marco que englobe la seguridad, como muestra la Tabla 7. En muchas organizaciones la estrategia no es implantar el estándar en toda la organización, sino que se empiece por una parte de la misma y sucesivamente se va ampliando el alcance, de tal forma que la adaptación a la norma es más progresiva y el impacto en la organización es menor(Merino Bada & Cañizares Sales, 2012).

Tabla 7

Al identificar el alcance del SGSI se obtiene

Sistema de gestión de Seguridad
Política
Acciones correctivas y preventivas
Planificación y evaluación de riesgos

Operación e implementación
Revisión de Gestión

Nota. Adaptada de (Merino Bada & Cañizares Sales, 2012)

2.4.3 Análisis de Riesgos

El análisis de riesgo se encarga de identificar los riesgos que podrían afectar a que una organización no pueda cumplir sus objetivos sin importar el tipo de negocio a que se dedique la empresa, por ello es necesario determinar un nivel de riesgo asumible, e identificar las áreas que requieren de salvaguardas o a su vez controles acorde al tipo de riesgo detectado (Merino Bada & Cañizares Sales, 2012).

El análisis de riesgos es un proceso de identificación y evaluación del riesgo a sufrir un ataque, y como consecuencia perder datos, tiempo y horas de trabajo, comparándolo con el coste que significa la prevención del suceso. La figura 4 muestra la relación entre el riesgo, amenazas y vulnerabilidades. Su análisis no solo nos lleva a establecer un nivel adecuado de seguridad, sino que nos permite conocer mejor el sistema que vamos a proteger. (DGMAPIAE, 2012)en la Tabla 8 muestra los pasos para el análisis de riesgo.

Figura 4

Relación entre riesgos amenazas y vulnerabilidades

Nota. Fuente (Avellaneda Javier, 2008)

Tabla 8

Tareas definidas para el análisis de riesgos

Actividad
Identificar los activos
Identificar las amenazas
Desarrollar un plan de tratamiento de riesgo
Implantar los controles
Revisar el riesgo
Seguimiento y medición

Nota. Fuente (Merino Bada & Cañizares Sales, 2012)

2.4.4 Gestión de riesgos

La gestión de riesgo se basa en el análisis de los resultados que se obtienen de la evaluación de riesgos, en el cual consiste seleccionar los controles o salvaguardas con el único objetivo de gestionar y tratar adecuadamente el riesgo hasta disminuirlo a niveles asumibles por los encargados de la dirección (Merino Bada & Cañizares Sales, 2012). Para ello se toma como referencia las acciones que se ejecutan sobre un riesgo como muestra la Tabla 9. Para tratar al riesgo dependiendo la gravedad se le asignará un valor, los pasos para realizar ese análisis muestra la Tabla 10, la valorización o nivel de riesgo dependerá de la organización o institución. La figura 5 muestra la estructura de la gestión de riesgos.

Tabla 9

Acciones a ejecutar sobre el riesgo

Acciones	
Mitigarlo/Reducirlo	Se basa en aplicar salvaguardas o medidas, que disminuyen el impacto en caso de que se materialice una amenaza, o que se disminuya la probabilidad de ocurrencia de la misma.
Transferirlo	Se basa en traspasar el riesgo a un tercero (contrato outsourcing, póliza de seguros, etc.).
Asumirlo/Aceptarlo	Se acepta el riesgo residual sin aplicar medidas. De manera usual, esta medida se adopta cuando el coste de mitigar el riesgo, supere el coste de los activos.
Evitarlo	Si la prestación de un servicio supone un riesgo no asumible y la Dirección decide no gestionarlo, el servicio se deja de prestar.

Nota. Adaptado de (Merino Bada & Cañizares Sales, 2012)

Tabla *10*

Tareas definidas para la gestión de riesgos

Actividad
Definir el umbral de riesgo asumible por la Dirección
Seleccionar los controles para mitigar el riesgo
Desarrollar un plan de tratamiento de riesgo
Implantar los controles
Revisar el riesgo
Seguimiento y medición

Nota. Fuente(Merino Bada & Cañizares Sales, 2012)

Figura 5

Estructura que conlleva la Gestión de riesgos

Nota. Fuente (López Agustín, 2020)

2.4.5 Selección de controles a implementar.

Los objetivos de control y controles deben seleccionarse e implementarse de forma que permita cumplir los requisitos identificados en la evaluación de riesgos. Esta selección debe tener en cuenta los criterios de aceptación de riesgos definidos en áreas anteriores, además los requisitos legales, reglamentarios y contractuales. (Merino Bada & Cañizares Sales, 2011, pág. 135)

2.4.6 Declaración de aplicabilidad.

SOA (Statement Of Applicability) es una lista que indica todos los controles seleccionados y su justificación del porqué de su selección, todo esto dependiendo al análisis y la decisión tomada en cuanto al tratamiento de riesgos. “Una buena y completa declaración de aplicabilidad nos muestra un mapa de nuestro SGSI y nos ayuda a aumentar la trazabilidad entre los distintos elementos del SGSI”(Merino Bada & Cañizares Sales, 2012). En la tabla 11, se establecen los requerimientos de aplicabilidad.

Tabla 11

Requisitos que debe contener una declaración de aplicabilidad

Requisitos
Incluir los objetivos de control y controles seleccionados
Incluir los objetivos de control y controles preexistentes
Incluir razones para la selección de los mismos
Incluir exclusiones de objetivos de control y controles que tiene de anexo la norma 27001
Incluir justificación para dichas exclusiones

Nota. (Merino Bada & Cañizares Sales, 2012)

2.4.7 Revisión del sistema.

El proceso de revisión del sistema se encarga de recopilar toda la información sobre el funcionamiento del SGSI, con los datos obtenidos se elabora un informe de alto nivel. El informe contendrá la situación actual del SGSI y adicional los planes que se hayan podido establecer basándose en el resultado obtenido de cada proceso de mejora continua(Gómez Fernández & Fernández Rivero, 2018)

"Esta revisión permite evaluar las oportunidades de mejora y la necesidad de efectuar cambios en el sistema de Gestión de Seguridad de la información, incluyendo la política y los objetivos. La revisión ordinaria anual del SGSI" (Merino Bada & Cañizares Sales, 2011, pág. 223).

2.5 Modelo PDCA

La ISO 27001 es una solución de mejora continua, al iniciar el desarrollar un SGSI, este debe adaptarse a un modelo PDCA (Plan-Do-Check-Act) o también conocido como ciclo Deming, usado tradicionalmente en los sistemas de gestión de la calidad. El ciclo PDCA está dividido en pasos, y cada uno de esos pasos contiene una serie de acciones por cumplir a lo largo del tiempo con el fin de lograr medir las mejoras alcanzadas (Costas José, 2010). La Tabla 12 muestra un breve rasgo del modelo PDCA.

Tabla 12

Ciclo de mejora continua del modelo PDCA

		Siglas en inglés
Planificar	Establecer el alcance del SGSI Realizar el análisis de riesgo Realizar la gestión de riesgo Seleccionar los controles Definir autoridades y responsabilidades	Plan (P)

Hacer	Definir e implementar un plan de tratamiento de riesgos Implantar el SGSI Implantar los controles Formación y concienciación	Do (D)
Verificar	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección	Check (C)
Actuar	Actuar acciones correctivas Adoptar acciones de mejora	Act (A)

Nota. Adaptado de (Costas José, 2010)

2.5.1 Planear (PLAN)

Fase en la cual se planifica y establece el SGSI. Se define los objetivos en términos del negocio de la organización, identifica los activos, tecnologías y se determinar las políticas que permitirá alcanzar los objetivos propuestos, para mejorar la seguridad de la organización.

2.5.2 Hacer (DO)

Fase donde se implementa y gestiona el SGSI. Se ejecutan las políticas, controles, procesos y procedimientos, de acuerdo al análisis de riesgos. Es necesario disponer de procedimientos el cual identifique quién debe hacer cada tarea, asignando así equitativamente responsabilidades a los admiradores de Red, para ello se debe realizar una capacitación adecuada.

2.5.3 Revisar (CHECK)

Fase el cual lleva a cabo la monitorización y revisión del SGSI. Se verifica que los procesos se ejecuten de forma prevista y que estas permitan alcanzar los objetivos establecidos, llegando a estos de forma eficiente.

2.5.4 Actuar (ACT)

En esta fase tiene como propósito mantener y mejorar el SGSI, realizando revisiones internas ejecutando acciones correctivas, preventivas y necesarias para enmendar los fallos detectados, realizando modificaciones en el sistema para así cumplir el objetivo de fase de mejora continua que establece el ciclo PDCA.

2.6 Política de seguridad dentro de una SGSI

Una política de seguridad reunirá las líneas generales y los principios que rigen a cada actividad de seguridad organizacional, dentro de un documento que esté aprobado por la dirección, cada política deberá tener directrices generales y el inicio de actuación que deberá seguir la organización dentro del área de seguridad (Gómez Fernández & Fernández Rivero, 2018).La política debe establecerse acorde al tipo de negocio, por ello es necesario identificar las principales características de la organización, además deberá reflejar sus objetivos de seguridad de la información, tomando como punto de partida la confidencialidad integridad y disponibilidad de la información, el desarrollo de una política será en un documento sólido indicando las bases fundamentales para lograr la gestión de seguridad de la información, cada política debe estar asociada con la estrategia de gestión de riesgos de la organización, para establecer ciertos puntos de partida y realizar la evaluación de los mismos (Merino Bada & Cañizares Sales, 2012).

Para ser válido a una política de seguridad esta debe ser revisada y aprobada por la alta dirección para dar a conocer el compromiso con la seguridad de la información.

2.7 Elaboración del cuerpo documental

Al momento de desarrollar un SGSI conlleva elaborar un cuerpo normativo, este tipo de documentación debe ser editable, estar legalmente aprobada con fecha y firma de responsables. Cuando se habla del cuerpo normativo. “Nos referimos con un cuerpo normativo a las políticas, normas, manuales, procedimientos, procedimientos técnicos, registros, guías e instrucciones técnicas, en definitiva, a todo el soporte documental que sustente el SGSI” (Merino Bada & Cañizares Sales, 2012, pag.173)En la tabla 13 muestra la estructura de un cuerpo documental.

La documentación puede ser presentada en diversos formatos: documentos en papel, archivos de texto, hojas de cálculo, archivos de video o audio, entre otros. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada. (López Agustín, 2020)

Tabla 13

Estructura básica de todo cuerpo documental

Estructura del cuerpo documental
Política
Norma
Procedimiento

Nota. Fuente (Merino Bada & Cañizares Sales, 2012, pag.173)

2.8 Formación y concienciación

En una organización, el personal debe estar implicado en el SGSI, la comunicación entre las partes que lo integren es un factor clave, todos deben ser capacitados y concienciados siendo partícipes de cada uno de los procesos, objetivos y

responsabilidades que se deriven de cada una de las actividades que se lleven a cabo (Merino Bada & Cañizares Sales, 2012).

Es conveniente comenzar con acciones de formación que permitan difundir entre todo el personal las novedades que incorpora en la organización el SGSI, su importancia y los objetivos perseguidos. En este caso podrá realizarse una formación general común a todos los trabajadores. Posteriormente, las acciones de formación deberán estar segmentadas de acuerdo a los perfiles a los que irán dirigidas, capacitando al personal en los aspectos específicos de su trabajo. (Gómez Fernández & Fernández Rivero, 2018, pag.71)

La Dirección será quien designe los recursos humanos, también es quien tiene la responsabilidad de dar a conocer las necesidades de formación para el personal de la organización, además esta deberá sugerir que acciones de formación se ejecuten de manera oportuna cubriendo las necesidades (Merino Bada & Cañizares Sales, 2011). Esperando que los procesos se realicen por completo en tiempos adecuados permitiendo evaluar los resultados de la capacitación.

2.9 Mejora continua

"Los Sistemas de Gestión de Seguridad de la Información desarrollados según la ISO 27001, al igual que muchos otros sistemas de gestión, se basan en el concepto de mejora continua. El modelo PDCA es una estrategia de mejora continua de calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart." (Merino Bada & Cañizares Sales, 2012, pag.36)ISO/IEC 27002.

La ISO 27002 pretende que la organización conozca de forma puntual los activos que posee y a su vez ofrece una lista de objetivos de control comúnmente aceptados y las mejores prácticas, para ser utilizado como una guía de implementación en la selección e implementación de controles para lograr la seguridad de la información (ISO-IEC, 2018).

2.9.1 Propósito

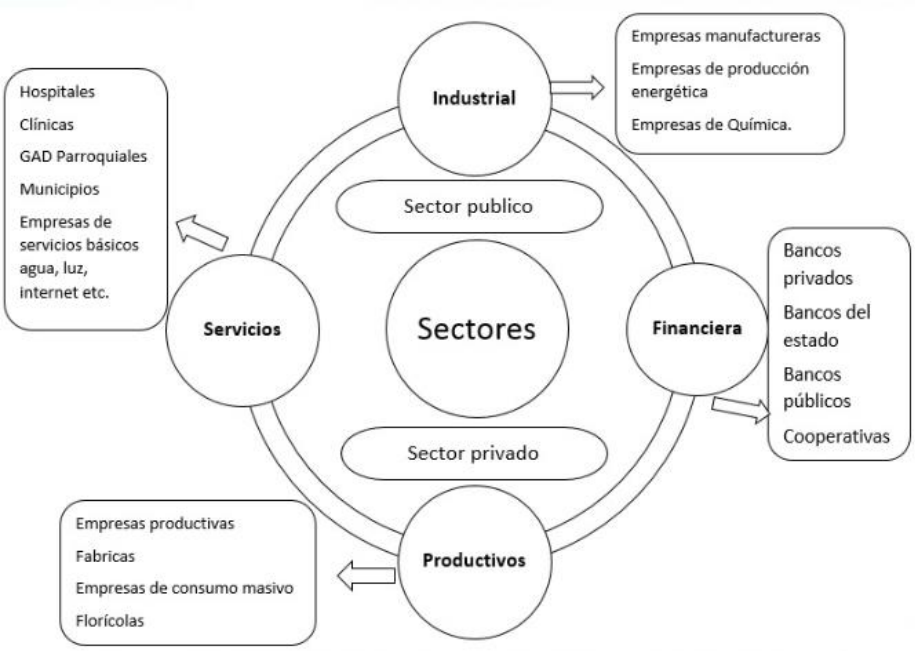
ISO / IEC 27002 proporciona orientación sobre la aplicación de los controles de seguridad de la información. En concreto, las cláusulas de 5 a 18 proporcionan asesoramiento, aplicación específica y orientación sobre las mejores prácticas en apoyo de los controles especificados en la norma ISO / IEC 27001(ISOTools, 2016).

2.10 Sectores interesados en la implementación del SGSI

La ISO 27001 es una base y guía para la implementación de un SGSI en cualquier empresa u organización ya sea pública o privada. Siendo sugestivo y algo necesario en los siguientes sectores como muestra la Figura 6.

Figura 6

Relación entre riesgos amenazas y vulnerabilidades



Nota. Adaptada de (ISOTools, 2016)

2.10.1 Sector público.

Tanto instituciones y organismos que son administrados por el Estado, actualmente se han previsto que, ¨El sector público y la administración en general también

son ámbitos muy interesados en la norma ISO 27001. El principal motivo es que permiten poner en marcha sistemas y protocolos que garanticen la confidencialidad y gestión adecuada de la gran cantidad de datos que manejan, muchos de ellos personales y con alto nivel de criticidad¨. (ISOTools, 2017, pág. 21), en la tabla 14 muestra algunos beneficios de la implementación de un SGSI.

Tabla 14

Algunos beneficios que brinda la ISO/IEC 27001 en el sector público

#	**Beneficios**
1	Gestionar la seguridad de la información y a su vez puede mejorar la organización entre los miembros de trabajo.
2	Genera confianza a los ciudadanos y organizaciones que cooperan con instituciones públicas.
3	Ayuda a integrar la seguridad en los procesos de negocio de la institución.
4	Colabora a identificar los riesgos de seguridad de la información de forma regular.

Nota. Adaptada de (ISOTools, 2016)

2.11 Metodología de Análisis de Riesgos

Una parte fundamental dentro del análisis y gestión de la seguridad de la información, es conocer y controlar los riesgos a los cuales está expuesta la información de la compañía. Cuando las empresas buscan cómo implementar modelos de gestión de seguridad suelen adoptar metodologías que brinden un marco de trabajo definido que facilite la administración de los riesgos y además permita mejorarla. Para este proyecto se ha tomado como guía MAGERIT v3 el cual contiene guías para poder trabajar de mejor manera. En la Tabla 15 indica algunos objetivos de MAGERIT.

2.11.1 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

Es una metodología de análisis y gestión de riesgos que fue elaborada por el consejo superior de administración electrónica al considerar que la gestión de riesgos es una parte fundamental para tener un buen gobierno, además ayuda a gestionar los riesgos con la implementación de medidas de seguridad. La Tabla 15 muestra los objetivos de MAGERIT V3.

Tabla 15

Objetivos de MAGERIT V3

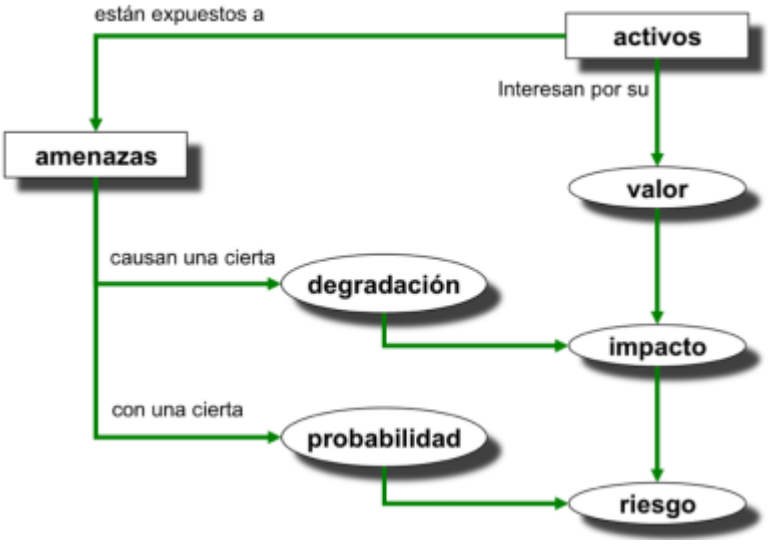
Objetivos que persigue MAGERIT
Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación (TIC).
Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirecto.
Prepara a la Organización para procesos de evaluación auditoría, certificación o acreditación, según corresponda en cada caso.

Nota. (DGMAPIAE, 2012)

"El análisis de riesgos como indica la Figura 7 es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:" (Amutio Gómez, Candau, & Mañas, 2012, pág. 22).

Figura 7

Determinar el Riesgo

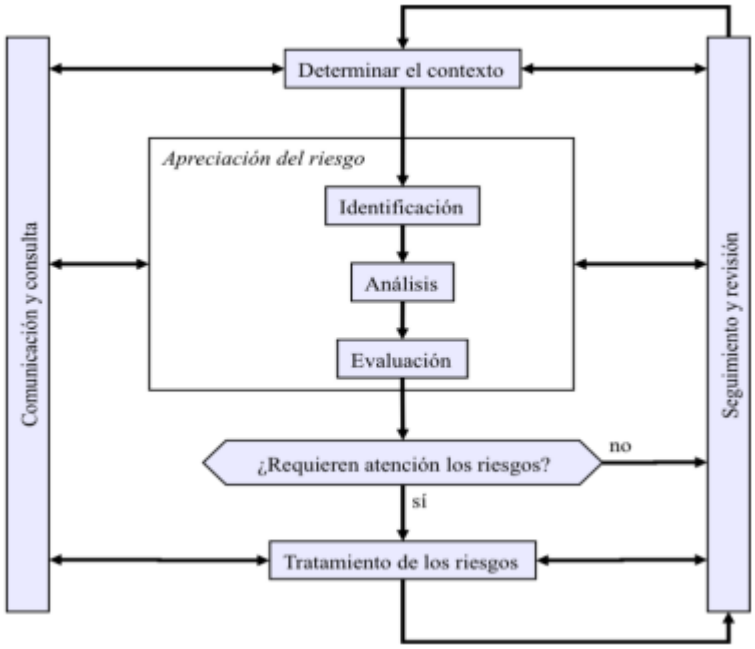


Nota. Fuente (DGMAPIAE, 2012)

La Figura 8, muestra el proceso de gestión de riesgos según MAGERIT v3

Figura 8

Proceso de Gestión de Riesgos



Nota. Fuente adaptada de (DGMAPIAE, 2012)

2.12 Empresas que han implementado el SGSI a nivel del Nacional

La CNT fue felicitada y a la vez galardonada al recibir la Certificación ISO 27001, que la respalda como una empresa que "dispone de un sistema de Seguridad de la Información conforme a la Norma UNE-ISO/IEC 27001:2007". César Regalado Iglesias, gerente general, recibió el alcance de Certificación, por parte de la Asociación Española de Normalización y Certificación AENOR (Ecuador), en un acto que contó con la presencia de varios gerentes y autoridades. (CNT, 2015)

"Dentro del último informe mundial de la Organización Internacional de Normalización (ISO), se han entregado 22.293 certificados ISO 27.001 en el mundo, de los cuales 272 corresponden a Centro y Sudamérica y 5 han sido otorgados en Ecuador" (CNT, 2015)

Roberto Almeida, gerente general de AENOR ECUADOR, recalcó que: “la CNT sigue siendo la única empresa pública en haber recibido este reconocimiento y se ubica en el tipo de empresas de categoría mundial que no solo buscan calidad, sino que se preocupan por la seguridad en la información que manejan”.(CNT, 2015)

2.13 Leyes, normas y reglamentos nacionales

El 19 de septiembre de 2013 se emitió el Acuerdo Ministerial No. 166, publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013, que dispone que las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID), implementen el Esquema Gubernamental de Seguridad de la Información (EGSI), Norma Técnica Ecuatoriana INEN ISO/IEC 27002 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. En concordancia con el Plan Nacional de Gobierno Electrónico 2014-2017 del Ecuador, reforzando el principio de garantizar seguridad y confianza y como parte del Plan Estratégico de Seguridad y Protección de Datos, el EGSI es un instrumento de vital importancia para todos los actores del Plan Nacional: ciudadanos, servidores, empresas, gobierno y otros actores del estado. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019)

2.13.1 Esquema gubernamental de seguridad de la información (EGSI)

El EGSI establece una serie de directrices aplicadas para la Gestión de Seguridad de la Información (GSI), con el objetivo de dar una mejora continua en las instituciones públicas. “El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.”(Castillo Cristian, 2013) para resumir en la Tabla 17 indica todas las cláusulas y objetivos de una EGSI a nivel nacional.

2.13.2 Constitución de la República del Ecuador

La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición por autoridad competente y de acuerdo con la ley.

¨Dentro de las normas de control interno de la contraloría general del Estado, indica los mecanismos que deberá ejecutar la unidad de tecnológica de la información para proteger, salvaguardar y evitar pérdidas, fugas de medios físicos y de la de información que se procese mediante medios informáticos, dentro del apéndice 410-10, se encuentran las medidas aplicar¨(Contraloría General del Estado, 2020).

2.13.3 Código orgánico integral penal

"El uso de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años" (Asamblea Nacional, 2019)

Dentro del COIP indica que será sancionada con pena privativa de libertad de uno a tres años, para la persona que modifique la información en terminales móviles o a su vez intercambie, comercialice o compre datos de equipos móviles, todo esto lo indica en el art 191 y art 192 del COIP. (Asamblea Nacional, 2019)

El delito informático está tipificado en el Código Orgánico Penal Integral del Ecuador aprobado en el año 2014, en el artículo 190, que señala, la apropiación

fraudulenta por medios electrónicos, existen varios delitos, pero haremos énfasis en los más relacionados para este proyecto.

Art. 202 inciso 1.- Violación de claves o sistemas de seguridad, para acceder u obtener información protegida contenida en sistemas de información.

Art. 202.2 Cesión, publicación, utilización o transferencia de datos personales sin autorización.

Art. 262 Destrucción o supresión de documentos o información por empleado público depositario de la misma.

Art. 553.2 Los que utilizaren fraudulentamente sistemas de información o redes electrónicas para facilitar la apropiación de un bien ajeno o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos(Zambrano-Mendieta et al., 2016)*Ley de propiedad intelectual*

Según el registro Oficial 320 de 19 de mayo de 1998 se publicó la Ley de Propiedad Intelectual y quien ejercerá las atribuciones y competencias establecidas por la Ley de Propiedad Intelectual será el Instituto Ecuatoriano de la Propiedad Intelectual (IEPI), dando a entender al gozo de la protección de las creaciones intelectuales como un derecho fundamental de los ecuatorianos, fomentando así la libre competencia y el desarrollo tecnológico del país, así mismo penalizando la falta o el uso indebido o plagio de la información sin consentimiento del autor. (SENADI, 2007)

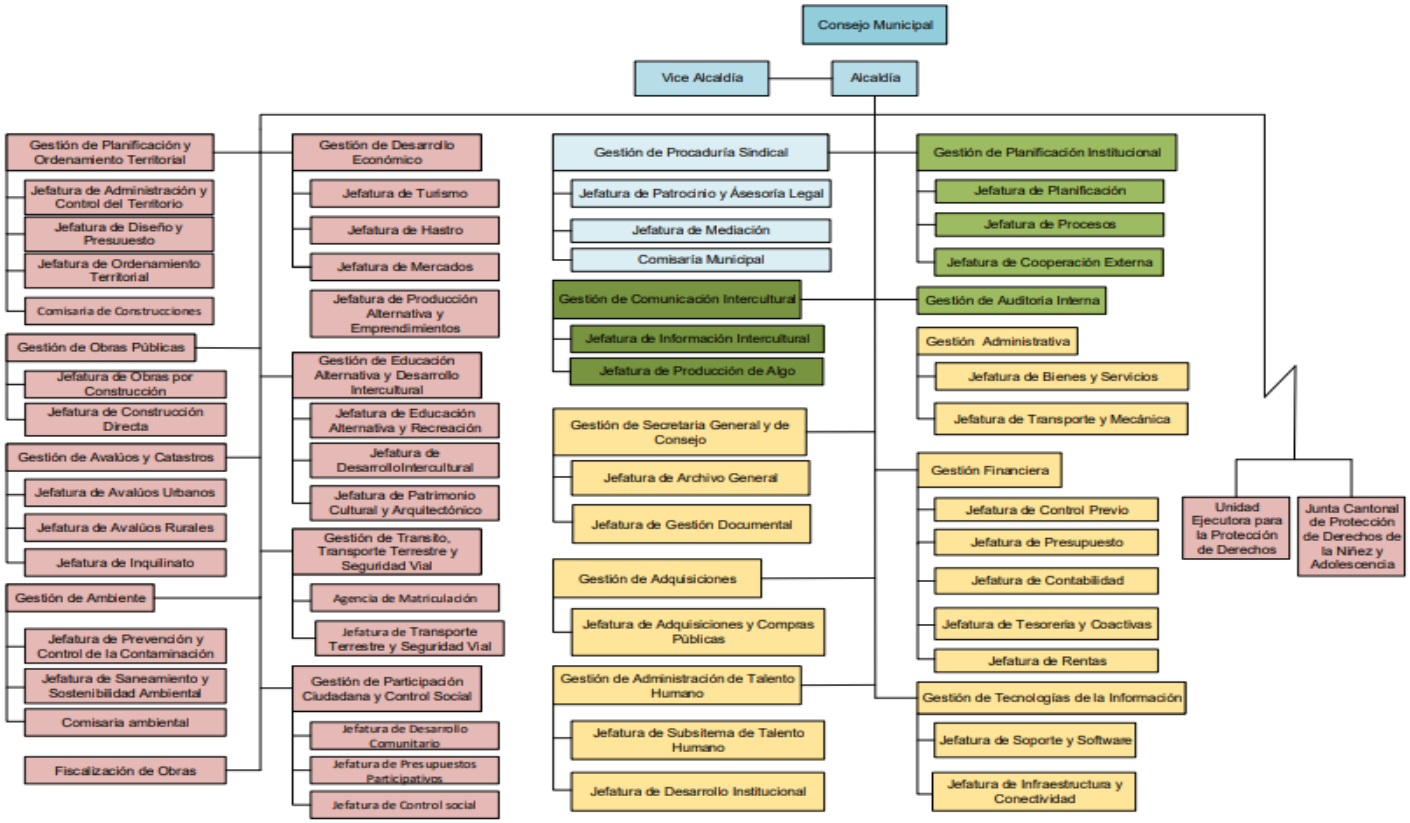
3 CAPÍTULO III: LEVANTAMIENTO DE INFORMACIÓN Y ESTADO ACTUAL DEL GADIP DEL MUNICIPIO DE CAYAMBE

El GADIP del municipio de Cayambe tiene varios departamentos cada una de ellas con sus respectivas funciones a cumplir, en la Figura 9 muestra la estructura de organizacional del GADIPMC y en la Figura 10 indica el departamento en el cual se llevará a cabo el diseño de SGSI, será en el área de Gestión de Tecnologías de la Información.

3.1 Estructura organizacional del GADIPMC

Figura 9

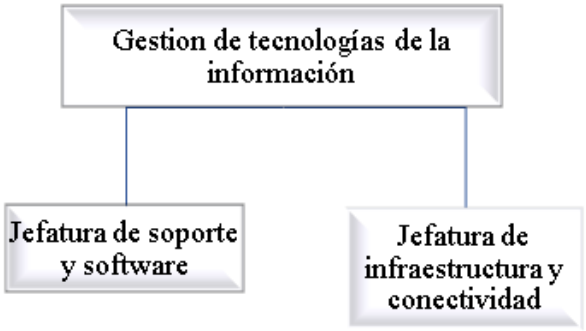
Organigrama del GADIPMC



Nota. Fuente GADIPM

Figura 10

Estructura Organizacional del Departamento de Tecnologías de la Información



Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

3.1.1 Departamentos que posee el GADIPMC

EL GADIPMC está conformado por varios departamentos en la cual denota en Tabla 16

Tabla 16

Departamentos del GADIPMC

Departamentos GADIPMC
Departamento de comunicación intercultural
Departamento financiero
Departamento Administrativo
Departamento de Adquisiciones
Departamento de Avalúos y Catastros
Departamento de Ambiente
Departamento de Desarrollo Económico
Departamento de Educación Alternativa y Desarrollo Intercultural

Departamento de Tránsito y Transporte Terrestre y Seguridad Vial	
Departamento de Planificación Institucional	
Departamento de Administración del Talento Humano	
Departamento de Tecnologías de la Información	

Nota. Fuente adaptada de Dirección de Administración y Talento Humano GADIPMC

3.1.2 Departamento de Tecnologías de la Información

Misión

Gestionar la dotación del servicio y soporte técnico para la infraestructura de tecnologías de la información y comunicación es mediante la adecuada adquisición y mantenimiento de equipos informáticos y de comunicaciones, diseñando y ejecutando las directrices estratégicas de Gestión de las Tecnologías de información y Comunicación, generando desarrollo de soluciones tecnológicas, de comunicaciones y la atención permanente de apoyo hacia los usuarios, para mantener la operatividad de la infraestructura tecnológica de la institución. En la Tabla 17 indica las atribuciones del departamento de Tecnologías de la Información.

Tabla 17

Atribuciones y Responsabilidades del Departamento de Tecnologías de la Información

	Atribuciones y Responsabilidades
Responsable	Director/a de Tecnologías de la información y Comunicación.
Nivel de Reporte	Alcalde del GADIPMC

Jerarquía del proceso	Habilitante de Apoyo
a)	Definir políticas, estándares y normativa en el ámbito tecnológico aplicables en el GADIPMC
b)	Asegurar el mejoramiento y automatización de los procesos, acorde con las necesidades institucionales y el desarrollo tecnológico disponible.
c)	Definir y mantener el modelo institucional de Datos.
d)	Definir las Políticas de Seguridad y controlar su aplicación.
e)	Asesorar a diferentes áreas del GADIPMC acerca de proyectos de innovación Tecnológica de Información y Comunicación (TIC)
f)	Aprobar las propuestas de solución a diferentes fallas, imprevistos o datos tecnológicos que afectan el normal desenvolvimiento tecnológico y de comunicaciones.
g)	Aprobar el Plan de contingencia tecnológica y sus actualizaciones según la situación actual y los requerimientos institucionales
h)	Disponer la gestión oportuna sobre la aplicación de medidas correctivas y/o preventivas de la utilización y funcionamiento de la tecnología informática de comunicaciones con la que dispone la institución.
i)	Autorizar la entrega de suministros e insumos para los equipos y periféricos informáticos.
j)	Dirigir y aprobar los términos de referencia para la elaboración de especificaciones técnicas para los proyectos de infraestructura de sistemas para la institución.
k)	Administrar la Base de Datos Institucional, garantizando la seguridad, integridad, oportunidad y disponibilidad de la

información.

l) Proponer y dar seguimiento a los contratos de desarrollo, mantenimiento y soporte técnico de aplicaciones informáticas de terceros.

m) Emite las directrices técnicas para la legalización de un estudio de mercado para la renovación y adquisición de equipos tecnológicos.

n) Coordinar la elaboración del presupuesto de TIC en base a los requerimientos tecnológicos de la institución.

o) Revisar y aprobar el plan de acción de soporte de la infraestructura tecnológica y de atención a los usuarios.

p) Planificar la instalación de software base y/o migración de hardware conforme los requerimientos institucionales.

q) Disponer la elaboración de las notificaciones a los usuarios sobre, claves y otros elementos para la operación de la infraestructura tecnológica.

r) Definir, Ejecutar y evaluar las posibles soluciones ante las vulnerabilidades de seguridad informática en la infraestructura y sistemas de la institución.

s) Generar productos tecnológicos bilingües

t) Elaborar y ejecutar el Plan Operativo Anual de la Dirección y realizar su seguimiento y;

u) Las demás asignadas por la máxima autoridad.

Nota. Fuente adaptada de Dirección de Administración y Talento Humano GADIPMC

3.1.3 Principales servicios que brinda el GADIPMC

El GADIP del municipio de Cayambe brinda los siguientes servicios a la Sociedad. En la Tabla 18 indica los diferentes servicios.

Tabla 18

Servicios que Brinda el GADIPMC

Servicios que Ofrece a la Ciudadanía
Impuesto Prediales
Pago del agua y basura
Uso del suelo
Estados de cuenta del Predial
Planos-Avalúos y catastros
Consultas de impuestos

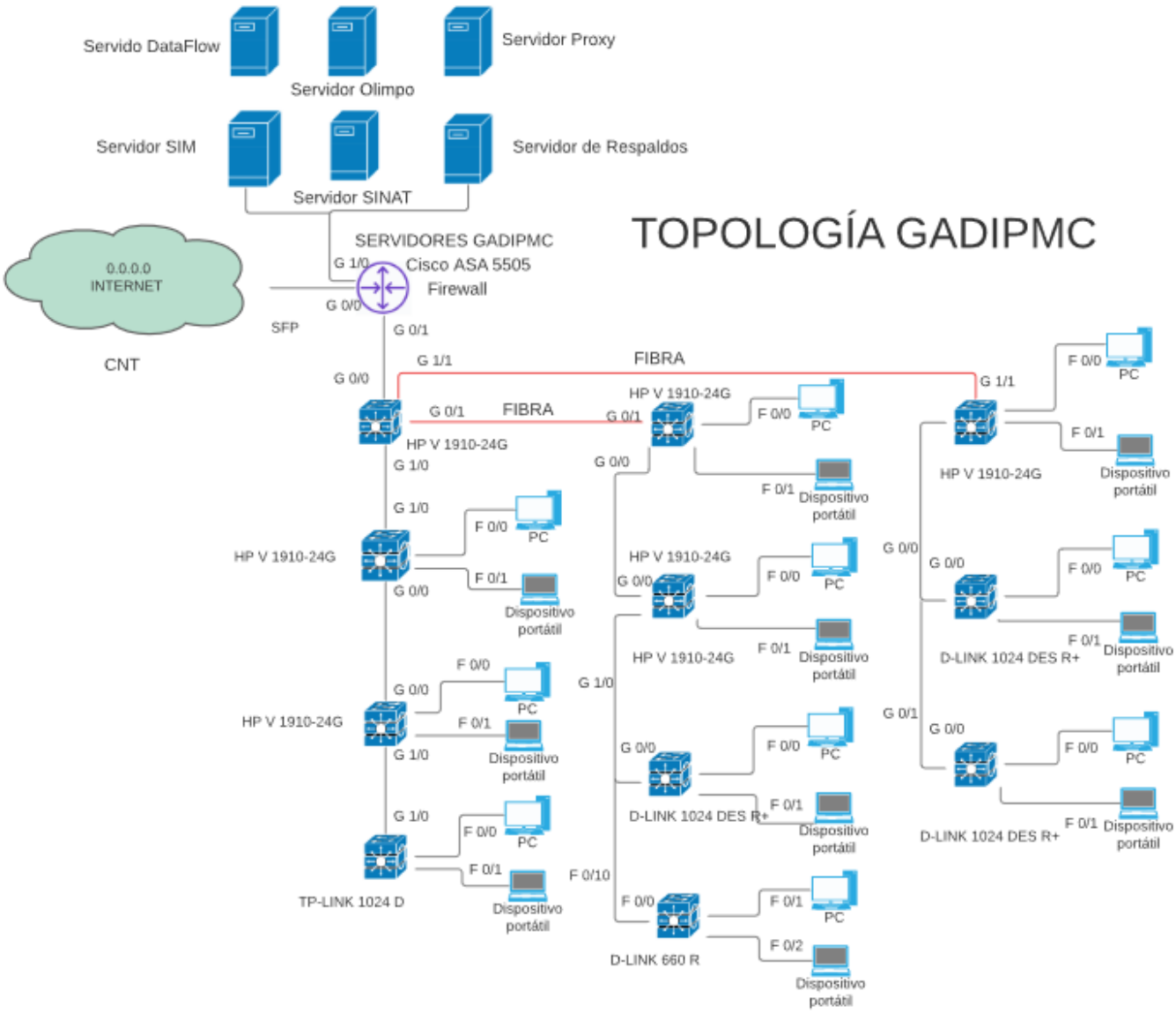
Fuente adaptada de: Dirección de Administración y Talento Humano.

3.2 Topología física de la red del GADIPMC

Equipos principales de la Red del GADIPMC, se detalla que el área de estudio es en la Dirección de Tecnologías de la Información del GADIPMC, pero se ha visto necesario generar la topología que tiene el GADIPMC como muestra en la Figura 11.

Figura 11

Topología de la Red GADIPMC



Nota. Fuente adaptada del Departamento de las TI GADIPMC

3.3 Direccionamiento IP

La dirección IP principal usada es la 172.24.0.0/21, pertenece a una dirección IPv4 privada de clase B, la cual se ha realizado la distribución adecuada para cada uno de las direcciones que posee el GADIPMC cada dirección IP será asignada de forma estática, en la Tabla 19 indica el direccionamiento IP para los departamentos de la institución.

Tabla 19

Distributivo de Direcciones IP

Direccionamiento IP			
Departamento	Red	Rango Asignable	Broadcast
Dirección de Avalúos y Catastros	172.24.0.0/26	172.24.0.1 - 172.24.0.62	172.24.0.63
Dirección Administrativa	172.24.0.64/26	172.24.0.65 - 172.24.0.126	172.24.0.127
Dirección de Participación Ciudadana y Control Social	172.24.0.128/26	172.24.0.129 - 172.24.0.190	172.24.0.191
Dirección Financiera	172.24.0.192/26	172.24.0.193 - 172.24.0.254	172.24.0.255
Alcaldía	172.24.1.0/27	172.24.1.1 - 172.24.1.30	172.24.1.31
Dirección de Planificación Institucional	172.24.1.32/27	172.24.1.33 - 172.24.1.62	172.24.1.63
Dirección de Comunicación Intercultural	172.24.1.64/27	172.24.1.65 - 172.24.1.94	172.24.1.95
Procuraduría Síndica	172.24.1.96/27	172.24.1.97 - 172.24.1.126	172.24.1.127
Secretaria General y de Concejo	172.24.1.128/27	172.24.1.129 - 172.24.1.158	172.24.1.159
Dirección de Tecnologías de la Información	172.24.1.160/27	172.24.1.161 - 172.24.1.190	172.24.1.191
Dirección de Administración del	172.24.1.192/27	172.24.1.193 -	172.24.1.223

Talento Humano		172.24.1.222	
Dirección de Planificación y Ordenamiento Territorial	172.24.1.224/27	172.24.1.225 - 172.24.1.254	172.24.1.255
Dirección de Desarrollo Económico y Turismo	172.24.2.0/27	172.24.2.1 - 172.24.2.30	172.24.2.31
Dirección de Educación Alternativa y Desarrollo Intercultural	172.24.2.32/27	172.24.2.33 - 172.24.2.62	172.24.2.63
Dirección de Ambiente	172.24.2.64/27	172.24.2.65 - 172.24.2.94	172.24.2.95
Dirección de Obras Públicas	172.24.2.96/27	172.24.2.97 - 172.24.2.126	172.24.2.127

Fuente adaptada de: Dirección de Tecnologías de la Información del GADIPMC

3.4 El Proveedor de Servicios de Internet

CNT brinda el servicio mediante dos hilos de fibra óptica, canales dedicados con un nivel de compartición 1:1 y la distribución de megas se la realiza de la siguiente manera como muestra la Tabla 20.

Tabla 20

Hilos de Fibra Óptica que Provee ISP CNT-EP

ISP CNT-EP		
Hilos de fibra	Velocidad	Uso Dedicado
1 Hilo de fibra	500 Mbps	Todas las direcciones y departamentos del GADIPMC
1 Hilo de fibra	150 Mbps	Compras Públicas

Nota. Fuente adaptada de Dirección de Tecnologías de la Información del GADIPMC

3.5 Data Center del GADIPMC (subsistemas)

El data center alberga equipos de comunicación, sistemas informáticos, sistemas de climatización, energía y seguridad, la conexión principal de proveedor de internet se distribuye a través de la Red local a los usuarios finales. En la tabla 21 indica todos los subsistemas y elementos de cada subsistema.

Tabla 21

Subsistemas del Data Center del GADIPMC

Subsistema	Parámetros del Subsistema
Telecomunicaciones	Cable horizontal y vertical
	Cuarto de entrada/oficina de dirección
	Áreas de distribución
	Medios de transmisión -fibra óptica y cable UTP Cat 6A
	2 hilos de fibra del proveedor de internet
	Elementos activos
	Carencia de switch de core
	Patch paneles
	Patch cord
	Documentación sobre certificación del cableado
	Carece de documentación detallada sobre cada servidor del GADIPMC

	Cableado de racks
	Carece redundancia entre equipos
Arquitectónico	Tipo de construcción
	Protección no inflamable
	Techo y piso falso
	Área UPS
	Control de acceso
	CCTV
Eléctrico	Cantidad de acceso
	Puntos únicos de falla
	Redundancia UPS
	Línea de interconexión eléctrica y UPS
	Puesta a tierra provisional no adecuada
	Generador de energía
Mecánico	Sistema de climatización
	Cañerías y drenajes
	Control HVAC detector de humo por aspiración ASD

Nota. Fuente: Dirección de Tecnologías de la Información del GADIPMC.

Para el ingreso al Data Center la puerta está acorde a los requerimientos como muestra la Figura 12, el cuál es una puerta de grandes dimensiones, con sus respectivos sensores magnéticos para abrir y cerrar la puerta.

Figura 12

Puerta del Data Center

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

A continuación, en la Figura 13 indica el ingreso del cableado sobre el piso falso, con eso se puede evidenciar que si cumplen con normativas de cableado estructurado

Figura 13

Piso Falso Acorde a la Normativa de Un Data Center

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC

En la Figura 14 se logra visualizar el ingreso del cable al techo falso, acorde a normativas de Data Center.

Figura 14

Techo Falso Acorde a Normativa de un Data Center

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

Para el acceso al Data Center, esta implementado un control de acceso mediante el registro de la huella dactilar, el cual solo personal autorizado tendrá acceso al mismo como muestra en la Figura 15.

Figura 15

Biométrico para acceso al Data Center

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

En la Figura 16 se logra verificar la señalética correspondiente donde muestra la salida del Data Center, se logra constatar que hay buenas prácticas por esa parte.

Figura 16

Señalética Adecuada que Indica la Salida del Data Center

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

En la Tabla 22 muestra todos los elementos que se encuentra en el Data Center GADIPMC.

Tabla 22

Elementos del Data Center del GADIPMC

Elementos del Data Center	Unidades	Detalles
Smart UPS RT 1500 VA marca APC	1	Implementado
UPS Tripp Lite de 2.2 KVA	1	Implementado
UPS Computer Power de 6 KVA	1	Implementado
Router inalámbrico cisco Small Business (provee WIFI equipo conectado a la red inalámbrica)	3	Implementado
Router Cisco system 800 s (proveedor de internet para red LAN interna y red inalámbrica)	1	Implementado
Aire acondicionado marca LG	1	Implementado

Router Cisco ASA 5505 S (VPN SIGTIERRAS)	1	Implementado
Switch Cisco 2960 S	5	Implementado
Switch HP v1910 -24 G	7	Implementado
Switch Cisco SF 100-24	6	Implementado
Switch HPE 1920 JL382A	4	Implementado
Servidores	6	Implementado
Patch panels para cable cat 6	9	Implementado
Patch cord	3	Implementado
Documentación sobre certificación del cableado	-	Si
Carece de documentación detallada sobre cada servidor del GADIPMC	-	Si
Cableado de racks	-	SI
Carece redundancia entre equipos	-	NO

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

Conmutadores (Switchs)

Los Switchs permiten la comunicación entre equipos dentro de la red interna del municipio, elemento que constituyen las redes de área local o LAN del GADIPMC. En la Tabla 23 indica los equipos conmutación. Y en la Tabla 24 detalla los principales servidores del municipio.

Tabla 23

Switchs que Posee el GADIPMC

Switch	Descripción del equipo
Cisco 2960 S	**Switch** administrable: si **Número de puertos:** 24

	Soporta AC/DC: solo AC **Capa de trabajo:** Capa 2 **Función que desempeña:** Realiza la interconexión de la Red interna (LAN) del municipio. Entre otros equipos, para dar el servicio a los distintos departamentos de la planta baja del GADIPMC
Switch HP v 1910 -24G	**Switch administrable**: si **Número de puertos:** 24 **Soporta AC/DC:** solo AC **Capa de trabajo:** Capa 3 **Función que desempeña:** Realiza la interconexión de la Red interna (LAN) del municipio. Entre otros equipos, para dar el servicio a los distintos departamentos de la planta alta del GADIPMC.
HPE 1920 JL382A	**Switch administrable:** si **Número de puertos:** 24 **Soporta AC/DC:** solo AC **Capa de trabajo:** Capa 3 **Función que desempeña:** Realiza la interconexión de la Red interna (LAN) del municipio. Entre otros equipos, para dar el servicio a los distintos departamentos de la planta alta de la institución. Equipo conectado al Backbone.
	Switch administrable: No

Cisco SF 100-24	**Número de puertos:** 24 **Soporta AC/DC:** solo AC **Capa de trabajo:** Capa 2 **Función que desempeña:** Realiza la interconexión de entre otros equipos (antenas), para dar el servicio de internet de manera inalámbrica a escuelas y parques.

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

Tabla 24

Principales Servidores del GADIPMC

Servidores	Características	
Servidor Olimpo	**Marca**	HP proliant DL 380G7
	Sistema Operativo	Microsoft Windows Server 2003
	Procesador	Intel® Xeon® Six-Core: E5649 (2.53GHz)
	Memoria RAM	Estándar 6 GB (3 x 2 GB) RDIMM en Modelo 633405-001
	Descripción del servidor	Sistema contable financiero Servidor de BD, trabaja con información referente al área de contabilidad, presupuesto, tesorería, coactivas, las recaudaciones y rentas, etc. Maneja datos de suma importancia.
Servidor SIM (Sistema de Información Municipal)	**Marca**	Lenovo system x3550 m5v
	Sistema Operativo	Microsoft Windows Server
	Procesador	Intel® Xeon® E5-2600 serie v4
	Memoria RAM	Memoria TruDDR4 SDRAM 64 GB (4Rx4, 1,2V)

	Descripción del servidor	Maneja los registros públicos municipales donde se administra la información esencial sobre particulares e inmuebles dentro del municipio. Presenta la información que los particulares necesitan saber para obtener alguna autorización o servicio público (Ejemplo: licencias, permisos, contratos, certificados, constancias, boletas de pago).
Servidor SINAT(Sigtierras)	**Marca**	DELL
	Sistema Operativo	Linux CentOS6
	Procesador	Intel® Xeon® Processor 3.00 GHz
	Memoria RAM	8 Gb
	Descripción del servidor	Servidor que administra los datos de levantamiento predial, para la construcción y actualización del catastro rural, contiene fotografías aéreas y ortofotográficas, e información que contribuya a la regularización de su tenencia y está ayude a llevar, una planificación del desarrollo y ordenamiento territorial a nivel del Ecuador.
Servidor de Proxy	**Marca**	DIKTA
	Sistema Operativo	Linux CentOS 6
	Procesador	Intel i7-3610QM 3,30 GHz
	Memoria RAM	8 Gb
	Descripción del servidor	Servidor que funciona como punto intermedio entre los empleados administrativos y la internet, este servidor realiza filtrados a ciertos contenidos que la organización considere como maliciosos o páginas que provoquen algún nivel de desconcentración, que afecte al rendimiento de los trabajadores del GADIPMC.
Servidor Dataflow	**Marca**	DIKTA
	Sistema Operativo	Microsoft Windows 7
	Procesador	Intel i7-3610QM 3,30 GHz

	Memoria RAM	8 Gb
	Descripción del servidor	Sistematiza procesos de seguimiento de trámites ingresados al GADIPMC, posee una interfaz muy intuitiva y fácil de usar.
Servidor de Respaldo	**Marca**	HP DL 380
	Sistema Operativo	Windows Server 2003
	Procesador	Intel Xeon 3.40 Ghz
	Memoria RAM	4 GB
	Descripción del servidor	Servidor donde se realizan respaldos de toda la información de otros servidores y activos de información muy importantes para el GADIPMC.

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC

Energía eléctrica

Cuenta con líneas directas tomadas desde un poste hasta el tablero de distribución de energía. Dentro de este tablero está realizada la conexión entre el sistema eléctrico común, el sistema de alimentación ininterrumpido (UPS) y un generador de eléctrico, en la Figura 17 muestra el tablero de distribución eléctrica

Figura 17

Tablero de distribución de energía del GADIPMC

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC

3.6 Sistema de alimentación ininterrumpido (UPS)

Son equipos que proveen energía de calidad de manera ininterrumpida siempre y cuando los respaldos sean de alta capacidad, usados para los principales servidores del GADIPMC y equipos de backbone. Los UPS están configurados en paralelo dentro del tablero de distribución de energía, con el fin de aumentar la seguridad y confiabilidad de energía. En la Tabla 25 muestra las características del UPS GADIPMC

Tabla 25

UPS que Posee el GADIPMC

UPS	Características Generales
Computer Power de 6KVA.	Tiene una pantalla LCD, controlador DSP, conversión de frecuencia 50/60 Hz y función de apagado de emergencia. Tiene arranque en frío desde baterías. Tiene puertos USB y RS-232. Comunicación a través de SNMP Cargador de baterías inteligente. Voltaje de salida seleccionable. Tiene baterías hot-swappable. Es compatible con generador.
UPS marca Tripp Lite de 2.2 KVA.	Elimina la distorsión armónica, y los impulsos eléctricos Soporta voltajes desde 80 V -hasta 150V Puerto USB y serial para comunicación Compatible con software de monitoreo y control Watchdog de tripp Lite Dos bancos de carga incorporados y

	controlables individualmente Posee 7 tomacorrientes.
Smart UPS RT 1500 VA marca APC.	Da notificaciones predictivas de falla Posee alarmas sonoras Compatible con generador Posee regulación de tensión y frecuencia Reemplazo de baterías en caliente Bypass interno automático Adaptabilidad para torre o rack Posee puerto serial para conectividad Indicadores de estado mediante leds

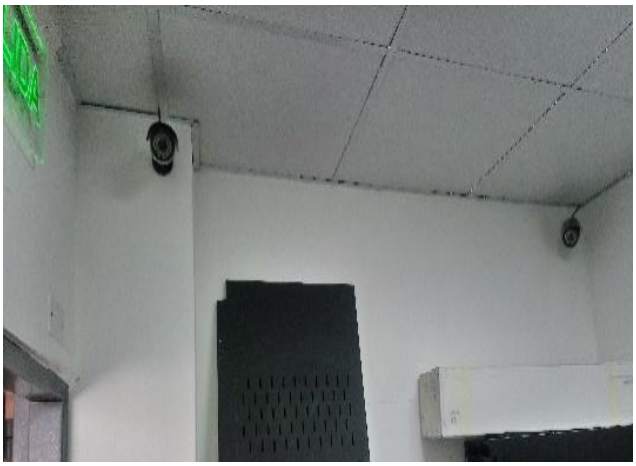
Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC

3.7 Cámaras de video vigilancia

Existen tres cámaras instaladas en puntos específicos, dentro del Data Center y en el área del Departamento de Tecnologías GADIPMC, el cual graba en todo momento, para su posterior revisión en caso de existir alguna situación extraña o pérdida de los equipos. En la Figura 18 muestra las cámaras instaladas y en la Figura 19 indica la distribución de las cámaras dentro de esa área, esa distribución se asemeja a la realidad y no he ha ubicado los demás puntos de cámaras debido a que solo se hará el estudio en el departamento de las TIC´s.

Figura 18

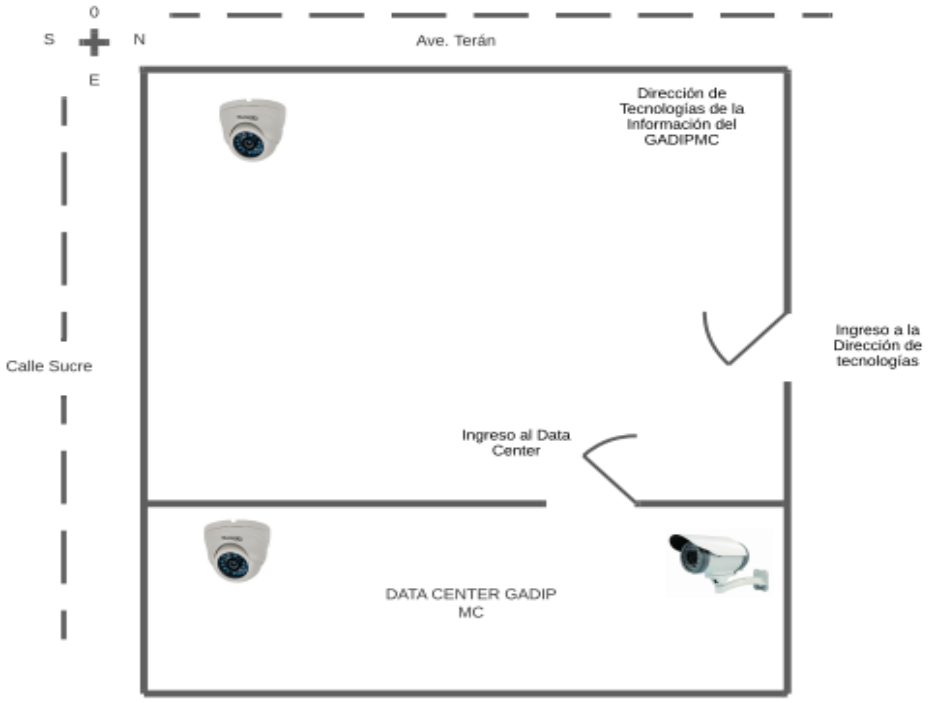
Cámaras de video vigilancia



Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

Figura 19

Cámaras de video vigilancia



Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

3.8 Sistema de Aire acondicionado

Encargado de mantener el ambiente en temperaturas adecuadas, para que cada equipo trabaje de forma eficiente, alargando la vida útil de los equipos de comunicación del Data Center del GADIPMC, en la Figura 20 indica el equipo de aire acondicionado que está siendo usado.

Figura 20

Sistema de aire acondicionado marca LG

Nota. Fuente Dirección de Tecnologías de la Información del GADIPMC.

4 CAPÍTULO IV: ANÁLISIS Y GESTIÓN DE RIESGOS

El presente capítulo contiene el análisis y gestión de riesgos del GADIPMC para ello se basa en la metodología MAGERIT, misma que busca identificar y mitigar posibles amenazas que puedan comprometer la disponibilidad, integridad y confidencialidad de la información municipal.

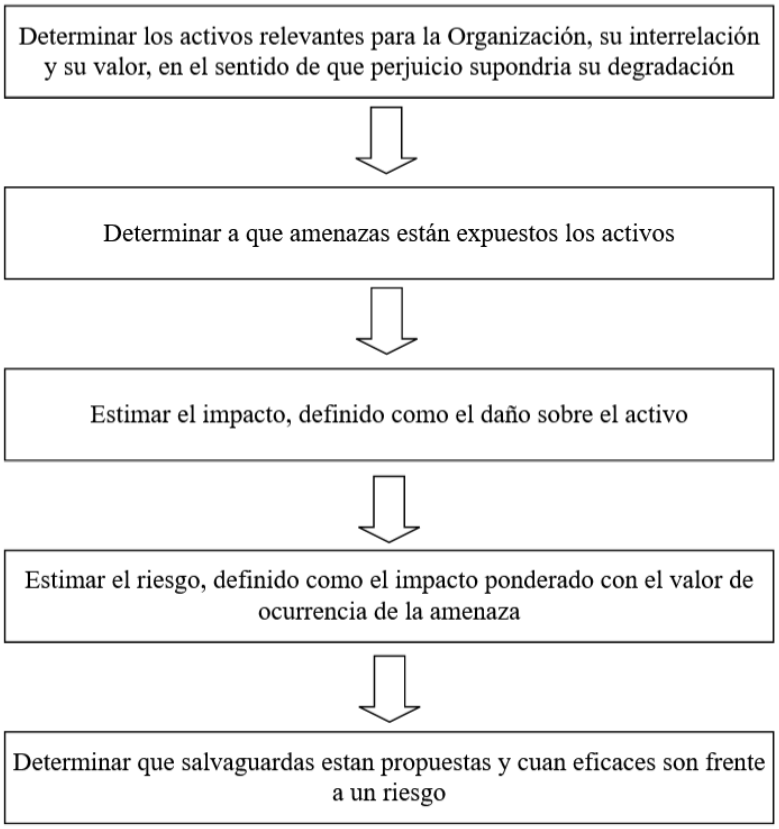
4.1 Análisis de Riesgos

Para determinar las estimaciones de vulnerabilidad ante posibles amenazas y el impacto que se pueda generar en el GADIPMC. Se usará la metodología Magerit V3, el análisis de riesgo permite evaluar y mejorar los criterios de seguridad logrando establecer una visión general sobre los elementos que pueden ocasionar una pérdida de valor de sus activos de información.

Dentro de Magerit el análisis de riesgo es un proceso metódico para determinar los riesgos siguiendo los siguientes pasos que muestra en la Figura 21.

Figura 21

Esquema para determinar los riesgos según MAGERIT



Nota. Adaptada de (DGMAPIAE, 2012a)

4.1.1 Activos

Siendo el activo un recurso valioso para la organización misma que puede sufrir algún tipo de ataque, sea de forma intencional o accidental con consecuencias negativas para la institución. Como parte del proceso se realiza la clasificación de los activos. En la Tabla 26 indica los tipos de activos según la metodología MAGERIT V3. En el capítulo 3 se llevó a cabo el levantamiento de información y en este nuevo capítulo se podrá clasificar y relacionar a qué grupo pertenece, con el fin de darle el tratamiento que corresponde.

Tabla 26

Tipos de Activos

Código	Tipo de Activo
[essential]	Activos Esenciales
[arch]	Arquitectura del sistema
[DI]	Datos/información
[K]	Claves criptográficas
[S]	Servicios
[SW]	Software / Aplicaciones informáticas
[HW]	Equipamiento informático(hardware)
[COM]	Redes de Comunicaciones
[Media]	Soportes de información
[AUX]	Equipamiento Auxiliar
[L]	Instalaciones
[P]	Personal

Nota. Adaptada de (DGMAPIAE, 2012a)

4.2 Valoración de los Activos

Para realizar la valoración de los activos es necesario partir como base, el triángulo de la seguridad informática que son: Disponibilidad, Integridad y Confiabilidad, en la Tabla 27 indica la escala general de los activos en cuanto al punto de vista de MAGERIT v3, escala GADIP y el análisis cualitativo.

Tabla 27

Criterio de Valoración de Activos

Escala Según Magerit	Escala Según GADIP MC	Escala Cualitativa	Criterio
1-2	1	**MB:** Muy Bajo	Daño menor
3-5	2	**B**: Bajo	Daño importante
6-8	3	**M**: Medio	Daño grave
9	4	**A**: Alto	Daño muy grave
10	5	**MA**: Muy alto	Daño extremadamente grave

Nota. Adaptado de (DGMAPIAE, 2012a)

La escala de referencia para el proyecto es la propuesta por el GADIPMC, siendo la misma que se hace relación entre la escala de MAGERIT y la cualitativa.

Confidencialidad

La información debe ser accesible sólo para las personas lícitas, evitando que los datos estén disponibles a personas no autorizadas, la escala está dada en la Tabla 28 siendo referente a la confidencialidad.

Tabla 28

Criterio de valoración con Respecto a la Confidencialidad

Valor	Escala Cualitativa	Criterio
1	Despreciable	Es totalmente irrelevante, no aplica
2	Bajo	La divulgación de la información, no impacta de forma negativa la institución.

3	Medio	El daño es leve, el incidente se limita en una sola área de la institución.
4	Alto	El acceso a la información de forma no autorizada comprometería a varias áreas de la institución.
5	Muy alto	La divulgación de información que tiene el GADIPMC, afectaría de forma negativa a la imagen institucional, generando desconfianza, disminuyendo la credibilidad de toda la organización.

Nota. Adaptado de (DGMAPIAE, 2012b)

Integridad

Respaldo que la información no sufre algún tipo de alteración, que atente a la veracidad y credibilidad de los datos, en la tabla 29 muestra el valor con respecto a la integridad.

Tabla 29

Criterio de Valoración con Respecto a la Integridad

Valor	**Escala Cualitativa**	**Criterio**
1	Muy bajo	La pérdida de este activo no impacta de forma negativa a la institución. Resulta irrelevante.
2	Bajo	La modificación de este activo generaría daños menores, no impacta de forma negativa la institución.

3	Medio	La veracidad de los datos tiene que ser al menos en un 50%, la alteración de este activo afecta levemente al GADIPMC.
4	Alto	Al menos se necesita que la información sea verídica en un 75%, afectaría a procesos internos que realiza la institución.
5	Muy alto	Estos activos no pueden sufrir alguna modificación del contenido, La alteración del activo impacta de forma negativa a la institución. La información debe ser verdadera en un 99.9%

Nota. Fuente adaptada de: (DGMAPIAE, 2012b)

Disponibilidad

Asegura la accesibilidad a los activos por parte de usuarios autorizados, en la tabla 30 detalla la valoración en cuanto a disponibilidad.

Tabla 30

Criterio de Valoración con Respecto a la Disponibilidad

Valor	**Escala Cualitativa**	**Criterio**
1	Muy bajo	Irrelevante a efectos prácticos
2	Bajo	La no disponibilidad o ausencia del activo NO impacta de forma negativa la institución.
		La ausencia o no disponibilidad de este activo impacta levemente a la Institución,

3	Medio	este activo debe estar disponible al menos en un 50% de su totalidad.
4	Alto	Daño grave, la no disponibilidad del activo afectaría varias áreas del GADIPMC, retrasando los procesos internos que realiza la institución. Este activo debe estar disponible al menos el 75% de su totalidad.
5	Muy alto	Daño muy grave, la ausencia o no disponibilidad del activo impacta de forma negativa a la Institución, se necesita que el activo esté disponible al menos el 99%.

Nota. Fuente adaptada recuperado de (DGMAPIAE, 2012b)

En base a los datos de las tablas 26, 27, 28, 29 y 30 se procede a identificar y valorar conforme a la confidencialidad, integridad y disponibilidad a cada uno de los activos que posee el Departamento de Tecnologías del GADIPMC, al realizar el levantamiento de información los datos recopilan en una tabla (véase anexo 2)

En base al libro de MAGERIT, el valor de los activos es igual a la sumatoria de su valor por disponibilidad, integridad y confidencialidad, este resultado viene a ser el valor para cada activo. El resumen se denota en la Tabla 31.

Tabla 31

Valoración de los Activos Referentes a CID (Confidencialidad, Integridad y Disponibilidad

Nombre	Tipo	Valor total
Servidor Olimpo	[SW]	14
Servidor SIM	[SW]	14
Servidor SINAT	[SW]	14
Servidor Proxy	[SW]	9
Servidor de respaldos	[SW]	13
Software de Virtualización de servidores	[SW]	13
Servidore de Telefonia IP	[SW]	10
Servido Data Flow	[SW]	9
Switch Cisco 2960	[HW]	14
Router Cisco ASA 5505	[HW]	14
Servidor de máquinas virtuales	[HW]	7
Switch HP v1910-24 G	[HW]	14
Switch Cisco SF 100-24	[HW]	14
Chasis Blade	[HW]	8
Equipo de Seguridad perimetral	[HW]	13
Switch HPE 1920 JL382A	[HW]	12
Enlace Fibra	[COM]	14
Enlace mercado diario	[COM]	11
Edificio Jarrín	[COM]	11
Enlace Comercial Popular	[COM]	14
Enlaces Repetidores	[COM]	12
Aire acondicionado	[AUX]	7
UPS	[AUX]	11
Generador eléctrico	[AUX]	7
Servicio de teléfono convencional	[S]	4
Servicio de internet	[S]	11
Servidor de correo Institucional	[S]	7
Servidor DNS	[S]	11
Servidor Web	[S]	14
Acceso Remoto a Servidores	[S]	13
Servicio de antivirus	[S]	5

Disco Duro 1 TB	[S]	13
Flash Memory	[S]	12

Nota. Fuente adaptada del GADIPMC

Dentro de la organización es necesario conocer las posibles amenazas que pueden afectar a los activos de información, a continuación, se presentan unas tablas para cada amenaza existente, luego de todo el proceso se tendrá que generar una tabla con todas las amenazas por cada activo y con eso se definirá los riesgos para cada uno de ellos.

4.3 Desastres naturales

Daños que pueden suceder sin necesidad de intervención de los seres humanos, son de origen accidental. En la Tabla 32 indica la valoración con respecto a desastres naturales, para una mejor comprensión de las tablas se marcará un valor de "X" como se detalla en las tablas anteriores y estará vacío en donde no aplica la amenaza.

Tabla 32

Criterio de Valoración con Respecto a Desastres Naturales

Amenaza Desastres Naturales **Origen:** Natural (accidental)		**Tipos de Activos**											
		Datos / Información [DI]			Servicios [S]			Software- Aplicaciones informáticas [SW]			Equipos Informáticos [HW]		
Cod	**Des**	C	I	D	C	I	D	C	I	D	C	I	D
N.1	Fuego			x			x			x			x
N.2	Daños por agua			x			x			x			x
N.*	Desastres Naturales			x			x			x			x

Nota. Fuente adaptada de (DGMAPIAE, 2012b)

4.4 Amenaza Industrial

Acontecimientos que pueden ocurrir de forma accidental, originándose de las principales actividades industriales causadas de forma deliberada, afectando a varios niveles de la organización, acabando con los recursos de información. En la tabla 33 indica los activos que podrían ser afectados según la amenaza industrial.

Tabla 33

Criterio de Valoración con Respecto a Amenaza Industrial

Amenaza Industrial **Origen:** Entorno (accidental), Humano (accidental o deliberado)		**Tipos de Activos**											
		Datos / Información [DI]			Servicios [S]			Software- Aplicaciones informáticas [SW]			Equipos Informáticos [HW]		
Cod	**Des**	C	I	D	C	I	D	C	I	D	C	I	D
L.1	Fuego												X
L.2	Daños por agua												X
L.*	Desastres industriales												X
L.3	Contaminación mecánica												X
L.4	Contaminación electromagnética												X
L.5	Avería Física/Lógica												X
L.6	Corte eléctrico												X
L.7	Condiciones inadecuadas												X
L8	Fallo servicios comunicación												X
L.9	Interrupción servicios												X

L.10	Degradación soportes almacenamiento	X
L.11	Emanaciones electromagnéticas	X

Nota. Fuente adaptada de (DGMAPIAE, 2012b)

4.5 Errores y fallos no intencionados

Amenazas que son deliberadas, tiene un gran parecido a los errores no mal intencionados generados por las personas dentro de la organización, en la Tabla 34 detalla la valoración en cuanto a fallos no intencionados

Tabla 34

Criterio de Valoración a Fallos no Intencionados

Amenaza Errores y fallos no intencionados **Origen:** Humano (accidental)		**Tipos de Activos**											
		Datos / Información [DI]			Servicios [S]			Software- Aplicaciones informáticas [SW]			Equipos Informáticos [HW]		
Cod	**Descripción**	C	I	D	C	I	D	C	I	D	C	I	D
E.1	Errores de los usuarios	X	X	X	X	X	X	X	X	X			
E.2	Errores del administrador	X	X	X	X	X	X	X	X	X	X	X	X
E.3	Errores de monitorización		X			X							
E.4	Errores de configuración		X			X							
E.8	Difusión de software dañino							X	X	X			X
E.9	Errores de encaminamiento				X	X	X	X	X	X			X
E.10	Errores de secuencia								X				X
E.14	Escapes de información			X					X				
E.15	Alteración accidental de la información		X			X			X				
E.18	Destrucción de la información	X	X	X	X			X	X	X			

E.19	Fugas de información	X	X	X	X	X	X	X	X	X		
E.20	Vulnerabilidades de los programas							X	X	X		
E.21	Errores de mantenimiento/actualización de programas					X	X	X	X	X		
E.23	Errores de mantenimiento/actualización de equipos								X	X		X
E.24	Caída del sistema por agotamiento de recursos			X			X			X		
E.25	Pérdida de equipos											X

Nota. Fuente adaptada de (DGMAPIAE, 2012b)

4.6 Ataques Intencionados

Acciones no éticas causadas por las personas, cuyo fin es satisfacer necesidades propias del individuo, sin importar las graves consecuencias que pueda provocar en la institución. En la Tabla 35 indica los ataques presentados en los activos.

Tabla 35

Criterio de Valoración a Ataques Intencionados

Amenaza Ataques intencionados **Origen:** Humano (deliberado)		**Tipos de Activos**											
		Datos / Información [DI]			Servicios [S]			Software-Aplicaciones informáticas [SW]			Equipos Informáticos [HW]		
Cod	**Des**	C	I	D	C	I	D	C	I	D	C	I	D
A.3	Manipulación de los registros de actividad		X		X			X					
A.4	Manipulación de la configuración	X	X	X			X	X	X	X			X
A.5	Suplantación de la identidad del usuario		X	X		X	X		X	X			
A.6	Abuso de privilegios de acceso	X	X	X	X	X	X	X	X	X	X	X	X

A.7	Uso no previsto				X	X	X	X	X	X	X	X	X
A.8	Difusión de software dañino							X	X	X			
A.9	[Re]-encaminamiento de mensajes						X			X			
A.10	Alteración de secuencia					X			X				
A.11	Acceso no autorizado		X	X		X	X		X	X		X	X
A.13	Repudio			X		X				X			
A.15	Modificación deliberada de la información		X			X			X				
A.18	Destrucción de la información	X		X	X			X		X			
A.19	Divulgación de información	X			X			X		X			
A.22	Manipulación de programas							X	X	X			
A.23	Manipulación de los equipos										X	X	X
A.24	Denegación de servicio			X			X			X			
A.25	Robo									X			X
A.26	Ataque destructivo			X			X				X		

Nota. Fuente adaptada de (DGMAPIAE, 2012b)

4.7 Correlación entre errores y ataques

Los errores y los ataques siempre van a la par, tanto que se pueden realizar las siguientes combinaciones:

Las amenazas que solo pueden ser errores, nunca ataques deliberados

Amenazas que nunca son errores, siempre son ataques deliberados con fines destructivos

Amenazas que pueden producirse tanto por error como deliberadamente. En la tabla 36 detalla las amenazas que pueden afectar a los activos.

Tabla 36

Clasificación de la gravedad de las vulnerabilidades

Número	Error	Ataque
1	Error de los usuarios	
2	Error del administrador	
3	Error de monitorización (log)	Manipulación de los registros de actividad
4	Error de configuración	Manipulación de la configuración
5		Suplantación de identidad
6		Abuso de privilegios de acceso
7		Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Error de [re]-encaminamiento	[Re]-encaminamiento de mensajes
10	Error de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico

13		Repudio
14	Escape de información	Interceptación de información (escucha)
15	Alteración accidental de la información	Modificación deliberada de la información
18	Destrucción de información	Destrucción de información
19	Fugas de información	Revelación de información
20	Vulnerabilidad de los programas	
21	Errores de mantenimiento/ actualización de programas(software)	
22		Manipulación de programas
23	Error de mantenimiento / actualización de equipos (hardware)	Manipulación de equipos
24	Caída de sistema por agotamiento de recursos	Denegación de servicios
25	Pérdida de equipos	Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal

29	extorsión
30	Ingeniería social(picaresca)

Nota. Fuente adaptada de (DGMAPIAE, 2012b)

4.8 Determinación del impacto

Es el impacto potencial a la medida del daño sobre el activo derivado de la materialización de una amenaza (MAGERIT – versión 3.0, 2012). Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es el impacto directo que éstas tendrán sobre el sistema. En la Tabla 37 indica la escala a usar para la valoración de la magnitud del impacto y riesgo.

Tabla 37

Escala cualitativa y cuantitativa de la Magnitud de Impacto y Riesgo

Escala cualitativa	Detalle	Escala cuantitativa
MB	Muy bajo	1
B	Bajo	2
M	Medio	3
A	Alto	4
MA	Muy alto	5

Nota. Adaptado de (DGMAPIAE, 2012a)

El impacto se puede calcular con esta tabla de doble entrada

4.9 Degradación

Cuán perjudicado resultaría el valor del activo. La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como

una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". En la Tabla 38 indica cómo determinar el impacto partir de la degradación y el valor del activo

Tabla 38

Tabla para Determinar Estimación del impacto

Impacto		**Degradación**		
		1%	**10%**	**100%**
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Nota. Adaptado de (DGMAPIAE, 2012a)

Estimación del riesgo

Para un mejor entendimiento se detalla en la Tabla 39, la escala a manejar en cuanto a impacto, probabilidad y riesgo.

Tabla 39

Escalas cualitativas y cualitativa para un análisis entre Impacto, Probabilidad y el Riesgo

Escala cualitativa			**Escala cuantitativa**
Impacto	**Probabilidad**	**Riesgo**	**Escala a usar**
MA: Muy alto	**MA:** Prácticamente seguro	**MA**: Crítica	5
A: Alto	**A**: Probable	**A**: Importante	4
M: Medio	**M**: Posible	**M**: Apreciable	3
B: Bajo	**B**: Poco probable	**B**: Bajo	2

MB: Muy bajo	**MB**: Muy raro	**MB**: Despreciable	1

Nota. Fuente adaptado de (DGMAPIAE, 2012a)

Una vez establecido las escalas se puede realizar combinaciones de las tablas para un mejor análisis de los riesgos, en conjunto con el impacto y la probabilidad de ocurrencia, en la Tabla 40 muestra la combinación y relación entre las mismas y aquellos activos que reciban una calificación de muy alto (MA) deberían ser objeto de atención inmediata.

Tabla 40

El cálculo para encontrar el Riesgo mediante la combinación del impacto y la 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

Nota. Adaptado de (DGMAPIAE, 2012a)

Es importante entender el alcance completo de las decisiones y eventos en un contexto económico, social o ambiental, ayudando a los planificadores y responsables de políticas a tomar decisiones más informadas y anticipar tanto los beneficios como los posibles efectos secundarios negativos. El cálculo de la estimación del impacto se puede realizar con una tabla de doble entrada. El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo:

4.10 Cálculo de Riesgo

La fórmula tradicional de cálculo del riesgo está definida en función del impacto y la probabilidad:

Riesgo=Probabilidad×Impacto

Sin embargo, esta fórmula no siempre tiene en cuenta todos los factores contextuales que pueden influir en la gravedad del riesgo. Una de las principales limitaciones de la formulación tradicional es su incapacidad para tener en cuenta factores adicionales que pueden ser importantes en determinados contextos. La importancia de un recurso en términos de su valor estratégico para la organización no siempre se refleja plenamente en términos de probabilidad e impacto únicamente. Introducción de la Valoración independiente del activo, para abordar esta limitación, se propone la fórmula extendida para el cálculo del riesgo

El cálculo del riesgo se lo realizará mediante la siguiente fórmula:

Riesgo= Probabilidad*Impacto+Valoración

En esta formulación, la "valoración" es una medida adicional que puede incluir factores como la importancia estratégica del activo, el costo de contención y la percepción del riesgo por parte de las partes interesadas. Esta clasificación se puede calcular mediante un método ponderado basado en entrevistas, encuestas y análisis cualitativos. Incluir evaluaciones adicionales permite una evaluación de riesgos más completa. Capta factores contextuales que pueden ser importantes a la hora de tomar decisiones estratégicas.

Los riesgos no se pueden eliminar, solo mitigar, es por ello que se establece un nivel de tolerancia, en la Tabla 41 muestra el valor a los riesgos y el valor aproximado para cada uno de ellos.

Tabla 41

Nivel de Tolerancia

Tolerancia	**Rango**
Totalmente tolerable (TT)	0-15

Regularmente tolerable (RT)	16-24
No tolerable (NT)	25-40

Nota. Fuente adaptada de (DGMAPIAE, 2012a)

Se enlista en una tabla general (véase anexo 3) en el cual indica los activos el riesgo de cada uno de ellos, se obtiene el valor de las no tolerancias y se toma criterios para la selección de las políticas de seguridad de la información cada una respectivamente con su control, en la Tabla 42 muestra el filtrado de las no tolerancias identificadas, las cuales deberán ser mitigadas, transferidas o eliminadas.

Tabla 42

Nivel no Tolerancias de los Activos del GADIPMC

Nombre /Activo	Valor	Descripción	Probabilidad	Impacto	Riesgo	Tolerancia
SW-SVR-OLIMPO	14	Avería de origen físico o lógico	3	4	26	NT
		Acceso no autorizado	3	4	26	NT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
SW-SVR-SIM	14	Avería de origen físico o lógico	3	4	26	NT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
SW-SVR-SINAT	14	Avería de origen físico o lógico	3	4	26	NT
		Abuso de privilegios de acceso	3	4	26	NT
		Acceso no autorizado	3	4	26	NT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
SW-SVR-RESPALDO	13	Modificación deliberada de la información	4	4	29	NT
		Avería de origen físico o lógico	3	4	25	NT
		Destrucción de información	4	4	29	NT
HW-SW-CSC-	13	Fuego	3	4	25	NT

ACC		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
HW-RT-CSC	13	Fuego	3	4	25	NT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
HW-SW-HP-24	13	Fuego	3	4	25	NT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
HW-SW-CSC-24SF	13	Fuego	3	4	25	NT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
HW-SW-HPE	12	Corte del suministro eléctrico	4	4	28	NT
COM-ENLACE-FIBRA	14	Fallo de servicios de comunicaciones	4	4	30	NT
S-INTERNET	11	Fallo de servicios de comunicaciones	4	5	31	NT

Siguiendo con el proceso de gestión de riesgo se pasa a revisar las salvaguardas.

4.11 Nivel de madurez

Para reducir o enfrentar a los riesgos, es necesario conocer el grado de desarrollo y efectividad de una medida de protección o control. En la tabla 43 se muestra los niveles la eficacia o nivel de madurez de las salvaguardas.

Tabla 43

Niveles de Madurez

Eficacia	Nivel	Tipo de activo	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicia/ad hoc	Iniciando
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado

90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Nota. Fuente adaptada de: (DGMAPIAE, 2012a)

4.12 Salvaguardas propuestas

Las salvaguardas propuestas son basadas en los criterios de la Tabla 42, actualmente en el municipio no cuentan con una documentación adecuada sobre salvaguardas, es por eso que mediante el análisis se hará la recomendación de alguna de ellas con el objetivo de proteger los activos de la institución pública. Estas medidas pueden incluir controles técnicos, procedimientos operativos, prácticas de gestión y otros elementos que ayudan a mitigar riesgos y mantener la seguridad de la información. En la Tabla 44 muestra las salvaguardas propuestas.

Tabla 44

Salvaguardas propuestas para el GADIPMC

Salvaguardas para el GADIPMC		
Seguridad de la información	**Descripción**	**Nivel de madurez**
Control de acceso	Implementar sistemas de autenticación y autorización para acceder a redes y sistemas municipales.	L2
	Utilizar contraseñas robustas, autenticación de dos factores (2FA) y controles de acceso basados en roles (RBAC).	L1
Copias de seguridad	Realizar copias de seguridad regulares de datos críticos y almacenarlas en ubicaciones seguras, tanto localmente como en la nube	L2
	Probar periódicamente la restauración de copias de seguridad para asegurar su eficacia.	L2
Protección contra malware	Instalar y actualizar regularmente software antivirus y antimalware.	L0
	Implementar políticas de seguridad para el uso de dispositivos externos y correos electrónicos	L0

	Capacitación en Seguridad de la Información: Impartición de programas de capacitación en seguridad de la información para empleados municipales, incluyendo concienciación sobre phishing, manejo seguro de contraseñas y buenas prácticas de seguridad en el uso de sistemas informáticos	L0
Cifrado de datos	Cifrar datos sensibles tanto en tránsito como en reposo.	L0
	Utilizar certificados SSL/TLS para asegurar las comunicaciones web.	L1
Seguridad física	**Descripción**	**Nivel de madurez**
Controles de acceso físico	Implementar sistemas de control de acceso para edificios municipales, como tarjetas de identificación y lectores biométricos.	L4
	Monitorear entradas y salidas con cámaras de seguridad y guardias de seguridad.	L4
Protección de Infraestructura Crítica	Asegurar instalaciones esenciales como plantas de tratamiento de agua, estaciones eléctricas y centros de datos con medidas de seguridad adicionales.	L3
Continuidad del servicio	**Descripción**	**Nivel de madurez**
Plan de Continuidad del Negocio (BCP)	Desarrollar y mantener un BCP para asegurar que los servicios críticos puedan continuar operando en caso de una interrupción.	L0
	Realizar simulacros y pruebas del BCP para asegurar su eficacia.	L0
Plan de Recuperación ante Desastres (DRP)	Implementar un DRP para restaurar sistemas y servicios críticos después de un desastre.	L0
	Mantener un inventario actualizado de recursos y un plan claro de roles y responsabilidades.	L1
Educación y Concienciación	**Descripción**	**Nivel de madurez**

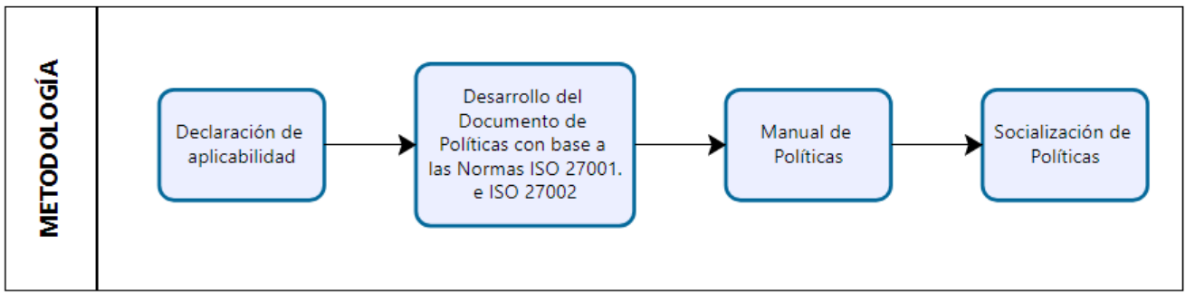
Formación en Seguridad	Proveer formación regular a los empleados sobre mejores prácticas de seguridad de la información, cómo reconocer ataques de phishing y otras amenazas comunes.	L2
Concienciación Comunitaria	Realizar campañas de concienciación para informar a la comunidad sobre cómo protegerse y reportar incidentes de seguridad.	L1
Políticas y Procedimientos	**Descripción**	**Nivel de madurez**
Políticas de Seguridad	Establecer políticas claras sobre el uso de tecnología, manejo de datos y comportamiento esperado de los empleados en relación con la seguridad.	L0
Procedimientos de Respuesta a Incidentes	Desarrollar y mantener procedimientos para la identificación, análisis y respuesta a incidentes de seguridad.	L0
	Designar un equipo de respuesta a incidentes y entrenarlo regularmente.	L0

5 CAPÍTULO V: DISEÑO DEL SGSI

Este capítulo contiene la metodología que se propone para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) para el GADIP del municipio de Cayambe el cual se basa en un enfoque sistemático y adaptable, teniendo en cuenta las características específicas del municipio de Cayambe, en base al análisis y gestión de riesgos se seleccionan los controles referentes a la norma ISO 27001, tomando en cuenta el nivel de la no tolerancia que indica la tabla 37 y en base a las salvaguardas propuestas en la Tabla 39. En la figura 22 indica el esquema de la metodología para el GADIPMC.

Figura 22

Metodología para el GADIPMC



Para la selección de los controles, se debe tener en cuenta lo siguiente:

Los controles de seguridad dependen del criterio y decisión de la organización y deberán cubrir la necesidad específica de la misma, partiendo de la aceptación del riesgo y el tratamiento del mismo, los objetivos de control y controles parten de los resultados obtenidos después de realizar el análisis y gestión de riesgos en el capítulo anterior.

5.1 Declaración de Aplicabilidad (SoA) del Municipio de Cayambe

La Declaración de Aplicabilidad (SoA) del GADIPMC especifica los controles de seguridad seleccionados para el Sistema de Gestión de Seguridad de la Información (SGSI) según ISO/IEC 27001. Este documento incluye todos los procesos, sistemas y recursos de

información relacionados con la administración de la institución, servicios de infraestructura y la justificación, la inclusión o exclusión de cada control, asegurando que el control se implemente adecuadamente para proteger la información y cumplir con los requisitos legales, regulatorios y operativos específicos del municipio, en la Tabla 45 muestra los controles que se han elegido, y para reconocer los controles que se han excluido revisar el anexo 4.

Tabla 45

Tabla de Declaración de aplicabilidad para el GADIPMC

Identificador de control	**Control ISO/IEC 27001**	**Aplicabilidad**	**Justificación**
5.1	Políticas de seguridad de la información	Aplica	Las políticas de seguridad de la información y las políticas específicas del tema se definen y aprueban por la dirección, se publican, se comunican y se reconocen por los empleados relevantes y las partes interesadas relevantes y se implementan a intervalos planificados y cuando hay cambios en los mismos
5.3	Segregación de funciones	Aplica	Deben mantenerse separadas las obligaciones conflictivas y las áreas de responsabilidad.
5.4	Responsabilidades de la dirección	Aplica	De acuerdo con la política de seguridad de la información establecida por la organización y las políticas y procedimientos específicos del tema, la gerencia debe exigir que todos los

			empleados apliquen la seguridad de la información.
5.7	Inteligencia de amenazas	Aplica	Para crear inteligencia de amenazas, se recopila y analiza información sobre amenazas a la seguridad de la información.
5.9	Inventario de la información y otros activos asociados	Aplica	Es necesario crear y mantener un inventario de información, así como de cualquier otro activo relacionado.
5.12	Clasificación de la información	Aplica	Sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes que indiquen las partes interesadas. La información se clasifica de acuerdo con las necesidades de seguridad de la información de la organización.
5.13	Etiquetado de la información	Aplica	Usando el esquema de clasificación de la información de la organización como guía, se debe crear y poner en práctica un conjunto adecuado de procedimientos para etiquetar la información.

5.15	Control de acceso	Aplica	Con base en las necesidades del negocio y la seguridad de la información, se desarrollarán e implementarán pautas para regular el acceso físico y lógico a los datos y otros activos relacionados.
5.17	Información de autenticación	Aplica	Debe existir un proceso de gestión para regular cómo se distribuye y gestiona la información de autenticación, y también debe incluir la formación del personal sobre cómo manejarla correctamente.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	Los eventos de seguridad de la información deben ser evaluados por la organización antes de ser etiquetados como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	Aplica	Los incidentes relacionados con la seguridad de la información deben manejarse de acuerdo con los procedimientos formales.
5.34	Privacidad y protección de la información personal	Aplica	La organización debe identificar y cumplir los requisitos pertinentes. Mantener la privacidad y proteger la información de identificación personal de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

5.37	Procedimientos operativos documentados	Aplica	Los procedimientos operativos de las instalaciones de procesamiento de información, deben ser registrados y puestos a disposición de los miembros del personal que los requieran.
6.3	Concienciación, educación y formación en materia de seguridad de la información	Aplica	Se debe proporcionar al personal de la institución y a las partes interesadas pertinentes, la concientización, la educación y la capacitación adecuada en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema.
6.7	Trabajo a distancia	Aplica	Las medidas de seguridad se implementan cuando los empleados trabajan de forma remota para proteger los datos que se manejan, procesan o almacenan externamente.
8.3	Restricción de acceso a la información	Aplica	De acuerdo con la política de control de acceso específica de la materia establecida, se restringirá el acceso a la información y otros activos relacionados.

8.5	Autenticación segura	Aplica	Las técnicas y los procedimientos de autenticación segura se implementan en función de las restricciones de acceso a los datos y las políticas de control de acceso basadas en el sujeto.
8.7	Protección contra el malware	Aplica	Al concienciar a los usuarios, se implementará y respaldará la protección contra malware.
8.22	Filtrado WEB	Aplica	Los servicios de información, usuarios y grupos de sistemas de información deben estar aislados en la red de la organización.
8.23	Segregación en redes	Aplica	El acceso a sitios web externos está controlado para reducir la exposición a contenido dañino.

5.2 Desarrollo del Documento de políticas

Continuando con el avance del proyecto, se realiza la conversión de los controles del SGSI en políticas, misma que viene a ser una práctica efectiva para asegurar la implementación y gestión estructurada de medidas de seguridad dentro de la institución. Los controles necesarios para mitigar los riesgos específicos de seguridad de la información, han sido seleccionados después de analizar las no tolerancias y tomando como base las salvaguardas propuestas. Este paso se basa en la evaluación de riesgos y las necesidades de seguridad.

DOCUMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE

Introducción

El GADIP del Municipio de Cayambe reconoce que la información es un activo esencial, base para lograr promover el buen desarrollo integral local, los activos de información de la institución (información, ambiente de trabajo y empleados) que impulsan sus esfuerzos para mantener la confidencialidad, integridad, disponibilidad, continuidad de las operaciones de gestión, gobierno y/o gestión de riesgos, crean una cultura y conciencia de seguridad tanto en el público interno (funcionarios del GADIPMC) y público externo.

El proyecto del SGSI plantea lineamientos de la norma ISO 27001:2022. Para ello, todo el personal del establecimiento público debe conocer, participar y seguir las políticas, procedimientos, estándares, recomendaciones y demás directrices definidas en el Sistema de Gestión de la Seguridad de la Información (SGSI) ISO 27001, logrando así, anticipar que todos los empleados también tengan un compromiso continuo con la protección y el uso efectivo de los activos de información en todo el organismo público, lo cual es una parte esencial para lograr la visión y la misión de la institución.

Alcance de las políticas de la información

Los activos de información más importantes deben tener una política de seguridad que cumpla con la norma ISO 27001:2022. Estas políticas también se aplicarán a cualquier empleado, consultor, contratista, trabajador temporal o terceros que tengan acceso a los activos de información, el alcance de las políticas podría incluir las siguientes áreas:

- Acceso a la información
- Protección de la información
- Monitoreo y auditoría

- Responsabilidad
- Concientización

Propósito de las políticas ISO/IEC 27001:2022

El propósito de una política de seguridad de la información, es proteger los activos de información tanto como de amenazas internas o externas, ya sea de origen intencionales, naturales o accidentales, es decir proporcionando un marco sistemático y estructurado para la gestión de seguridad de la institución pública.

Alcance del documento comprende los siguientes aspectos:

- Política general de la seguridad ISO 27001:2022
- Comité de seguridad de la información
- Políticas por dominios
- Violaciones a la política
- Roles y responsabilidades
- Procedimientos asociados
- Manual de políticas
- Formatos (véase anexo 5)

Política general de la seguridad ISO 27001:2022

Establecer un programa de seguridad de la información que defina y establezca roles y responsabilidades para las actividades de operaciones, gestiones relacionadas con la seguridad de la información, las políticas de seguridad de la información deben ser definidas, aprobadas e implementadas, revisadas y actualizadas para proteger los activos del GADIPMC, guiados por la norma ISO/IEC 27001:2022

El GADIPMC es consciente de la importancia de la gestión de la información, el diseño e implementación de un sistema de gestión de seguridad de la información busca crear

confianza en el desempeño de sus funciones con el estado y los ciudadanos, cumplimiento con los procesos de ley y de acuerdo con la misión y visión establecida por la institución pública

Políticas por dominios

En base a la Declaración de Aplicabilidad, se enfocará en 3 de los 4 dominios que indica el estándar ISO 27001: 2022 y se ha considera los siguientes:

Organizativos

Seguridad de la información

Segregación de funciones

Responsabilidades de la dirección

Inteligencia de amenazas

Inventario de la información y otros activos asociados

Clasificación de la información

Control de acceso

Información de autenticación

Evaluación y decisión sobre eventos de seguridad de la información

Respuesta a incidentes de seguridad de la información

Privacidad y protección de la información personal

Procedimientos operativos documentados

Personas

Concienciación, educación y formación en materia de seguridad de la información

Trabajo a distancia

Tecnológicos

Restricción de acceso a la información

Autenticación segura

Protección contra el malware

Filtrado WEB

Segregación en redes

Sanciones –violaciones de las políticas

El incumplimiento SGSI se aplicará las sanciones de acuerdo al reglamento interno de la municipalidad, y dependerá de la gravedad del aspecto no cumplido. Pueden ser desde una llamado de atención verbal, escrito y hasta una sanción con descuento al rol de pagos en caso de reincidir.

Revisión de las políticas

Los miembros del Comité de Seguridad de la Información y el Oficial de Seguridad de la Información del GADIPMC deberán estar presentes cuando se revise la política del Sistema de Gestión de Seguridad de la Información una vez al año.

Roles y responsabilidades

GADIP MC se compromete a respaldar la seguridad de todos los activos, su cuidado tomando las medidas necesarias y avalando el cumplimiento de todas las leyes y normas relevantes. Designar a una persona para que esté a cargo de llevar la responsabilidad de vigilar las medidas de seguridad para la información del GADIPMC y todos sus departamentos. Los mismos que asignan funciones y responsabilidades dentro del área de trabajo, para manejar las tareas relacionadas con la creación, el mantenimiento, la difusión, la documentación y, finalmente, la aprobación de políticas y estándares de seguridad de la información.

Cada dirección se incorporará a los principios de segregación funcional entre sus deberes y responsabilidades, informará a un regulador o en el caso de ausencia de uno, a su comité de auditoría, y actuará como un enlace con las autoridades y grupos de intereses especiales en asuntos de seguridad de la información.

Comité de seguridad de la información

El Comité de Seguridad de la Información (CSI) estará presidido por el encargado del departamento de Tecnologías de la información y compuesto por personas que sean responsables o tengan roles en las siguientes áreas: Talento RRHH, administración, planificación, dirección estratégica, comunicación social, unidades creadoras de valor y el ámbito jurídico participará como consultor. El comité se reúne cada dos meses durante el primer año después de la publicación del SGSI y pasado el primer año se deberán reunir por lo menos una vez al año.

Oficial de seguridad de la información

En el GADIP MC el coordinador llevará a cabo las siguientes funciones:

- Contribuir al desarrollo y evaluación de políticas, normas, metodologías, prácticas y planes relacionados con la seguridad de la información.
- Determinar las amenazas y riesgos que atenten a los activos de información del municipio.
- Informar al Comité de seguridad de la información los resultados de la gestión del SGSI.
- Difundir temas referentes a la seguridad de la información.
- Dar seguimiento a eventos incidentes suscitados con respecto a la seguridad de la información.
- Dar mejoras al SGSI

Propietario

Están a cargo de la información producida y utilizada para las operaciones tanto dentro como fuera del municipio y tiene las siguientes responsabilidades:

- Involucrarse en el proceso de identificación de los activos de información y categorizar en función de su nivel de disponibilidad, confidencialidad e integridad.
- Definir usuario que tenga permisos para acceder a fuentes de información, dependerá

del cargo y de ser necesario habrá niveles de acceso.

- Cualquier vulnerabilidad encontrada que afecte sus activos de información debe informarse al oficial de seguridad de la información.

Custodio de la información

Son los encargados de monitorear, hacer cumplir las políticas y controles de seguridad en los activos de información que se encuentran bajo su administración. Son responsables también de la gestión diaria de la seguridad de los activos de información bajo su administración, así como del seguimiento del cumplimiento de las políticas y controles de seguridad en dichos activos y tiene como otras actividades como:

- Administrar los accesos a los activos de información y establecer los procesos para realizar backups con el fin de recuperar la información, los procesos deberán estar elaborados en un documento que se usará cuando se requiera.

Usuario

El personal del GADIP MC, sin importar la modalidad de contratación o nivel jerárquico, las personas naturales o jurídicas que prestan servicios en el municipio, así como las personas y entidades públicas o privadas que utilizan la información. Tienen como responsabilidades:

- Respetar y cumplir normas, reglamentos y políticas de seguridad de la información.
- En un entorno de trabajo remoto, presencial o mixto, no divulgar ni utilizar información sensible sobre los sistemas, plataformas, aplicaciones u otros recursos informáticos proporcionados para fines ajenos a sus funciones; en su lugar, haga un uso adecuado de ellos manteniendo la confidencialidad y la protección de datos adecuadas.
- Reportar incidentes dentro de la seguridad de la información al oficial de seguridad de la información.

Procedimientos asociados

- Gestión de riesgos: Identificar, evaluar y tratar los riesgos de seguridad de la información
- Controles de Acceso: Gestionar y controlar el acceso a los sistemas de información.
- Guías y recomendaciones
- Gestión de incidentes de seguridad: Detectar, reportar, gestionar y resolver incidentes de seguridad de la información.
- Gestión de la continuidad del negocio: Asegurar la continuidad de las operaciones críticas del municipio en caso de interrupciones
- Gestión de cambios: Controlar y gestionar los cambios en los sistemas de información para minimizar los riesgos.
- Gestión de Activos: Gestionar y proteger los activos de información del municipio.
- Capacitación y Concienciación: Asegurar que todo el personal esté consciente de las políticas de seguridad de la información y sepa cómo implementarlas.

5.3 Manual de políticas

El documento formal que establece las directrices, normas y procedimientos que una organización debe seguir para proteger su información. Este manual abarca aspectos como el control de acceso, la protección de datos, la gestión de incidentes, la formación en seguridad y sirve para asegurar que todo el personal del GADIMC y partes interesadas comprendan sus responsabilidades y adopten prácticas adecuadas para prevenir riesgos, garantizar la confidencialidad, integridad y disponibilidad de la información, cumpliendo con las normativas y estándares aplicables vigentes.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de seguridad de la información**	**Dominio:** Organizativo **Fecha:**
Resumen	La Política de Seguridad de la Información del Municipio de Cayambe establece las directrices y procedimientos necesarios para proteger la integridad, confidencialidad y disponibilidad de la información manejada por el municipio. Esta política se aplica a todos los empleados, contratistas y terceros que interactúan con los sistemas de información del municipio.	
Objetivo	La Política de Seguridad de la Información tiene como objetivo establecer lineamientos y principios para proteger la confidencialidad, integridad y disponibilidad de la información dentro de GADIPMC.	
Alcance	Esta política se aplica a todos los empleados, contratistas y terceros que realizan funciones en el GADIPMC	
Políticas		
Confidencialidad **Criterio:** La información debe ser accesible solo para aquellos individuos con autorización explícita. **Medidas:** Uso de controles de acceso, encriptación de datos sensibles y clasificación de la información (pública, interna, confidencial). **Integridad** **Criterio:** La información debe ser precisa y completa, y sus modificaciones deben ser realizadas solo por personas autorizadas. **Medidas:** Implementación de controles de integridad de datos, registros de auditoría y controles de versiones de documentos.		

<table>
<tr><td colspan="2">Disponibilidad

Criterio: La información debe estar disponible para su uso cuando sea necesario.

Medidas: Implementación de planes de recuperación ante desastres, procedimientos de respaldo y recuperación de datos.</td></tr>
<tr><td>Responsabilidades</td><td>Comité de Seguridad de la Información

Desarrollar y mantener la política de seguridad de la información.

Realizar evaluaciones de riesgo periódicas.

Revisar y aprobar todas las políticas y procedimientos de seguridad de la información.

Jefe de Seguridad de la Información

Implementar y gestionar el SGSI (Sistema de Gestión de Seguridad de la Información).

Coordinar las actividades de respuesta a incidentes.

Capacitar al personal en prácticas de seguridad de la información.

Monitorear el cumplimiento de la política y reportar a la alta dirección.

Usuarios Finales

Cumplir con la política de seguridad de la información y procedimientos asociados.

Informar de inmediato cualquier incidente de seguridad al Jefe de Seguridad de la Información.

Proteger las credenciales de acceso y no compartirlas con terceros.

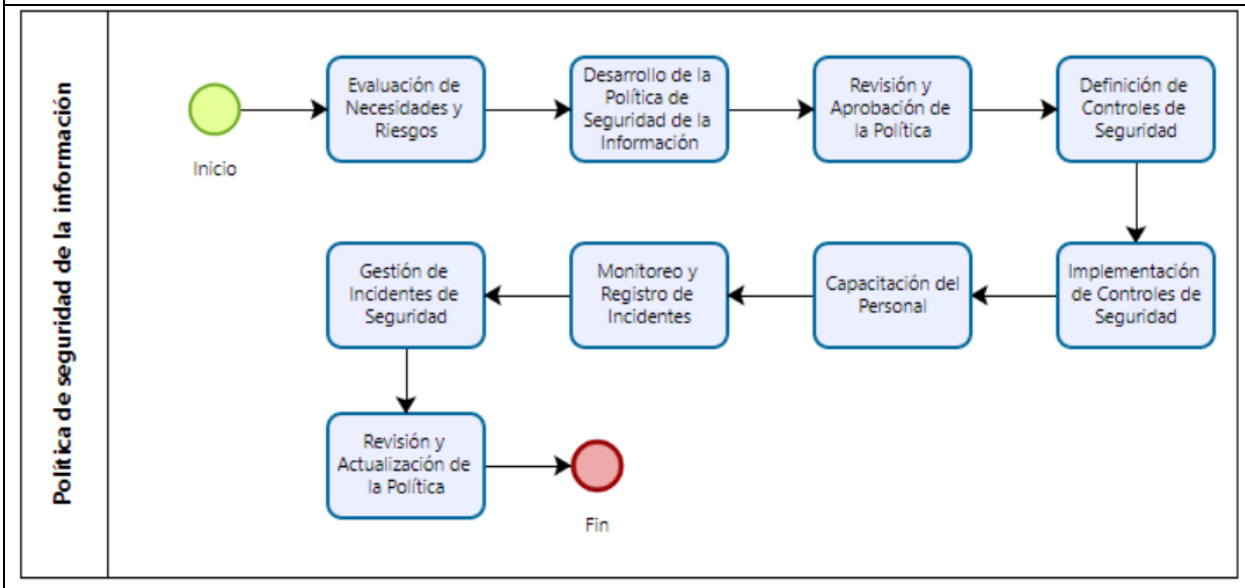
Departamentos de TI

Implementar y mantener los controles de seguridad técnicos.

Realizar copias de seguridad de la información y asegurar su recuperación.</td></tr>
</table>

	Monitorear y mantener la infraestructura de TI para asegurar su disponibilidad y protección.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.

Diagrama de flujo para la política



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

Evaluación de Necesidades y Riesgos: Identificación y evaluación de las necesidades de seguridad y los riesgos asociados.

Desarrollo de la Política de Seguridad de la Información: Creación de la política de seguridad de la información.

Revisión y Aprobación de la Política: Revisión y aprobación de la política por las partes interesadas.

Definición de Controles de Seguridad: Establecimiento de controles de seguridad específicos basados en los riesgos identificados.

Implementación de Controles de Seguridad: Implementación de los controles de seguridad definidos.

Capacitación del Personal: Capacitación del personal sobre la política de seguridad de la información y sus responsabilidades.

Monitoreo y Registro de Incidentes: Monitoreo continuo y registro de incidentes de seguridad.

Gestión de Incidentes de Seguridad: Establecimiento de procedimientos para la gestión de incidentes de seguridad.

Revisión y Actualización de la Política: Revisión y actualización periódica de la política de seguridad de la información.

Auditorías y Evaluaciones: Realización de auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política.

Revisión y Mejora Continua: Revisión y mejora continua de la política basada en los resultados de auditorías y evaluaciones.

Fin: Finalización del proceso de implementación y gestión de la política.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de segregación de funciones**	**Dominio:** Organizativo
		Fecha:
Resumen	Una política de segregación de funciones es un principio de control interno que tiene como objetivo asignar y distribuir tareas y responsabilidades de una manera que minimice el riesgo de fraude o error.	
Objetivo	La Política de Segregación de Funciones del GADIPMC tiene como objetivo asegurar que las responsabilidades y funciones críticas se asignen y ejecuten de manera que minimicen el riesgo de fraude, errores o conflictos de intereses, garantizando la integridad de nuestras operaciones y la confianza de nuestros clientes y empleados.	
Alcance	Esta política se aplica a todos los empleados, contratistas y terceros que realizan funciones en el GADIP MC	
Políticas		
Separación de Funciones: Los empleados no deben tener la capacidad de autorizar, aprobar, ejecutar y revisar una transacción en su totalidad. Estas funciones deben ser asignadas a diferentes individuos o equipos. Por ejemplo, el empleado que aprueba una compra no debe ser el mismo que realiza el pago. Rotación de Funciones: Se debe promover la rotación periódica de funciones clave para evitar que un empleado adquiera un control indebido o excesivo sobre un proceso o área de la institución. La rotación debe ser implementada de manera que se mantenga la continuidad operativa sin comprometer la integridad.		

Revisiones y Auditorías Internas: Debe llevarse a cabo una revisión y auditoría interna regular de las actividades y transacciones para detectar posibles incumplimientos de la política y tomar medidas correctivas cuando sea necesario.

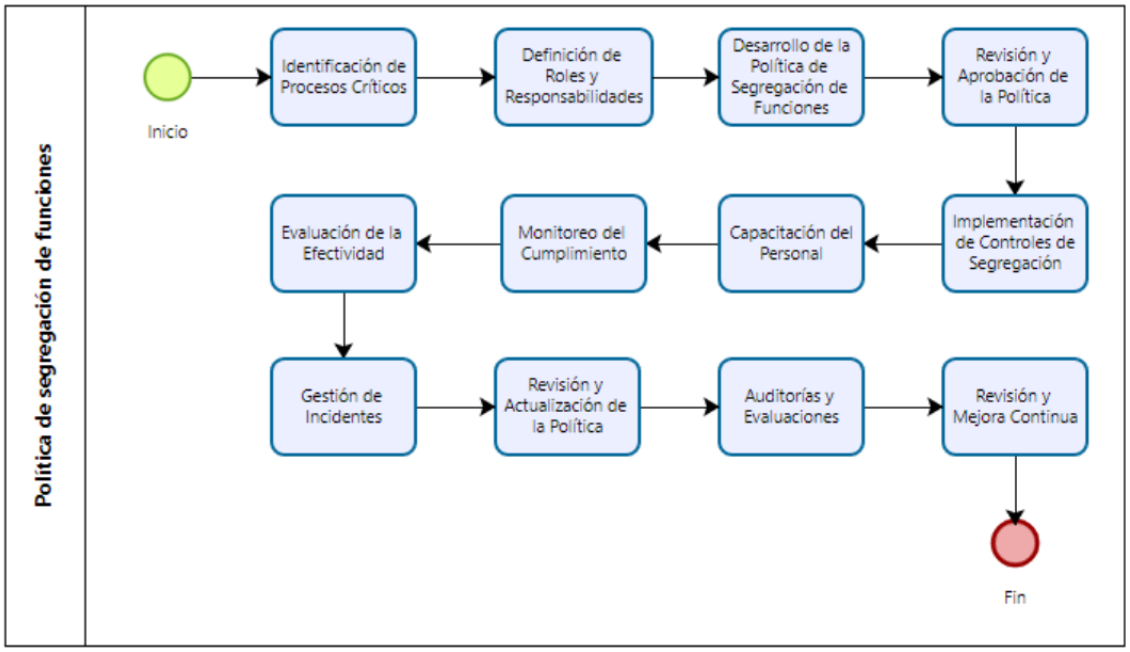
Segregación de Acceso a Sistemas: El acceso a sistemas y datos debe ser limitado y basarse en las responsabilidades laborales de un empleado. Los permisos de acceso deben revisarse y actualizarse periódicamente.

Reporte de Violaciones: Cualquier empleado que tenga conocimiento o sospeche una violación de esta política debe informar de inmediato a su supervisor, el departamento de recursos humanos o el equipo de auditoría interna del GADIP MC.

Capacitación: Todos los empleados deben recibir capacitación sobre esta política y sus responsabilidades con respecto a la segregación de funciones.

Responsabilidades	Esta política será revisada periódicamente para garantizar su eficacia y se actualizará según sea necesario para reflejar cambios en las operaciones de la empresa o en las regulaciones aplicables.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.

Diagrama de flujo para la política



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de segregación de funciones.

Identificación de Procesos Críticos: Identificar los procesos críticos del municipio que requieren segregación de funciones para prevenir conflictos de interés y asegurar la integridad de las operaciones.

Definición de Roles y Responsabilidades: Establecer roles y responsabilidades específicos para cada proceso identificado, asegurando que ninguna persona tenga control completo sobre todas las fases de un proceso crítico.

Desarrollo de la Política de Segregación de Funciones: Crear una política de segregación de funciones que detalle los procedimientos, roles, responsabilidades y estándares a seguir.

Revisión y Aprobación de la Política: Revisar y aprobar la política de segregación de funciones por las partes interesadas para asegurar su validez y aplicabilidad.

Implementación de Controles de Segregación: Implementar controles de segregación en los procesos críticos identificados, utilizando herramientas y técnicas adecuadas para asegurar la

separación de funciones.

Capacitación del Personal: Capacitar al personal sobre la política de segregación de funciones, incluyendo sus responsabilidades y la importancia de la segregación para la seguridad y eficiencia del municipio.

Monitoreo del Cumplimiento: Monitorear continuamente el cumplimiento de la política de segregación de funciones, identificando cualquier desviación o incumplimiento.

Evaluación de la Efectividad: Evaluar periódicamente la efectividad de la segregación de funciones, utilizando indicadores de desempeño y feedback para identificar áreas de mejora.

Gestión de Incidentes: Establecer procedimientos para la gestión de incumplimientos o incidentes relacionados con la segregación de funciones, incluyendo la identificación, reporte y corrección de problemas.

Revisión y Actualización de la Política: Revisar y actualizar periódicamente la política de segregación de funciones para asegurar su relevancia, efectividad y alineación con las necesidades cambiantes del municipio.

Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política de segregación de funciones y la efectividad de los controles implementados.

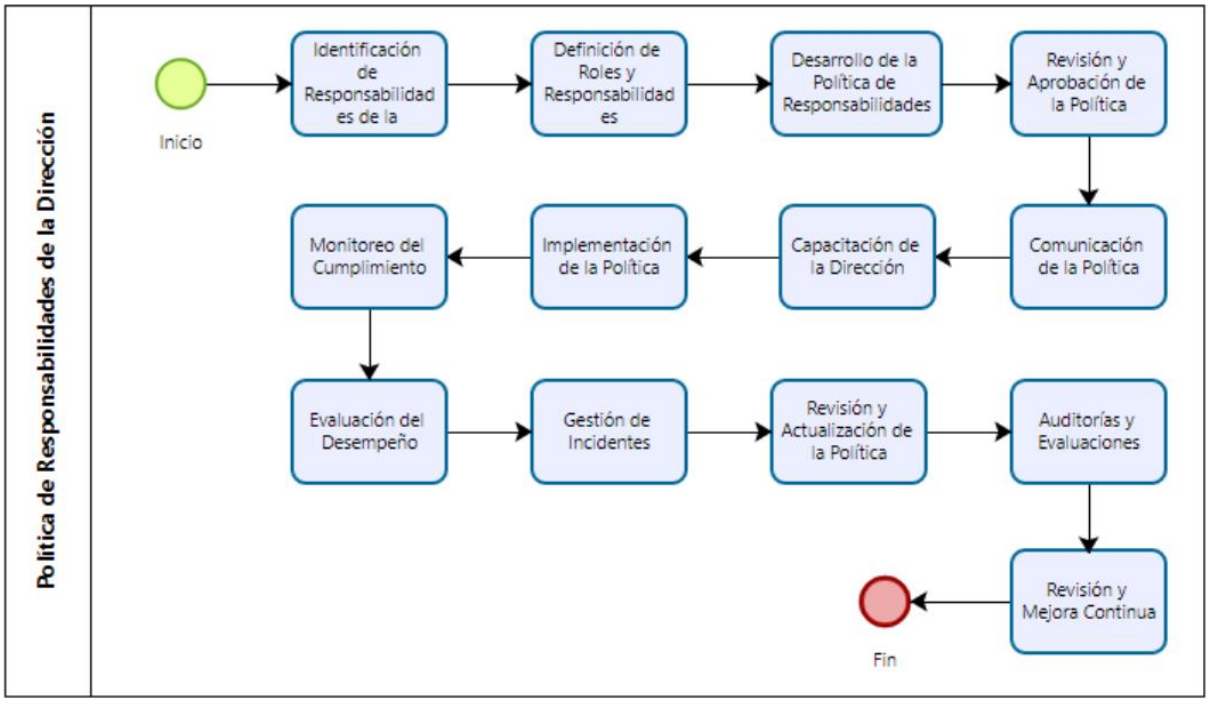
Revisión y Mejora Continua: Revisar y mejorar continuamente la política de segregación de funciones basada en los resultados de las auditorías, evaluaciones y nuevas necesidades o amenazas.

Fin: Finalización del proceso, asegurando que la política de segregación de funciones esta en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de responsabilidades de la dirección**	**Dominio:** Organizativo **Fecha:**
Resumen	La política de responsabilidades es un documento que define la estructura y el alcance de la responsabilidad de la alta dirección de una organización, las responsabilidades se definen y se designan acorde las necesidades de la institución.	
Objetivo	La Política de Responsabilidades de la Dirección del GADIPMC tiene como objetivo establecer pautas claras para los directivos y líderes de la organización, definiendo sus roles y responsabilidades en la toma de decisiones estratégicas, la gestión de recursos y la promoción de la cultura y valores de la municipalidad.	
Alcance	Esta política se aplica a todos los miembros de la alta dirección del Municipio de Cayambe, incluyendo el alcalde, vicealcalde, directores de departamentos y otros funcionarios de alto nivel	
Políticas		
Toma de Decisiones Estratégicas: Los directivos tienen la responsabilidad de participar en la formulación y revisión de la estrategia empresarial, así como en la toma de decisiones que afecten a la dirección y el rumbo de la institución. Deben evaluar los riesgos y oportunidades asociados con las decisiones estratégicas y considerar el impacto en los empleados y clientes.		

Asignación de Recursos: Los directivos deben asegurarse de que los recursos del municipio se asignen de manera eficiente y alineada con los objetivos estratégicos. Esto incluye la asignación de presupuestos, personal y otros recursos necesarios para el logro de metas y objetivos. **Desarrollo y Gestión de Equipos:** Los directivos tienen la responsabilidad de reclutar, desarrollar y retener talento dentro de sus equipos. Deben fomentar un entorno de trabajo inclusivo y promover el crecimiento profesional de los empleados. Deben proporcionar orientación y dirección clara a sus equipos, estableciendo expectativas de rendimiento y proporcionando retroalimentación constructiva. **Comunicación y Transparencia:** Los directivos deben comunicar de manera clara y transparente los objetivos, la estrategia y el desempeño de sus departamentos, sus equipos y a otros stakeholders relevantes. Deben fomentar una cultura de apertura y colaboración, alentando la comunicación efectiva entre los diferentes niveles de la organización. **Cumplimiento y Ética Empresarial** Los directivos deben promover y cumplir con los más altos estándares de ética en todas las operaciones de la institución. Deben tomar medidas inmediatas en caso de identificar o sospechar cualquier actividad que pueda contravenir políticas o regulaciones. **Desarrollo y Mantenimiento de la Cultura Empresarial:** Los directivos tienen la responsabilidad de promover y mantener la cultura y valores de la institución en todos los niveles de la organización. Deben actuar como modelos a seguir, demostrando los comportamientos y actitudes deseados.	
Responsabilidades	**Directores de Departamentos:** Deberán garantizar el cumplimiento de esta política dentro de su área, así como promover la capacitación y el

	mensaje de responsabilidad a sus equipos. **Funcionarios Públicos:** Cada empleado es responsable de cumplir con sus funciones y reportar cualquier irregularidad que afecte la gestión pública. **Oficina de Recursos Humanos:** Se encargará de implementar programas de capacitación y evaluación de desempeño, y de gestionar las sanciones correspondientes.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de responsabilidades de la dirección.

Identificación de Responsabilidades de la Dirección: Identificar las responsabilidades clave que la dirección debe asumir en el marco de la gestión y operación del municipio.

Definición de Roles y Responsabilidades: Establecer roles específicos y responsabilidades claras para cada miembro de la dirección, alineados con los objetivos y necesidades del municipio.

Desarrollo de la Política de Responsabilidades: Crear una política que defina claramente las responsabilidades de la dirección, incluyendo la toma de decisiones, supervisión de proyectos, gestión de recursos y cumplimiento de normativas.

Revisión y Aprobación de la Política: Revisar y aprobar la política de responsabilidades por las partes interesadas para asegurar su validez y aplicabilidad.

Comunicación de la Política: Comunicar la política de responsabilidades a todos los miembros de la dirección y partes interesadas relevantes para asegurar su comprensión y aceptación.

Capacitación de la Dirección: Capacitar a los miembros de la dirección sobre sus roles y responsabilidades definidos en la política, asegurando que comprendan sus deberes y cómo cumplirlos.

Implementación de la Política: Implementar la política de responsabilidades en las operaciones del municipio, asegurando que todos los miembros de la dirección cumplan con sus roles y responsabilidades.

Monitoreo del Cumplimiento: Monitorear continuamente el cumplimiento de las responsabilidades por parte de la dirección, identificando cualquier desviación o incumplimiento.

Evaluación del Desempeño: Evaluar periódicamente el desempeño de la dirección en el cumplimiento de sus responsabilidades, utilizando indicadores de desempeño.

Gestión de Incidentes: Establecer procedimientos para la gestión de incumplimientos o incidentes relacionados con las responsabilidades de la dirección, incluyendo la identificación, reporte y corrección de problemas.

Revisión y Actualización de la Política: Revisar y actualizar periódicamente la política de responsabilidades para asegurar su relevancia, efectividad y alineación con las necesidades cambiantes del municipio.

Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política de responsabilidades y la efectividad de su implementación.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de responsabilidades basada en los resultados de auditorías, evaluaciones y nuevas necesidades o amenazas.

Fin: Finalización del proceso, asegurando que la política de responsabilidades de la dirección está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de inteligencia de amenazas**	**Dominio:** Organizativo **Fecha:**
Resumen	Una política de inteligencia de amenazas es un conjunto de pautas y procedimientos que utiliza una organización para recopilar, analizar y utilizar información relacionada con la seguridad y las amenazas cibernéticas.	
Objetivo	El objetivo de esta política es establecer las directrices y procedimientos para la recopilación, análisis y uso de la inteligencia de amenazas cibernéticas y de seguridad para proteger los activos de la organización.	
Alcance	Esta política se aplica a todos los empleados, contratistas y terceros que tienen acceso a los sistemas y datos de la organización	

Políticas

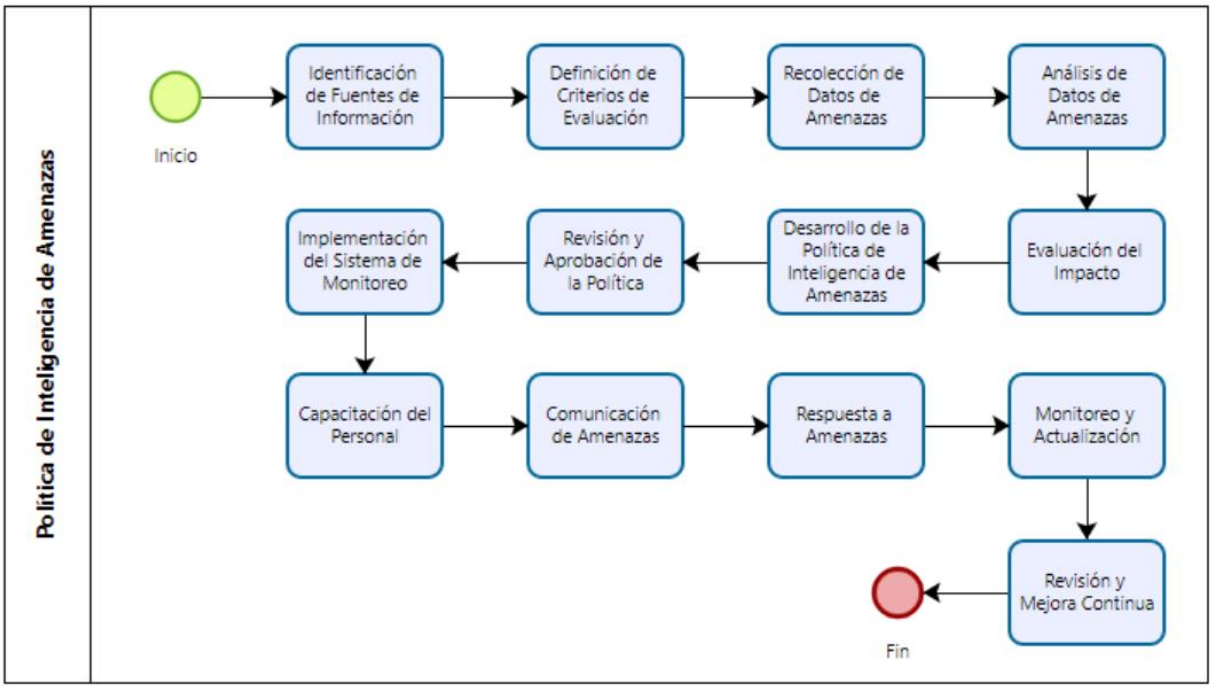
Recopilación de Datos: El equipo de inteligencia de amenazas recopilará información de fuentes públicas, privadas y colaborativas sobre amenazas cibernéticas y de seguridad. Esto incluye la monitorización de sitios web, foros, redes sociales y fuentes gubernamentales.

Análisis de Inteligencia: La información recopilada se analizará para determinar la credibilidad y relevancia de las amenazas. Se asignarán niveles de gravedad y se proporcionará información detallada sobre cada amenaza.

Distribución de Información: La inteligencia de amenazas se compartirá con el equipo de seguridad de la información y otros departamentos relevantes. Se proporcionarán alertas de amenazas y recomendaciones de mitigación.

Respuesta a Amenazas: El equipo de seguridad de la información utilizará la inteligencia de amenazas para tomar medidas proactivas y reactivas para proteger los activos de la organización.

Esto puede incluir parches de seguridad, cambios en la configuración y notificación a partes interesadas.	
Responsabilidades	Equipo de Inteligencia de Amenazas: El equipo de inteligencia de amenazas será responsable de recopilar, analizar y distribuir información sobre amenazas cibernéticas y de seguridad. Deberán mantenerse actualizados sobre las últimas tendencias y amenazas. Equipo de Seguridad de la Información**:** El equipo de seguridad de la información utilizará la inteligencia de amenazas para identificar y mitigar posibles amenazas a la infraestructura y datos de la institución. Empleados y Usuarios**:** Todos los empleados y usuarios deben estar atentos a las alertas de amenazas y seguir las recomendaciones de seguridad proporcionadas por el equipo de seguridad de la información.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Política de inteligencia de amenazas

Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de inteligencia de amenazas.

Identificación de Fuentes de Información: Identificar fuentes de inteligencia de amenazas tanto internas (logs de seguridad, incidentes anteriores) como externas (boletines de seguridad, feeds de amenazas, comunidades de seguridad).

Definición de Criterios de Evaluación: Establecer criterios para evaluar la relevancia y fiabilidad de la información recibida de las fuentes identificadas.

Recolección de Datos de Amenazas: Recolectar datos de amenazas de las fuentes identificadas utilizando herramientas y técnicas adecuadas.

Análisis de Datos de Amenazas: Analizar los datos recolectados para identificar patrones, tendencias y posibles amenazas, utilizando técnicas de análisis de inteligencia.

Evaluación del Impacto: Evaluar el impacto potencial de las amenazas identificadas en los activos

y operaciones del municipio.

Desarrollo de la Política de Inteligencia de Amenazas: Crear una política de inteligencia de amenazas que defina los procedimientos, responsabilidades y estándares a seguir.

Revisión y Aprobación de la Política: Revisar y aprobar la política de inteligencia de amenazas por las partes interesadas para asegurar su validez y aplicabilidad.

Implementación del Sistema de Monitoreo: Implementar un sistema de monitoreo continuo para detectar amenazas en tiempo real y recibir alertas.

Capacitación del Personal: Capacitar al personal sobre la política de inteligencia de amenazas, incluyendo la identificación, análisis y respuesta a las amenazas.

Comunicación de Amenazas: Comunicar las amenazas identificadas a las partes relevantes de manera oportuna y clara para que se tomen las medidas necesarias.

Respuesta a Amenazas: Implementar medidas de respuesta para mitigar las amenazas, como parches de seguridad, configuraciones de firewall, cambios en procedimientos operativos, etc.

Monitoreo y Actualización: Monitorear continuamente la situación de amenazas y actualizar la inteligencia de amenazas según sea necesario.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de inteligencia de amenazas basándose en los resultados del monitoreo, análisis y nuevas amenazas identificadas.

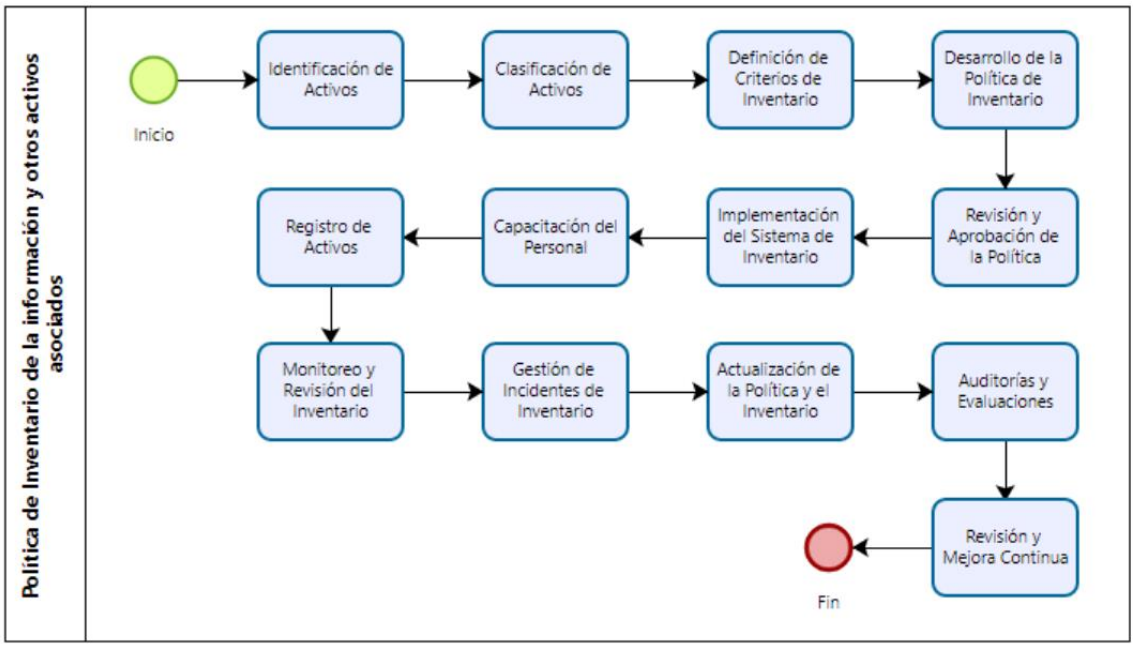
Fin: Finalización del proceso, asegurando que la política de inteligencia de amenazas está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor**: Lenin Jami
VERSIÓN 1.0	**Política de Inventario de la información y otros activos asociados**	**Dominio:** Organizativo **Fecha:**
Resumen	Una Política de Inventario de la Información y otros activos asociados es fundamental para garantizar la gestión adecuada de los activos de información de una organización y protegerlos de manera efectiva	
Objetivo	El objetivo de esta política es establecer directrices y procedimientos para la creación, mantenimiento y actualización de un inventario de la información y otros activos asociados en el GADIPMC. Este inventario es esencial para garantizar la seguridad, disponibilidad y confidencialidad de la información crítica y otros activos de la organización.	
Alcance	Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que manejen o tengan acceso a activos de información y otros activos asociados en la institución.	
Políticas		
Identificación de Activos: Los responsables de activos identificarán y enumerarán todos los activos de información y otros activos asociados en sus áreas de responsabilidad. Esto incluye, pero no se limita a sistemas de información, bases de datos, documentos físicos, hardware, software y dispositivos móviles. **Clasificación de Activos:** Cada activo se clasificará según su nivel de confidencialidad, integridad y disponibilidad. Se utilizará una metodología de clasificación predefinida.		

<table>
<tr><td colspan="2">Registro de Activos: Los activos se registrarán en una base de datos de inventario de activos de información y otros activos asociados. Este registro contendrá información detallada sobre cada activo, incluyendo su ubicación, propietario, clasificación y fecha de adquisición.
Actualización del Inventario: El inventario se actualizará regularmente para reflejar cambios en los activos, como adquisiciones, desactivaciones o transferencias. Los responsables de activos serán responsables de mantener esta información actualizada.
Acceso y Seguridad: El acceso al inventario estará restringido a personas autorizadas. Se implementarán medidas de seguridad adecuadas para proteger la confidencialidad de la información contenida en el inventario.
Auditorías y Revisiones: Se realizarán auditorías periódicas con el fin de verificar el cumplimiento de esta política y la precisión del inventario. Se corregirán las discrepancias identificadas durante estas revisiones.
Eliminación Segura: Cuando se retiren activos de información o se den de baja otros activos asociados, se seguirán los procedimientos de eliminación segura, que incluirán la destrucción de la información de manera adecuada y la documentación de la eliminación.</td></tr>
<tr><td>Responsabilidades</td><td>Director del departamento de Tics: Será responsable de supervisar la implementación y cumplimiento de esta política, así como de proporcionar los recursos necesarios para su ejecución.
Responsables de Activos: Cada unidad o departamento designará un responsable de activos de información y otros activos asociados. Estos responsables serán los encargados de identificar, clasificar y mantener un registro de los activos bajo su supervisión.</td></tr>
</table>

Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política será revisada y actualizada anualmente o cuando sea necesario debido a cambios en la tecnología o en las operaciones de la organización.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios y regirse a la vigencia del mismo

Diagrama de flujo para la política



Descripción de cada paso

Inicio: Comienza el proceso de implementación de la política de inventario de la información y otros activos asociados.

Identificación de Activos: Identificar todos los activos de información y otros activos asociados que maneja el municipio, como hardware, software, datos, documentos y otros recursos.

Clasificación de Activos: Clasificar los activos según su tipo, importancia y sensibilidad,

considerando factores como la criticidad para las operaciones del municipio y la confidencialidad de la información contenida.

Definición de Criterios de Inventario: Establecer criterios claros para incluir activos en el inventario, determinando qué información debe ser registrada para cada tipo de activo (por ejemplo, nombre, ubicación, propietario, valor, etc.).

Desarrollo de la Política de Inventario: Crear una política de inventario de información y otros activos asociados que detalle los procedimientos, responsabilidades y estándares a seguir.

Revisión y Aprobación de la Política: Revisar y aprobar la política de inventario por las partes interesadas para asegurar su validez y aplicabilidad.

Implementación del Sistema de Inventario: Implementar el sistema de inventario en los sistemas y procesos del municipio, asegurando que todas las herramientas necesarias estén en su lugar.

Capacitación del Personal: Capacitar al personal sobre la política de inventario, incluyendo cómo registrar y mantener el inventario de activos y sus responsabilidades en el proceso.

Registro de Activos: Registrar todos los activos en el inventario según los criterios definidos, asegurando que la información sea precisa y completa.

Monitoreo y Revisión del Inventario: Monitorear y revisar periódicamente el inventario para asegurar su exactitud, relevancia y actualización continua.

Gestión de Incidentes de Inventario: Establecer procedimientos para la gestión de incidentes relacionados con el inventario, incluyendo la detección, reporte y respuesta a errores o discrepancias en el inventario.

Actualización de la Política y el Inventario: Revisar y actualizar periódicamente la política de inventario y el inventario en sí para adaptarse a nuevos requisitos, amenazas o cambios en el

entorno.

Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política de inventario y la efectividad del sistema de inventario.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de inventario basándose en los resultados de las auditorías, evaluaciones y nuevas amenazas o requisitos.

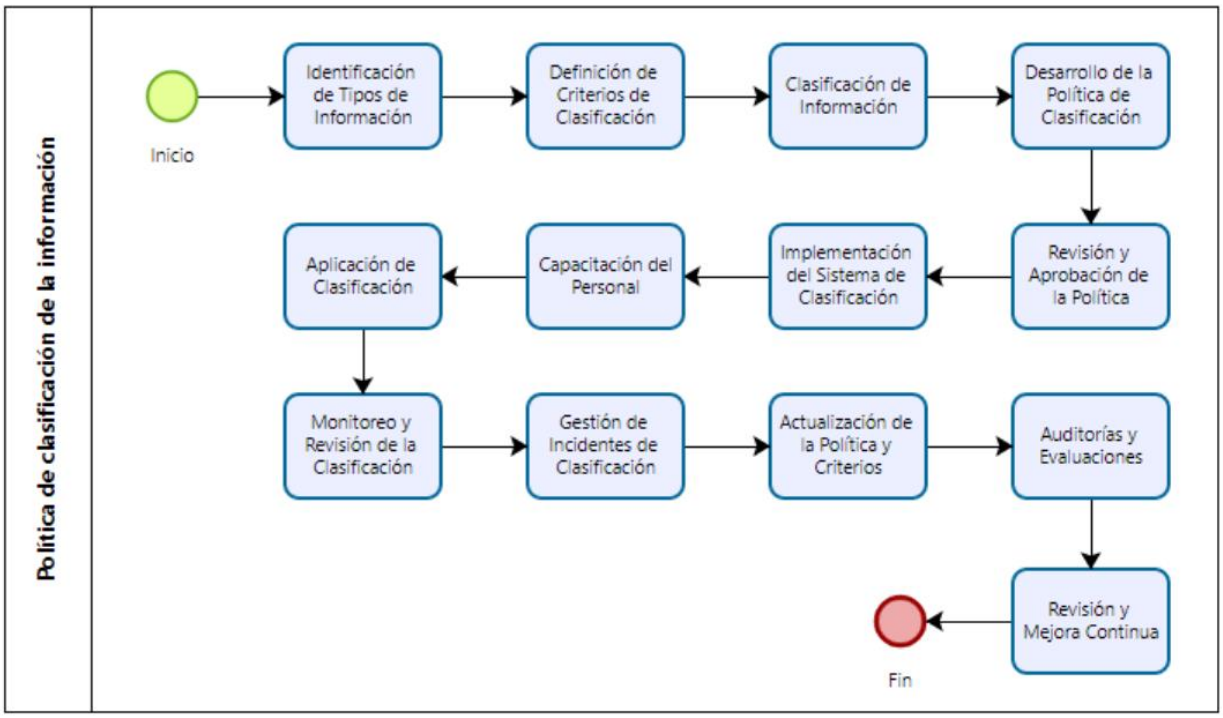
Fin: Finalización del proceso, asegurando que la política de inventario de información y otros activos asociados está en operación y es efectiva

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de clasificación de la información**	**Dominio:** Organizativo
		Fecha:
Resumen	Las políticas de clasificación de la información son pautas que una organización establece para categorizar y proteger la información de manera adecuada. Estas políticas son esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información más importante de la institución.	
Objetivo	El objetivo de esta política es establecer un marco para clasificar la información de la organización según su nivel de confidencialidad, garantizando así su protección adecuada.	

Alcance	Esta política se aplica a todos los empleados, contratistas y personal externo que manejan información de la institución.
Políticas	
Categorización de la Información: La información de la organización se categorizará en tres niveles de confidencialidad **Información Pública:** La información que no requiere ninguna protección especial y se puede compartir públicamente. Esto incluye comunicaciones de marketing, información de contacto pública y documentos de dominio público. **Información Confidencial:** La información que debe protegerse de manera adecuada para evitar divulgaciones no autorizadas. Esto incluye datos de clientes, contratos y otros datos sensibles. El acceso a esta información sólo estará permitido a personal autorizado. **Información Altamente Confidencial:** La información altamente sensible que requiere la máxima protección. Datos de investigación y desarrollo, contraseñas y otros datos extremadamente delicados. El acceso a esta información está limitado a un grupo selecto de individuos y se aplica un control de acceso riguroso. **Procedimientos:** Se establecerán procedimientos específicos para clasificar, almacenar, transmitir y eliminar información de acuerdo con su nivel de confidencialidad. Estos procedimientos incluirán: Métodos de etiquetado de documentos y archivos. Controles de acceso y autenticación para información confidencial y altamente confidencial. Políticas de retención y eliminación de información. Protocolos de seguridad para la transmisión de datos.	
Responsabilidades	Los empleados y contratistas deben ser conscientes de la categorización de la información con la que trabajan y tratarla de acuerdo con su nivel de confidencialidad.

	Los administradores de sistemas deben implementar medidas de seguridad adecuadas para proteger la información de acuerdo con su categorización. El departamento de recursos humanos es responsable de educar a los empleados sobre estas políticas y llevar a cabo entrenamientos periódicos.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.

Diagrama de flujo para la política



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de clasificación de la información.

Identificación de Tipos de Información: Identificar los diferentes tipos de información que maneja el municipio, como documentos, bases de datos, correos electrónicos, etc.

Definición de Criterios de Clasificación: Establecer criterios claros y específicos para clasificar la información según su sensibilidad y criticidad, tales como pública, interna, confidencial y sensible.

Clasificación de Información: Clasificar la información según los criterios definidos, asegurando que cada tipo de información recibe la clasificación adecuada.

Desarrollo de la Política de Clasificación: Crear una política de clasificación de la información que detalle los procedimientos, criterios de clasificación, responsabilidades y estándares a seguir.

Revisión y Aprobación de la Política: Revisar y aprobar la política de clasificación por las partes interesadas para asegurar su validez y aplicabilidad.

Implementación del Sistema de Clasificación: Implementar el sistema de clasificación en los sistemas y procesos del municipio, asegurando que todas las herramientas necesarias estén en su lugar.

Capacitación del Personal: Capacitar al personal sobre la política de clasificación, incluyendo cómo clasificar correctamente la información y sus responsabilidades en el proceso.

Aplicación de Clasificación: Aplicar la clasificación a la información según los criterios definidos, asegurando que todas las nuevas informaciones y documentos reciban la clasificación correspondiente.

Monitoreo y Revisión de la Clasificación: Monitorear y revisar periódicamente la aplicación de la clasificación para asegurar el cumplimiento de la política y la correcta clasificación de la información.

Gestión de Incidentes de Clasificación: Establecer procedimientos para la gestión de incidentes relacionados con la clasificación de información, incluyendo la detección, reporte y respuesta a errores de clasificación. **Actualización de la Política y Criterios**: Revisar y actualizar periódicamente la política de clasificación y los criterios utilizados para adaptarse a nuevos requisitos, amenazas o cambios en el entorno. **Auditorías y Evaluaciones**: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política de clasificación y la efectividad del sistema de clasificación. **Revisión y Mejora Continua**: Revisar y mejorar continuamente la política de clasificación basándose en los resultados de las auditorías, evaluaciones y nuevas amenazas o requisitos. **Fin**: Finalización del proceso, asegurando que la política de clasificación de información está en operación y es efectiva.

ALCALDÍA CAYAMBE unidosrenacemos	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE**	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de control de acceso**	**Dominio:** Organizativo **Fecha:**
Resumen	Una política de control de acceso es un conjunto de reglas y pautas que determinan quién puede acceder a qué recursos en un sistema de información.	
Objetivo	El objetivo de esta política es garantizar que la información y los recursos importantes de GADIP MC estén protegidos adecuadamente y que el acceso a estos recursos sea de una manera controlada y autorizada.	

Alcance	Todo el personal que maneja información de la empresa debe cumplir con esta política, incluidos empleados, contratistas y partes externas.

Políticas

El mínimo privilegio

Se aplica el principio de privilegio mínimo. Esto significa que los usuarios sólo tienen acceso a los recursos que necesitan para realizar su trabajo. El acceso a los sistemas y datos se evalúa y proporciona en función de los requisitos laborales y se reduce o elimina a medida que esos requisitos cambian.

Autenticación y Autorización

Todos los usuarios deben estar debidamente autenticados antes de acceder a los sistemas y datos de GADIPMC. La autorización se basa en la autenticación y se otorga según las políticas de acceso y los requisitos operativos.

Registro de Acceso y monitoreo

Se implementa un sistema de control de acceso para monitorear y controlar todas las actividades de acceso al sistema y a los datos. Estos registros se revisan periódicamente y se toman medidas si se produce alguna actividad inusual o sospechosa.

Contraseñas

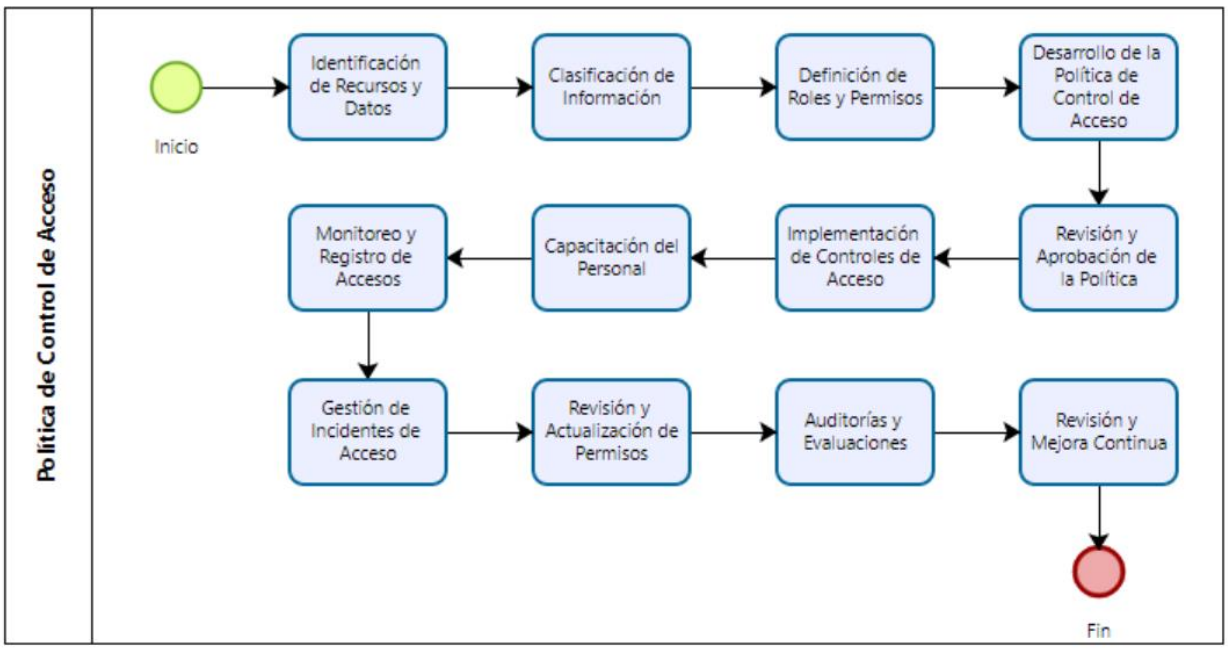
Se ejecutará una política sólida de administración de contraseñas, que incluye requisitos de longitud, complejidad y cambio periódico. Las contraseñas se mantienen confidenciales y no se comparten entre usuarios.

Educación y Concienciación

Los empleados reciben capacitación y concientización sobre políticas de control de acceso y seguridad de la información. Deben ser conscientes de sus responsabilidades en la protección de los activos de la institución.

Control de Dispositivos Móviles

Los dispositivos móviles utilizados para acceder a los recursos del municipio deben cumplir con las políticas de seguridad establecidas, incluida la configuración de una contraseña y la capacidad de que, en caso de pérdida o robo, los datos se puedan borrar vía remoto.	
Responsabilidades	Esta política se revisa y actualiza periódicamente para garantizar que proteja eficazmente los activos de la empresa y cumpla con las amenazas y requisitos legales en evolución.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de control de acceso.

Identificación de Recursos y Datos: Identificar todos los recursos (sistemas, aplicaciones, datos) que requieren control de acceso para proteger la información sensible.

Clasificación de Información: Clasificar la información y recursos según su sensibilidad y criticidad para determinar el nivel de acceso necesario.

Definición de Roles y Permisos: Definir roles de usuario y asignar permisos de acceso a los recursos según la clasificación de la información, asegurando que solo el personal autorizado pueda acceder a la información sensible.

Desarrollo de la Política de Control de Acceso: Crear una política de control de acceso que detalle los roles, permisos, procedimientos de autorización y responsabilidades.

Revisión y Aprobación de la Política: Revisar y aprobar la política por las partes interesadas para asegurar su validez y aplicabilidad.

Implementación de Controles de Acceso: Implementar los controles de acceso en los sistemas y aplicaciones, utilizando mecanismos como listas de control de acceso (ACL), control de acceso basado en roles (RBAC) y autenticación multifactor (MFA).

Capacitación del Personal: Capacitar al personal sobre la política de control de acceso, incluyendo sus responsabilidades y el uso correcto de los sistemas de control de acceso.

Monitoreo y Registro de Accesos: Establecer sistemas para monitorear y registrar todos los accesos a los recursos y datos sensibles, detectando y respondiendo a accesos no autorizados.

Gestión de Incidentes de Acceso: Establecer procedimientos para la gestión de incidentes relacionados con el acceso, incluyendo la detección, reporte y respuesta a accesos no autorizados.

Revisión y Actualización de Permisos: Revisar y actualizar periódicamente los roles y permisos de acceso para reflejar cambios en roles, responsabilidades y estructura organizativa. **Auditorías y Evaluaciones**: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política de control de acceso y la efectividad de los controles implementados. **Revisión y Mejora Continua**: Revisar y mejorar continuamente la política basada en los resultados de las auditorías, evaluaciones y nuevas amenazas o requisitos. **Fin**: Finalización del proceso, asegurando que la política de control de acceso está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de información de autenticación**	**Dominio**: Organizativo **Fecha:**
Resumen	Esta política establece pautas y procedimientos para gestionar la autenticación de usuarios en los sistemas de información del Municipio de Cayambe para garantizar la seguridad, integridad y confidencialidad de los datos y servicios de la ciudad.	
Objetivo	Identificar y alinear mecanismos de autenticación para el acceso a los sistemas informáticos de la ciudad de Cayambe, garantizando que solo las personas autorizadas tengan acceso a datos y recursos sensibles.	
Alcance	Esta política aplica a todos los empleados, contratistas, proveedores y cualquier otra persona que necesite acceso a los sistemas de información de la Ciudad de Cayambe.	
Políticas		

Autenticación de usuario:

Todos los usuarios deben estar autenticados con un nombre de usuario y contraseña únicos. Las contraseñas deben cumplir requisitos mínimos de complejidad (al menos 8 caracteres, incluidas letras mayúsculas y minúsculas, números y símbolos).

Mecanismos de autenticación adicionales:

Se debe implementar la autenticación de dos factores (2FA) para acceder a los sistemas críticos. El departamento de TI debe administrar y monitorear los dispositivos de autenticación, como tokens y aplicaciones móviles.

Gestión de contraseñas:

Las contraseñas deben cambiarse cada 90 días. Debería prohibirse la reutilización de las últimas 5 contraseñas. Si lo olvidan, los usuarios deben completar un proceso de recuperación seguro verificado por TI.

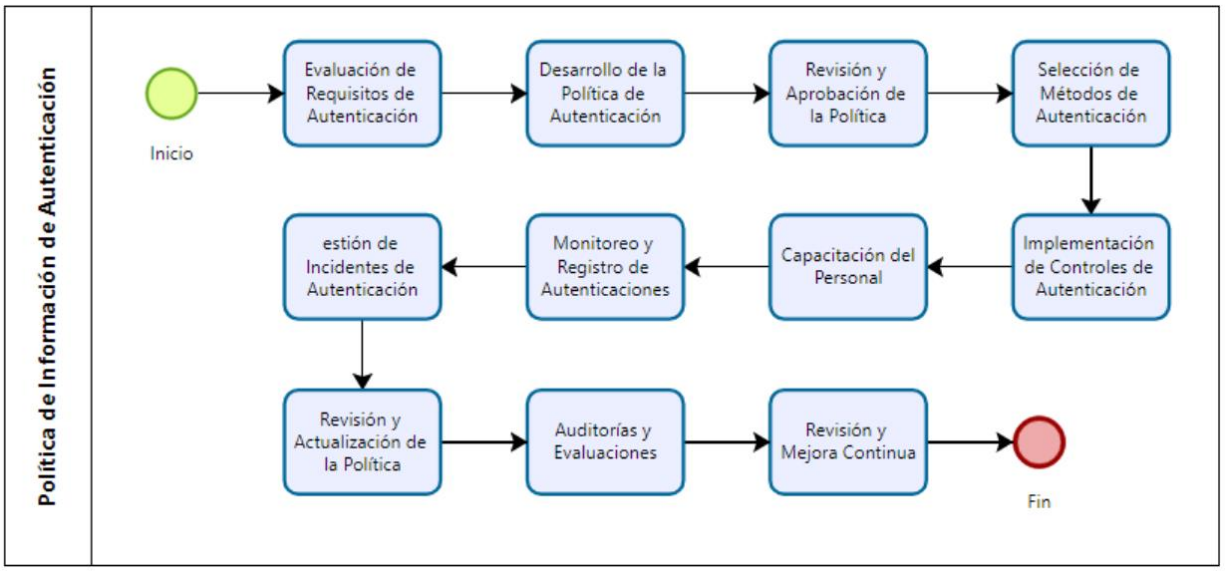
Control de acceso:

El acceso a los sistemas debe basarse en el principio de privilegio mínimo, otorgando sólo aquellos privilegios necesarios para realizar funciones oficiales.

Responsabilidades	**Usuarios:** deben seguir esta política y reportar cualquier actividad sospechosa. **Departamento de TI:** Responsable de implementar, monitorear y mantener el sistema de autenticación, así como capacitar y brindar soporte a los usuarios. **Administrador de la ciudad:** debe asegurarse de que los recursos necesarios estén disponibles para implementar y mantener esta política.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del

	empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.

Diagrama de flujo para la política



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de información de autenticación.

Evaluación de Requisitos de Autenticación: Identificar y analizar los requisitos de autenticación necesarios para proteger los sistemas y la información del municipio.

Desarrollo de la Política de Autenticación: Crear una política de información de autenticación que defina las directrices, métodos y responsabilidades para la autenticación segura.

Revisión y Aprobación de la Política: Revisar y aprobar la política de autenticación por las partes interesadas para asegurar su validez y aplicabilidad.

Selección de Métodos de Autenticación: Seleccionar los métodos de autenticación más

adecuados, como contraseñas fuertes, autenticación multifactor (2FA), biometría, entre otros.

Implementación de Controles de Autenticación: Implementar los controles de autenticación seleccionados en todos los sistemas y aplicaciones del municipio.

Capacitación del Personal: Capacitar al personal sobre la política de autenticación, incluyendo el uso adecuado de los métodos de autenticación y la importancia de la seguridad de la información.

Monitoreo y Registro de Autenticaciones: Establecer sistemas para monitorear y registrar los eventos de autenticación, detectando y respondiendo a actividades sospechosas.

Gestión de Incidentes de Autenticación: Establecer procedimientos para la gestión de incidentes de autenticación, incluyendo la detección, reporte y respuesta a accesos no autorizados.

Revisión y Actualización de la Política: Revisar y actualizar periódicamente la política de autenticación para asegurar su efectividad y cumplimiento continuo.

Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política y la efectividad de los controles implementados.

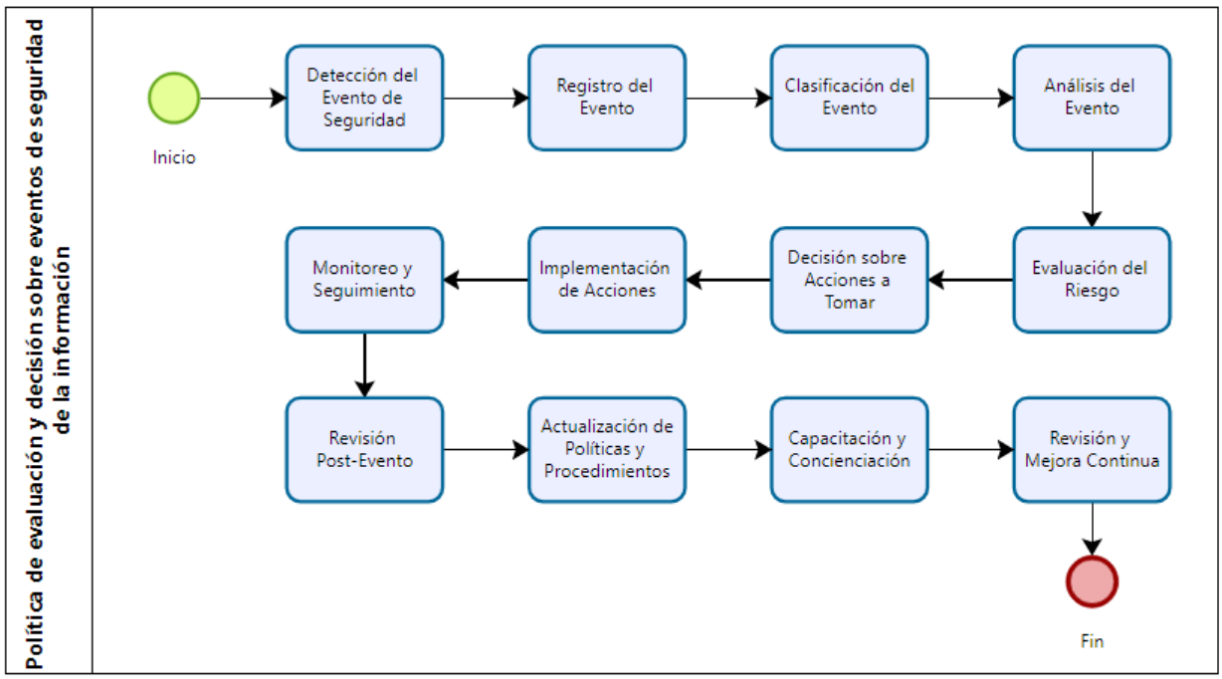
Revisión y Mejora Continua: Revisar y mejorar continuamente la política de autenticación basada en los resultados de las auditorías, evaluaciones y nuevas amenazas o requisitos.

Fin: Finalización del proceso, asegurando que la política de información de autenticación está en operación y es efectiva

ALCALDÍA CAYAMBE unidosrenacemos	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE**	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de evaluación y decisión sobre eventos de seguridad de la información**	**Dominio:** Organizativo **Fecha:**
Resumen	Esta política establece lineamientos y procedimientos para la evaluación,	

	gestión y toma de decisiones de incidentes de seguridad de la información en el Municipio de Cayambe. Su propósito es proteger la integridad, seguridad y disponibilidad de la información de la ciudad contra amenazas y vulnerabilidades
Objetivo	El objetivo de esta política es proporcionar un marco ordenado para identificar, evaluar y responder a incidentes de seguridad de la información, asegurando que se tomen decisiones oportunas e informadas para minimizar los riesgos y proteger los activos de información del municipio.
Alcance	Esta política aplica a todos los empleados, contratistas, proveedores y terceros del municipio de Cayambe que procesan información. Incluye todos los sistemas, redes y datos, independientemente de su formato y ubicación.
Políticas	
Identificación de Eventos de Seguridad: Todos los eventos que puedan comprometer la seguridad de la información deben ser identificados y reportados inmediatamente al equipo de TI o al responsable de seguridad de la información. **Evaluación de Impacto:** Los eventos reportados serán evaluados en términos de su impacto potencial en la confidencialidad, integridad y disponibilidad de la información. **Clasificación de Incidentes:** Los incidentes serán clasificados según su gravedad (bajo, medio, alto, crítico) para determinar la respuesta adecuada. **Respuesta y Mitigación:** Se desarrollarán y ejecutarán planes de respuesta para contener y mitigar los impactos de los incidentes, incluyendo la recuperación de sistemas y datos afectados. **Notificación y Comunicación:** Las partes interesadas pertinentes serán notificadas sobre el incidente y las acciones tomadas, conforme a las leyes y regulaciones aplicables.	

Responsabilidades	**Empleados y Contratistas:** Reportar inmediatamente cualquier evento de seguridad de la información. **Responsable de Seguridad de la Información:** Supervisar la implementación de esta política, coordinar la respuesta a incidentes y asegurar la comunicación efectiva de eventos de seguridad. **Equipo de TI:** Implementar y mantener las medidas de seguridad, gestionar las herramientas de monitoreo y respuesta a incidentes. **Alta Dirección:** Proveer apoyo y recursos necesarios para la implementación efectiva de esta política.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción yj las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Descripción de cada paso:

Inicio: Comienza el proceso de evaluación y toma de decisiones sobre eventos de seguridad de la información.

Detección del Evento de Seguridad: Identificación de un evento de seguridad a través de sistemas de monitoreo, alertas o reportes del personal.

Registro del Evento: Documentar el evento de seguridad en un registro, incluyendo detalles como fecha, hora, descripción del evento y cómo se detectó.

Clasificación del Evento: Clasificar el evento según su naturaleza (p. ej., incidente, amenaza, vulnerabilidad), gravedad y potencial impacto en la organización.

Análisis del Evento: Realizar un análisis detallado del evento para entender su causa raíz, alcance y posibles consecuencias.

Evaluación del Riesgo: Evaluar el riesgo asociado con el evento, considerando factores como la probabilidad de ocurrencia y el impacto potencial.

Decisión sobre Acciones a Tomar: Determinar las acciones correctivas y preventivas necesarias para mitigar el evento de seguridad, tales como contención, erradicación y recuperación.

Implementación de Acciones: Implementar las acciones decididas, asegurando que se ejecuten de manera efectiva y en tiempo oportuno.

Monitoreo y Seguimiento: Monitorear el evento y realizar un seguimiento de la efectividad de las acciones implementadas, asegurando que el problema esté completamente resuelto.

Revisión Post-Evento: Realizar una revisión post-evento para evaluar la respuesta y las lecciones aprendidas, identificando mejoras potenciales en el proceso.

Actualización de Políticas y Procedimientos: Actualizar las políticas y procedimientos de seguridad basados en las lecciones aprendidas y las mejores prácticas identificadas.

Capacitación y Concienciación: Capacitar al personal sobre las nuevas políticas y procedimientos implementados para asegurar su comprensión y cumplimiento.

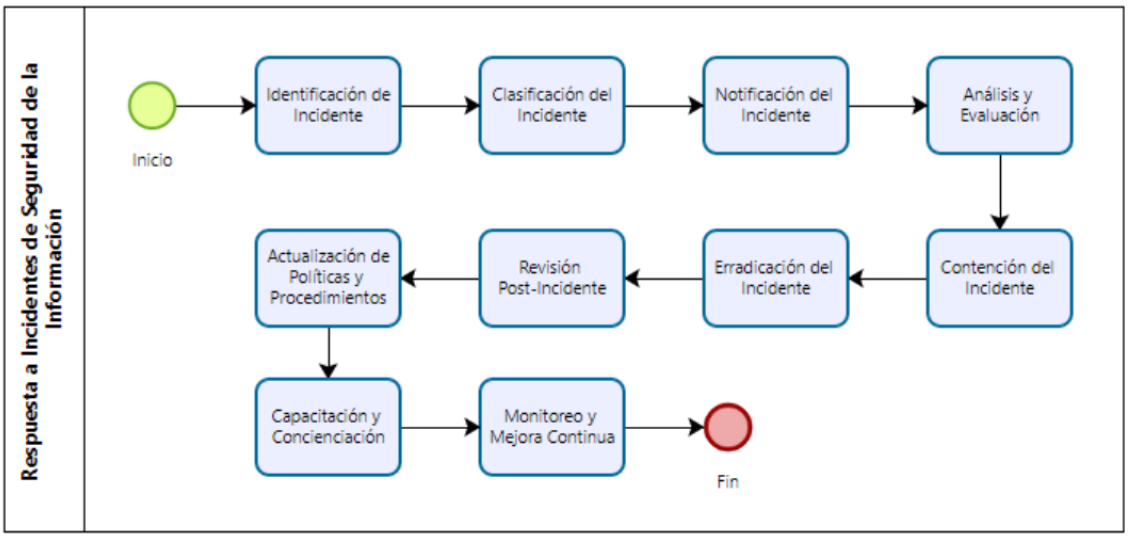
Revisión y Mejora Continua: Revisar y mejorar continuamente el proceso de evaluación y toma de decisiones sobre eventos de seguridad, adaptándose a nuevas amenazas y cambios en el entorno.

Fin: Finalización del proceso, asegurando que la política de evaluación y decisión sobre eventos de seguridad de la información está en operación y es efectiva

ALCALDÍA CAYAMBE unidosrenacemos	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE**	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de respuesta a incidentes de seguridad de la información**	**Dominio:** Organizativo **Fecha:**
Resumen	Esta política establece los procedimientos y responsabilidades para	

	gestionar incidentes de seguridad de la información en el Municipio de Cayambe para minimizar su impacto y evitar que se repitan en el futuro.
Objetivo	El objetivo de esta política es asegurar una respuesta organizada y eficaz ante incidentes de seguridad de la información, asegurar la continuidad del negocio, proteger la información confidencial y asegurar el cumplimiento de los requisitos regulatorios vigentes.
Alcance	Esta política aplica a todos los empleados, contratistas, proveedores y cualquier otra persona que tenga acceso a los sistemas de información del Municipio de Cayambe.
Políticas	
Reconocer incidentes de seguridad: todos los empleados deben estar capacitados para reconocer e informar posibles incidentes de seguridad de la información. **Aviso:** Los incidentes deben informarse de inmediato al Equipo de Respuesta a Emergencias (ERI) de la ciudad. Evaluación y clasificación: ERI evaluará y clasificará el incidente en función de su gravedad e impacto potencial. **Contención:** Se tomarán medidas inmediatas para contener el incidente y evitar su propagación. Eliminación: se identificará y eliminará la causa del evento. Recuperación: Los sistemas afectados serán restaurados y verificados para que funcionen normalmente. **Análisis post-incidente:** Se realizará un análisis detallado para sacar conclusiones y mejorar las medidas de seguridad.	
Responsabilidades	**Equipo de Respuesta a Emergencias (ERI):** Responsable de coordinar la respuesta a incidentes de seguridad, incluida la evaluación, contención, eliminación y recuperación.

	Empleados: deben informar inmediatamente cualquier violación de seguridad y seguir las instrucciones de ERI. **Departamento de Tecnología de la Información (DTI):** Apoya a ERI en la implementación de medidas técnicas y proporcionando los recursos necesarios para responder a incidentes. **Gestión:** Asegúrese de que haya recursos suficientes para implementar eficazmente esta política y que todo el personal esté completamente capacitado.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de respuesta a incidentes de seguridad de la información.

Identificación de Incidente: Detectar y reportar el incidente de seguridad a través de sistemas de monitoreo, alertas, y notificaciones del personal.

Clasificación del Incidente: Clasificar el incidente según su gravedad, impacto en la organización y urgencia de la respuesta.

Notificación del Incidente: Notificar a las partes interesadas relevantes y al equipo de respuesta a incidentes, asegurando una respuesta rápida y coordinada.

Análisis y Evaluación: Realizar un análisis detallado del incidente para entender su naturaleza, alcance y causa raíz.

Contención del Incidente: Implementar medidas inmediatas para contener el incidente y prevenir su propagación o impacto adicional.

Erradicación del Incidente: Eliminar la causa del incidente, como malware, accesos no autorizados o vulnerabilidades explotadas.

Recuperación: Restaurar los sistemas y servicios afectados a su estado normal de operación, asegurando que estén libres de amenazas residuales.

Revisión Post-Incidente: Realizar una revisión post-incidente para analizar las causas, la efectividad de la respuesta y las áreas de mejora.

Actualización de Políticas y Procedimientos: Actualizar las políticas y procedimientos de seguridad basados en las lecciones aprendidas del incidente.

Capacitación y Concienciación: Capacitar al personal sobre la política de respuesta a incidentes, las lecciones aprendidas y las mejores prácticas.

Monitoreo y Mejora Continua: Monitorear continuamente los sistemas de seguridad y mejorar la política y los procedimientos de respuesta a incidentes basándose en nuevas amenazas y

experiencias. **Fin:** Finalización del proceso de implementación y gestión de la política, asegurando que esté en operación y sea efectiva.

	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE**	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de privacidad y protección de la información personal**	**Dominio:** Organizativo **Fecha:**
Resumen	Esta política establece los lineamientos y procedimientos para la recopilación, uso, almacenamiento y protección de datos personales de los residentes del Municipio de Cayambe. Se compromete a garantizar la privacidad y seguridad de los datos personales de acuerdo con las leyes y regulaciones aplicables.	
Objetivo	El objetivo de esta política es proteger los datos personales de los ciudadanos, empleados y cualquier otra persona cuyos datos sean administrados por el Municipio de Cayambe, asegurando la confidencialidad, integridad y disponibilidad del uso de esos datos.	
Alcance	Esta política aplica a todas las agencias, empleados y contratistas del Municipio de Cayambe que recopilan, procesan, almacenan o disponen de datos personales. Incluye cualquier dato recopilado en forma electrónica o física.	
Políticas		
Recolección de datos: Sólo se recogen datos personales que sean necesarios y relevantes para una		

<table>
<tr><td colspan="2">finalidad concreta, y siempre con el consentimiento expreso del interesado.

Uso de los datos: Los datos personales sólo serán utilizados para los fines específicos para los que fueron recabados y con el consentimiento del titular.

Almacenamiento y seguridad de datos: Los datos personales se almacenarán de forma segura utilizando medidas técnicas y organizativas apropiadas para protegerlos contra el acceso no autorizado, pérdida, destrucción o daño.

Acceder y editar datos: Los ciudadanos tienen derecho a acceder a sus datos personales y a que se corrija cualquier información inexacta o desactualizada.

Cesión de datos: No se cederán datos personales a terceros sin el consentimiento expreso del titular, salvo obligación legal.

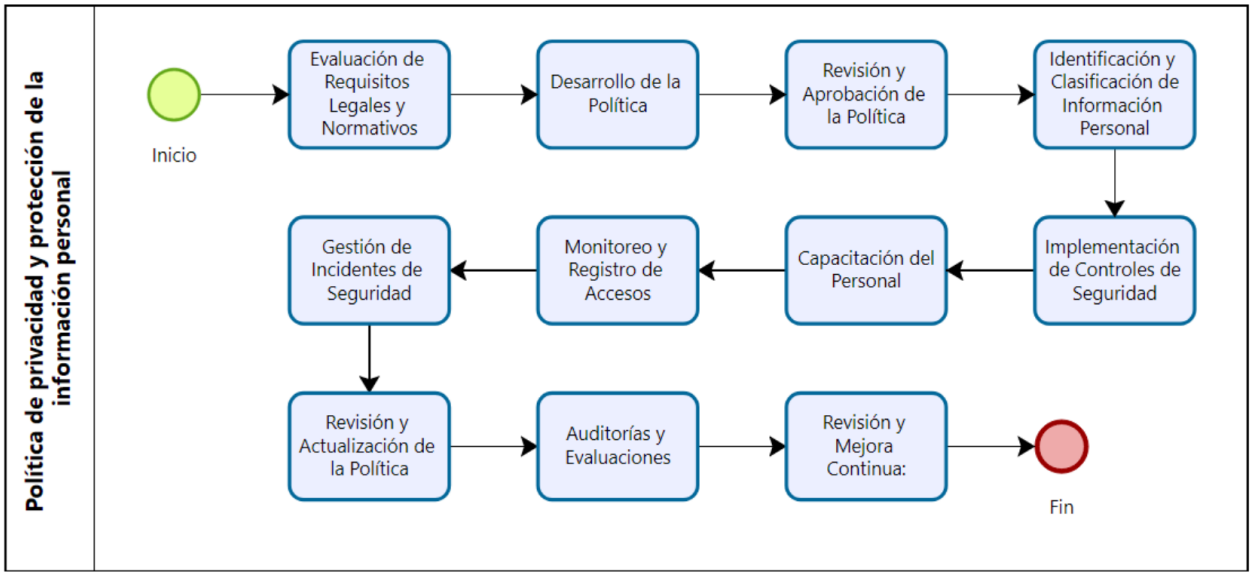
Destrucción de datos: La información personal se destruirá de forma segura cuando ya no sea necesaria para los fines para los que fue recopilada.</td></tr>
<tr><td>Responsabilidades</td><td>Delegado de Protección de Datos (DPO): Designar a una persona responsable de supervisar el cumplimiento de esta política y las leyes de protección de datos aplicables.

Empleados y contratistas: Siga las reglas descritas en esta política e informe cualquier violación de seguridad o de datos de inmediato.

Ciudadanos: proporcione información auténtica y actualizada y coopere con su municipio para corregir su información si es necesario.</td></tr>
<tr><td>Sanciones</td><td>El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.</td></tr>
</table>

Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.

Diagrama de flujo para la política



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de privacidad y protección de información personal.

Evaluación de Requisitos Legales y Normativos: Identificar y comprender los requisitos legales y normativos aplicables a la privacidad y protección de información personal.

Desarrollo de la Política: Crear una política de privacidad y protección de información personal que cumpla con los requisitos legales y normativos identificados.

Revisión y Aprobación de la Política: Revisar y aprobar la política por las partes interesadas para asegurar su validez y aplicabilidad.

Identificación y Clasificación de Información Personal: Identificar y clasificar la información

personal que se manejará, basándose en su sensibilidad y criticidad.

Implementación de Controles de Seguridad: Implementar controles de seguridad adecuados para proteger la información personal contra accesos no autorizados, pérdida, divulgación o destrucción.

Capacitación del Personal: Capacitar al personal sobre la política de privacidad y los controles de seguridad implementados, asegurando su comprensión y cumplimiento.

Monitoreo y Registro de Accesos: Establecer sistemas para monitorear y registrar los accesos a la información personal, detectando y respondiendo a actividades sospechosas.

Gestión de Incidentes de Seguridad: Establecer procedimientos para la gestión de incidentes de seguridad relacionados con la información personal, incluyendo detección, reporte, y respuesta.

Revisión y Actualización de la Política: Revisar y actualizar periódicamente la política de privacidad y protección de información personal para asegurar su efectividad y cumplimiento continuo.

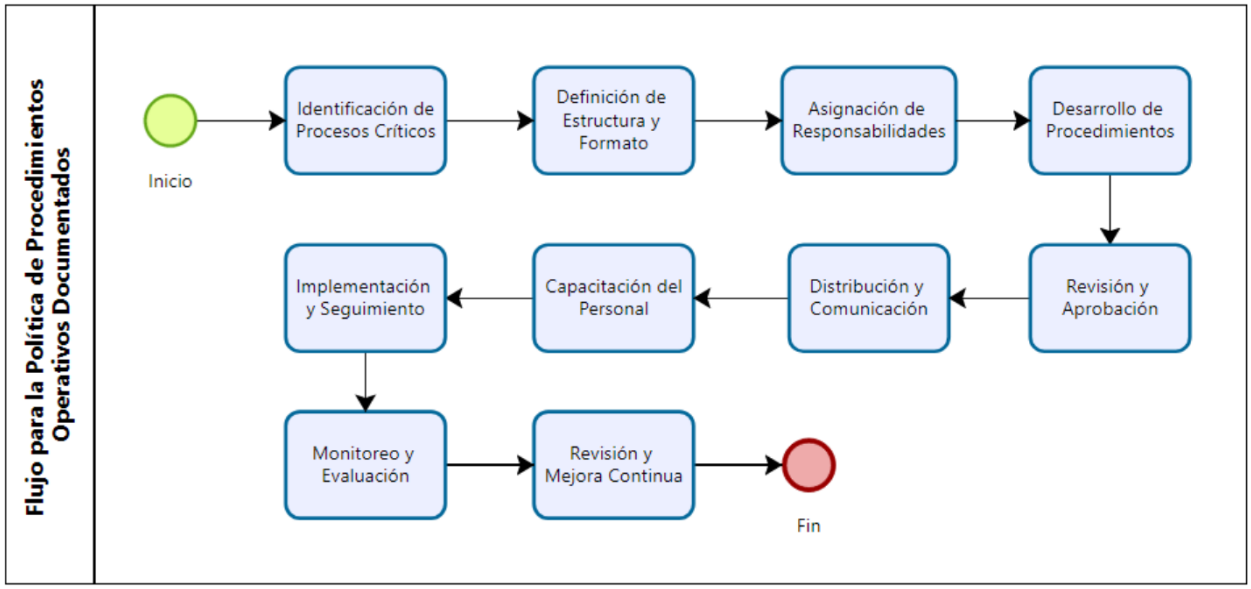
Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento de la política y la efectividad de los controles implementados.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política basada en los resultados de las auditorías y evaluaciones, adaptándose a nuevas amenazas y requisitos.

Fin: Finalización del proceso de implementación y gestión de la política, asegurando su operación efectiva y continua.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de procedimientos operativos documentados**	**Dominio:** Organizativo **Fecha:**
Resumen	Esta política proporciona orientación sobre la documentación, implementación, revisión y actualización de procedimientos operativos en el Municipio de Cayambe. Su propósito es asegurar la eficiencia, transparencia y coherencia en las operaciones del gobierno municipal, promoviendo la mejora continua y el cumplimiento de la normativa aplicable.	
Objetivo	El objetivo de esta política es proporcionar una base clara y consistente para la documentación y gestión de los procesos operativos en el Municipio de Cayambe. Esto asegura la implementación consistente y efectiva de todas las actividades y tareas, mejorando la calidad del servicio y la satisfacción de los ciudadanos.	
Alcance	Esta política aplica a todos los departamentos y funcionarios del Municipio de Cayambe. Todos los procesos operativos que afecten las operaciones del municipio deben ser registrados, implementados y controlados de acuerdo con los lineamientos descritos en esta política.	
Políticas		
Documentación estandarizada: todos los procesos de trabajo deben documentarse en un formato estándar que incluya propósito, alcance, pasos detallados, partes responsables e hitos. **Capacitación:** Todos los empleados deben recibir capacitación adecuada en procedimientos de trabajo documentados adecuados a sus responsabilidades.		

Revisión y aprobación: Todos los procedimientos deben ser revisados y aprobados por la Gerencia de Operaciones antes de su implementación. **Accesibilidad:** Los procedimientos operativos documentados deben estar disponibles para todos los empleados del Municipio.	
Responsabilidades	**Junta de Gestión de Operaciones:** Responsable de revisar, aprobar y actualizar los procedimientos operativos escritos. **Gerente de Departamento:** Asegúrese de que los procedimientos operativos en áreas relevantes estén documentados e implementados de acuerdo con la política. **Empleados:** Siga los procedimientos operativos documentados e informe cualquier desviación o problema a su supervisor.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.
Diagrama de flujo para la política	



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de procedimientos operativos documentados.

Identificación de Procesos Críticos: Identificar los procesos operativos críticos del municipio que necesitan ser documentados para asegurar su correcta ejecución.

Definición de Estructura y Formato: Establecer una estructura y formato estándar para la documentación de procedimientos, asegurando uniformidad y claridad.

Asignación de Responsabilidades: Asignar responsabilidades claras para la creación, revisión, actualización y mantenimiento de los procedimientos documentados.

Desarrollo de Procedimientos: Desarrollar y redactar los procedimientos operativos documentados, asegurando que sean claros, completos y accesibles.

Revisión y Aprobación: Revisar los procedimientos documentados por las partes interesadas y obtener su aprobación formal para asegurar su validez y aplicabilidad.

Distribución y Comunicación: Distribuir los procedimientos operativos documentados a todo el

personal relevante y asegurarse de que estén disponibles cuando se necesiten.

Capacitación del Personal: Capacitar al personal sobre los nuevos procedimientos operativos documentados para asegurar su comprensión y correcta implementación.

Implementación y Seguimiento: Implementar los procedimientos operativos documentados y realizar un seguimiento para asegurar su cumplimiento y efectividad.

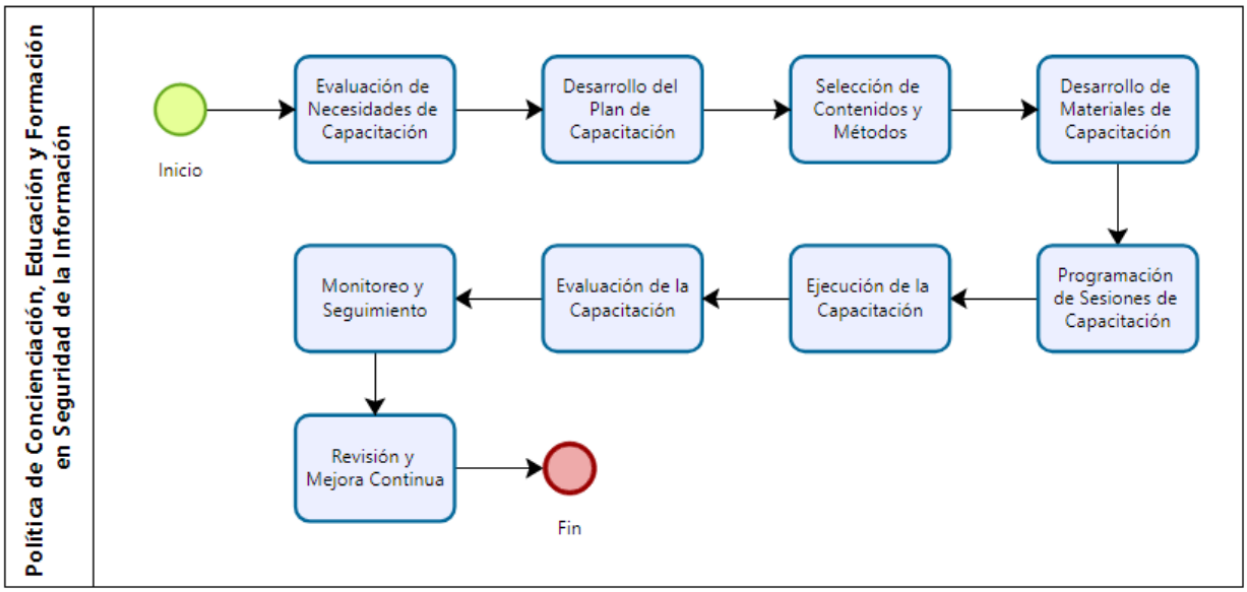
Monitoreo y Evaluación: Monitorear y evaluar continuamente la efectividad de los procedimientos operativos documentados, identificando áreas de mejora.

Revisión y Mejora Continua: Revisar y mejorar continuamente los procedimientos operativos documentados basándose en los resultados del monitoreo y la evaluación, así como en los cambios en los procesos o el entorno.

Fin: Finalización del proceso, asegurando que la política de procedimientos operativos documentados está en operación y es efectiva.

Resumen	Esta política tiene como objetivo proporcionar un marco para la concientización, educación y capacitación sobre seguridad de la información para los empleados del Municipio de Cayambe. La implementación adecuada de esta política ayudará a proteger la integridad, seguridad y disponibilidad de la información administrada por el gobierno de la ciudad
Objetivo	Asegúrese de que todos los empleados del Municipio de Cayambe comprendan y practiquen prácticas seguras de gestión de la información. Esto se logra a través de programas de capacitación y concientización que promueven una cultura de seguridad en toda la organización.
Alcance	Esta política aplica a todos los empleados, contratistas y empleados del Municipio de Cayambe que tengan acceso a la información y los sistemas de información del Municipio.
Políticas	
Evaluación de necesidades: Realizar evaluaciones periódicas para determinar las necesidades de capacitación en seguridad de la información. **Programas de Capacitación:** Desarrollar e implementar programas de capacitación adecuados a los diferentes niveles de responsabilidad y áreas laborales. **Concientización continua:** realizar campañas y eventos de concientización periódicos para garantizar que la seguridad de la información sea una preocupación para todos los empleados. **Evaluar la efectividad:** Medir la efectividad de los programas de capacitación a través de evaluaciones y encuestas.	
Responsabilidades	**Gerente de seguridad de la información:** coordina la implementación de políticas, desarrolla programas de capacitación y evalúa su efectividad. **Liderazgo:** asegúrese de que su equipo participe en actividades de

	capacitación y divulgación. **Empleados:** Participar activamente en programas de capacitación y seguir los procedimientos de seguridad establecidos.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.



Descripción de cada paso

Inicio: Comienza el proceso de implementación de la política de concienciación, educación y formación en seguridad de la información.

Evaluación de Necesidades de Capacitación: Identificar las necesidades de capacitación en

seguridad de la información para los empleados del municipio, considerando los riesgos y amenazas específicos.

Desarrollo del Plan de Capacitación: Crear un plan de capacitación que detalle los objetivos, contenidos, métodos y cronograma de la formación en seguridad de la información.

Selección de Contenidos y Métodos: Seleccionar los contenidos educativos y los métodos de formación más adecuados, como talleres, seminarios, e-learning, entre otros.

Desarrollo de Materiales de Capacitación: Crear materiales de capacitación, incluyendo presentaciones, guías, videos y otros recursos educativos.

Programación de Sesiones de Capacitación: Planificar y programar las sesiones de capacitación, asegurando la participación de todos los empleados.

Ejecución de la Capacitación: Realizar las sesiones de capacitación según el plan establecido, asegurando la transmisión efectiva de conocimientos.

Evaluación de la Capacitación: Evaluar la efectividad de las sesiones de capacitación mediante encuestas, pruebas y feedback de los participantes.

Monitoreo y Seguimiento: Monitorear continuamente el nivel de concienciación y el cumplimiento de las prácticas de seguridad de la información, realizando seguimientos periódicos.

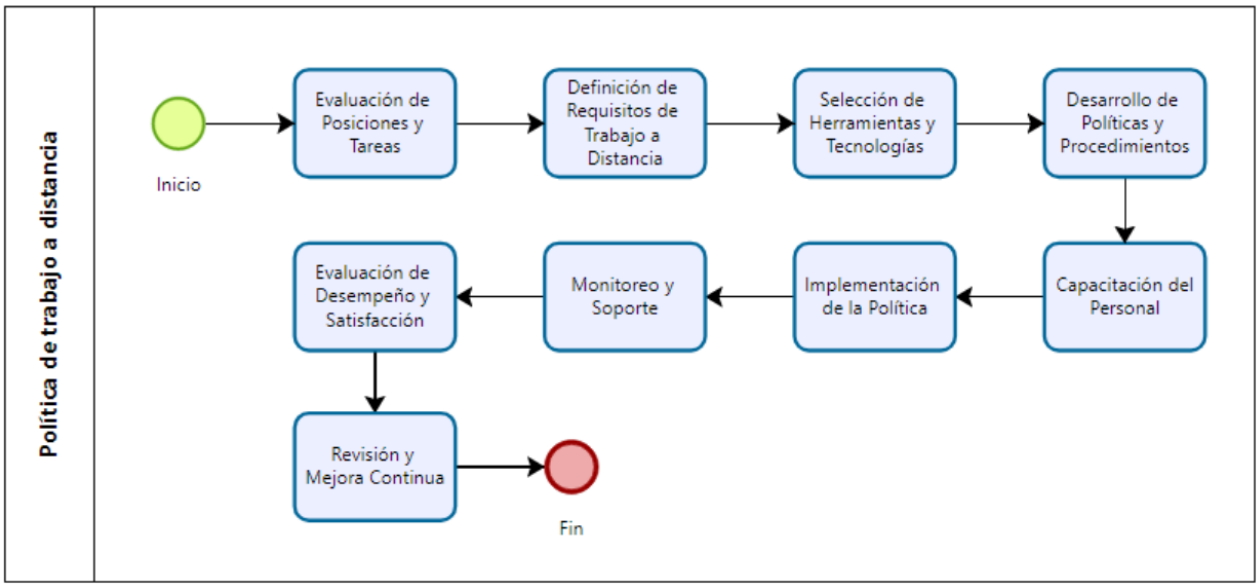
Revisión y Mejora Continua: Revisar y mejorar continuamente la política y los programas de capacitación basándose en los resultados de las evaluaciones y el monitoreo.

Fin: Finalización del proceso, asegurando que la política de concienciación, educación y formación en seguridad de la información está en operación y es efectiva

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de trabajo a distancia**	**Dominio:** Personas **Fecha:**
Resumen	Esta política establece los lineamientos y procedimientos para implementar el teletrabajo en el Municipio de Cayambe. El objetivo es proporcionar un marco claro para el trabajo a distancia, garantizando la eficiencia operativa y la seguridad de la información, al tiempo que se promueve la flexibilidad y el equilibrio entre la vida laboral y personal.	
Objetivo	Gestionar el trabajo remoto para garantizar la eficiencia y eficacia. Proteger la confidencialidad, integridad y disponibilidad de la información de la ciudad. Promover la adaptación a un entorno laboral flexible, beneficiando tanto a los empleados como al gobierno de la ciudad.	
Alcance	Esta política aplica a todos los empleados del Municipio de Cayambe que trabajan de forma remota, parcial o total. También incluye personal directivo y de recursos humanos encargado de gestionar y supervisar el trabajo remoto.	
Políticas		
El trabajo a distancia se aplicará en emergencias u ocasiones especiales calificarán para la autorización de empleo en el hogar, basándose en la directrices emitidas por el ministerio de Trabajo acuerdo ministerial MDT-2020-181 Un trabajador realiza todas o parte de sus funciones fuera de las oficinas, instalaciones o tareas de la empresa, como desde su casa u otra ubicación, la modalidad de prestación de servicios no presenciales en jornadas regulares e irregulares utilizando		

la tecnología de la información y la comunicación (TIC), tanto para gestionarla como para supervisarla y administrarla, por tanto se establece que: Se deberá establecer horarios de trabajo según actividades a realizar. El trabajador deberá dar buen uso de la información otorgada, sistemas, usuario y clave para las mismas. Se debe usar VPN para establecer conexiones remotas a los recursos informáticos los cuales deben ser creados por el departamento de tecnologías de la información. El equipo de cómputo para el teletrabajo debe ser provisto por el GADIP MC, el equipo deberá tener la configuración, seguridad e instalación de software a usar. Las computadoras personales se pueden usar para trabajar en casa siempre que acepte usar un software antivirus auténtico y actualizado y, si es necesario, configurar una conexión VPN para acceder a los recursos autorizados. En el caso de usar computadores personales, no deberán almacenar información relevante de la institución, para esto el jefe inmediato deberá establecer medidas de control, registro de actividades diarias solicitando informes o algún medio verificable. La vigencia de la clave de acceso al sistema para teletrabajo dependerá de la política de seguridad de la información. El trabajador no deberá instalar algún software distinto a los ya instalados, ya que el mismo puede afectar el buen funcionamiento del equipo. El usuario que aplique teletrabajo deberá conocer y cumplir de las políticas de seguridad de la información	
Responsabilidades	Empleados: Deben cumplir con los requisitos y procedimientos descritos en esta política, mantener la productividad y garantizar la seguridad de la información. Gerente: debe aprobar las solicitudes de trabajo remoto, monitorear el desempeño de los empleados y garantizar que se cumplan los criterios

	establecidos. Recursos Humanos: Debe gestionar los procesos de solicitud y aprobación de trabajo remoto, brindar capacitación y actualizar esta política según sea necesario. TI: Debes asegurarte de que los empleados cuenten con el soporte técnico necesario y que los sistemas y herramientas utilizados para el trabajo remoto cumplan con los estándares de seguridad.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.



Descripción de cada paso

Inicio: Comienza el proceso de implementación de la política de trabajo a distancia.

Evaluación de Posiciones y Tareas: Identificar las posiciones y tareas que pueden ser realizadas de forma remota, considerando la naturaleza del trabajo y los requisitos operativos.

Definición de Requisitos de Trabajo a Distancia: Establecer los requisitos y condiciones necesarias para el trabajo remoto, incluyendo criterios de elegibilidad, horario de trabajo, y responsabilidades.

Selección de Herramientas y Tecnologías: Seleccionar las herramientas y tecnologías necesarias para el trabajo remoto, como software de comunicación, herramientas de colaboración, y acceso seguro a la red.

Desarrollo de Políticas y Procedimientos: Definir las políticas y procedimientos específicos para el trabajo a distancia, incluyendo políticas de seguridad de la información, uso aceptable de equipos, y protocolos de comunicación.

Capacitación del Personal: Capacitar a los empleados sobre la política de trabajo a distancia y el uso adecuado de las herramientas tecnológicas, asegurando que comprendan sus responsabilidades y los procedimientos a seguir.

Implementación de la Política: Poner en marcha la política de trabajo a distancia, asegurando que todos los empleados elegibles tengan acceso a las herramientas y recursos necesarios.

Monitoreo y Soporte: Monitorear el desempeño de los empleados que trabajan a distancia y proporcionar soporte técnico y administrativo continuo para resolver cualquier problema que surja.

Evaluación de Desempeño y Satisfacción: Evaluar el desempeño de los empleados y su satisfacción con el trabajo a distancia a través de encuestas y revisiones periódicas.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de trabajo a distancia basándose en los resultados del monitoreo y la evaluación, así como en los comentarios de los empleados.

Fin: Finalización del proceso, asegurando que la política de trabajo a distancia está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de restricción de acceso a la información**	**Dominio:** Tecnológico
		Fecha:
Resumen	Una política de restricción de información es un conjunto de reglas y pautas establecidas por una organización para proteger la confidencialidad, integridad y disponibilidad de la información confidencial.	
Objetivo	La política de restricción de información tiene como objetivo proteger los importantes recursos de información de GADIP MC y garantizar el intercambio y la difusión de información adecuada y segura. Esta política proporciona pautas para controlar el acceso a la información y se aplica a todos los empleados, contratistas, proveedores y terceros que tienen acceso a la información de la organización.	
Alcance	Esta política se aplica a todos los sistemas, datos y recursos de información que son propiedad o están controlados por GADI MC, independientemente de su ubicación física.	
Criterios para implementar la política		
Clasificación de la información La información se clasificará en tres niveles de sensibilidad:		

Pública, Interna y Confidencial, de acuerdo con la política de clasificación de información de la organización.

Acceso basado en la necesidad

El acceso a la información se proporcionará según sea necesario. Los usuarios sólo tendrán acceso a la información necesaria para el desempeño de sus funciones laborales.

Políticas de contraseñas

Se implementará una política de contraseñas seguras para controlar el acceso a los sistemas y recursos de tecnología de información.

Controles de acceso

Se implementarán controles de acceso técnicos, como listas de control de acceso (ACL), autenticación de dos factores y registros de auditoría para garantizar que solo las personas autorizadas tengan acceso a la información confidencial.

Gestión de usuarios

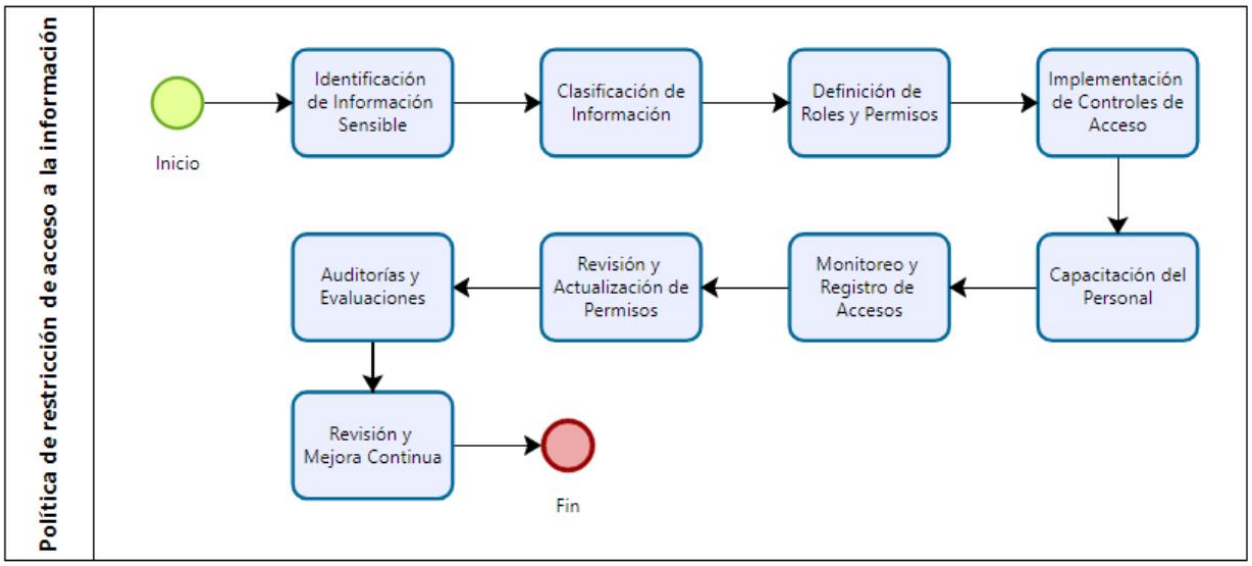
Los usuarios y los permisos se gestionarán de forma centralizada y el acceso se comprobará y actualizará periódicamente.

Divulgación y compartición de información

La divulgación y el intercambio de información confidencial requerirán el consentimiento expreso de la persona o departamento responsable de esa información.

Responsabilidades	Cada empleado y usuario de la información es responsable de proteger la información confidencial a la que tiene acceso y de informar cualquier incidente de seguridad o violación de las políticas.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.

Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.



Descripción de cada paso

Inicio: Comienza el proceso de implementación de la política de restricción de acceso a la información.

Identificación de Información Sensible: Identificar los datos e información que requieren acceso restringido debido a su sensibilidad o criticidad.

Clasificación de Información: Clasificar la información según niveles de sensibilidad y criticidad (pública, interna, confidencial, entre otras).

Definición de Roles y Permisos: Definir los roles y permisos necesarios para acceder a la información clasificada, estableciendo quién puede acceder a qué información.

Implementación de Controles de Acceso: Configurar y aplicar controles de acceso a la información basada en los roles y permisos definidos, utilizando tecnologías como ACLs (listas de control de acceso), RBAC (control de acceso basado en roles), entre otros.

Capacitación del Personal: Educar al personal sobre la política de restricción de acceso y sus

responsabilidades para asegurar el cumplimiento. **Monitoreo y Registro de Accesos:** Establecer un sistema para monitorear y registrar todos los accesos a la información sensible para detectar y responder a accesos no autorizados. **Revisión y Actualización de Permisos:** Revisar y actualizar regularmente los permisos de acceso para reflejar cambios en roles, responsabilidades o estructura organizativa. **Auditorías y Evaluaciones:** Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento y la efectividad de la política de restricción de acceso. **Revisión y Mejora Continua:** Revisar y mejorar continuamente la política de restricción de acceso basada en los resultados del monitoreo, auditorías y nuevas amenazas o requisitos. **Fin:** Finalización del proceso, asegurando que la política de restricción de acceso está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de autenticación segura**	**Dominio:** Tecnológico **Fecha:**
Resumen	Para evitar el acceso no autorizado a los sistemas y datos de una organización, es fundamental contar con una política de autenticación segura. A continuación, se da a conocer lo que contempla la política de autenticación segura que el GADIPMC puede utilizar.	
Objetivo	Asegurar que solo los usuarios autorizados tengan acceso a los sistemas y recursos de la organización, minimizando el riesgo de acceso no autorizado o compromisos de seguridad.	

Alcance	Todos los empleados, contratistas independientes, consultores y cualquier otra persona que necesite acceso a los recursos y sistemas de la organización están sujetos a esta política.

Criterios para implementar la política

Requisitos de contraseña:

Las contraseñas deben tener un mínimo de 12 caracteres.

Deben incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.

Las contraseñas no deben contener palabras completas del diccionario ni datos personales fácilmente predecibles (como nombres, fechas de nacimiento, número de cédulas o números de teléfono).

Las contraseñas deben cambiarse cada 90 días. No se deben reutilizar las últimas 5 contraseñas.

Autenticación de Múltiples Factores (MFA)

Todos los accesos a sistemas críticos y datos sensibles deben requerir MFA.

Los factores de autenticación pueden incluir:

Algo que el usuario sabe (contraseña o PIN).

Algo que el usuario tiene (token de hardware, aplicación de autenticación).

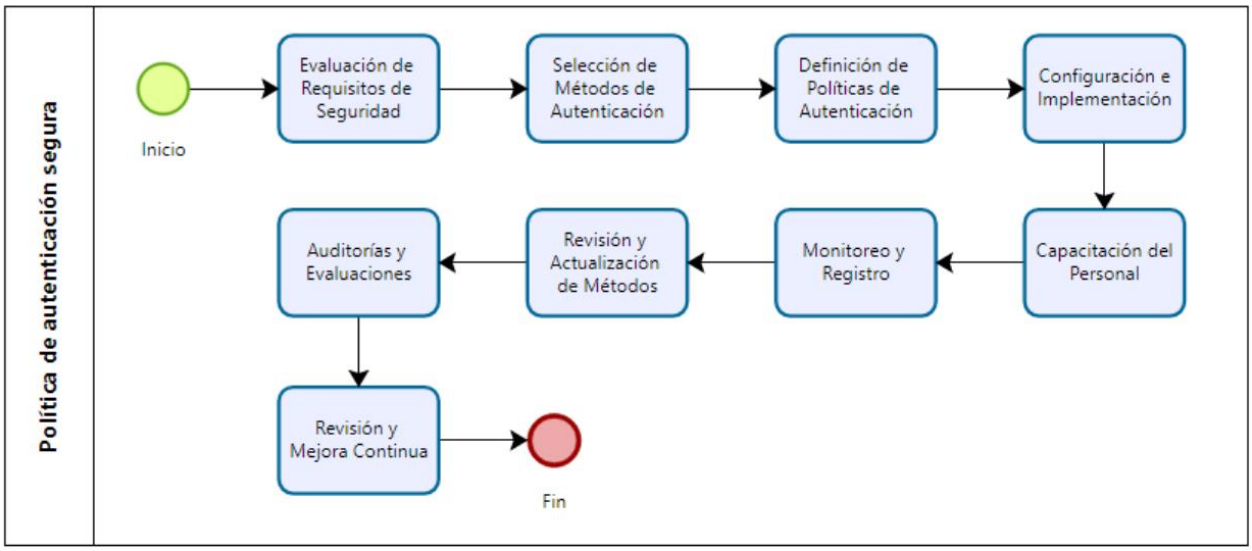
Algo que el usuario es (biometría, como huella dactilar o reconocimiento facial).

Acceso remoto

Todo acceso remoto debe utilizar conexiones seguras (VPN con autenticación MFA).

Solo se deben permitir dispositivos autorizados y gestionados por el departamento de TI	
Responsabilidades	**Usuarios** Crear contraseñas que cumplan con los requisitos establecidos. No compartir contraseñas con nadie. Informar de inmediato cualquier sospecha de compromiso de sus credenciales al equipo de TI. Asegurar que las sesiones estén cerradas cuando no estén en uso. **Departamento de TI** Implementar y mantener tecnologías de autenticación segura. Proveer herramientas y capacitación para la creación y gestión de contraseñas seguras. Configurar y gestionar sistemas de autenticación de múltiples factores. Monitorear y auditar los accesos para detectar y responder a accesos no autorizados. Desbloquear cuentas y restablecer contraseñas cuando sea necesario, después de verificar la identidad del usuario. Revisar y actualizar regularmente esta política y los procedimientos relacionados.

	Alta Dirección Asegurar el cumplimiento de esta política por parte de todos los empleados y contratistas. Proveer los recursos necesarios para la implementación y mantenimiento de la autenticación segura.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política se revisará periódicamente para garantizar su relevancia y eficacia.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.



Descripción de cada paso

Inicio: Comienza el proceso de implementación de la política de autenticación segura.

Evaluación de Requisitos de Seguridad: Identificar las necesidades y requisitos específicos de seguridad para la autenticación en el municipio.

Selección de Métodos de autenticación: Elegir los métodos de autenticación más adecuados, como contraseñas fuertes, autenticación multifactor (2FA), biometría, entre otros.

Definición de Políticas de Autenticación: Establecer políticas claras sobre la gestión de contraseñas, el uso de autenticación multifactor y otros métodos de autenticación.

Configuración e Implementación: Configurar e implementar los métodos de autenticación seleccionados en todos los sistemas y aplicaciones del municipio.

Capacitación del Personal: Educar al personal sobre la política de autenticación segura y cómo utilizar correctamente los métodos de autenticación.

Monitoreo y Registro: Establecer procedimientos para monitorear los eventos de autenticación y registrar actividades para detectar y responder a incidentes de seguridad.

Revisión y Actualización de Métodos: Revisar y actualizar regularmente los métodos de autenticación para asegurar que se mantengan efectivos contra nuevas amenazas.

Auditorías y Evaluaciones: Realizar auditorías y evaluaciones periódicas para asegurar el cumplimiento y la efectividad de la política de autenticación.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de autenticación segura basándose en los resultados del monitoreo y las auditorías.

Fin: Finalización del proceso, asegurando que la política de autenticación segura está en operación y es efectiva

VERSIÓN 1.0	**Política de protección contra el malware**	**Dominio:** Tecnológico **Fecha:**
Resumen	La política de protección contra el malware se encarga de proteger los sistemas y datos municipales de cualquier software malicioso. Esta política busca asegurar la integridad, confidencialidad y disponibilidad de la información, a la vez que protege a los usuarios y recursos tecnológicos del municipio	
Objetivo	El objetivo de esta política es definir las medidas preventivas y correctivas necesarias a implementar para proteger los sistemas de información y datos del municipio contra el malware. Esto incluye la identificación, prevención, y respuesta rápida a cualquier incidente relacionado con software malicioso	
Alcance	Esta política aplica a todos los empleados, contratistas, voluntarios y cualquier otra persona que utilice los recursos tecnológicos del Municipio de Cayambe. Incluye todos los dispositivos, redes y sistemas de información del municipio	
Políticas		
Software de Seguridad: Instalar y mantener actualizado un software antivirus y antimalware en todos los dispositivos del municipio. Configurar el software para realizar escaneos automáticos y programados de todos los sistemas. **Actualización de Sistemas:** Asegurar que todos los sistemas operativos, aplicaciones y hardware estén actualizados con los		

<table>
<tr><td colspan="2">últimos parches y actualizaciones de seguridad.

Monitoreo y Detección:

Establecer sistemas de monitoreo continuo para detectar y responder a actividades de índole sospechoso o malicioso.

Realizar auditorías y análisis de vulnerabilidades de manera regular.

Educación y Concienciación:

Proveer capacitación periódica a todos los empleados sobre las buenas prácticas de seguridad y cómo reconocer y reportar posibles amenazas de malware.</td></tr>
<tr><td>Responsabilidades</td><td>Departamento de TI:

Implementar herramientas y procedimientos de seguridad necesarios.

Monitorear los sistemas y responder ante incidentes de malware.

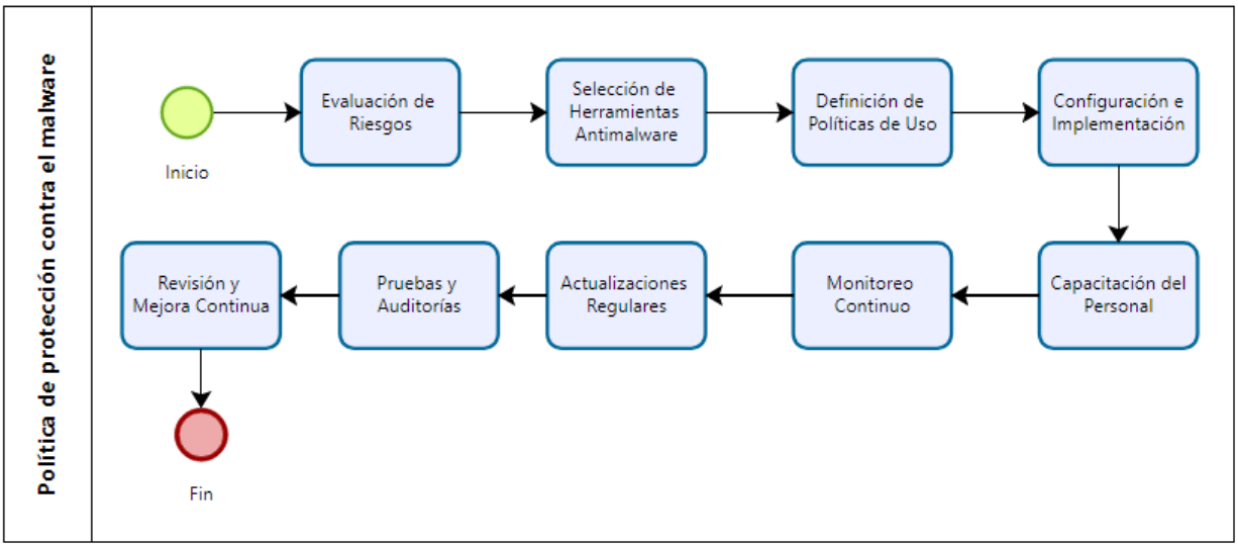
Proveer capacitación y soporte técnico al personal administrativo.

Personal administrativo del GADIPMC:

Seguir las directrices de la política y reportar cualquier actividad sospechosa.

No descargar, instalar o ejecutar software no autorizado o aplicaciones sospechosas.</td></tr>
<tr><td>Sanciones</td><td>El incumplimiento de esta política puede resultar en medidas</td></tr>
</table>

	disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	Esta política será revisada anualmente por el departamento de TI en coordinación con la dirección del municipio para asegurar su relevancia y efectividad
Actualización	Las actualizaciones serán comunicadas a todos los empleados y usuarios de la red municipal.



Proceso de cada paso

Inicio: Comienza el proceso para establecer una política de protección contra el malware.

Evaluación de Riesgos: Identificar las amenazas de malware y evaluar los riesgos asociados para el municipio.

Selección de Herramientas Antimalware: Elegir las soluciones de software antimalware adecuadas para proteger los sistemas del municipio.

Definición de Políticas de Uso: Establecer políticas claras sobre el uso de herramientas antimalware y prácticas de seguridad.

Configuración e Implementación: Configurar e implementar las herramientas antimalware en

todos los sistemas y dispositivos del municipio.

Capacitación del Personal: Educar al personal sobre la política de protección contra malware y cómo utilizar las herramientas adecuadamente.

Monitoreo Continuo: Establecer procedimientos para monitorear continuamente los sistemas en busca de malware y responder a incidentes.

Actualizaciones Regulares: Asegurar que las herramientas antimalware y los sistemas operativos se actualicen regularmente para proteger contra nuevas amenazas.

Pruebas y Auditorías: Realizar pruebas y auditorías periódicas para evaluar la efectividad de la protección contra malware.

Revisión y Mejora Continua: Revisar y mejorar continuamente la política de protección contra malware basándose en los resultados del monitoreo y auditorías.

Fin: Finalización del proceso, asegurando que la política está en operación y es efectiva.

Este diagrama de flujo te ayudará a visualizar y seguir los pasos necesarios para implementar una política de protección contra malware eficaz en el municipio de Cayambe.

ALCALDÍA CAYAMBE unidosrenacemos	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE**	**Autor:** Lenin Jami
VERSIÓN 1.0	**Política de filtrado Web**	**Dominio:** Tecnológico
		Fecha:
Resumen	La política de filtrado web tiene como propósito garantizar un acceso seguro, eficiente y ético de los recursos de internet en todas las dependencias de la institución. La política busca proteger la infraestructura tecnológica, prevenir el acceso a contenido inapropiado y garantizar el cumplimiento de	

	normativas y leyes vigentes.
Objetivo	El objetivo de esta política es establecer pautas claras para el uso del servicio de internet, promoviendo un entorno de trabajo productivo y seguro, buscando prevenir el uso inadecuado de los recursos de Red, a su vez proteger la información sensible del municipio y asegurar el cumplimiento de normativas legales
Alcance	Esta política aplica a todos los empleados, contratistas, voluntarios y cualquier otra persona que utilice los recursos de internet del GADIPMC. Esto incluye el acceso desde dispositivos municipales asignados y equipos personales dentro de la Red del municipio.

Política

Clasificación de Sitios Web:

Permitidos: Sitios relacionados con actividades laborales, educativos, gubernamentales y otros necesarios para el cumplimiento de funciones del municipio.

Restringidos: Redes sociales, sitios de entretenimiento, juegos en línea y otros servicios no relacionados con las actividades laborales, los cuales generan una distracción y pérdida de tiempo en horas de trabajo.

Prohibidos: Sitios con contenido inseguro, ilegal, pornográfico, violento, de apuestas, y cualquier otro que pueda comprometer la seguridad o integridad del sistema interno.

Monitoreo y Reportes:

Implementar sistemas de monitoreo que registren el uso de internet y acceso a páginas o servicios, mismos que generen reportes periódicos.

<table>
<tr><td colspan="2">Realizar revisiones regulares para asegurar el cumplimiento de la política.

Excepciones:

Las excepciones a esta política deben ser aprobadas y documentadas una vez establecido los alcances y limitaciones que se acuerden entre el Departamento de Tecnologías de la información y demás miembros del Directivo</td></tr>
<tr><td>Responsabilidades</td><td>Departamento de TI:

Implementar y mantener los sistemas de filtrado Web

Monitorear el cumplimiento de la política y documentar los reportes de seguimiento

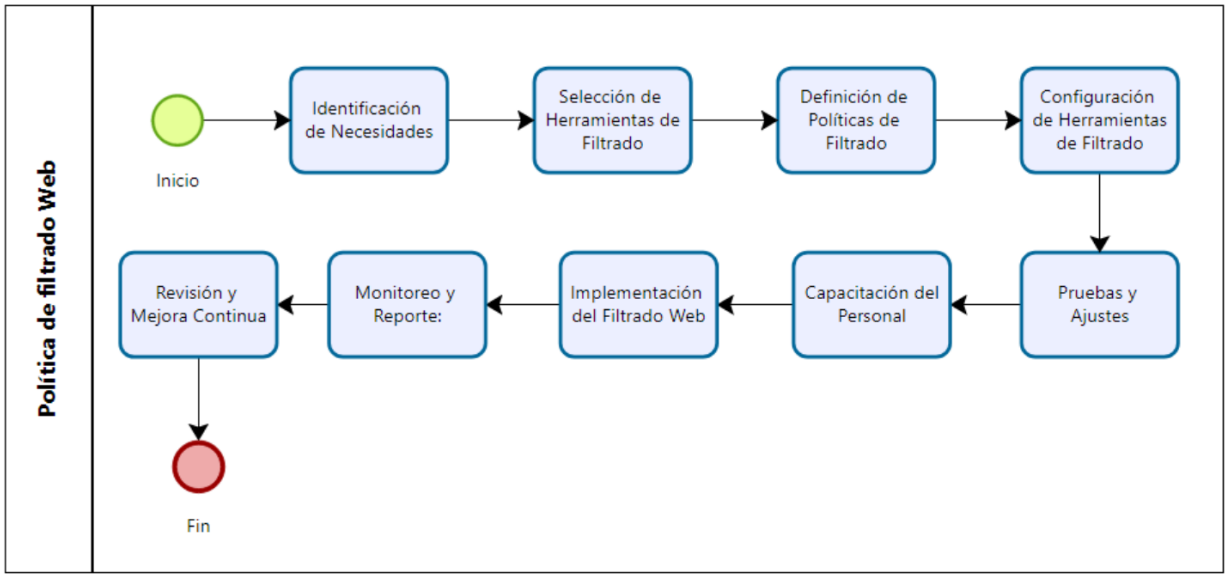
Revisar y actualizar la política según sea necesario.

Personal administrativo del GADIPMC:

Usar el servicio de internet de manera responsable y conforme a esta política.

Reportar cualquier actividad sospechosa con respecto al acceso de páginas WEB que se consideren como una amenaza</td></tr>
<tr><td>Sanciones</td><td>El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.</td></tr>
<tr><td>Revisión</td><td>Esta política será revisada anualmente por el departamento de TI en coordinación con la dirección del municipio para asegurar su relevancia y efectividad</td></tr>
</table>

Actualización	Las actualizaciones serán comunicadas a todos los empleados y usuarios de la red municipal.



Descripción de cada paso

Inicio: Inicio del proceso de implementación de la política de filtrado web.

Identificación de Necesidades: Evaluar las necesidades del municipio para el filtrado web, incluyendo objetivos y requisitos específicos.

Selección de Herramientas de Filtrado: Elegir las soluciones de software o hardware que se utilizarán para el filtrado web.

Definición de Políticas de Filtrado: Establecer políticas claras sobre qué tipos de contenido deben ser bloqueados o permitidos.

Configuración de Herramientas de Filtrado: Configurar las herramientas seleccionadas de acuerdo con las políticas definidas.

Pruebas y Ajustes: Realizar pruebas iniciales del sistema de filtrado y ajustar las configuraciones según los resultados.

Capacitación del Personal: Educar al personal sobre la política y el uso adecuado de las herramientas de filtrado web.

Implementación del Filtrado Web: Activar el sistema de filtrado web en la red del municipio. **Monitoreo y Reporte:** Establecer procedimientos para el monitoreo continuo del tráfico web y generar reportes de uso y cumplimiento. **Revisión y Mejora Continua:** Revisar periódicamente la política y las configuraciones para mejorar la efectividad y adaptarse a nuevas necesidades. **Fin:** Finalización del proceso, asegurando que la política está en operación y es efectiva.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL GADIP DEL MUNICIPIO DE CAYAMBE	Autor: Lenin Jami
VERSIÓN 1.0	**Política de segregación en redes**	Dominio: Organizativo Fecha:
Resumen	Esta política propone establecer un marco de referencia para la segregación de redes en el Municipio de Cayambe para mejorar la seguridad, el desempeño y la gestión de la infraestructura de redes. La segregación en la red ayuda a proteger los datos confidenciales, optimizar los recursos y reducir el riesgo de acceso no autorizado y ciberataques	
Objetivo	Establecer un entorno de red seguro y eficiente, mediante la implementación de técnicas de segregación de red para garantizar la integridad, seguridad y disponibilidad de los recursos y datos del Municipio de Cayambe.	
Alcance	Esta política se aplica a todas las redes y sistemas de información del GADIPMC, incluidas comunicaciones internas, externas, inalámbricas y todas las demás formas de comunicación electrónica utilizadas en la institución	
Política		

Segmentación de Red.

La red municipal se dividirá en segmentos independientes basados en funciones y niveles de seguridad.

Se implementarán VLANs (Redes de Área Local Virtuales) para separar el tráfico de red de diferentes departamentos y funciones.

Se establecerán DMZ (Zonas Desmilitarizadas) para servicios públicos accesibles desde internet.

Controles de Acceso

Se usarán firewalls y sistemas de prevención de intrusiones (IPS) para controlar y monitorear el tráfico entre los diferentes segmentos de la red.

Se implementarán políticas de acceso basado en roles (RBAC) para limitar el acceso a los recursos según el rol del usuario.

Autenticación y autorización

Todos los dispositivos y usuarios deben autenticarse mediante sistemas robustos de autenticación, como 2FA (autenticación de dos factores).

Se implementarán políticas estrictas de contraseñas y renovaciones periódicas

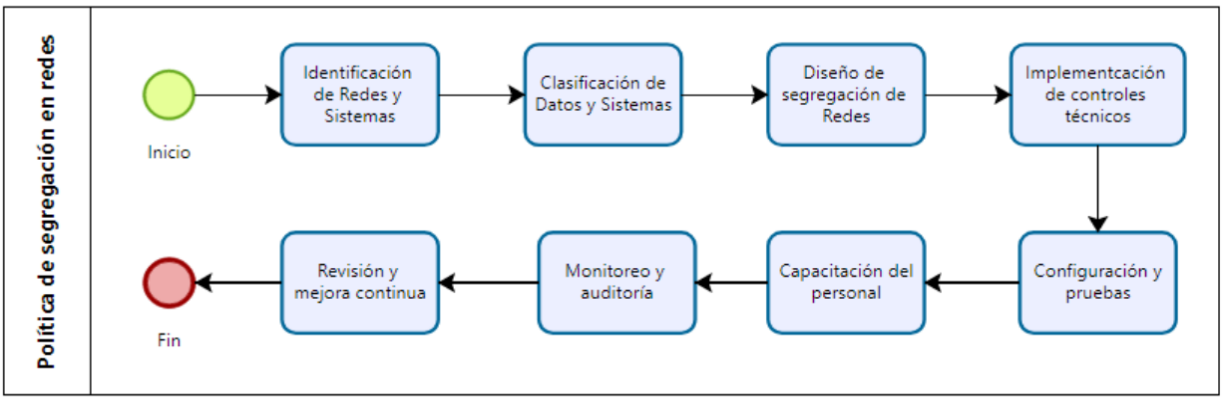
Monitoreo y Auditoría

Se utilizarán sistemas de monitoreo continuo para detectar y responder a actividades sospechosas o no autorizadas.

Los registros de acceso y eventos de seguridad se revisarán regularmente para detectar posibles brechas de seguridad

Responsabilidades	**Departamento de Tecnología de la Información (TI):** Desarrollar, implementar y mantener la infraestructura de red segregada. Configurar y gestionar los dispositivos de red y seguridad. Realizar auditorías periódicas y mantener registros de eventos de seguridad.

	Usuarios Finales: Cumplir con las políticas de seguridad y directrices de acceso. Reportar cualquier actividad sospechosa o incidentes de seguridad al departamento de TI. **Administración Municipal:** Proveer recursos y apoyo necesarios para la implementación de la política. Supervisar el cumplimiento de las políticas de seguridad y tomar medidas correctivas cuando sea necesario.
Sanciones	El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensiones o terminación del empleo, según la gravedad de la infracción y las políticas internas de la institución.
Revisión	La política de segregación en redes será revisada y actualizada al menos una vez al año o cuando ocurra un cambio significativo en la infraestructura de TI o en la naturaleza de las amenazas de seguridad.
Actualización	Se realizarán actualizaciones según sea necesario para abordar cambios en la tecnología y las amenazas de seguridad.



Descripción de cada paso

Inicio: Inicio del proceso para establecer una política de segregación en redes.

Identificación de Redes y Sistemas: Catalogar todas las redes y sistemas existentes en el

municipio.

Clasificación de Datos y Sistemas: Determinar la sensibilidad y criticidad de los datos y sistemas para priorizar la segregación.

Diseño de la Segregación de Redes: Crear un plan detallado de cómo se dividirán las redes, incluyendo la creación de subredes y segmentación.

Implementación de Controles Técnicos: Aplicar controles técnicos necesarios para asegurar la separación adecuada de redes, como VLANs y firewalls.

Configuración y Pruebas: Configurar las nuevas redes segregadas y realizar pruebas para asegurar que funcionan correctamente y son seguras.

Capacitación del Personal: Educar al personal sobre la nueva estructura de red y sus responsabilidades para mantener la seguridad.

Monitoreo y Auditoría: Establecer mecanismos para monitorear las redes y auditar su uso para asegurar el cumplimiento de la política.

Revisión y Mejora Continua: Revisar regularmente la política y la implementación para identificar y aplicar mejoras.

Fin: Finalización del proceso, asegurando que la política está en plena operación y es efectiva.

5.4 Socialización del SGSI

La socialización y entrega del Sistema de Gestión de Seguridad de la Información (SGSI) del Municipio de Cayambe se realizó a través una reunión informativa al personal del Departamento de Tecnologías de la Información. Durante esa actividad, se presentarán los objetivos, beneficios y procedimientos del SGSI para garantizar que todos comprendan sus funciones y responsabilidades en la protección de la información. Además, se distribuirán materiales de apoyo, como documento de políticas, manuales y formatos guía, se motiva a que el proyecto sea implementado, promoviendo una cultura de seguridad y cumplimiento continuo

de SGSI. En la Figura 23y figura 24, se logra visualizar la reunión, entrega de materiales, y recepción del certificado de haber entregado y socializado el proyecto de tesis.

Figura 23

Entrega y socialización del SGSI para el GADIPMC

Figura 24

Recepción de certificado de entrega y socialización del SGSI al Departamento de

Para la implementación a futuro del Sistema de Gestión de Seguridad de la Información (SGSI) en el Municipio de Cayambe puede basar en el ciclo PDCA (Planificar-Hacer-Verificar-Actuar). Durante la fase de planificación (planificación), se identifican las amenazas

a la seguridad y se desarrollan políticas y objetivos para mitigarlas. Durante la implementación (Do), se implementarán las reglas y procedimientos establecidos. La fase de verificación (verificación) incluye monitorear y evaluar la efectividad de las actividades realizadas a través de auditorías y revisiones periódicas. Finalmente, en la fase de acción, se realizan mejoras continuas en función de los resultados de la evaluación para garantizar que el SGSI se mantenga actualizado y eficaz en la protección de la información del municipio.

GOBIERNO AUTÓNOMO DESCENTRALIZADO
INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

CERTIFICACIÓN

Cayambe, 26 de julio del 2024

Señores
UNIVERSIDAD TÉCNICA DEL NORTE
Presente. -

De mis consideraciones.

Siendo receptores del proyecto de tesis del Sr. Egresado LENIN JULIAN JAMI LEMA con cédula N.º 1723258511, quien desarrollo su proyecto de tesis con el tema "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA EL GADIP DEL MUNICIPIO DE CAYAMBE", me es grato informar que se ha cumplido el proceso de entrega y socialización, por lo que se recibe el proyecto como culminado y realizado en su totalidad por parte del egresado.

Es todo en cuanto puedo certificar en honor a la verdad, el interesado puede hacer el uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,

GADIP MUNICIPIO DE CAYAMBE
CAYAMBE
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Carlos Trujillo
Director del Departamento de Tecnologías de la información (E)
GADIP del Municipio de Cayambe

unidos**renacemos** / ayllukunawan**wiñarinchik**

5.5 Conclusiones

Un sistema de gestión de seguridad de la información (SGSI) es fundamental para garantizar la protección de la información confidencial de una organización. Este tipo de sistemas permiten gestionar de forma integral los riesgos asociados a la seguridad de la información, implementando medidas de control que aseguren la confidencialidad, integridad y disponibilidad de los datos.

La implementación de un SGSI requiere un compromiso firme por parte de la dirección de Tecnologías de la Información, así como de la participación activa de todos los empleados. Es necesario que exista una cultura de seguridad de la información que permita cumplir con los objetivos y metas establecidos.

La norma ISO 27001 es una referencia internacional que establece los requisitos mínimos que deben cumplir los SGSI. La certificación en ISO 27001 permite demostrar que una organización ha implementado un SGSI eficaz.

La gestión de riesgos es uno de los pilares fundamentales de un SGSI. Es necesario identificar los riesgos asociados a la seguridad de la información, analizar su impacto y probabilidad, y establecer medidas de control que permitan maximizarlos.

La formación y concienciación de los empleados es clave para el éxito de un SGSI. Todos los empleados deben conocer las políticas y procedimientos establecidos, así como sus responsabilidades en materia de seguridad de la información.

La monitorización y revisión continua del SGSI es necesaria para garantizar su eficacia y adecuación a los cambios en el entorno de la organización.

En definitiva, un SGSI es un elemento fundamental para garantizar la protección de la información confidencial de una organización. Su implementación y mantenimiento requieren de un esfuerzo constante por parte de toda la organización, pero los beneficios en términos de seguridad de la información y reputación de la empresa son indudables.

5.6 Recomendaciones

La implementación de un sistema de gestión de seguridad de la información (SGSI) es un proceso complejo y crítico para cualquier organización. Aquí hay algunas recomendaciones que pueden ayudar en el proceso:

Identificar los activos de información críticos de la organización, empresa o institución y clasificarlas en función de su importancia y nivel de riesgo.

Establezca una política de seguridad de la información que refleje la cultura, los objetivos y las necesidades de la organización.

Asigne responsabilidades claras para la gestión de la seguridad de la información, incluyendo la designación de un responsable de seguridad de la información.

Usar formatos claros para poder recopilar la información necesaria de cada activo

Usar la herramienta EAR/PILAR de MAGERIT V3. Que puede ayudar a simplificar procesos, para poder determinar amenazas, riesgos y para tener una mejor guía en cuanto a la aplicabilidad de salvaguardas.

Revisar siempre las ultimas actualizaciones de la Norma ISO 27001, y considerar los cambios a ejecutar

5.7 Referencias

Areitio Javier. (2008). *Seguridad de la información. Redes, informática y sistemas de información - AREITIO BERTOLIN, JAVIER - Google Libros*. https://books.google.co.ve/books?id=_z2GcBD3deYC&printsec=copyright#v=onepage&q&f=false

Arribas, G. N. (2018). *Introducción a las vulnerabilidades*.

Asamblea Nacional. (2019). *CÓDIGO ORGÁNICO INTEGRAL PENAL Año I-Nº 180*. www.registroficial.gob.ec

Avellaneda Javier. (2008). *Publicada la ISO 27005:2008 | Gobierno de la ciberseguridad*. https://seguridad-de-la-informacion.blogspot.com/2008/06/publicada-la-iso-270052008.html

Bejarano Forero, E. (2017). *Seguridad en redes*. https://digitk.areandina.edu.co/handle/areandina/1419

Carrasco Alejandro. (2014). *Amazon.com: Seguirdad perimetral en redes de computadores: Fundamentos teóricos y casos prácticos (Spanish Edition): 9783848473793: Carrasco, Alejandro, Mateos, Carlos J.: Libros*. https://www.amazon.com/-/es/Alejandro-Carrasco/dp/3848473798

Castillo Cristian. (2013). *Esquema Gubernamental-EGSI*.

CNT. (2015). *Certificados obtenidos - CNT Ecuador*. https://empresas.cnt.com.ec/certificados

Contraloría General del Estado. (2020). *NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO*.

Costas José, P. J. (2010). *Entender el Modelo PDCA de mejora continua*.

DGMAPIAE. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/

GADIPMC. (2022). *Misión & Visión | Gadip Municipio de Cayambe*. https://www1.municipiocayambe.gob.ec/gadip/mision-vision/

Gómez Fernández, Luis., & Fernández Rivero, P. Pablo. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* 165.

INTERCER. (2013). *ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*. http://www.intercer.es/ISO%2027001.html

ISO-IEC. (2018). *ISO-IEC-27005-2018 - normas iso - INTERNACIONAL ESTÁNDAR 27005 ISO/CEI Tecnología de la información - Studocu*. https://www.studocu.com/es-mx/document/instituto-tecnologico-de-ciudad-guzman/seguridad-informatica/iso-iec-27005-2018-normas-iso/77388256

ISOTools. (2016). *ISO 27001 - Sistemas de Gestión de Seguridad de la Información*. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

José González Rus, J., de la Mata Barranco, N. J., Morón Lerma, E., Mata Martín, R. M., Moreno Verdejo, J., Morales Prats, F., Viota Maestre, M., Manuel Ortiz Márquez, J., Roig Bustos, L., Carreras del Rincón, L., Narváez Rodríguez, A., Sanchís Crespo, C., & Adán del Río, C. (2007). *Universidad de Deusto • • • • • • • • Cuadernos penales José María Lidón Delito e informática: algunos aspectos*.

López Agustín, R. S. (2020). *ISO 270001 ES*. https://www.iso27000.es/index.html

Merino Bada, Cristina., & Cañizares Sales, Ricardo. (2012). *Implantación de un sistema de gestión de seguridad de la información según ISO 27001 : un enfoque práctico*. https://books.google.com/books/about/Implantaci%C3%B3n_de_un_sistema_de_gesti%C3%B3n.html?hl=es&id=hYKtpwAACAAJ

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *Subsecretaria Gobierno Electrónico y Registro Civil – Ministerio de Telecomunicaciones y de la Sociedad de la Información*. https://www.telecomunicaciones.gob.ec/2-2/

NQA. (2024). *NQA-ISO-27001-Guia-de-implantacion*.

Olano, D., Tutor, A., & López De Vergara Méndez, J. E. (2016). *Aplicabilidad de las normas ISO 27000 en el contexto de la Internet de las Cosas*.

SENADI. (2007). *Derecho de Autor y Derechos Conexos – Servicios*. https://www.derechosintelectuales.gob.ec/descargas/

UNIR FP. (2023). *Los 4 principios de la seguridad informática y su implementación | UNIR FP*. UNIR FP. https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/

Vega Edgar. (2021). *SEGURIDAD DE LA INFORMACIÓN*.

Zambrano-Mendieta, J. E., Dueñas-Zambrano, K. I., & Macías-Ordoñez, L. M. (2016). Delito Informótico. Procedimiento Penal en Ecuador. *Dominio de Las Ciencias*, *2*(2), 204–215. https://doi.org/10.23857/DC.V2I2.159

ANEXOS

Anexo1-Norma ISO 27001:2022

DOMINIOS, OBJETIVOS DE CONTROLES NORMATIVA ISO 27001-27002		
	Identificador de control	**Nombre del control**
CONTROLES ORGANIZACIONALES	5.1	Políticas de seguridad de la información
	5.2	Funciones y responsabilidades en materia de seguridad de la información
	5.3	Segregación de funciones
	5.4	Responsabilidades de la dirección
	5.5	Contacto con las autoridades
	5.6	Contacto con grupos de interés especial
	5.7	Inteligencia de amenazas**(nuevo)**
	5.8	Seguridad de la información en la gestión de proyectos
	5.9	Inventario de la información y otros activos asociados - **CAMBIOS**
	5.10	Uso aceptable de la información y otros activos asociados - **CAMBIOS**
	5.11	Devolución de activos
	5.12	Clasificación de la información
	5.13	Etiquetado de la información
	5.14	Transferencia de información
	5.15	Control de acceso
	5.16	Gestión de la identidad
	5.17	Información de autenticación - NUEVO
	5.18	Derechos de acceso - CAMBIOS
	5.19	Seguridad de la información en las relaciones con los proveedores
	5.20	Gestión de la seguridad de la información en los acuerdos con los proveedores
	5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC - NUEVO
	5.22	Monitoreo, revisión y gestión de cambios de los servicios de los proveedores - CAMBIOS
	5.23	Seguridad de la información para el uso de servicios en la nube - NUEVO
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información - CAMBIOS

	5.25	Evaluación y decisión sobre eventos de seguridad de la información
	5.26	Respuesta a incidentes de seguridad de la información
	5.27	Aprendizaje de los incidentes de seguridad de la información
	5.28	Recogida de pruebas
	5.29	Seguridad de la información durante la interrupción - CAMBIOS
	5.30	Preparación de las TIC para la continuidad del negocio - NUEVO
	5.31	Identificación de los requisitos legales, reglamentarios y contractuales
	5.32	Derechos de propiedad intelectual
	5.33	Protección de registros
	5.34	Privacidad y protección de la información personal
	5.35	Revisión independiente de la seguridad de la información
	5.36	Cumplimiento de políticas y normas de seguridad de la información
	5.37	Procedimientos operativos documentados
CONTROLES DE PERSONAS	6.1	Selección de personal
	6.2	Términos y condiciones de empleo
	6.3	Concienciación, educación y formación en materia de seguridad de la información
	6.4	Proceso disciplinario
	6.5	Responsabilidades después de la terminación o cambio de empleo
	6.6	Acuerdos de confidencialidad o no divulgación
	6.7	Trabajo a distancia - NUEVO
	6.8	Reporte de eventos de seguridad de la información
CONTROLES FÍSICOS	7.1	Perímetro de seguridad física
	7.2	Controles físicos de entrada
	7.3	Seguridad de oficinas, salas e instalaciones
	7.4	Supervisión de la seguridad física
	7.5	Protección contra amenazas físicas y ambientales
	7.6	Trabajar en áreas seguras
	7.7	Escritorio y pantalla despejados
	7.8	Ubicación y protección de los equipos

	7.9	Seguridad de los activos fuera de las instalaciones
	7.10	Medios de almacenamiento - NUEVO
	7.11	Servicios de apoyo
	7.12	Seguridad del cableado
	7.13	Mantenimiento de equipos
	7.14	Seguridad en la eliminación o reutilización de equipos
COTRLES TECNOLÓGICOS	8.1	Dispositivos de punto final del usuario - NUEVO
	8.2	Derechos de acceso con privilegios
	8.3	Restricción de acceso a la información
	8.4	Acceso al código fuente
	8.5	Autenticación segura
	8.6	Gestión de la capacidad
	8.7	Protección contra el malware
	8.8	Gestión de las vulnerabilidades técnicas
	8.9	Gestión de la configuración
	8.10	Eliminación de información - NUEVO
	8.11	Enmascaramiento de datos - NUEVO
	8.12	Prevención de la fuga de datos - NUEVO
	8.13	Copia de seguridad de la información
	8.14	Redundancia de las instalaciones de procesamiento de la información
	8.15	Registro de datos
	8.16	Actividades de supervisión
	8.17	Sincronización de relojes
	8.18	Uso de programas de utilidad privilegiados
	8.19	Instalación de software en sistemas operativos
	8.20	Controles de red
	8.21	Seguridad de los servicios de red
	8.22	Filtrado web - NUEVO
	8.23	Segregación en redes
	8.24	Uso de criptografía
	8.25	Ciclo de vida de desarrollo seguro
	8.26	Requisitos de seguridad de las aplicaciones - NUEVO
	8.27	Arquitectura de sistemas seguros y principios de ingeniería - NUEVO
	8.28	Codificación segura
	8.29	Pruebas de seguridad en el desarrollo y la aceptación
	8.30	Desarrollo externalizado

	8.31	Separación de los entornos de desarrollo, prueba y producción
	8.32	Gestión del cambio
	8.33	Información de pruebas
	8.34	Protección de los sistemas de información durante la auditoría y las pruebas - NUEVO

Anexos 2 Valoración de Activos

Confidencialidad**[C]**

Integridad **[I]**

Disponibilidad **[D]**

Valoración de los Activos Referentes a CID (Confidencialidad, Integridad y Disponibilidad)

Código	**Nombre**	**Tipo**	**Responsable**	**[C]**	**[I]**	**[D]**	**Valor total**
SW-OLIMPO	Servidor Olimpo	[SW]	dpto. de TICs	4	5	5	14
SW-SIM	Servidor SIM	[SW]	dpto. de TICs	4	5	5	14
SW-SINAT	Servidor SINAT	[SW]	dpto. de TICs	4	5	5	14
SW-PROXY	Servidor Proxy	[SW]	dpto. de TICs	3	3	3	9
SW-RESPALDO	Servidor de respaldos	[SW]	dpto. de TICs	3	5	5	13
SW-VIRTUALIZACIÓN	Software de Virtualización de servidores	[SW]	dpto. de TICs	4	4	5	13
SW-TELEF-IP	Servidore de Telefonia IP	[SW]	dpto. de TICs	4	1	5	10
SW-DATAFLOW	Servido Data Flow	[SW]	dpto. de TICs	3	3	3	9
HW-Sw-CSC-ACC	Switch Cisco 2960	[HW]	dpto. de TICs	4	4	5	14
HW-RT-CSC	Router Cisco ASA 5505	[HW]	dpto. de TICs	4	4	5	14
HW-VIRTUALIZACIÓN	Servidor de máquinas virtuales	[HW]	dpto. de TICs	1	1	5	7
HW-Sw-HP-24	Switch HP v1910-24 G	[HW]	dpto. de TICs	4	5	5	14
HW-Sw-CSC-24SF	Switch Cisco SF 100-24	[HW]	dpto. de TICs	4	4	5	14
HW-CHASIS	Chasis Blade	[HW]	dpto. de TICs	4	3	1	8
HW-Firewall	Equipo de Seguridad perimetral	[HW]	dpto. de TICs	4	5	4	13
HW-Sw-HPE	Switch HPE 1920 JL382A	[HW]	dpto. de TICs	4	4	4	12
COM-ENLACE-FIBRA	Enlace Fibra	[COM]	dpto. de TICs	4	5	5	14
COM-ENLACE-MERCADO	Enlace mercado diario	[COM]	dpto. de TICs	3	4	4	11

COM-ENLACE-EJARRIN	Edificio Jarrín	[COM]	dpto. de TICs	3	4	4	11
COM-ENLACE-C. POPULAR	Enlace Comercial Popular	[COM]	dpto. de TICs	4	4	5	14
COM-ENLACES-REPETIDORES	Enlaces Repetidores	[COM]	dpto. de TICs	2	3	5	12
AUX-CLIMATIZACIÓN	Aire acondicionado	[AUX]	dpto. de TICs	1	1	5	7
AUX-UPS	UPS	[AUX]	dpto. de TICs	5	1	5	11
AUX-GENERADOR-E	Generador eléctrico	[AUX]	dpto. de TICs	1	1	5	7
S-TELÉFONO	Servicio de teléfono convencional	[S]	dpto. de TICs	1	1	4	4
S-INTERNET	Servicio de internet	[S]	dpto. de TICs	5	1	5	11
S-MAIL	Servidor de correo Institucional	[S]	dpto. de TICs	3	1	3	7
S-DNS	Servidor DNS	[S]	dpto. de TICs	4	1	5	11
S-WEB	Servidor Web	[S]	dpto. de TICs	5	5	4	14
S-ACCESO REMOTO	Acceso Remoto a Servidores	[S]	dpto. de TICs	4	5	4	13
S-ANTIVIRUS	Servicio de antivirus	[S]	dpto. de TICs	1	1	3	5
Media-Disco Duro 1 TB	Disco Duro 1 TB	[S]	dpto. de TICs	4	4	5	13
Media-Flash memory	Flash Memory	[S]	dpto. de TICs	3	3	3	12

Fuente: Recuperado del GADIPMC

Dentro de la organización necesario conocer las posibles amenazas que pueden afectar a los activos de información, a continuación, se presenta una tabla para cada amenaza existente.

Anexo 3 Tabla de Nivel de tolerancia

Riesgo= Probabilidad*Impacto+Valoración

Nombre /Activo	valor	Descripción	Probabilidad	Impacto	Riesgo	Tolerancia
SW-SVR-OLIMPO	14	Avería de origen físico o lógico	3	4	26	NT
		Errores de los usuarios	3	2	20	RT
		Errores del administrador	2	3	20	RT
		Error de mantenimiento/actualización de programa SW	2	1	16	RT
		Abuso de privilegios de acceso	1	1	15	TT
		Acceso no autorizado	3	4	26	NT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
		Manipulación de programas	2	1	16	RT
SW-SVR-SIM	14	Avería de origen físico o lógico	3	4	26	NT
		Errores de los usuarios	3	2	20	RT
		Errores del administrador	2	3	20	RT
		Error de mantenimiento/actualización de programa SW	2	1	16	RT
		Abuso de privilegios de acceso	1	1	5	TT
		Acceso no autorizado	2	2	18	RT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
		Manipulación de programas	2	1	16	TT
SW-SVR-SINAT	14	Avería de origen físico o lógico	3	4	26	NT
		Errores de los usuarios	3	2	20	RT
		Errores del administrador	2	3	20	RT
		Error de mantenimiento/actualización de programa SW	2	1	16	RT
		Abuso de privilegios de acceso	3	4	26	NT
		Acceso no autorizado	3	4	26	NT
		Modificación deliberada de la información	3	4	26	NT
		Destrucción de información	3	4	26	NT
		Manipulación de programas	2	1	16	RT
SW-SVR-PROXY	9	Avería de origen físico o lógico	3	4	21	RT

		Errores de los usuarios	3	2	15	TT
		Errores del administrador	2	3	15	TT
		Error de mantenimiento/actualización de programa SW	2	1	11	TT
		Abuso de privilegios de acceso	1	1	10	TT
		Acceso no autorizado	2	2	13	RT
		Modificación deliberada de la información	2	2	13	RT
		Destrucción de información	2	3	15	RT
		Manipulación de programas	2	1	11	TT
SW-SVR-RESPALDO	13	Avería de origen físico o lógico	3	4	25	NT
		Errores de los usuarios	3	2	19	RT
		Errores del administrador	2	3	19	RT
		Error de mantenimiento/actualización de programa SW	2	1	15	TT
		Abuso de privilegios de acceso	1	3	17	TT
		Acceso no autorizado	2	2	17	RT
		Modificación deliberada de la información	4	4	29	NT
		Destrucción de información	4	4	29	NT
		Manipulación de programas	2	3	19	TT
SW-SVR-DFLOW	9	Avería de origen físico o lógico	3	4	21	RT
		Errores de los usuarios	3	2	15	TT
		Errores del administrador	2	3	15	TT
		error de mantenimiento/actualización de programa SW	2	1	11	TT
		Abuso de privilegios de acceso	1	1	10	TT
		Acceso no autorizado	2	2	13	TT
		Modificación deliberada de la información	2	2	13	TT
		Destrucción de información	2	3	15	TT
		Manipulación de programas	2	1	11	TT
HW-SW-CSC-ACC	13	Fuego	3	4	25	RT
		Daños por agua	2	4	21	RT
		Desastres naturales	1	4	17	RT
		Desastres industriales	1	4	17	RT
		Contaminación mecánica	1	4	17	RT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
		Condiciones inadecuadas de temperatura o humedad	3	1	16	RT
		Errores del administrador	2	2	17	RT

		Errores de mantenimiento / actualización de equipos HW	1	3	16	RT
		Caída del sistema por agotamiento de recursos	2	3	19	RT
HW-RT-CSC	13	Fuego	3	4	25	NT
		Daños por agua	2	4	21	RT
		Desastres naturales	1	2	15	TT
		Desastres industriales	1	2	15	TT
		Contaminación mecánica	1	4	17	RT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
		Condiciones inadecuadas de temperatura o humedad	3	2	19	RT
		Errores del administrador	2	3	19	RT
		Errores de mantenimiento / actualización de equipos HW	2	4	21	RT
		Caída del sistema por agotamiento de recursos	2	4	21	RT
HW-SW-HP-24	13	Fuego	3	4	25	NT
		Daños por agua	2	4	21	RT
		Desastres naturales	1	2	15	TT
		Desastres industriales	1	2	15	TT
		Contaminación mecánica	1	2	15	TT
		Avería de origen físico o lógico	3	4	25	RT
		Corte del suministro eléctrico	4	4	29	NT
		Condiciones inadecuadas de temperatura o humedad	2	3	19	RT
		Errores del administrador	2	3	19	RT
		Errores de mantenimiento / actualización de equipos HW	2	2	17	RT
		Caída del sistema por agotamiento de recursos	2	3	19	RT
HW-SW-CSC-24SF	13	Fuego	3	4	25	NT
		Daños por agua	2	4	21	RT
		Desastres naturales	1	2	15	TT
		Desastres industriales	1	2	15	TT
		Contaminación mecánica	1	2	15	TT
		Avería de origen físico o lógico	3	4	25	NT
		Corte del suministro eléctrico	4	4	29	NT
		Condiciones inadecuadas de temperatura o humedad	2	2	17	RT
		Errores del administrador	2	3	19	RT
		Errores de mantenimiento / actualización de equipos HW	1	2	15	TT
		Caída del sistema por agotamiento de recursos	2	3	19	RT

HW-SW-HPE	12	Fuego	3	4	24	RT
		Daños por agua	2	4	18	RT
		Desastres naturales	1	2	14	TT
		Desastres industriales	1	2	14	TT
		Contaminación mecánica	1	2	14	TT
		Avería de origen físico o lógico	3	3	21	RT
		Corte del suministro eléctrico	4	4	28	NT
		Condiciones inadecuadas de temperatura o humedad	2	3	18	RT
		Errores del administrador	2	3	18	RT
		Errores de mantenimiento / actualización de equipos HW	1	2	14	TT
		Caída del sistema por agotamiento de recursos	2	3	18	RT
COM-ENLACE-FIBRA	14	Fallo de servicios de comunicaciones	4	4	30	NT
		Errores del administrador	2	3	20	RT
		Suplantación de la identidad del usuario	1	2	16	RT
		Acceso no autorizado	2	2	18	RT
		Análisis de tráfico	2	2	18	RT
		Interceptación de información (escucha)	2	2	18	RT
COM-ENLACE-MCD	11	Fallo de servicios de comunicaciones	3	3	20	RT
		Errores del administrador	2	3	17	RT
		Suplantación de la identidad del usuario	1	2	13	TT
		Acceso no autorizado	2	2	15	TT
		Análisis de tráfico	2	2	15	TT
		Interceptación de información (escucha)	2	2	15	TT
COM-ENLACE-EJARRIN	11	Fallo de servicios de comunicaciones	4	4	25	NT
		Errores del administrador	2	2	15	TT
		Suplantación de la identidad del usuario	1	2	13	TT
		Acceso no autorizado	2	2	15	TT
		Análisis de tráfico	2	2	15	TT
		Interceptación de información (escucha)	2	2	15	TT
COM-ENLACE-CPOPULAR	13	Fallo de servicios de comunicaciones	3	4	25	NT
		Errores del administrador	2	2	17	RT
		Suplantación de la identidad del usuario	1	2	15	TT
		Acceso no autorizado	2	2	17	RT
		Análisis de tráfico	2	2	17	RT
		Interceptación de información (escucha)	2	2	17	RT

COM-ENLACES-RPTDS	10	Fallo de servicios de comunicaciones	2	2	17	RT
		Errores del administrador	1	2	17	RT
		Suplantación de la identidad del usuario	1	1	11	TT
		Acceso no autorizado	1	1	11	TT
		Análisis de tráfico	1	1	11	TT
		Interceptación de información (escucha)	1	1	11	TT
AUX-CLIMATIZACIÓN	6	Fuego	1	2	8	TT
		Daños por agua	1	2	8	TT
		Desastres naturales	1	1	7	TT
		Desastres industriales	1	1	7	TT
		Contaminación mecánica	1	1	7	TT
		Avería de origen físico o lógico	3	2	12	TT
		Corte del suministro eléctrico	4	3	18	RT
		Condiciones inadecuadas de temperatura o humedad	2	2	10	TT
		Errores del administrador	1	2	8	TT
AUX-UPS	11	Fuego	2	3	17	RT
		Daños por agua	1	2	13	TT
		Desastres naturales	1	1	12	TT
		Desastres industriales	1	1	12	TT
		Contaminación mecánica	1	1	12	TT
		Avería de origen físico o lógico	2	3	17	RT
		Corte del suministro eléctrico	4	3	23	RT
		Condiciones inadecuadas de temperatura o humedad	2	2	15	TT
		Errores del administrador	2	2	15	TT
AUX-GENERADOR-E	6	Fuego	1	3	9	TT
		Daños por agua	2	2	10	TT
		Desastres naturales	1	1	7	TT
		Desastres industriales	1	1	7	TT
		Contaminación mecánica	1	1	7	TT
		Avería de origen físico o lógico	3	3	15	TT
		Corte del suministro eléctrico	4	3	18	RT
		Condiciones inadecuadas de temperatura o humedad	2	2	10	TT
		Errores del administrador	2	2	10	TT
S-TELEFONO	4	Fuego	1	3	7	TT
		Daños por agua	1	2	6	TT
		Desastres naturales	1	1	5	TT
		Desastres industriales	1	1	5	TT
		Contaminación mecánica	1	1	5	TT
		Avería de origen físico o lógico	2	2	8	TT
		Corte del suministro eléctrico	2	1	6	TT

		Condiciones inadecuadas de temperatura o humedad	1	1	5	TT
		Errores del administrador	2	2	8	TT
		Errores de mantenimiento / actualización de equipos HW	2	1	6	TT
		Caída del sistema por agotamiento de recursos	2	1	6	TT
S-INTERNET	11	Fallo de servicios de comunicaciones	4	5	31	NT
		Errores del administrador	2	3	17	RT
		Repudio	1	2	13	TT
		Suplantación de la identidad del usuario	1	1	12	TT
		Uso no previsto	1	2	12	TT
S-MAIL	6	Fuego	1	2	8	TT
		Daños por agua	1	1	7	TT
		Desastres naturales	1	1	7	TT
		Desastres industriales	1	1	7	TT
		Contaminación mecánica	1	1	7	TT
		Avería de origen físico o lógico	2	2	10	TT
		Corte del suministro eléctrico	1	1	7	TT
		Condiciones inadecuadas de temperatura o humedad	1	1	7	TT
		Errores del administrador	2	1	8	TT
		Errores de mantenimiento / actualización de equipos HW	2	1	8	TT
		Caída del sistema por agotamiento de recursos	3	1	9	TT
S-DNS	6	Fuego	1	3	9	TT
		Daños por agua	1	3	9	TT
		Desastres naturales	1	1	7	TT
		Desastres industriales	1	1	7	TT
		Contaminación mecánica	1	1	7	TT
		Avería de origen físico o lógico	1	3	9	TT
		Corte del suministro eléctrico	2	2	10	TT
		Condiciones inadecuadas de temperatura o humedad	2	2	10	TT
		Errores del administrador	2	2	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	2	8	TT
		Caída del sistema por agotamiento de recursos	1	2	8	TT

Anexo 4 – Declaración de Aplicabilidad

Dominio	**Identificador de control**	**Control ISO/IEC 27001**	**Aplicabilidad**	**Justificación**
CONTROLES ORGANIZACIONALES	5.1	Políticas de seguridad de la información	Aplica	Las políticas de seguridad de la información y las políticas específicas del tema se definen, aprueban por la dirección, se publican, se comunican y se reconocen por los empleados relevantes y las partes interesadas relevantes, y se implementan a intervalos planificados y cuando hay cambios en los mismos
	5.2	Funciones y responsabilidades en materia de seguridad de la información	No aplica	Los roles y responsabilidades para la seguridad de la información deben especificarse y distribuirse de acuerdo

				con los requisitos de la organización.
	5.3	Segregación de funciones	Aplica	Deben mantenerse separadas las obligaciones conflictivas y las áreas de responsabilidad.
	5.4	Responsabilidades de la dirección	Aplica	De acuerdo con la política de seguridad de la información establecida por la organización y las políticas y procedimientos específicos del tema, la gerencia debe exigir que todos los empleados apliquen la seguridad de la información.
	5.5	Contacto con las autoridades	No aplica	Las organizaciones deben ponerse en contacto con las autoridades

				correspondientes y mantenerlas informadas.
	5.6	Contacto con grupos de interés especial	No aplica	Establecer y mantener relaciones con grupos de interés especializados, otros foros de seguridad profesional y asociaciones profesionales que sean importantes para las organizaciones
	5.7	Inteligencia de amenazas**(nuevo)**	Aplica	Para crear inteligencia de amenazas, se recopila y analiza información sobre amenazas a la seguridad de la información.
	5.8	Seguridad de la información en la gestión de proyectos	No aplica	La gestión de proyectos incluye un componente de seguridad de la información.

	5.9	Inventario de la información y otros activos asociados - **CAMBIOS**	Aplica	Es necesario crear y mantener un inventario de informacipon, así como de cualquier otro activo relacionado.
	5.10	Uso aceptable de la información y otros activos asociados - **CAMBIOS**	No aplica	Se establecerán, documentarán y pondrán en práctica lineamientos para el adecuado uso y manejo de la información y demás activos relacionados.
	5.11	Devolución de activos	No aplica	Al cambiar o terminar su empleo, contrato o acuerdo, el personal y otras partes interesadas devolverán todos los activos de la organización en su poder, según corresponda.

	5.12	Clasificación de la información	Aplica	Sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes que indique las partes interesadas, la información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización.
	5.13	Etiquetado de la información	Aplica	Usando el esquema de clasificación de la información de la organización como guía, se debe crear y poner en práctica un conjunto adecuado de procedimientos para etiquetar la información.

	5.14	Transferencia de información	No aplica	Para todos los tipos de instalaciones de transferencia, tanto dentro de la organización como entre la organización y partes externas, debe haber reglas, procedimientos o acuerdos que rijan la transferencia de información.
	5.15	Control de acceso	Aplica	Con base en las necesidades del negocio y la seguridad de la información, se desarrollarán e implementarán pautas para regular el acceso físico y lógico a los datos y otros activos relacionados.
	5.16	Gestión de la identidad	No aplica	Se gestionará el ciclo de vida completo de la identidad.

	5.17	Información de autenticación - NUEVO	Aplica	Debe existir un proceso de gestión para regular cómo se distribuye y gestiona la información de autenticación, y también debe incluir la formación del personal sobre cómo manejarla correctamente.
	5.18	Derechos de acceso - CAMBIOS	No aplica	De acuerdo con la política y las reglas de control de acceso específicas del tema de la organización, los derechos de acceso a la información y otros activos relacionados deben otorgarse, revisarse, modificarse y eliminarse.
	5.19	Seguridad de la información en las relaciones con los proveedores	No aplica	Para gestionar los riesgos para la seguridad de la información que

				plantea el uso de los bienes o servicios del proveedor, se deben establecer e implementar procesos y procedimientos.
	5.20	Gestión de la seguridad de la información en los acuerdos con los proveedores	No aplica	Dependiendo del tipo de relación que tengan el proveedor y la organización, se desarrollarán y acordarán con cada proveedor los requisitos pertinentes de seguridad de la información.
	5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC - NUEVO	No aplica	Para gestionar los riesgos de seguridad de la información relacionados con la cadena de suministro de bienes y servicios de TIC, se deben establecer y poner en

				marcha procesos y procedimientos.
	5.22	Monitoreo, revisión y gestión de cambios de los servicios de los proveedores - CAMBIOS	No aplica	Se requiere que la empresa supervise, revise, evalúe y gestione de forma rutinaria los cambios en los procedimientos y métodos de seguridad de la información del proveedor de servicios.
	5.23	Seguridad de la información para el uso de servicios en la nube - NUEVO	No aplica	De acuerdo con los requisitos de seguridad de la información de la organización, se deben establecer los procedimientos para adquirir, usar, administrar y terminar los servicios en la nube.

	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información - CAMBIOS	No aplica	Los procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información deben ser definidos, establecidos y comunicados por la organización para planificar y prepararse para ello.
	5.25	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	Los eventos de seguridad de la información deben ser evaluados por la organización antes de ser etiquetados como incidentes de seguridad de la información.
	5.26	Respuesta a incidentes de seguridad de la información	Aplica	Los incidentes relacionados con la seguridad de la información deben manejarse de acuerdo

				con los procedimientos formales.
	5.27	Aprendizaje de los incidentes de seguridad de la información	No aplica	Los controles de seguridad de la información se fortalecerán y mejorarán utilizando el conocimiento obtenido de los incidentes de seguridad de la información.
	5.28	Recogida de pruebas	No aplica	La institución debe desarrollar y poner en marcha procedimientos para localizar, recopilar, adquirir y conservar pruebas de incidentes relacionados con la seguridad de la información.
	5.29	Seguridad de la información durante la	No aplica	La organización debe planificar cómo se mantendrá la seguridad de los datos en un nivel

		interrupción - CAMBIOS		adecuado durante una interrupción.
	5.30	Preparación de las TIC para la continuidad del negocio - NUEVO	No aplica	La preparación para las TIC debe planificarse, implementarse, mantenerse y probarse de acuerdo con: Objetivos de continuidad del negocio y requisitos de continuidad de TI.
	5.31	Identificación de los requisitos legales, reglamentarios y contractuales	No aplica	Los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información, así como la estrategia de la organización para cumplirlos, deben identificarse, registrarse y mantenerse actualizados.

	5.32	Derechos de propiedad intelectual	No aplica	La organización establece procedimientos apropiados para la protección Derechos de propiedad intelectual
	5.33	Protección de registros	No aplica	Los registros deben protegerse contra robo, sabotaje, falsificación, acceso no autorizado y publicación.
	5.34	Privacidad y protección de la información personal	Aplica	La organización debe identificar y cumplir los requisitos pertinentes. mantener la privacidad y proteger la información de identificación personal de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

	5.35	Revisión independiente de la seguridad de la información	No aplica	Debe evitarse el robo, el sabotaje, la falsificación, el acceso no autorizado y la publicación de los registros.
	5.36	Cumplimiento de políticas y normas de seguridad de la información	No aplica	Los registros deben protegerse de la publicación, el acceso no autorizado, el sabotaje, el robo y la falsificación.
	5.37	Procedimientos operativos documentados	Aplica	Procedimientos operativos de las instalaciones de procesamiento de información. deben ser registrados y puestos a disposición de los miembros del personal que los requieran.

CONTROLES DE PERSONAS	6.1	Selección de personal	No aplica	Todos los solicitantes de empleo se someterán a verificaciones de antecedentes tanto antes de comenzar a trabajar para la empresa como de manera continua. Estas comprobaciones se realizarán de acuerdo con las necesidades de la organización, la clasificación de la información a acceder y los riesgos percibidos, así como las leyes, reglamentos y normas éticas aplicables.
	6.2	Términos y condiciones de empleo	No aplica	Los contratos de trabajo deben definir las obligaciones relacionadas con la seguridad de la

				información del personal y la organización.
	6.3	Concienciación, educación y formación en materia de seguridad de la información	Aplica	Se debe proporcionar al personal de la institución y a las partes interesadas pertinentes la concientización, la educación y la capacitación adecuadas en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema.

	6.4	Proceso disciplinario	No aplica	Se formalizará el proceso disciplinario y se brindará información para emprender acciones contra los empleados culpables de infringir la política de seguridad de la información y demás partes interesadas relevantes.
	6.5	Responsabilidades después de la terminación o cambio de empleo	No aplica	Las responsabilidades y obligaciones relacionadas con la protección de datos, que siguen siendo válidas después del final o el cambio de la relación laboral, se definen, implementan y comunican a los empleados relevantes y otras partes interesadas.

	6.6	Acuerdos de confidencialidad o no divulgación	No aplica	La identificación, documentación, revisión periódica y firma del personal y otras partes interesadas pertinentes son necesarias para los acuerdos de confidencialidad o no divulgación que reflejan los requisitos de la organización para la protección de la información.
	6.7	Trabajo a distancia - NUEVO	Aplica	Las medidas de seguridad se implementan cuando los empleados trabajan de forma remota para proteger los datos que se manejan, procesan o almacenan externamente.

	6.8	Reporte de eventos de seguridad de la información	No aplica	La organización debe proporcionar un mecanismo para que los empleados notifiquen los incidentes de seguridad de la información detectados o sospechados de manera oportuna a través de los canales apropiados.

CONTROLES FÍSICOS	7.1	Perímetro de seguridad física	No aplica	Las áreas que contienen información y activos estarán protegidas por perímetros de seguridad definidos.
	7.2	Controles físicos de entrada	No aplica	Deben utilizarse puntos de acceso y controles de entrada apropiados para

				proteger las áreas seguras.
	7.3	Seguridad de oficinas, salas e instalaciones	No aplica	Diseñar e implementar la seguridad física de las oficinas, salas e instalaciones de la institución.
	7.4	Supervisión de la seguridad física	No aplica	Las instalaciones deben ser monitoreadas constantemente para detectar accesos físicos no autorizados.
	7.5	Protección contra amenazas físicas y ambientales	No aplica	Es necesario diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas. Los daños a la infraestructura pueden ser deliberados o accidentales.

	7.6	Trabajar en áreas seguras	No aplica	Las medidas de seguridad están diseñadas e implementadas para operar en lugares seguros.
	7.7	Escritorio y pantalla despejados	Aplica	Es importante definir y hacer cumplir adecuadamente las reglas de pantalla limpia para las instalaciones de procesamiento de información, así como las reglas de escritorio limpio para documentos y dispositivos de almacenamiento extraíbles.
	7.8	Ubicación y protección de los equipos	No aplica	El equipo se colocará de forma segura y protegida.

	7.9	Seguridad de los activos fuera de las instalaciones	No aplica	Se protegerán los activos fuera del sitio
	7.10	Medios de almacenamiento - NUEVO	No aplica	Los medios de almacenamiento deben manipularse de acuerdo con las pautas de manejo y el esquema de clasificación de la organización a lo largo de su vida útil de adquisición, uso, transporte y eliminación.
	7.11	Servicios de apoyo	No aplica	El equipo de procesamiento de datos debe estar protegido contra cortes de energía y otras interrupciones debido a fallas en el soporte del servicio público.

	7.12	Seguridad del cableado	No aplica	Los cables de servicios de información auxiliar, de datos y de alimentación deben estar protegidos contra interferencias, intercepciones y daños.
	7.13	Mantenimiento de equipos	No aplica	Para asegurar la accesibilidad, consistencia y confidencialidad de los datos, el equipo se mantendrá adecuadamente.
	7.14	Seguridad en la eliminación o reutilización de equipos	No aplica	Los dispositivos que contienen almacenamiento se verifican para garantizar que todos los datos confidenciales y el software con licencia se eliminen o sobrescriban de forma segura antes de

				eliminarlos o reutilizarlos.

COTRLES TECNOLÓGICOS	8.1	Dispositivos de punto final del usuario	No aplica	Los datos almacenados, procesados o accedidos por los dispositivos finales del usuario están protegidos.
	8.2	Derechos de acceso con privilegios	No aplica	El otorgamiento y uso de derechos de acceso privilegiado está limitado y administrado.
	8.3	Restricción de acceso a la información	Aplica	De acuerdo con la política de control de acceso específica de la materia establecida, se restringirá el acceso a la información y otros activos relacionados.

	8.4	Acceso al código fuente	No aplica	Las bibliotecas de software, las herramientas de desarrollo y el acceso de solo lectura al código fuente se administrarán adecuadamente.
	8.5	Autenticación segura	Aplica	Las técnicas y los procedimientos de autenticación segura se implementan en función de las restricciones de acceso a los datos y las políticas de control de acceso basadas en el sujeto.
	8.6	Gestión de la capacidad	No aplica	El uso de recursos se supervisa y se ajusta en función de las necesidades de capacidad actuales y previstas.

	8.7	Protección contra el malware	Aplica	Al concienciar a los usuarios, se implementará y respaldará la protección contra malware.
	8.8	Gestión de las vulnerabilidades técnicas	No aplica	Es necesario recopilar información sobre las debilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas debilidades e implementar las contramedidas necesarias.
	8.9	Gestión de la configuración	No aplica	Las configuraciones de seguridad, hardware, software, servicios y redes, entre otras, deben establecerse, documentarse, ponerse en práctica, controlarse

				periódicamente y revisarse.
	8.10	Eliminación de información	No aplica	Los datos almacenados en sistemas de información, dispositivos u otros soportes de datos se eliminan cuando ya no se necesitan.
	8.11	Enmascaramiento de datos	No aplica	El enmascaramiento de datos debe usarse de acuerdo con el control de acceso basado en políticas de la organización y otras prácticas basadas en temas, así como los requisitos comerciales, teniendo en cuenta la ley aplicable.
	8.12	Prevención de la fuga de datos	No aplica	Los sistemas, redes y cualquier otro equipo que maneje, almacene o transmita datos

				sensibles estarán sujetos a medidas de prevención de fuga de datos.
	8.13	Copia de seguridad de la información	No aplica	De acuerdo con la política de respaldo específica del tema acordada, se mantendrán y probarán periódicamente copias de respaldo de la información, el software y los sistemas.
	8.14	Redundancia de las instalaciones de procesamiento de la información	No aplica	El equipo de procesamiento de datos se implementa con suficiente redundancia para cumplir con los requisitos de usabilidad.
	8.15	Registro de datos	No aplica	Se producirán, almacenarán, protegerán y

				analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.
	8.16	Actividades de supervisión	No aplica	Se deben vigilar las redes, los sistemas y las aplicaciones en busca de actividad inusual, y se deben tomar las medidas adecuadas para evaluar cualquier posible incidente de seguridad de la información.
	8.17	Sincronización de relojes	No aplica	Los dispositivos de cronometraje utilizados por los sistemas de procesamiento de información de la organización deben estar sincronizados con

				las fuentes de tiempo autorizadas.
	8.18	Uso de programas de utilidad privilegiados	No aplica	El uso de utilidades que anulan los controles del sistema y de las aplicaciones debe limitarse y controlarse estrictamente.
	8.19	Instalación de software en sistemas operativos	No aplica	Para gestionar de forma segura la instalación de software en los sistemas operativos, se implementarán políticas y medidas.
	8.20	Controles de red	No aplica	La información en los sistemas y aplicaciones se salvaguardará mediante la gestión, el control y la protección de redes y dispositivos de red.

	8.21	Seguridad de los servicios de red	No aplica	La identificación, implementación y control de medidas de seguridad, estándares de servicio y requisitos de servicio para servicios de red.
	8.22	Filtrado WEB	Aplica	Los servicios de información, usuarios y grupos de sistemas de información deben estar aislados en la red de la organización.
	8.23	Segregación en redes	Aplica	El acceso a sitios web externos está controlado para reducir la exposición a contenido dañino.
	8.24	Uso de criptografía	No aplica	Deben definirse y aplicarse reglas para el uso eficaz del cifrado, incluida la gestión de claves de cifrado.
	8.25	Ciclo de vida de desarrollo seguro	No aplica	Se desarrollan y supervisan reglas para

				el desarrollo seguro de software y sistemas.
	8.26	Requisitos de seguridad de las aplicaciones - NUEVO	No aplica	Los requisitos de seguridad de la información deben identificarse, definirse y validarse durante el desarrollo o la adquisición de la aplicación.
	8.27	Arquitectura de sistemas seguros y principios de ingeniería - NUEVO	No aplica	Los principios del diseño de sistemas seguros deben determinarse, documentarse, mantenerse e implementarse en todas las actividades de desarrollo de sistemas de información.
	8.28	Codificación segura	No aplica	Los principios de codificación segura se aplicarán en el desarrollo de software.

	8.29	Pruebas de seguridad en el desarrollo y la aceptación	No aplica	Los procesos de prueba de seguridad de la información se definen e implementan a lo largo del ciclo de vida del desarrollo.
	8.30	Desarrollo externalizado	No aplica	La organización dirige, controla y revisa las actividades relacionadas con el desarrollo de sistemas externos.
	8.31	Separación de los entornos de desarrollo, prueba y producción	No aplica	Los entornos de desarrollo, prueba y producción deben estar segregados y protegidos.
	8.32	Gestión del cambio	No aplica	Los cambios en los equipos de procesamiento de información y los sistemas de información están sujetos al proceso de gestión de cambios.

	8.33	Información de pruebas	No aplica	Los datos de prueba se seleccionan, protegen y gestionan adecuadamente.
	8.34	Protección de los sistemas de información durante la auditoría y las pruebas - NUEVO	No aplica	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

Anexo 5- Formatos guía

GADIP del Municipio de Cayambe	
Formato de Reporte de Incidentes de Seguridad	
Detalles del Incidente	
Fecha y Hora del Incidente:	
Lugar del Incidente:	
Reportado por:	
Descripción del incidente	
Tipo de Incidente:	

Descripción Detallada	
Acciones Inmediatas tomadas	
Acción 1:	
Acción 2:	
Análisis de la causa	
Causa Principal del Incidente:	
Medidas Correctivas y Preventivas	
Medida Correctiva:	
Medida Preventiva:	
Lecciones aprendidas	
Aprobaciones	
Aprobado por:	
Fecha:	
Observaciones:	

GADIP del Municipio de Cayambe	
Formato de identificacipon de activos	
Información General del Activo	
ID del Activo:	
Nombre del Activo:	
Descripción del Activo:	
Tipo de Activo	
☐ Activos Esenciales	
☐ Arquitectura del sistema	
☐ Datos/Información	
☐ Claves criptográficas	
☐ Servicios	

☐ Software / Aplicaciones informáticas	
☐ Equipamiento informático(hardware)	
☐ Redes de Comunicaciones	
☐ Soportes de información	
☐ Equipamiento Auxiliar	
☐ Instalaciones	
☐ Personal	
☐ Otros:….....	
Propiedad y Responsabilidad:	
Propietario del Activo:	
Responsable de la Gestión:	
Ubicación Física:	
Departamento:	
Clasificación del Activo:	
Nivel de Confidencialidad:	
☐ Pública	
☐ Interna	
☐ Confidencial	
☐ Sensible	
Nivel de Disponibilidad:	
☐ Alta	
☐ Media	
☐ Baja	
Nivel de Integridad:	
☐ Alta	
☐ Media	
☐ Baja	
Valor del Activo:	
Valor Financiero:	
Valor Operativo:	
Valor Estratégico:	
Uso del Activo:	
Uso Principal:	
Frecuencia de Uso:	
☐ Diario	
☐ Semanal	
☐ Mensual	
☐ Otro:	
Usuarios del Activo:	

Seguridad del Activo	
Medidas de Seguridad Implementadas	
☐ Control de Acceso Físico	
☐ Control de Acceso Lógico	
☐ Encriptación	
☐ Backup	
☐ Antivirus/Antimalware	
☐ Otro:	
☐ Ninguno	
Riesgos Asociados	
☐ Acceso No Autorizado	
☐ Pérdida de Datos	
☐ Daño Físico	
☐ Interrupción del Servicio	
☐ Otro:	
Ciclo de Vida del Activo:	
Fecha de Adquisición:	
Fecha de Implementación:	
Vida Útil Estimada:	
Plan de Mantenimiento:	
Fecha de Retiro/Disposición:	
Comentarios Adicionales:	

GADIP del Municipio de Cayambe	
Formato de Evaluación de Riesgos	
Información General del Activo:	
ID del Activo:	
Nombre del Activo:	
Propietario del Activo:	
Ubicación Física:	
Identificación de Riesgos	
ID del Riesgo:	

Descripción del Riesgo:	
Fuente del Riesgo:	
☐ Interna	
☐ Externa	
Tipo de Riesgo:	
☐ Tecnológico	
☐ Operacional	
☐ Humano	
☐ Ambiental	
☐ Legal/Regulatorio	
☐ Otro:	
Análisis del Riesgo:	
Amenazas Asociadas:	
Vulnerabilidades del Activo:	
Impacto Potencial:	
☐ Bajo	
☐ Medio	
☐ Alto	
Descripción del Impacto:	
Probabilidad de Ocurrencia:	
☐ Alta (Prácticamente seguro)	
☐ Probable	
☐ Posible	
☐ Poco probable	
☐ Muy raro	
Descripción de la Probabilidad:	
Evaluación del Riesgo	
Nivel de Riesgo (Impacto x Probabilidad):	
☐ Critico	
☐ Importante	
☐ Apreciable	
☐ Bajo	
☐ Despreciable	
Criterio de Evaluación Utilizado:	
Tratamiento del Riesgo:	
Opciones de Tratamiento:	
☐ Aceptar el Riesgo	

☐ Mitigar el Riesgo	
☐ Transferir el Riesgo	
☐ Evitar el Riesgo	
Medidas de Control Propuestas:	
Responsable de la Implementación:	
Fecha de Implementación:	
Seguimiento y Revisión	
Indicadores de Monitoreo:	
Frecuencia de Revisión:	
☐ Mensual	
☐ Trimestral	
☐ Anual	
☐ Otro:	
Resultados de Revisiones Anteriores:	
Comentarios Adicionales:	
Aprobación	
Revisado por:	
Fecha de Revisión:	
Aprobado por:	
Fecha de Aprobación:	

GADIP del Municipio de Cayambe	
Formato de Plan de Tratamiento de Riesgos	
Información General del Riesgo:	
ID del Riesgo:	
Nombre del Activo:	
Descripción del Riesgo:	
Fecha de Identificación:	
Propietario del Riesgo:	
Evaluación del Riesgo:	

Impacto Potencial:	
☐ Muy Bajo	
☐ Bajo	
☐ Medio	
☐ Alto	
☐ Muy alto	
Probabilidad de Ocurrencia:	
☐ Alta(Prácticamente seguro)	
☐ Probable	
☐ Posible	
☐ Poco probable	
☐ Muy raro	
Nivel de Riesgo (Impacto x Probabilidad)	
☐ Critico	
☐ Importante	
☐ Apreciable	
☐ Bajo	
☐ Despreciable	
Estrategia de Tratamiento del Riesgo:	
Opciones de Tratamiento:	
☐ Aceptar el Riesgo	
☐ Mitigar el Riesgo	
☐ Transferir el Riesgo	
☐ Evitar el Riesgo	
Justificación de la Estrategia:	
Medidas de Control Propuestas:	
Medida de Control 1	
Descripción:	
Responsable:	
Fecha de Implementación:	
Recursos Necesarios:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Medida de Control 2	
Descripción:	
Responsable:	

Fecha de Implementación:	
Recursos Necesarios:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Medida de Control 3	
Descripción:	
Responsable:	
Fecha de Implementación:	
Recursos Necesarios:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Monitoreo y Revisión:	
Indicadores de Éxito:	
Frecuencia de Monitoreo:	
☐ Mensual	
☐ Trimestral	
☐ Semestral	
☐ Anual	
☐ Otro:	
Responsable del Monitoreo:	
Resultados del Monitoreo Anterior:	
Comentarios Adicionales:	
Aprobación:	
Revisado por:	
Fecha de Revisión:	
Aprobado por:	
Fecha de Aprobación:	

GADIP del Municipio de Cayambe
Formato de Auditoría Interna

Información General	
ID de la Auditoría:	
Fecha de la Auditoría:	
Área o Departamento Auditado:	
Auditor Principal:	
Miembros del Equipo Auditor:	
Objetivos de la Auditoría	
Objetivo 1:	
Objetivo 2:	
Objetivo 3:	
Alcance de la Auditoría	
Procesos Incluidos:	
Sistemas y Aplicaciones Incluidas:	
Período Cubierto:	
Criterios de Auditoría	
Normas y Estándares Aplicables:	
Políticas y Procedimientos Internos:	
Regulaciones y Legislaciones Relevantes:	
Resultados de la Auditoría	
Hallazgos Positivos:	
Descripción:	
Evidencias:	
No Conformidades:	
ID de No Conformidad:	
Descripción:	
Evidencias:	
Gravedad:	
☐ Menor	
☐ Mayor	
Criterio Afectado:	
Observaciones y Oportunidades de Mejora:	
Descripción:	
Evidencias:	

Recomendaciones:	
Plan de Acción	
Acción Correctiva 1:	
Descripción:	
Responsable:	
Fecha de Implementación:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Acción Correctiva 2:	
Descripción:	
Responsable:	
Fecha de Implementación:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Acción Correctiva 3:	
Descripción:	
Responsable:	
Fecha de Implementación:	
Estado:	
☐ Planeado	
☐ En Proceso	
☐ Completado	
Seguimiento y Revisión	
Responsable del Seguimiento:	
Fecha de Revisión del Seguimiento:	
Estado de las Acciones Correctivas:	
☐ Completadas	
☐ En Proceso	
☐ Pendientes	
Comentarios sobre el Seguimiento:	
Comentarios Adicionales:	
Aprobación	
Revisado por:	
Fecha de Revisión:	
Aprobado por:	

Fecha de Aprobación:	