Maestría en

Gestión de Riesgos

AUTORES:

Marco Vinicio Orellana Moya

Jean Carlos Vaca Cabrera

Robert Peter Pacheco Intriago

TUTORES:

Paloma Manzano Martínez

Enrique Molina Suarez

David Genaro Benavides Gutiérrez

Diseño de un sistema de gestión de riesgos basado en la norma ISO 31000:2018 para el GAD Municipal del Tena

Quito, (diciembre 2025)

Certificación de autoría

Nosotros, **(Marco Vinicio Orellana Moya, Jean Carlos Vaca Cabrera, Robert Peter Pacheco Intriago),** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
MARCO VINICIO ORELLANA MOYA
Validar únicamente con FirmaEC

Firma del graduando

(Marco Vinicio Orellana Moya)

Firmado electrónicamente por:
JEAN CARLOS VACA CABRERA
Validar únicamente con FirmaEC

Firma del graduando

(Jean Carlos Vaca Cabrera)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ROBERT PETER PACHECO INTRIAGO

Firma del graduando

(Robert Peter Pacheco Intriago)

Autorización de Derechos de Propiedad Intelectual

Nosotros, **(Marco Vinicio Orellana Moya, Jean Carlos Vaca Cabrera, Robert Peter Pacheco Intriago)**, en calidad de autores del trabajo de investigación titulado ***Diseño de un sistema de gestión de riesgos basado en la norma ISO 31000:2018 para el GAD Municipal del TENA***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (mes año)

Firmado electrónicamente por:
MARCO VINICIO ORELLANA MOYA
Validar únicamente con FirmaEC

Firma del graduando

(Marco Vinicio Orellana Moya)

Firmado electrónicamente por:
JEAN CARLOS VACA CABRERA
Validar únicamente con FirmaEC

Firma del graduando

(Jean Carlos Vaca Cabrera)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ROBERT PETER PACHECO INTRIAGO

Firma del graduando

(Robert Peter Pacheco Intriago)

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez y David Genero Benavides Gutiérrez,** declaramos que los graduandos: **(Marco Vinicio Orellana Moya, Jean Carlos Vaca Cabrera, Robert Peter Pacheco Intriago)** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

MANZANO MARTINEZ PALOMA - 24244436K

Firmado digitalmente por MANZANO MARTINEZ PALOMA - 24244436K
Fecha: 2026.04.17 07:00:41 +02'00'

Paloma Manzano Martínez

Director/a de la Maestría en Gestión de Riesgos

Firmado electrónicamente por:
DAVID GENARO BENAVIDES GUTIERREZ
Validar únicamente con FirmaEC

David Genera Benavides Gutiérrez

Coordinador/a de la Maestría en Gestión de Riesgos

DEDICATORIA

Este trabajo está dedicado, a mi amada esposa, quien desde el me apoyo y me impulso a continuar con en mi crecimiento como profesional, superar mis límites y me dio empuje para continuar con mis estudios, a mis hijos que son mi motor, mi fuerza y me motivan a entregar todo en cada acción, paso y meta que me propongo.

Marco Vinicio Orellana Moya

"Las aguas calmas no hacen buenos marineros" Franklin D. Roosevelt. Dedico este trabajo a mis padres, hermanos y sobrinos, quienes con su ejemplo me han enseñado que las adversidades forjan el coraje y los desafíos moldean el carácter. Gracias por mostrarme que los errores no son fracasos, sino que son parte indispensable del camino para alcanzar el éxito.

Jean Carlos Vaca Cabrera

Este trabajo está dedicado, en primer lugar, a Dios, mi familia y demás docentes que me inculcaron el valor del esfuerzo, la responsabilidad y la superación. Con su ejemplo me han impulsado, convirtiéndose en la principal fuente de motivación y apoyo constante para alcanzar con éxito esta etapa profesional.

Robert Peter Pacheco Intriago

AGRADECIMIENTOS

Los autores (Marco Vinicio Orellana Moya, Jean Carlos Vaca Cabrera y Robert Peter Pacheco Intriago) expresamos nuestro sincero agradecimiento a la **Universidad Internacional del Ecuador (UIDE)** por darnos la oportunidad de fortalecer nuestras competencias profesionales, conocimientos y contribuir, a través de este trabajo, al desarrollo de la gestión pública en el país.

Extendemos nuestro reconocimiento a nuestros **tutores académicos**, **Paloma Manzano Martínez**, **Enrique Molina Suárez** y **David Genaro Benavides Gutiérrez además de los docentes a lo largo de la maestría**, por su constante guía, orientación técnica y valiosos aportes durante el desarrollo no solo de la investigación si no de la maestría.

Agradecemos de manera especial al **Gobierno Autónomo Descentralizado Municipal del Tena**, por la apertura institucional, la información facilitada y el apoyo brindado en el proceso de levantamiento de datos, análisis y validación de resultados.

Finalmente, expresamos nuestra gratitud a nuestras familias, por su comprensión, apoyo incondicional y motivación constante, los cuales son nuestro motor para culminar con éxito este proyecto académico.

RESUMEN

La investigación tuvo como propósito diseñar un sistema de gestión de riesgos basado en la norma internacional ISO 31000:2018 para la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Gobierno Autónomo Descentralizado Municipal del Tena, considerando la inexistencia de un marco normativo estructurado que permitiera proteger adecuadamente los activos institucionales y la información sensible frente a amenazas de carácter tecnológico, humano y físico, por lo que se planteó la necesidad de proponer un modelo normativo orientado a garantizar la confidencialidad, El desarrollo implicó la creación de un marco metodológico basado en un enfoque cualitativo centrado en las descripciones, que incorporó análisis diagnósticos mediante la utilización de controles de cumplimiento e inventarios de activos. Se realizaron evaluaciones de riesgos basadas en las probabilidades e impactos de los peligros, estableciendo una clasificación jerárquica del riesgo relacionada con los niveles de importancia de activos. El plan resultante se ajustó a las normas ISO 31000, con el objetivo de mejorar la estabilidad institucional y la gestión general del riesgo dentro de los entornos urbanos.

Palabras Claves: Gestión de Riesgos, ISO 31000:2018, Seguridad de la Información, GAD Municipal del Tena, Activos Críticos, Resiliencia Institucional.

ABSTRAC

The purpose of this research was to design a risk management system based on the international standard ISO 31000:2018 for the Directorate of Citizen Security and Risk Management of the Decentralized Autonomous Municipal Government of Tena. This was prompted by the lack of a structured regulatory framework to adequately protect institutional assets and sensitive information from technological, human, and physical threats. Therefore, the need arose to propose a regulatory model aimed at guaranteeing confidentiality. The development involved creating a methodological framework based on a qualitative approach focused on descriptions, which incorporated diagnostic analyses using compliance controls and asset inventories. Risk assessments were conducted based on the probabilities and impacts of hazards, establishing a hierarchical risk classification related to asset importance levels. The resulting plan was aligned with ISO 31000 standards, with the objective of improving institutional stability and overall risk management within urban environments.

Keywords: Risk Management, ISO 31000:2018, Information Security, Municipal GAD of Tena, Critical Assets, Institutional Resilience.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPITULO 1

INTRODUCCION

El Gobierno Autónomo Descentralizado Municipal de Tena es la entidad pública responsable de la administración, gestión y desarrollo del cantón Tena, ubicado en la provincia de Napo, Ecuador. Como órgano de gobierno local, esta institución tiene la misión de promover el bienestar social, económico y ambiental de su población mediante la implementación de políticas públicas, prestación de servicios y regulación territorial.

Dada la creciente complejidad y dinamismo de las funciones municipales, así como la importancia de garantizar la seguridad y eficiencia en la gestión de la información, resulta fundamental estructurar un sistema de gestión de riesgos acorde con los lineamientos de la norma ISO 31000:2018. Este proyecto se centra en la Dirección de Seguridad Ciudadana y Gestión de Riesgos, área clave que maneja información sensible y crítica para la toma de decisiones y la protección de la ciudadanía.

La aplicación de la norma ISO 31000:2018 permitirá identificar, evaluar y controlar los riesgos en los procesos de información, fortaleciendo la capacidad institucional para prevenir amenazas, asegurar la continuidad operativa y garantizar la transparencia y confianza hacia la gestión municipal. Así, se contribuye al desarrollo sostenible y a la

seguridad integral del cantón, alineando la gestión municipal con estándares internacionales reconocidos y buenas prácticas de administración pública.

Este estudio propone para la seguridad de la información en la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Municipio del Tena y la implantación de un sistema de gestión de riesgos basado en la norma ISO 31000:2018.

Se busca establecer un enfoque integral para identificar, analizar, evaluar y tratar los riesgos asociados a los procesos de manejo y almacenamiento de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos. El estudio promueve la implementación de controles específicos para mitigar amenazas como accesos no autorizados, pérdida o manipulación indebida de registros, y fallas en los sistemas tecnológicos.

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO

1.1. Definición del Proyecto

El proyecto consiste en la implementación de un sistema de gestión de riesgos basado en la norma internacional ISO 31000:2018 en la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Gobierno Autónomo Descentralizado Municipal de Tena. Este sistema está orientado a identificar, analizar, evaluar y tratar los riesgos asociados a los procesos de información que soportan las operaciones de la Institución.

El objetivo principal es fortalecer la seguridad de la información mediante un enfoque estructurado, integral y dinámico que permita prevenir posibles amenazas como accesos no autorizados, pérdida o alteración de datos, y fallas en los sistemas tecnológicos, así como potenciar oportunidades de mejora en la gestión.

El proyecto incluye; la definición del contexto organizacional interno y externo, la participación de las partes interesadas, el diseño e implementación de controles específicos para el tratamiento del riesgo, y la supervisión continua para asegurar la eficacia y adecuación del sistema de gestión de riesgos.

1.2. Naturaleza o Tipo de Proyecto

Este tipo de proyecto busca estructurar y formalizar los procesos para identificar, analizar, evaluar y tratar los riesgos asociados con la gestión de la información en la Dirección de Seguridad Ciudadana y Riesgos del Municipio del Tena. Es un proyecto de carácter propositivo que implica el establecer políticas, procedimientos, controles y un marco de gestión de riesgos enmarcado al contexto municipal, con el fin de proteger activos claves como datos, sistemas tecnológicos y procesos críticos.

1.3. Objetivos

1.3.1. Objetivo General

Proponer un modelo de gestión que aplique los principios y directrices de la norma ISO 31000:2018 a los procesos de información de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Municipio del Tena para mejorar la gestión integral de riesgos y proteger la información institucional.

1.3.2. Objetivo Especifico

- Identificar y evaluar los riesgos asociados a los procesos usados por la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GADM de Tena.
- Diseñar e implementar controles para mitigar los riesgos detectados en los procesos que desarrolla la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GADM de Tena, conforme a los lineamientos de la ISO 31000:2018.

- Establecer un proceso de mejora continua enfocada en la protección de datos personales que se recopilan, almacena, y gestionan durante el desarrollo de las actividades y procesos de la Dirección de Gestión de Riesgos del GADM de Tena.

1.4. Justificación e importancia del trabajo de investigación

El presente trabajo de investigación radica en que la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Gobierno Autónomo Descentralizado Municipal de Tena recopila, almacena y gestiona información personal que puede ser considerada como sensible durante los procesos que desarrolla con relación a la seguridad ciudadanía y la gestión de riesgos en el Cantón. La inexistencia de un sistema estructurado que permita gestionar los riesgos en los procesos puede exponer a la Institución a amenazas que pueden comprometer la integridad, disponibilidad y confidencialidad de los datos, afectar la toma de decisiones y generar impactos negativos en la confianza ciudadana.

La aplicación de la norma ISO 31000:2018 ofrece un marco reconocido internacionalmente que permite implementar un sistema integral de gestión de riesgos, facilitando la identificación, el análisis y control de los riesgos minimizando pérdidas, mejorando la eficiencia operativa y asegurando la continuidad de los servicios públicos. Además, la propuesta desarrollada en el presente trabajo permitirá fomentará una cultura organizacional orientada en la prevención, permitirá cumplir con la normativa legal y crear

bases sólidas para la toma de decisiones informadas que contribuyan al cumplimiento de las atribuciones y competencias de la Dirección de Seguridad Ciudadana y Gestión de Riesgos y a la resiliencia institucional ante eventos adversos que comprometan el desarrollo el cumplimiento de los procesos que desarrolla la instancia mencionada, a la vez que asegurar la integridad de la información personal recopilada y almacenada en su desarrollo.

CAPITULO 2

LA ORGANIZACIÓN

2. Perfil de la Organización.

2.1. Nombre, actividades, mercados servidos y principales cifras

2.1.1. Nombre de la Empresa

Gobierno Autónomo Descentralizado Municipal de Tena (GAD Municipal de Tena).

2.1.2. Misión, visión, valores

2.1.2.1. Misión.

Planear, implementar y sostener acciones institucionales para el servicio ciudadano del cantón, con proyectos, obras y servicios de calidad de manera equitativa, oportuna y solidaria, que aseguren un desarrollo social, ordenado y económico de la población, con la participación directa y efectiva de los diferentes actores sociales, dentro de un liderazgo político honesto, responsable y participativo en el marco de la transparencia y la ética institucional, potenciando y optimizando al máximo su talento humano, altamente capacitado comprometido y motivado al servicio público y social. (Gobierno Autónomo Descentralizado Municipal de Tena, 2025)

2.1.2.2. Visión.

Convertir al Cantón en un referente dinámico de cambio, cuyas características de crecimiento, estén marcadas en el desarrollo de sus potencialidades turísticas y productivas, a través de una institución moderna eficiente y autosostenible, con la participación activa de sus habitantes y la articulación de las instituciones públicas y privadas, que se sumen al trabajo en post del cambio que queremos, con responsabilidad social en armonía con la naturaleza, consolidando la identidad tenense de un pueblo trabajador, hospitalario y solidario. (Gobierno Autónomo Descentralizado Municipal de Tena, 2025)

2.1.2.3. Valores.

El GADM de Tena para cumplir con su misión y alcanzar su visión pone en práctica valores y principios institucionales, los cuales son los pilares que se sustentan todas las actividades y procesos que desarrolla la Institución, y siendo considerados como:

> El conjunto de principios, creencias, reglas que regulan la gestión de la organización. Constituyen la filosofía de la Institución y el soporte de la cultura organizacional. Las mismas, tienen el carácter de permanentes y su validez no depende de las circunstancias. (Gobierno Autónomo Municipal de Tena, 2012)

Son de carácter obligatorio para todos los servidores y funcionarios que forman parte de la Institución, debido a que forman parte del marco jurídico cantonal, al encontrarse detalladas en la Ordenanza de Código de Ética, Valores y Principios de las Servidoras y Servidores Públicos del Gobierno Autónomo Descentralizado Municipal de Tena, promulgada en el año 2012 y vigente a la fecha.

Los valores están conformados por 20 numerales del artículo 11 de la ordenanza mencionada, destacando; “Integridad”, “Honestidad”, “Responsabilidad”, “Imparcialidad”, “Respeto”, “Probidad” y “Confidencialidad” (Gobierno Atónomo Municipal de Tena, 2012) siendo esta última de las más relevantes en el contexto actual de País, de manera puntual en la protección de datos personal y en la implementación de la norma ISO 31000, 2018, reconociendo desde el año 2012 la protección de datos que se almacenen en la Institución, la ordenanza menciona también que el custodio de la información, debe realizar los esfuerzos necesarios para precautelar la seguridad y prevenir la revelación no autorizada de información.

2.1.3. Actividades, marcas, productos y servicios

Los Gobiernos Autónomos Descentralizados Municipales (GADM) cuentan con competencias y atribuciones exclusivas dentro de su ámbito territorial, sus responsabilidades se encuentras detalladas en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), mismo que, en sus artículos 54 y 55 describe las funciones y

atribuciones de todos los GADM a nivel nacional. Funciones del GADM de Tena según el COOTAD (2010) son:

- Promover el desarrollo sustentable de su circunscripción territorial cantonal, para garantizar la realización del buen vivir a través de la implementación de políticas públicas cantonales;
- Diseñar e implementar políticas de promoción y construcción de equidad e inclusión en su territorio;
- Establecer el régimen de uso del suelo y urbanístico, para lo cual determinará las condiciones de urbanización, parcelación, lotización, división o cualquier otra forma de fraccionamiento de conformidad con la planificación cantonal;
- Implementar un sistema de participación ciudadana para el ejercicio de los derechos y la gestión democrática de la acción municipal;
- Elaborar y ejecutar el plan cantonal de desarrollo, el de ordenamiento territorial y las políticas públicas en el ámbito de sus competencias y en su circunscripción territorial, de manera coordinada con la planificación nacional, regional, provincial y parroquia;
- Ejecutar las competencias exclusivas y concurrentes reconocidas por la Constitución y la ley y en dicho marco, prestar los servicios públicos y construir la

obra pública cantonal correspondiente con criterios de calidad, eficacia y eficiencia, observando los principios de universalidad, accesibilidad, regularidad, continuidad, solidaridad, interculturalidad, subsidiariedad, participación y equidad;

- Regular, controlar y promover el desarrollo de la actividad turística cantonal en coordinación con los demás gobiernos autónomos descentralizados, promoviendo especialmente la creación y funcionamiento de organizaciones asociativas y empresas comunitarias de turismo;
- Promover los procesos de desarrollo económico local en su jurisdicción, poniendo una atención especial en el sector de la economía social y solidaria;
- Implementar el derecho al hábitat y a la vivienda y desarrollar planes y programas de vivienda de interés social en el territorio cantonal;
- Implementar los sistemas de protección integral del cantón que aseguren el ejercicio garantía y exigibilidad de los derechos consagrados en la Constitución y en los instrumentos internacionales, lo cual incluirá la conformación de los consejos cantonales, juntas cantonales y redes de protección de derechos de los grupos de atención prioritaria. Para la atención en las zonas rurales coordinará con los gobiernos autónomos parroquiales y provinciales;

- Regular, prevenir y controlar la contaminación ambiental en el territorio cantonal de manera articulada con las políticas ambientales nacionales;
- Prestar servicios que satisfagan necesidades colectivas respecto de los que no exista una explícita reserva legal a favor de otros niveles de gobierno, así como la elaboración, manejo y expendio de víveres; servicios de faenamiento, plazas de mercado y cementerios;
- Regular y controlar el uso del espacio público cantonal y, de manera particular, el ejercicio de todo tipo de actividad que se desarrolle en él la colocación de publicidad, redes o señalización;
- Crear y coordinar los consejos de seguridad ciudadana municipal, con la participación de la Policía Nacional, la comunidad y otros organismos relacionados con la materia de seguridad, los cuales formularán y ejecutarán políticas locales, planes y evaluación de resultados sobre prevención, protección, seguridad y convivencia ciudadana;
- Regular y controlar las construcciones en la circunscripción cantonal, con especial atención a las normas de control y prevención de riesgos y desastres;
- Regular, fomentar, autorizar y controlar el ejercicio de actividades económicas, empresariales o profesionales, que se desarrollen en locales ubicados en la

circunscripción territorial cantonal con el objeto de precautelar los derechos de la colectividad;

- Promover y patrocinar las culturas, las artes, actividades deportivas y recreativas en beneficio de la colectividad del cantón;
- Crear las condiciones materiales para la aplicación de políticas integrales y participativas en torno a la regulación del manejo responsable de la fauna urbana;
- Fomentar actividades orientadas a cuidar, proteger y conservar el patrimonio cultural y memoria social en el campo de la interculturalidad y diversidad del cantón. (pág. 28 y 29)

Mientras que sus competencias se encuentran establecidas en el artículo siguiente, el número 55, del COOTAD (2010), el cual menciona:

- Planificar, junto con otras instituciones del sector público y actores de la sociedad, el desarrollo cantonal y formular los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, provincial y parroquial, con el fin de regular el uso y la ocupación del suelo urbano y rural, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad;
- Ejercer el control sobre el uso y ocupación del suelo en el cantón; c) Planificar, construir y mantener la vialidad urbana;

- Prestar los servicios públicos de agua potable, alcantarillado, depuración de aguas residuales, manejo de desechos sólidos, actividades de saneamiento ambiental y aquellos que establezca la ley;
- Crear, modificar, exonerar o suprimir mediante ordenanzas, tasas, tarifas y contribuciones especiales de mejoras;
- Planificar, regular y controlar el tránsito y el transporte terrestre dentro de su circunscripción cantonal;
- Planificar, construir y mantener la infraestructura física y los equipamientos de los espacios públicos destinados al desarrollo social, cultural y deportivo, de acuerdo con la ley. Previa autorización del ente rector de la política pública, a través de convenio, los gobiernos autónomos descentralizados municipales podrán construir y mantener infraestructura física y los equipamientos de salud y educación, en su jurisdicción territorial.
- Preservar, mantener y difundir el patrimonio arquitectónico, cultural y natural del cantón y construir los espacios públicos para estos fines;
- Elaborar y administrar los catastros inmobiliarios urbanos y rurales;
- Delimitar, regular, autorizar y controlar el uso de las playas de mar, riberas y lechos de ríos, lagos y lagunas, sin perjuicio de las limitaciones que establezca la

ley;

- Preservar y garantizar el acceso efectivo de las personas al uso de las playas de mar, riberas de ríos, lagos y lagunas;
- Regular, autorizar y controlar la explotación de materiales áridos y pétreos, que se encuentren en los lechos de los ríos, lagos, playas de mar y canteras;
- Gestionar los servicios de prevención, protección, socorro y extinción de incendios; y,
- Gestionar la cooperación internacional para el cumplimiento de sus competencias. (pág. 29)

Con base en el COOTAD y para desempeñar de manera adecuada las funciones y atribuciones establecidas en la Ley, el GADM de Tena ha creado, su Estatuto Orgánico por Procesos, el mismo, que detalla la forma en la que la Institución se encuentra organizada, su organigrama, designa las responsabilidades y funciones a cada dependencia, lo cual lo convierte en la piedra angular del funcionamiento del GADM. Según la Ordenanza Municipal (Gobierno Autónomo Descentralizado Municipal de Tena, 2025) el GADM de Tena cuenta con 17 Direcciones o áreas de nivel gerencial, una de ella y el motivo de este proyecto es la Dirección de Seguridad Ciudadana y Gestión de Riesgos, según el Estatuto Orgánico la Dirección mencionada cuenta con el siguiente portafolio de productos:

- Plan de Seguridad Cantonal de Tena implementado. • Plan Integral de Gestión de Riesgos para el Cantón Tena implementado.
- Plan Operativo Anual POA de la Dirección. • Plan Anual de Contratación PAC de la Dirección.
- Actas del Consejo Cantonal de Seguridad Integral del Cantón Tena. • Actas del Comité de Operaciones de Emergencia Cantonal.
- Actas de conformación de los comités de Seguridad Ciudadana.
- Informes de implementación de programas para optimización de recursos en materia de seguridad y convivencia ciudadana.
- Informes de la gestión de seguridad ciudadana y de la gestión de riesgos con indicadores de gestión.
- Informes de la dirección con indicadores de gestión. (pág. 127)

2.1.4. Ubicación de la sede

La sede del Gobierno Autónomo Descentralizado Municipal de Tena se encuentra ubicada en Barrio Central, en la intersección de la Calle Juan Montalvo 277 y Abdón Calderón, en la ciudad de Tena, provincia de Napo, Ecuador.

2.1.5. Ubicación de las operaciones

Las operaciones de Dirección de Seguridad Ciudadana del GADM de Tena son de carácter cantonal, es decir se desarrollan en todo el Cantón, sin embargo, sus oficinas se encuentran ubicadas en el Barrio Central, específicamente en la Calle Juan Montalvo y Juan León Mera, Tena, Ecuador, por lo tanto, la mayoría de las operaciones administrativas, técnicas y de gestión se desarrollan en esta principal ubicada en el centro de la ciudad.

2.1.6. Propiedad y forma jurídica

El Gobierno Autónomo Descentralizado Municipal de Tena es una entidad pública con personalidad jurídica de derecho público, con autonomía política, administrativa y financiera. Su forma jurídica corresponde a un gobierno local municipal según lo establecido en la Constitución de la República del Ecuador (Asamblea Nacional del Ecuador, 2008) y el Código Orgánica de Organización Territorial, Autonomía y Descentralización (Asamblea Nacional del Ecuador, 2010).

2.1.7. Mercados servidos o ubicación de sus actividades de negocio

Con base en el documento, el texto enfocado en la **Dirección de Seguridad Ciudadana y Gestión de Riesgos** es el siguiente:

La Dirección de Seguridad Ciudadana y Gestión de Riesgos del GADM de Tena presta sus servicios principalmente en el cantón Tena, ubicado en la provincia de Napo, en la región amazónica de Ecuador. Sus actividades de negocio según el Estatuto Orgánico por

Procesos (GADM de Tena, 2025) están orientadas a la ciudadanía local del cantón, con un enfoque territorial en:

- **Coordinar, articular y ejecutar** planes, programas y proyectos de seguridad ciudadana y gestión integral de riesgos de desastres para precautelar la convivencia pacífica de los habitantes en el Cantón Tena.
- **Implementar un sistema de gestión integral** que permita identificar, evaluar, prevenir y minimizar el impacto de los riesgos en la población y el territorio, priorizando la prevención, preparación y respuesta efectivaz
- **Coordinar acciones de protección** y convivencia ciudadana con los servidores públicos, la ciudadanía, la Policía Nacional y demás organismos competentes.
- **Fomentar la conformación de Comités** Parroquiales y Barriales de Seguridad Ciudadana y Gestión de Riesgos para articular acciones de convivencia pacífica y seguridad.

Por lo tanto, el mercado servido es la población del Cantón Tena, con servicios orientados a precautelar la convivencia pacífica y a la gestión de desastres, mediante la prevención, preparación, respuesta efectiva y recuperación oportuna, en coordinación con el Sistema Nacional Descentralizado de Gestión de Riesgos.

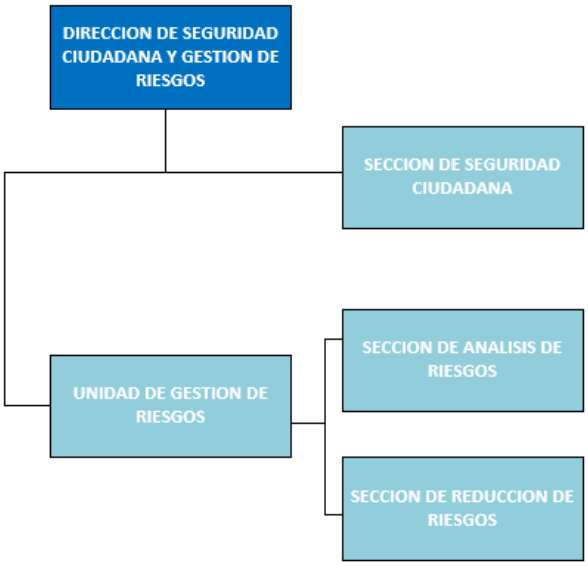
2.1.8. Tamaño de la organización

Dentro del modelo de gestión del Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Tena, la Dirección de Seguridad Ciudadana y Gestión de Riesgos se establece como un proceso agregador de valor. Su estructura orgánica está jerárquicamente organizada bajo la figura de un Director o Directora, quien lidera la totalidad de sus competencias y funciones. La Dirección se ramifica en dos componentes principales para abordar sus responsabilidades: una sección enfocada en la seguridad y una unidad dedicada a la gestión de riesgos, de forma paralela, se estructura la Unidad de Gestión de Riesgos, la cual, debido a la especialización de sus funciones, se subdivide a su vez en dos áreas técnicas: la Sección de Análisis de Riesgos y la Sección de Reducción de Riesgos. Esta configuración permite una gestión diferenciada entre las acciones de convivencia pacífica y las labores de prevención, mitigación y respuesta ante desastres.

El estatuto orgánico no especifica el número total de personal asignado a esta ni a otras direcciones, lo que impide una comparación cuantitativa directa de su tamaño en términos de recurso humano. Sin embargo, la complejidad de su estructura, que incluye una dirección, una unidad y tres secciones en total, es comparable a otras direcciones sustantivas del GAD Municipal como la Dirección de Gestión de Territorio o la Dirección de Gestión Ambiental. La jerarquía de los puestos designados, que contempla un Director, un Coordinador de Unidad y Analistas para cada sección, refleja una estructura robusta diseñada para cubrir las áreas críticas de seguridad y gestión de riesgos en el cantón.

Figura 1

Estatuto Orgánico de Procesos



Nota. El grafico representa el organigrama que conforma la Dirección de Seguridad Ciudadana y Gestión de Riesgos según Estatuto Orgánico por procesos del GADM Tena, 2025.

2.1.9. Información sobre empleados y otros trabajadores.

El Estatuto Orgánico por Procesos del GAD Municipal de Tena no detalla el número total de empleados de la **Dirección de Seguridad Ciudadana y Gestión de Riesgos**, pero sí define los puestos jerárquicos y de liderazgo que la conforman. Estos roles son responsables de la planificación estratégica y la ejecución operativa de las funciones de la Dirección.

Según el Estatuto Orgánico por Procesos (2025) la Dirección de Seguridad Ciudadana

está conformada por:

- **Director o Directora de Seguridad Ciudadana y Gestión de Riesgos**: Es la máxima autoridad de la dirección, responsable de coordinar y ejecutar todos los planes y proyectos para precautelar la convivencia pacífica y gestionar los riesgos en el cantón.
- **Coordinador de Unidad de Gestión de Riesgos**: Está a cargo de la unidad especializada en la gestión integral de riesgos. Su misión es establecer y ejecutar los lineamientos para la prevención y mitigación de desastres.
- **Analista 5 de Análisis de Riesgos**: Dirige la sección encargada de la identificación, análisis, evaluación y seguimiento de las amenazas naturales y antrópicas en el territorio.
- **Analista 5 de Reducción de Riesgos**: Lidera la sección que propone y diseña acciones y obras de mitigación para reducir la vulnerabilidad de la población frente a los riesgos identificados.
- **Sección de Seguridad Ciudadana:** conformada por un **Analista 5 de Seguridad Ciudadana**. Su función principal es diseñar e implementar medidas de prevención en materia de seguridad para el bienestar de la ciudadanía. (pág. 125 a 135)

2.1.10. Procesos claves relacionados con el objetivo propuesto.

Los procesos clave relacionados con el objetivo propuesto en la Dirección de Seguridad Ciudadana y Gestión de Riesgos descritas en el Estatuto Orgánico por Proceso del GADM de Tena (2025) son:

- Identificación, análisis y cartografía de amenazas y vulnerabilidades presentes en

el territorio cantonal, lo cual permite obtener información precisa para la gestión del riesgo.

- Evaluación de factores de riesgo que influyen en las parroquias, comunidades y asentamientos humanos, facilitando la priorización de acciones preventivas y de mitigación.
- Generación de escenarios de riesgos actuales y futuros basados en el análisis de amenazas, exposición y vulnerabilidades para anticipar posibles impactos y planificar respuestas efectivas.
- Elaboración de documentos estratégicos como la agenda de reducción de riesgos, aportar en los planes de desarrollo y ordenamiento territorial, planes de contingencia y plan operativo anual, siguiendo la normativa legal vigente.
- Análisis de exposición y vulnerabilidad de los elementos territoriales, acompañado de la creación y mantenimiento de bases de datos actualizadas con información demográfica, socioeconómica y ambiental que soportan la planificación institucional.
- Coordinación con estructuras y organizaciones barriales para fortalecer la participación ciudadana en la reducción de riesgos y la gestión de seguridad, promoviendo la corresponsabilidad y la resiliencia comunitaria.

2.1.11. Principales cifras, ratios y números que definen a la empresa

Población del cantón Tena: Según el Instituto Ecuatoriano de Estadísticas y Censos (INEC) con corte en el año 2023, la población del cantón se encuentra conformada por 80,816 habitantes y un crecimiento poblacional aproximadamente 2.4%por año, superior al promedio nacional. Gran parte de la población es joven, con alta dinamismo demográfico.

Área territorial: El cantón Tena abarca una extensión territorial de 3.897,41 km2 aproximados (Jimmy Reyes, 2022), área en donde la Dirección de Seguridad Ciudadana y Gestión de Riesgos puede ejercer sus competencias en las diferentes comunidades y asentamientos humanos conforme a las atribuciones y competencias que estable el COOTAD y el Estatuto Orgánico por Procesos.

2.1.12. Modelo de negocio

El modelo de gestión de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GADM de Tena se fundamenta en un marco de competencias establecido por el COOTAD y se operativiza a través de su Estatuto Orgánico por Procesos. El COOTAD (2010) en sus artículos 54 y 140, asigna a los GAD municipales la responsabilidad de gestionar los servicios de prevención, protección, socorro y extinción de incendios, así como la planificación, regulación y control en materia de seguridad y convivencia ciudadana, en coordinación con las entidades nacionales competentes.

En concordancia con mencionado marco legal, el GADM de Tena estructura su modelo de gestión para dar cumplimiento a dichas competencias, clasificando a la Dirección de Seguridad Ciudadana y Gestión de Riesgos como un **"**Proceso Agregador de Valor**"**. Esta categorización, definida en el Artículo 8 del Estatuto Orgánico por Procesos, significa que la dirección es una de las unidades responsables de generar el portafolio de servicios que responden directamente a la misión institucional y a las necesidades de la ciudadanía. Su función no es meramente de apoyo o asesoría, sino que es considerada una actividad sustantiva y central para el bienestar de los habitantes del cantón.

La Dirección materializa este modelo a través de una estructura interna que diferencia sus dos principales componentes de gestión. Por un lado, la **S**ección de Seguridad Ciudadana se encarga de implementar el Plan de Seguridad Cantonal, coordinando acciones con la Policía Nacional y la comunidad para fomentar la convivencia pacífica. Por otro lado, la Unidad de Gestión de Riesgos se enfoca en el Plan Integral de Gestión de Riesgos, abarcando el análisis, la reducción, la preparación y la respuesta ante desastres. Este enfoque dual asegura el cumplimiento de las competencias otorgadas a los GADM en el COOTAD, alineando la planificación estratégica municipal con la seguridad y la resiliencia del territorio.

2.1.13. Grupos de interés internos y externos

Los grupos de interés internos y externos del Gobierno Autónomo Descentralizado Municipal de Tena incluyen:

Grupos de Interés Internos:

- Autoridades municipales, como el Alcalde, Concejales y Directores de áreas.
- Servidores y funcionarios municipales, incluyendo técnicos, administrativos y operarios.
- Unidades y Direcciones relacionadas a las actividades de seguridad ciudadana y gestión riesgos, infraestructura de forma conjunta a la DSCGR.

Grupos de Interés Externos:

- Ciudadanía y residentes del cantón Tena, quienes son los principales beneficiarios de los servicios públicos y sujetos a las políticas municipales.
- Organizaciones sociales, barriales, gremiales, y grupos de atención prioritaria, tales como comunidades indígenas y asociaciones, sociales, políticas culturales, comunitarios, turísticas y deportivas.
- Empresas y actores económicos locales, incluyendo emprendedores y comerciantes.
- Instituciones públicas y privadas de acción social, como fuerzas de seguridad, organismos ambientales, universidades, y entidades de financiamiento.

2.1.14. Otros datos de interés

Entre los datos relevantes sobre el Gobierno Autónomo Descentralizado Municipal de Tena que pueden ser identificados en el sitio web de la Institución, (2025) se encuentran:

- Presupuesto: Para el ejercicio económico de 2025, el GAD Municipal de Tena aprobó una reforma presupuestaria que contempla ingresos corrientes en el orden de aproximadamente 9.9 millones de dólares, provenientes de impuestos, tasas,

contribuciones, ventas de bienes y servicios, entre otros. Este presupuesto refleja la política de racionalización del gasto y optimización de recursos ante los desafíos económicos actuales.

- Políticas públicas: El municipio mantiene un enfoque en la garantía de derechos, desarrollo sostenible, transparencia, rendición de cuentas y participación ciudadana, alineando el presupuesto con el Plan Cantonal de Desarrollo y Ordenamiento Territorial.
- Mecanismos de evaluación: Cuenta con comisiones permanentes que estudian y asesoran sobre la planificación presupuestaria y evalúan las reformas y liquidaciones anuales para asegurar el uso eficiente de los recursos.

CAPITULO 3

3. MANUAL DOCUMENTO DE SEGURIDAD

3.1. Análisis de riesgos.

3.1.1. Identificación de la organización y de sus centros de trabajo.

Gobierno Autónomo Descentralizado Municipal de Tena, la Dirección de Seguridad Ciudadana y Gestión de Riegos esta ubica en las calles Juan Montalvo y calle Juan León Mera

3.1.2. Representante legal y Responsable de seguridad

El Representante Legal: Mgs. Jimmy Xavier Reyes Mariño.

El responsable de Seguridad: Abg. Carlos Alberto Godoy Tapia

3.1.3. Actividades de la organización

Basándonos en el estatuto Orgánico del GADM de Tena (2025) la acción principal es:

a) Planificar programas y proyectos anuales, en base a lo que determina el PDOT, y el Plan de reactivación cultural, en lo referente al plan de gestión de patrimonio cultural;

b) Preservar y conservar el patrimonio edificado y monumentos del Cantón;

c) Gestionar la conservación y salvaguarda del patrimonio cultural y arquitectónico del cantón Tena;

d) Gestionar la calificación de Patrimonio Cultural Local de conformidad con el procedimiento establecido en la normativa vigente;

e) Establecer normas y medidas a adoptarse para salvaguardar la integridad de los sitios y monumentos que hayan sido o podrán ser cambiados o alterados por intervenciones o agregados forzosos;

f) Promover la participación pública o privada, nacional o extranjera para el financiamiento de los programas y proyectos de conservación del patrimonio cultural;

g) Desarrollar procesos técnicos de identificación, codificación y registro de los bienes patrimoniales tangibles e intangibles del cantón Tena;

h) Elaborar el registro, inventario, catalogación y catastro cantonal de todos los bienes que constituyen el patrimonio cultural del cantón Tena;

i) Mantener actualizado el catastro del patrimonio cultural del cantón;

j) Incluir en el plan de gestión de patrimonio cultural estudios para la delimitación del patrimonio arqueológico y paleontológico del cantón Tena;

k) Construir directrices y lineamientos para el mantenimiento, conservación y difusión del patrimonio cultural;

l) Mantener repositorios de la memoria social del cantón;

m) Promover la restitución y recuperación de los bienes patrimoniales expoliados, perdidos o degradados, en coordinación con entidades competentes;

n) Gestionar la declaratoria de patrimonio cultural nacional de los bienes históricos o culturales dentro del cantón;

o) Implementar lineamientos para el buen uso de lugares, espacios y repositorios de la memoria social en los que existan bienes culturales nacionales; y;

p) Las demás atribuciones y responsabilidades establecidas en las normas vigentes, las que disponga la máxima autoridad, el director de área y/o su jefe inmediato

3.1.4. Tratamiento de la organización y sus riesgos.

El tratamiento de la organización y sus riesgos en la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena se basa en una estructura organizacional definida con procesos claros para gestionar eficazmente la seguridad y la gestión de riesgos en el cantón.

Tabla 1.

Análisis de Riesgo por actividad

Actividad	Amenazas	Probabilidad(1-5)	Impacto (1-5)	Riesgo (P×I)
Planificación de programas y proyectos anuales según PDOT y Plan de Reactivación Cultural	Acceso no autorizado a documentos estratégicos, pérdida de información por fallos en respaldo	3	4	12
Preservación y conservación de patrimonio	Fuga de planos técnicos o datos sensibles	3	4	12

edificado y monumentos	a terceros no autorizados			
Actualización del catastro del patrimonio	Acceso no autorizado a datos actualizados por empleados temporales o contratistas	4	4	16
Construcciones directrices para mantenimiento y difusión	Publicación no autorizada de guías o manuales con información sensible	3	4	12
Mantener	Corrupción o borrado	3	5	15

repositorios de la memoria social del cantón	accidental de archivos históricos digitales			
Implementación de lineamientos para uso de repositorios de memoria social	Uso indebido de espacios digitales por personal no capacitado en seguridad	4	4	16

Nota. Esta tabla representa las amenazas más comunes que fueron identificados en La DSCGR, las cuales fueron evaluadas según criterios de probabilidad e impacto.

3.1.5. Consentimientos y notas informativas

Declaración de Consentimiento Informado para el Uso de Datos Personales en el GAD Municipal de Tena.

Yo, _____, mayor de edad, identificado(a) con cédula de ciudadanía número _____, en pleno uso de mis facultades mentales, declaro

que he sido debidamente informado(a) sobre el tratamiento que se dará a mis datos personales en el marco de la gestión de ayuda humanitaria coordinada por el GAD Municipal del Cantón Tena, en colaboración con entidades nacionales autorizadas.

Entiendo que mis datos personales serán recopilados únicamente con el fin de facilitar la entrega oportuna y eficaz de asistencia humanitaria, como alimentos, refugio, atención médica y apoyo psicosocial.

Autorizo expresamente al GAD Municipal del Cantón Tena y a sus aliados operativos a almacenar, procesar y compartir esta información con las instituciones estrictamente necesarias para la ejecución de la ayuda, bajo principios de confidencialidad, seguridad y minimización de datos. Asimismo, comprendo que puedo revocar este consentimiento en cualquier momento, solicitando la eliminación o bloqueo de mis datos, siempre que no comprometa la continuidad de la asistencia ya iniciada.

He sido informado(a) de que mis datos no serán utilizados para fines comerciales, publicitarios o distintos a la asistencia humanitaria, y que se aplicarán medidas técnicas y organizativas para protegerlos contra accesos no autorizados, pérdida o alteración.

Uso y Finalidad:

Los datos personales serán utilizados únicamente para identificar a personas afectadas y/o damnificados frente a la materialización de eventos adverso.

Identificar beneficiarios de asistencia humanitaria en casos de emergencias o desastres de origen natural y/o antrópico.

Identificar predios, sus propietarios, y su ubicación para el desarrollo de informes de exposición a riesgos y amenazas para la regulación del uso y gestión del suelo.

Los datos presentados en las solicitudes de aprobaciones de planes de contingencia para eventos, de concentración masiva de público para identificar los responsables legales del evento, y la emisión de autorizaciones.

Elaboración de Evaluaciones Iniciales de Necesidades (EVIN).

Almacenamiento de la Información:

Con referencia a las solicitudes realizadas para el desarrollo de informes de exposición de amenazas y aprobaciones de los planes de conciencia para eventos masivos se realiza en los equipos de la Dirección de Seguridad Ciudadana y Gestión de Riesgos.

Los datos de beneficiarios de asistencia humanitaria, al igual que los afectados y damnificados se lo realiza en las computadoras de los Técnicos de Gestión de Riesgos.

Tiempo de almacenamiento: se almacena la información por un periodo de 7 años, con base en la mencionado en la Ley Orgánica de la Contraloría General del Estado (LOCGE) y su Reglamento con el objetivo de poder demostrar el uso correcto de fondos públicos en casos de emergencias y la entrega de asistencia humanitario.

Trasferencia: los datos son trasferidos de forma nacional en casos en donde la capacidad de respuesta del GADM de Tena se vea sobre pasada para la entrega de asistencia humanitario, se remite el informe de Evaluación Inicial de Necesidades a la Secretaria Nacional de Gestión de Riesgos y Emergencias para la entrega de asistencia humanitario a los afectadas y damnificados por emergencias y desastres: los datos trasferidos son:

- Nombres
- Números de identificación
- Dirección
- Fecha de nacimiento
- Estimación de Ingresos
- Número de miembros de la familia

No existen decisiones automatizadas en la Institución, los datos son analizados y tratados de forma personal por parte de los colaboradores de la Dirección

En casos de la identificación de afectados y damnificados, al no otorgar sus datos no podrían acceder a asistencia humanitaria en casos de emergencias o desastres.

Para la aprobación de planes de contingencia y solicitudes de inspecciones para la elaboración de informes de exposición a riesgos y amenazas, no se podrá atender la solicitud

al no poder identificar al represéntate legal del predio a ser evaluado, o el promotor o represéntate legal del evento.

Para realizar las reclamaciones ante el tratamiento de datos personales deberán dirigirse a las instalaciones del Dirección de Seguridad Ciudadana y Gestión de Riesgos del GADM de Tena, y ubicados en la interacción de las calles Juan León Mera y Juan Montalvo segundo piso. Con un oficio dirigido hacia la Dirección de Seguridad Ciudadana y Gestión de Riesgos en el que exponga su deseo expreso de revocar el permiso de tratamiento y/o almacenamiento de datos personal o de ser el caso de mal uso de sus datos personales cuando se incurra en alguna de las causales descritas en el Art. 15 de la LOPDP:

- El tratamiento no cumpla con los principios establecidos en la presente ley;
- El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
- Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
- Haya vencido el plazo de conservación de los datos personales;
- El tratamiento afecte derechos fundamentales o libertades individuales;
- Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,

- Exista obligación legal.

Firmo voluntariamente este documento en señal de aceptación, en la ciudad de Tena, Napo, Ecuador el día _____ de _____ 20____.

Firma del interesado: _____

Nombre y Apellido: _____

Número de Identificación: _____

3.2. Registro de actividades de tratamiento

3.2.1. ***Grupos de información***

3.2.2. Sistemas de tratamiento y niveles de seguridad

3.2.3. Finalidades, categorías de datos, de interesados y de destinatarios

Tabla 2.

Tratamiento y seguridad de datos personales

Grupo de información	Sistema de tratamiento	Nivel de seguridad	finalidades	Categorías de datos/interesados/ destinatarios

Datos dentificativos	Papel/Digital	Medio	Gestión de trámites	Titulares/Administración pública
Datos de ontacto	Papel/Digital	Bajo	Notificaciones y comunicaciones	Titulares/Administración pública
Datos económicos	Papel/Digital	Medio	Notificaciones y comunicaciones	Titulares / Entidades financieras
Datos de exclusión social	Papel/Digital	Bajo	Gestión de proyectos	Titulares / Administración pública
Datos de Genero	Papel/Digital	Bajo	Gestión de proyectos	Titulares / Administración pública

3.2.4 Encargados de los tratamientos

Tabla 3.

Información de los encargados en el tratamiento de datos.

Razón social Identificador Localidad	Identificador	Localidad	Servicio prestado	Datos tratados
Proveedor de software QSIG	Software libre	Quito	sistemas de información geográfica	Datos técnicos e Información de catastral
Proveedor Carbonio	RUC:1731221923001	Quito	servicio de correo	Datos personales
Proveedor Cgweb	RUC:1791305035001	Quito	Gestión documentaria	Datos personales, nóminas, roles de pago (Sistema financiero)

3.3 Registros de dispositivos

Tabla 4.

Inventario de Dispositivos Digitales

Dispositivos Digitales	Cantidades	UBICACION
Computadoras de escritorio	*2*	*Área de Seguridad Ciudadana*

Computadoras de escritorio	*2*	*Área de Seguridad Gestión de Riesgos*
Computadoras portátiles (Laptop)	*1*	*Oficina del Director*
Impresoras escáneres de red	*1*	*Área de Gestión de Riesgos*
Dispositivos móviles (Tablets)	*1*	*Área de Gestión de Riesgos*
Routers de red	*1*	*Área de Seguridad*
TOTAL	***8***	

3.4 Registro de sistemas de información

Los encargados para el registro del sistema de información los realiza cada funcionario de la Dirección de Seguridad Ciudadana y Gestión de Riegos

- Sistema de Correo Institucional CARBONIO
- Sistemas de gestión documental QUIPUX
- QGIS

- Microsoft Office 365

3.5 Registro de Personal

3.5.1 Con Acceso a Datos

3.5.2 Sin acceso Datos

Tabla 5.

Acceso a datos por parte del personal

Personal	Acceso a datos	Tipo de datos que maneja
Director de Seguridad Ciudadana y Gestión de Riesgos	Acceso total	Datos referentes a catastros, permisos de actividades económicas, Índices de inseguridad por sector, áreas de susceptibilidad a riesgos, permisos de suelos
Coordinador de Seguridad Ciudadana y Gestión de Riesgos	Acceso total	Datos referentes a catastros, permisos de actividades económicas,

		Índices de inseguridad por sector, áreas de susceptibilidad a riesgos, permisos de suelos
Técnico de Gestión de Riesgos	Acceso parcial	Datos de Información Geográfica, EVIN, EDAN,
Técnico de Seguridad Ciudadana	Acceso parcial	Datos de Información de CMI (Control de Mando Integral), índices delictivos.
Personal de limpieza	No	Ninguno
Personal de mantenimiento	No	Ninguno

3.5.3. Accesos Físicos

Las llaves correspondientes a cada una de las instalaciones la poseen el conserje el cual es el encargado de abrir y cerrar oficinas dependiendo de la necesidad y el horario laboral.

3.6.1 con Acceso a Datos

Tabla 6.

Prestadores de servicios con acceso a datos

Razón social / Tipo de empresa	Identificador	Localidad	Servicio prestado	Tipo de acceso a datos
Empresa de instalación de cámaras y alarmas comunitarias	RUC: AAAA	Cuenca/Tena	Instalación de cámaras y alarmas en los barrios	Acceso a datos poblacionales
Firma consultora en proyectos de seguridad	RUC: BBBBB	Tena	Estudios de índices de percepción de seguridad en espacio publico	Acceso a bases de datos barriales y georreferenciación de sectores delictivos

3.6.2 Sin acceso a datos catalogados

Corresponden a aquellas empresas contratadas por el GAD Municipal del Tena que no necesitan acceso directo a los datos personales de los trabajadores o usuarios. Sin embargo, en caso de tener acceso ocasional a información sensible, deben cumplir con obligaciones de confidencialidad y reserva.

Tabla 6.

Prestadores de servicios sin acceso a datos

Razón social / Tipo de empresa	Identificador	Localidad	Servicio prestado	Tipo de acceso a datos
Empresa de Seguridad Privada en Instalaciones Municipales	RUC: CCCCC	Tena	Seguridad física de las Instalaciones Municipales	Sin Acceso a la base de datos de los funcionarios

Proveedores que Ganadores mediante el Portal de Compras públicas para la Adquisición de Bienes	RUC: DDDDD	Tena	Suministro de Bienes, materiales, para el GAD Tena	Sin Acceso a Datos poblacionales
Empresa de Mantenimiento de Bienes de la Dirección de Seguridad	UC: FFFFF	Tena	Mantenimiento de motocicletas, y vehículos de los Agentes de Control Municipal	Sin acceso a Datos poblacionales y CACM

3.7.Sistemas de Captación de Imágenes y Audio

3.7.1. Número de Cámaras

01 una cámara de circuito cerrado de televisión que monitorea el ingreso y salida del edificio dentro de las instalaciones de la dirección de Seguridad Ciudadana y Gestión de Riesgos.

3.7.2. Zonas de Influencia

La cámara de seguridad se encuentra ubicada en el ingreso del edificio Rueda específicamente en el ingreso hacia los niveles 1 y 2 del edificio la cámara identifica únicamente la puerta principal que dirige hacia las escaleras del edificio mencionado no se puede observar el exterior debido a que la cámara está ubicada sobre la puerta de ingreso enfocando hacia las escaleras.

3.7.3 Sistemas de Tratamiento y Almacenamiento

Las imágenes son recibidas y almacenadas en una sala de monitoreo centralizada qué se encuentran bajo el cargo de la dirección de control municipal. El tratamiento de esta información se rige por protocolos de seguridad para proteger la privacidad de los ciudadanos servidores y funcionarios municipales.

3.7.4. Usuarios Autorizados

El acceso a las imágenes en tiempo real y a las grabaciones está restringido al personal de la sala de monitoreo, al Director de Control Municipal y, en casos de emergencia o investigación, se comparte con la Dirección de Seguridad Ciudadana, el COE Cantonal y la Policía Nacional.

3.8.Dispositivos y Medidas de Seguridad

3.8.1. Análisis de las medidas de seguridad de los dispositivos

El análisis de las medidas de seguridad implementadas en los dispositivos utilizados por la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Municipio de Tena revela aspectos positivos y áreas de mejora importantes para fortalecer la protección de la información.

Los dispositivos como computadoras de escritorio, laptops, memorias USB y servicios de almacenamiento en la nube (Drive) cuentan con controles mínimos a la confidencialidad y protección mediante el uso de claves de acceso a la información ya que en dicho almacenamiento han sido creadas con cuentas de correo electrónico propias de los funcionarios sin tener ningún tipo de seguridad y restricciones.

Una limitación significativa observada es la falta de restricciones para el uso de memorias USB, lo que puede facilitar la introducción inadvertida de software malicioso o la fuga de datos sensibles. La conectividad libre y sin supervisión de estos dispositivos representa un vector de riesgo alto, especialmente en una institución vinculada a la seguridad ciudadana y gestión de riesgos.

3.8.2 Propuesta de mejora de las medidas de seguridad

Propuesta de mejora de las medidas de seguridad para los dispositivos de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Municipio de Tena se debe realizar conjuntamente con la Dirección de TIC´S del Gobierno Gobierno Autónomo Descentralizado Municipal de Tena, implementar sistemas de monitoreo continuo para detectar accesos no autorizados, comportamientos anómalos o intentos de vulneración, además, de realizar auditorías periódicas para revisar la efectividad de las medidas, cumplimiento de políticas y ajustar controles según resultados, además de realizar lo siguiente:

- Mantener y automatizar las actualizaciones de sistemas operativos y aplicaciones para garantizar parches de seguridad oportunos.
- Instalar sistemas de prevención contra la inserción no autorizada de dispositivos extraíbles (USB) mediante software especializado para bloquear o monitorear el uso.
- Adoptar soluciones de cifrado avanzado no solo en almacenamiento sino también en

comunicaciones internas y externas.

- Establecer políticas claras de gestión de contraseñas, incluyendo periodicidad obligatoria para cambio de claves y protocolos de recuperación seguros.
- Implementar autenticación multifactor (MFA) para acceso a dispositivos críticos, aumentando la seguridad más allá de la contraseña única.
- Definir perfiles de usuarios basados en roles para asignar permisos mínimos necesarios según funciones.

3.9.Puestos de trabajo

3.9.1 Análisis de medidas de seguridad por puesto de trabajo

Dirección de Seguridad con un Director de Seguridad. Dado que el Director maneja información crítica relacionada con la seguridad ciudadana, la coordinación con las fuerzas del orden y la gestión de riesgos, constituye un blanco prioritario para amenazas, coacciones o incluso ataques por parte de grupos delictivos u otros actores que buscan vulnerar la seguridad del cantón. La elevada sensibilidad de la información custodiada incrementa su exposición a riesgos tanto físicos como digitales.

Además, existen riesgos reputacionales asociados al cargo; errores en la gestión de incidentes, filtraciones de información o deficiencias en los mecanismos de prevención

pueden impactar negativamente la confianza tanto de la ciudadanía como de las autoridades en la Dirección. Esta pérdida de confianza puede deteriorar la efectividad operativa y el prestigio institucional.

Actualmente, las únicas medidas de seguridad presentes en el puesto de trabajo son el uso de una contraseña para el acceso al computador asignado. Asimismo, no existen controles o bloqueos para el uso de dispositivos USB, lo que incrementa la vulnerabilidad ante potenciales ataques informáticos o filtraciones de datos. Esta falta de mecanismos de protección robustos expone críticamente el puesto de la Dirección de Seguridad Ciudadana frente a amenazas operativas, tecnológicas y sociales provenientes de grupos de delincuencia organizada.

Coordinador de la Dirección de Seguridad Ciudadana y Gestión de Riesgos. El Coordinador de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Municipio de Tena desempeña un rol operativo y táctico fundamental, responsable de la planificación, supervisión y ejecución diaria de las actividades orientadas a garantizar el cumplimiento de los objetivos institucionales en materia de seguridad y gestión de riesgos. Este puesto exige una gestión eficiente y un control riguroso para mantener la seguridad pública y la mitigación de riesgos en el cantón.

Actualmente, las medidas de seguridad implementadas en el puesto se limitan al uso de contraseña para acceso al computador asignado. Sin embargo, no existen bloqueos ni

restricciones para el uso de dispositivos USB en dicho equipo, lo que representa una vulnerabilidad significativa frente a posibles amenazas de seguridad informática. Adicionalmente, el personal utiliza servicios de almacenamiento en la nube configurados con cuentas personales, en los cuales se suben documentos y archivos relacionados con la Dirección de Seguridad. Esta práctica puede conllevar riesgos de privacidad y seguridad, dado que la información institucional podría estar sujeta a accesos no autorizados o pérdidas de control sobre los datos.

Técnico de Seguridad Ciudadana. El análisis de medidas de seguridad de la información para el Técnico de Seguridad Ciudadana debe considerar el manejo diario de información altamente sensible, como los índices delictivos en espacio público, la ubicación de cámaras de vigilancia del GAD Municipal de Tena, y datos sobre consejos de seguridad ciudadana. Este puesto adquiere un nivel crítico de sensibilidad debido a la naturaleza estratégica de la información que administra, lo cual lo convierte en un objetivo potencial para grupos de delincuencia organizada.

El riesgo de reclutamiento o coacción hacia el técnico por parte de organizaciones criminales aumenta debido al acceso privilegiado a estos datos críticos, lo que hace imprescindible la implementación de controles administrativos y técnicos estrictos. Estos incluyen políticas claras de confidencialidad, monitoreo constante de accesos, capacitación en

protección de la información, y protocolos de segregación de funciones para minimizar la posibilidad de abuso o filtración.

Actualmente, las medidas de seguridad implementadas en el puesto se limitan a la utilización de una contraseña para el acceso al computador, sin que exista bloqueo o restricciones para el uso de dispositivos USB. Además, en el puesto se emplean nubes de almacenamiento creadas con cuentas personales de los funcionarios, donde se almacenan archivos y documentos de la Dirección de Seguridad Ciudadana. Esta práctica representa un riesgo elevado de exposición y fuga de información, pues dichos servicios pueden no contar con los controles de seguridad institucionales adecuados.

Técnico de Gestión de Riesgos. El Técnico de Gestión de Riesgos desarrolla actividades orientadas a la identificación, análisis, evaluación y mitigación de riesgos asociados a la seguridad de la información y la continuidad operativa. Al operar en un equipo con acceso protegido mediante contraseña, este profesional se convierte en un actor clave para salvaguardar datos y documentos críticos del cantón.

No obstante, el uso de una contraseña única, que podría ser débil, presenta vulnerabilidades significativas. Dicha contraseña puede ser comprometida mediante técnicas automatizadas de ataque, ingeniería social, o a través de malware especializado como keyloggers. Esto facilita el acceso no autorizado a sistemas y la consecuente exposición de

información sensible, con el riesgo adicional de pérdida o corrupción de los datos almacenados en el equipo.

3.9.2 Acuerdo de confidencialidad.

Datos identificativos de la organización. El representante legal del Gobierno Autónomo Descentralizado (GAD) Municipal del cantón Tena, el Mg. Jimmy Xavier Reyes Mariño, ubicado en Barrio Central, en la intersección de la Calle Juan Montalvo 277 y Abdón Calderón.

Datos identificativos del trabajador.

Nombre completo: _____

Cédula de identidad: _____

Cargo: _____

Área/dependencia: _____

Cláusulas:

PRIMERA: Actividad de tratamiento de acceso

El trabajador tendrá acceso autorizado a la información y datos personales manejados por la Dirección en cumplimiento de sus funciones, quedando sujeto a las normas de confidencialidad y seguridad establecidas.

SEGUNDA: Obligación de confidencialidad

El trabajador se compromete a mantener la confidencialidad absoluta sobre toda la información a la que tenga acceso, tanto durante como después de la relación laboral, absteniéndose de divulgar, transmitir, copiar o utilizar datos para fines no autorizados.

TERCERA: Obligación de cumplimiento de medidas de seguridad

El trabajador deberá cumplir estrictamente con las políticas, protocolos y medidas de seguridad implementados para proteger la información, tanto en aspectos técnicos como administrativos y físicos.

CUARTA: Consecuencias de vulnerar las obligaciones

El incumplimiento de las obligaciones establecidas en este acuerdo dará lugar a sanciones administrativas, civiles y penales conforme a la legislación vigente y normativa interna del municipio, incluyendo la posible terminación de la relación laboral.

QUINTA: Finalidad y uso de la recogida de los datos del trabajador por parte de la organización

Los datos personales serán utilizados exclusivamente para la gestión administrativa, operativa y de seguridad relacionadas con el acceso y desempeño en la Dirección.

SEXTA: Tiempo de almacenamiento de sus datos

Los datos personales serán conservados durante la vigencia de la relación laboral y los períodos adicionales que establezca la normativa aplicable para archivo y auditoría.

SEPTIMA: Ejercicio de derechos del trabajador y dónde ejercitarlos

El trabajador podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición (ARCO) ante el Delegado de Protección de Datos del Municipio del Tena, ubicado en Calle Juan Montalvo 277 y Abdón Calderón

Datos identificativos del Delegado de Protección de Datos (DPD) De la Dirección de Seguridad Ciudadana y Gestión de Riegos del GAD del Tena

Nombre: _____

Cargo:_____

Correo electrónico:_____

Teléfono: _____

Informaciones específicas sobre sistemas adicionales

- Videovigilancia: El trabajador está informado sobre el funcionamiento del sistema de videovigilancia instalado en las instalaciones, su finalidad y el tratamiento de las grabaciones, conforme a la ley.
- Sistema de localización GPS: En caso de utilizarse sistemas de localización GPS para vehículos o dispositivos, el trabajador será debidamente informado.
- Recogida de datos biométricos: Cualquier recogida de datos biométricos (huellas dactilares, reconocimiento facial, etc.) será realizada solo con conocimiento y

consentimiento del trabajador, garantizando el respeto a su privacidad.

Fecha:

---------- ----------

Firma del trabajador: Firma representante legal del Municipio:

Este acuerdo garantiza el compromiso del trabajador con las políticas de seguridad y confidencialidad de la Dirección, en cumplimiento con la Ley Orgánica de Protección de Datos Personales y las normativas internas del Municipio del Tena.

3.10 Encargado del tratamiento

Contrato de Encargado del Tratamiento

Se establecerá un contrato formal entre la Dirección y el encargado del tratamiento que incluya cláusulas específicas como:

- Definición del alcance del tratamiento de datos.
- Obligaciones de confidencialidad y seguridad.
- Responsabilidades en caso de incumplimiento normativo.
- Derechos y deberes conforme a la LOPDP.

- Procedimientos para la gestión de incidentes y brechas de seguridad.

- Revisión y actualización periódica del contrato.

CONTRATO DE ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

EL RESPONSABLE DEL TRATAMIENTO: Dirección de Seguridad Ciudadana y Gestión de Riesgos, legalmente representada por el Abg. César Abrahán Puma Sánchez en su calidad de Director de Seguridad Ciudadana y Gestión de Riesgos, con RUC 1560000270001 y domicilio en calle Juan Montalvo 277 y Abdón Calderón.

EL ENCARGADO DEL TRATAMIENTO: [Nombre de la Empresa/Proveedor] (en adelante, el "ENCARGADO"), legalmente representada por [Nombre del Representante], con RUC [Número de RUC] y domicilio en [Dirección].

Ambas partes, reconociendo su capacidad legal para contratar y obligarse, acuerdan suscribir el presente Contrato de Encargado del Tratamiento, sujeto a las siguientes cláusulas:

CLÁUSULA PRIMERA: IDENTIFICACIÓN DE LAS PARTES

1.1. Identificación del Responsable del Tratamiento

- Nombre: Dirección de Seguridad Ciudadana y Gestión de Riesgos de Tena (GAD TENA) Dirección: Calle Juan Montalvo 277 y Abdón Calderón. RUC: 1560000270001

Representante Legal: Abg. César Abrahán Puma Sánchez, Director de Seguridad Ciudadana y Gestión de Riesgos Contacto: alcaldia@tena.gob.ec,Teléfono: 6299 4800

1.2. Identificación del Encargado del Tratamiento

Nombre: [Nombre de la Empresa/Proveedor] Dirección: [Dirección] RUC: [Número de RUC] Representante Legal: [Nombre del Representante], [Cargo] Contacto: [Correo Electrónico], [Teléfono]

1.3. Identificación del Delegado de Protección de Datos (DPD) (si aplica)

Del Responsable (GAD TENA): [Nombre del DPD], [Contacto del DPD] (Si aplica, de lo contrario, indicar "No aplica" o "Pendiente de designación"). **Del Encargado:** [Nombre del DPD], [Contacto del DPD] (Si aplica, de lo contrario, indicar "No aplica" o "Pendiente de designación").

CLÁUSULA SEGUNDA: OBJETO, DURACIÓN Y NATURALEZA DEL TRATAMIENTO

2.1. Objeto del Contrato

El presente contrato tiene por objeto regular el acceso y tratamiento de datos personales por parte del ENCARGADO para la prestación de los servicios de

[Descripción del Servicio, ej. mantenimiento de sistemas de videovigilancia, gestión de base de datos de seguridad, desarrollo de software, etc.] en favor del GAD TENA.

2.2. Duración del Contrato

El presente contrato tendrá una duración de un año, desde la fecha de su firma y se renovará automáticamente por períodos iguales, salvo notificación en contrario de cualquiera de las partes con [Número] días de antelación a su vencimiento.

2.3. Naturaleza del Tratamiento

La naturaleza del tratamiento consiste en la gestión, el almacenamiento, la consulta, la organización, la estructuración, la modificación, la extracción, la utilización, la comunicación por transmisión, la difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales.

CLÁUSULA TERCERA: FINALIDAD, TIPO DE DATOS Y CATEGORÍA DE INTERESADOS

3.1. Finalidad del Tratamiento

La finalidad del tratamiento de datos personales es. garantizar la seguridad ciudadana, prevenir el delito, gestionar emergencias, siempre bajo las instrucciones del GAD TENA y en cumplimiento de sus funciones públicas.

3.2. Tipo de Datos Tratados

Los datos personales objeto de tratamiento incluyen, pero no se limitan a:

Datos identificativos:

Nombres y Apellidos: _____

Número de cédula: _____ _____

Dirección: _____

Teléfono: _____

Correo electrónico: _____

Datos de imagen/voz: Grabaciones de videovigilancia, registros de audio.

Datos de ubicación: Información geográfica obtenida de dispositivos o sistemas de monitoreo.

3.3. Categoría de Interesados

Las categorías de interesados cuyos datos personales serán tratados incluyen, pero no se limitan a:

- Ciudadanos del cantón Tena.
- Personal del GAD Tena (incluyendo Dirección de Seguridad Ciudadana).

- Visitantes y usuarios de espacios públicos.
- Personas involucradas en incidentes de seguridad.

CLÁUSULA CUARTA: INSTRUCCIONES PARA EL TRATAMIENTO Y MARCO NORMATIVO

4.1. Instrucciones para el Tratamiento

El ENCARGADO tratará los datos personales únicamente siguiendo las instrucciones documentadas del GAD TENA, incluyendo las relativas a las transferencias de datos personales. Si el ENCARGADO considera que alguna instrucción infringe la LOPDP o cualquier otra disposición en materia de protección de datos, informará inmediatamente al GAD TENA.

4.2. Marco Normativo y Estándares

El tratamiento de datos se regirá estrictamente por:

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador y su Reglamento.

El Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público (COESCOP), en lo que fuere aplicable.

Cualquier otra normativa aplicable en materia de protección de datos personales.

CLÁUSULA QUINTA: OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

El ENCARGADO se compromete a:

Confidencialidad: Mantener el más estricto secreto profesional respecto a los datos personales a los que tenga acceso, incluso tras la finalización del contrato, y garantizar que las personas autorizadas para tratar datos personales se comprometan a respetar la confidencialidad.

Medidas de Seguridad: Implementar medidas técnicas, organizativas y físicas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Asistencia al **responsable**: Asistir al GAD TENA en el cumplimiento de sus obligaciones de responder a las solicitudes de ejercicio de los derechos de los titulares de los datos (acceso, rectificación, eliminación, oposición, portabilidad, etc.).

Notificación de Incidentes: Notificar al GAD TENA sin dilación indebida y, en cualquier caso, en un plazo máximo de 24 horas desde que tenga conocimiento de cualquier violación de la seguridad de los datos personales.

Registro de Actividades: Mantener un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable.

Subcontratación: No subcontratar el tratamiento de datos personales sin la autorización previa por escrito del GAD TENA.

Auditorías: Poner a disposición del GAD TENA toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este contrato y permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del GAD TENA o de otro auditor autorizado por este.

CLÁUSULA SEXTA: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El GAD TENA se compromete a:

Licitud del Tratamiento: Garantizar que el tratamiento de datos personales es lícito y que ha obtenido las bases legitimadoras necesarias para el tratamiento de los datos que encarga al ENCARGADO.

Información al Encargado: Proporcionar al ENCARGADO toda la información necesaria para el correcto cumplimiento de sus obligaciones, incluyendo las instrucciones precisas para el tratamiento de los datos.

Supervisión: Supervisar el cumplimiento por parte del ENCARGADO de las medidas de seguridad y las obligaciones establecidas en el presente contrato y en la normativa aplicable.

Evaluación de Impacto: Realizar, cuando sea necesario, evaluaciones de impacto relativas a la protección de datos y consultar a la Autoridad de Protección de Datos Personales.

Notificación a la Autoridad: Notificar a la Autoridad de Protección de Datos Personales las violaciones de seguridad de los datos personales, cuando proceda.

CLÁUSULA SÉPTIMA: MEDIDAS PARA LA COMUNICACIÓN DE BRECHA DE SEGURIDAD

En caso de detectarse una violación de la seguridad de los datos personales, el ENCARGADO:

Notificará al GAD TENA de forma inmediata y, en todo caso, en un plazo máximo de 24 horas tras tener conocimiento, proporcionando al menos:

La naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

El nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.

Las posibles consecuencias de la violación de la seguridad de los datos personales.

Las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas para mitigar sus posibles efectos negativos.

Colaborará activamente con el GAD TENA en la investigación del incidente y en la implementación de las medidas correctivas necesarias.

CLÁUSULA OCTAVA: RESPONSABILIDAD E INCUMPLIMIENTO

El incumplimiento de las obligaciones establecidas en este contrato o en la LOPDP por parte del ENCARGADO dará lugar a:

La resolución inmediata del contrato de prestación de servicios, sin perjuicio de las acciones legales que correspondan.

La asunción de las indemnizaciones por daños y perjuicios que pudieran derivarse para el GAD TENA o para los titulares de los datos.

La responsabilidad directa ante las sanciones administrativas impuestas por la Autoridad de Protección de Datos, si el incumplimiento le fuera imputable.

CLÁUSULA NOVENA: REVISIÓN Y ACTUALIZACIÓN PERIÓDICA

Las partes acuerdan revisar el presente contrato anualmente o cuando existan cambios significativos en el tratamiento de datos, en la normativa aplicable o en la evaluación de riesgos.

CLÁUSULA DÉCIMA: ACUERDO DE FINALIZACIÓN DE RELACIÓN Y DESTINO DE LOS DATOS

A la terminación de la prestación de los servicios, el ENCARGADO deberá, a elección del GAD TENA:

Devolver al GAD TENA todos los datos personales y cualquier soporte o documento en que consten, incluyendo copias, en un formato estructurado, de uso común y lectura mecánica.

Destruir de forma segura todos los datos personales, incluyendo copias, certificando dicha destrucción por escrito al GAD TENA, salvo que exista una obligación legal que exija la conservación de los datos personales.

SUSCRIPCIÓN:

En la ciudad de Tena, a los [Día] días del mes de [Mes] de 2026.

Por el GAD TENA (Responsable)	**Por el ENCARGADO (Procesador)**
[Firma]	[Firma]
Nombre:	Nombre:
Cargo:	Cargo:

3.11. Análisis Web

3.11.1 Análisis, configuración y Política de cookies

Al ingresar a la página web del Municipio del Tena, se pudo observar que no existe una política de cookies clara, accesible y conforme a la normativa vigente. Según el artículo 22 de

la Ley de Servicios de la Sociedad de la Información (LSSI) y la LOPDP, se requiere el consentimiento informado del usuario antes de la instalación de cookies no esenciales. A continuación, se adjunta el link del Municipio del Tena: https://tena.gob.ec/

Podemos verificar en el aparatado del sitio, la conexión segura, podemos verificar que posee un certificado de Sectigo Public Server Authentication CA DV R36, emitido el 4 de junio de 2025y su caducidad es el 6 de julio de 2026.

En las cookies y datos del sitio, en el apartado "Gestionar los datos del sitio en el dispositivo" podemos verificar que le hemos dado acceso simplemente por navegar por que no se ha aceptado, ya que no posee aceptación de cookies al principio de la página web.

La ausencia de una política de cookies clara dificulta que los usuarios comprendan qué datos se recopilan, con qué finalidad (analíticas, publicidad, funcionamiento técnico) y si se utilizan cookies de terceros como Google Analytics o herramientas de gestión de consentimiento como Usercentrics.

Se recomienda clasificar las cookies en esenciales, analíticas, de rendimiento y de publicidad, y proporcionar un banner de cookies que permita al usuario aceptar, rechazar o configurar sus preferencias. La política debe estar disponible en un enlace permanente en el pie de página y detallar el tipo de cookies, su finalidad, duración y entidad responsable.

3.11.2 Formularios de contacto, newsletter, trabaja conmigo, registro

La página web del Municipio del Tena (**https://tena.gob.ec**) no posee formularios interactivos de contacto, newsletter, “trabaja con nosotros” ni registro ciudadano accesibles directamente desde las secciones analizadas.

En la sección de contacto (**https://tena.gob.ec/contacto/**), solo se muestra información general sobre redes sociales oficiales y enlaces a entidades adscritas, pero no se incluye un formulario web para envío de mensajes, ni campos para ingresar nombre, correo o asunto, lo cual limita la interacción ciudadana digital.

Tampoco se identifica una sección de newsletter o suscripción para recibir actualizaciones, ni un enlace a un formulario de empleo bajo títulos como “trabaja con nosotros”, “empleo” o “convocatorias”. Asimismo, no existe un sistema de registro de usuarios para acceder a servicios digitales, lo que sugiere que los trámites o interacciones ciudadanas probablemente se gestionen de forma presencial o a través de otros canales no integrados al sitio web.

3.11.3 Aviso legales

la página web oficial del municipio del Tena (tena.gob.ec), un apartado específico denominado "Aviso legal". Aunque se ofrece información institucional, de transparencia y contacto, no se localiza un documento, sección o enlace claramente nombrado como “Aviso legal” o que cumpla plenamente con los requisitos formales de identificación del responsable, términos de uso, protección de datos y propiedad intelectual.

Esto implica que el sitio no cumple de forma expresa con las mejores prácticas y obligaciones normativas respecto al aviso legal, como exige la Ley Orgánica de Protección de Datos Personales (LOPDP), la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y los principios de la Ley de Comercio Electrónico y la LSSI.

Medidas de Seguridad

3.12.1 Análisis, uso y medidas de seguridad en el uso de navegadores

Dado que esta Dirección de Seguridad y Convivencia Ciudadana y Gestión de Riesgos del Municipio del Tena maneja información sensible relacionada con seguridad pública, riesgos y operaciones municipales, los dispositivos electrónicos como computadores de escritorio, portátiles, y tablets utilizan navegadores de con las últimas versiones y parches de seguridad, bloqueo de ventanas emergentes, protección contra phishing y malware.

3.12.2 Hosting y Servidores

3.12.2.1 Medidas de seguridad

El Municipio del Tena posee hosting y servidores, un documento de contratación (N° SERVICIO IC-GADMTENA-2024-063) confirma que el municipio utiliza un servidor Proliant DL120 Gen9 de HP, sobre el cual se virtualiza el sistema catastral georreferenciado SIGPro mediante el entorno de software libre Proxmox. Este servidor almacena y procesa información

crítica de las direcciones de Gestión de Riesgos, Avalúos y Catastros, y fue objeto de mantenimiento para recuperación de datos, reinstalación del sistema operativo Ubuntu Server LTS, y configuración de herramientas como Tomcat, PostgreSQL y GeoServer.

El uso de un sistema operativo Ubuntu Server LTS (versión de soporte a largo plazo) y la virtualización mediante Proxmox indican un enfoque técnico moderno y seguro, que permite:

- Aislamiento de servicios.
- Actualizaciones controladas.
- Recuperación ante fallos.
- Gestión eficiente de recursos.

Además, la virtualización facilita la implementación de cortafuegos, monitoreo de tráfico y políticas de acceso, alineadas con buenas prácticas de ciberseguridad.

3.12.2.2 Prestadores de servicios

El GAD Municipal de Tena (N° SERVICIO IC-GADMTENA-2024-063) confirma la contratación de servicios técnicos para la renovación de licencias de software y mantenimiento de servidores. En particular, se menciona la contratación para Renovación de licencias del programa PUNIS V10.XLSM para 30 computadoras, con una vigencia de 3 años.

Mantenimiento del servidor Proliant DL120 Gen9 de HP, incluyendo recuperación de datos, reinstalación del sistema operativo Ubuntu Server LTS, y configuración de servicios como PostgreSQL, Tomcat y GeoServer.

Esto indica que el municipio contrata servicios especializados con proveedores externos para garantizar la operatividad de sus sistemas informáticos, especialmente en áreas técnicas que requieren conocimiento especializado.

3.12.3 Gestores de Correo electrónico

3.12.3.1 Medidas de seguridad

el GAD Municipal de Tena aunque cuenta con una estructura institucional y utiliza correo electrónico para la gestión administrativa (evidenciado en directorios de empleados y canales de contacto), no posee una política formal, lineamientos técnicos ni detalles sobre la configuración de seguridad del sistema de correo, además como la Implementación MFA para todos los usuarios del correo institucional.

3.12.3.2 Prestadores de servicios

prestador de servicios formal para el correo electrónico institucional del GAD Municipal de Tena. Aunque el municipio utiliza correos electrónicos para la gestión administrativa, no existe evidencia de un proveedor especializado contratado para gestionar un sistema de correo corporativo seguro y centralizado.

Proveedor técnico relacionado: PROACTINFO SOLUCIONES Y SERVICIOS CIA. LTDA.

Según el documento de contratación IC-GADMTENA-2024-063, el GAD Municipal de Tena contrató a PROACTINFO para el mantenimiento del sistema catastral SIGPRO. Este proveedor tiene contacto institucional (carlose@proactinfo.com) y podría estar relacionado con servicios tecnológicos, pero no se especifica que gestione el correo electrónico del municipio.

CAPITULO 4

PLAN DIRECTOR DE SEGURIDAD

4. DESCRIPCIÓN

El Plan Director de Seguridad para la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena establece un marco integral y estratégico para proteger la información institucional frente a amenazas, garantizando la confidencialidad, integridad y disponibilidad de los datos críticos que soportan la gestión operativa y administrativa del cantón. Este plan se orienta a gestionar los riesgos tecnológicos y de información mediante políticas claras, procedimientos estandarizados y controles técnicos-administrativos, en coherencia con normativas nacionales y estándares internacionales como ISO/IEC 27001.

El plan contempla la identificación de activos de información, valoración de riesgos específicos en contextos municipales de la dirección, diseño e implementación de controles para la prevención y mitigación de incidentes de seguridad, así como la formación y sensibilización continua del personal. Asimismo, se define la estructura organizativa de seguridad, asignando funciones y responsabilidades para la gestión efectiva del ciclo de seguridad de la información.

4.1.- CHECK LIST PDS.

Los objetivos de esta etapa son:

- Medir el desempeño de los procesos, es decir monitorizarlos
- Evaluar el cumplimiento de los indicadores establecidos durante el proceso de planificación
- Informar los resultados para su revisión

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al plan director de seguridad. Los controles se clasificarán en dos niveles de complejidad:

Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- Procesos (PRO): aplica a la dirección o al personal de gestión.
- Tecnología (TEC): aplica al personal técnico especializado.
- Personas (PER): aplica a todo el personal.

Tabla 7

Checks List PDS

NIVEL	ALCANCE	CONTROL	
A	PRO	**Analizar la situación actual de la empresa** Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	☐
A	PRO	**Alinear el PDS con la estrategia de la empresa** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	☐
A	PRO	**Definir los proyectos a ejecutar** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	☐

A	PRO	**Clasificar y priorizar los proyectos** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios en relación a su coste.	☐
A	PRO	**Aprobar el PDS** Apruebas y publicas la versión definitiva del PDS.	☐
A	PRO	**Ejecución del PDS** Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.	☐
A	PRO	**Certificación en seguridad** Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa.	☐

4.1.1. SITUACIÓN ACTUAL: ALCANCE, OBJETIVOS

4.1.1.1. Alcance

El alcance del Plan de Seguridad (PDS) para la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena se centrará en proteger la integridad, disponibilidad y confidencialidad de los procesos y sistemas claves que garantizan la seguridad y bienestar de la población, así como la efectiva gestión y respuesta ante emergencias.

El plan abarca las siguientes áreas y procesos principales:

Gestión de la Seguridad Ciudadana: Procesos relacionados con la prevención, control y monitoreo del orden público, incluyendo coordinación con fuerzas de seguridad, control de acceso a eventos y espacios públicos, así como supervisión de agentes de control municipal.

Gestión de Riesgos y Emergencias: Sistemas de identificación, análisis y mitigación de riesgos para la población y el entorno; planificación y ejecución de planes de contingencia, respuesta a emergencias, simulacros y recuperación tras eventos críticos.

Sistemas de Información y Comunicación: Protección y aseguramiento de las plataformas digitales y herramientas de comunicación institucional, como sistemas de monitoreo CCTV, radio comunicaciones, bases de datos de incidentes y reportes, garantizar la confidencialidad y disponibilidad de la información sensible.

Este PDS se desarrollará bajo lineamientos de normativas nacionales e internacionales de seguridad y gestión de riesgos, alineándose con las políticas institucionales y estándares

como la ISO 31000 para asegurar un enfoque integral y efectivo en la protección de los activos y bienestar comunitario.

4.1.1.2. RESPONSABILIDADES SOBRE LOS ACTIVOS

Se ha asignado las responsabilidades y los roles basándose en dos puntos fundamentales:

Se ha designado las responsabilidades necesarias para asegurar que el sistema de Gestión de Seguridad de la Información cumple con todos los requisitos de la norma ISO 27001.

Mas concretamente para la Dirección de Seguridad Ciudadana y Gestión de Riesgos se ha definido para monitorizar el desempeño del Sistema de Gestión de Seguridad de la Información e Informar a la alta dirección:

- Comité de seguridad de la Dirección
- Comité de seguridad de la Dirección de TIC´S

4.1.1.3. Objetivos

La Dirección de Seguridad Ciudadana y Gestión de Riesgos perteneciente al GAD Municipal del Tena ha pensado en proponer un Sistema de Gestión de Seguridad de la

Información para actuar como punto diferenciador de otras direcciones del GAD, con ello se pretende:

1. Mejorar la seguridad de los sistemas y redes que soportan la operatividad institucional, incluyendo bases de datos, plataformas de gestión de incidentes y comunicación, para garantizar su disponibilidad y resiliencia frente a amenazas cibernéticas.
2. Capacitar al personal sobre buenas prácticas, riesgos comunes y procedimientos para el manejo seguro de información digital, disminuyendo la vulnerabilidad causada por errores humanos o desconocimiento.

4.1.1.4. Análisis técnico de seguridad

El análisis técnico de seguridad realizado sobre los sistemas de información de la Dirección de Seguridad Ciudadana y Gestión de Riesgos evidencia un grado variable en la implantación de controles esenciales para la protección digital y física. Se identificó que la mayoría de los sistemas cuentan con software antivirus actualizado, sin embargo, existen algunas estaciones de trabajo con lapsos en la actualización periódica, lo que podría aumentar su vulnerabilidad. Los cortafuegos están implementados en los puntos críticos de la red, aunque su configuración requiere revisión para optimizar las reglas de filtrado y mejorar la detección de amenazas.

A continuación, se presenta un cuadro resumen con la valoración del grado de implantación de estos controles:

Tabla 8.

Valoración grado implantación

Control de Seguridad	Estado de Implantación	Observaciones y Recomendaciones
Antivirus	Bajo	Actualización general, pero con algunas demoras
Cortafuegos	Medio	Implementado, requiere ajustes en configuración
Páginas Web Seguras (HTTPS)	Medio	Uso de certificados, monitorear vulnerabilidades
Segmentación de Red	Medio	Presente en áreas críticas, necesita extensión
Controles de Acceso Físico	Bajo	Biométricos y vigilancia, mejorar control de visitantes

4.2. VERIFICACIÓN DE CONTROLES

La verificación de controles de seguridad constituye una fase esencial en la gestión de la seguridad de la información, cuyo propósito es evaluar de manera sistemática y objetiva el nivel de cumplimiento y eficacia de las políticas, procedimientos y medidas establecidas dentro de una organización. Este proceso consiste en aplicar una serie de listas de verificación o checklists, que permiten identificar la existencia o ausencia de controles, posibles vulnerabilidades, y áreas de mejora, garantizando que los riesgos estén adecuadamente gestionados y mitigados.

La metodología de verificación, basada en normas internacionales como la ISO/IEC 27001, involucra la revisión de aspectos críticos como la definición y actualización de políticas, asignación de responsabilidades, existencia de comités de seguridad, seguridad física y lógica, controles de acceso, gestión de incidentes y continuidad del negocio, entre otros aspectos relevantes. Un sistema bien implementado exige que cada control tenga responsable, fecha de revisión y una respuesta clara, facilitando el seguimiento y auditoría periódica. A continuación, se detalla en la Tabla Nro. la verificación de controles de Seguridad.

Tabla 9.

Verificaciones de Seguridad de la DSCGR

VERIFICACIÓN DE CONTROLES DE SEGURIDAD

Identificador	**Aspecto por evaluar**	**Respuesta**	**Responsable**	**Fecha**
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	NO		
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	NO		
ID_0003	¿Se han definido las responsabilidades en materia de	NO		

	seguridad de la información?	
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	NO
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad,	NO

	propiedad intelectual, etc.).			
ID_0006	¿Se dispone de un inventario de activos?	SI, porque permite conocer y controlar todos los recursos (físicos, lógicos y humanos) que tienen valor para la Direccion y que requieren protección frente a riesgos.	La Dirección de Administrativa	Enero-01-2025
ID_0007	¿Se ha definido quien es el responsable de los activos?	SI, porque asignar responsabilidad es claras	Cada uno de los funcionarios	Enero-01-2025

		garantiza que cada activo sea gestionado, protegido y mantenido de manera adecuada durante todo su ciclo de vida.		
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	SI, Obtener una perspectiva más completa sobre el desempeño, habilidades y comportamiento del candidato en entornos laborales anteriores, lo	Unidad de Talento Humano	Enero-01-2025

		que ayuda a evaluar su idoneidad para el puesto
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	NO
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	NO

ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	SI, para garantizar la consistencia, eficiencia y seguridad en el manejo de los sistemas y recursos tecnológicos de la organización	Dirección de Tecnologías de la Información	Enero-01-2
ID_0012	¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?	NO		
ID_0013	¿Se verifica regularmente la	NO		

	correcta realización de las copias se seguridad?	
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?.	NO
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	NO
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?.	NO

ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	NO		
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	SI, para proteger la información sensible de la organización, reduce el riesgo de ataques como fuerza bruta, phishing o reutilización de credenciales, y ayuda a cumplir con	Dirección de TIC´S	Enero-01-2025

		normativas y estándares de seguridad.		
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión?	SI, para prevenir el acceso no autorizado a la información y recursos de la organización.	Cada área de la Dirección de Seguridad	Enero-01-2025
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	SI, para identificar y responsabilizar a cada usuario por sus acciones dentro del sistema, facilitando la trazabilidad y el	Funcionario de la Dirección	Enero 01-2025

		control de accesos.
ID_0021	¿Se controla la instalación de software en sistemas en producción?	NO
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	NO
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los	NO

	incidentes de seguridad?	
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	NO
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	NO
ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	NO

	¿	
D_0027	Todos los requisitos relevantes de carácter legal se mantienen identificados?	NO
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	NO
ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la	NO

	información desde un punto de vista legal?	
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	NO

4.3. INVENTARIO DE ACTIVOS

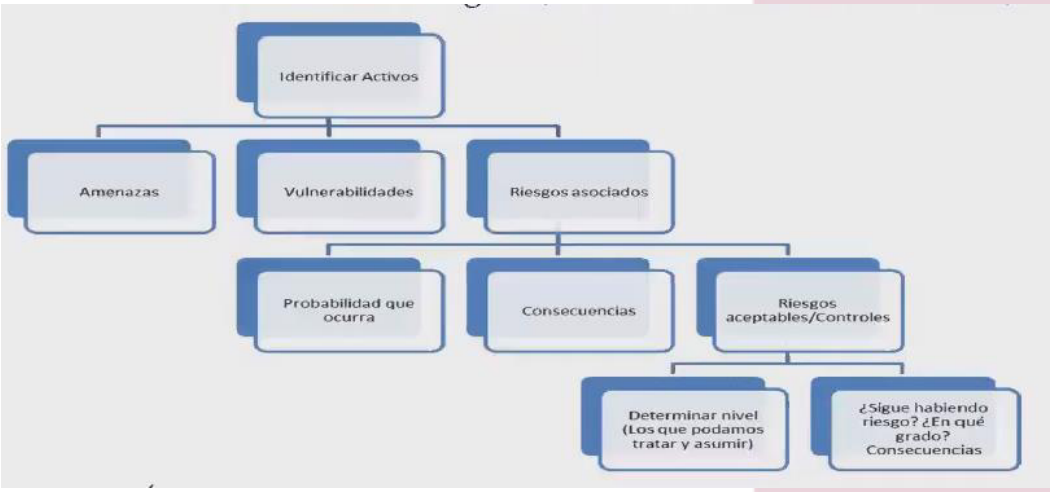
El inventario de activos es un componente fundamental dentro de la gestión de la seguridad de la información en cualquier organización, ya que permite identificar y registrar detalladamente los recursos que son esenciales para el funcionamiento y la protección de los procesos institucionales. En el caso específico del GAD Tena, este inventario abarca tanto

equipos físicos como routers, servidores, bases de datos y estaciones de computo, asignando responsables claros y estableciendo criterios de criticidad para cada activo.

Mediante a estructura detallada en la Figura Nro1 es un proceso estructurado que inicia con la identificación clara y detallada de los activos dentro de una organización. A partir de este inventario, se procede a evaluar las amenazas que podrían afectar esos activos, así como las vulnerabilidades presentes que incrementan la exposición ante posibles incidentes.

Figura 2.

Inventarios de activos



Este registro minucioso proporciona una visión clara y ordenada sobre la infraestructura tecnológica, ubicando los activos en sus áreas correspondientes y determinando cuáles son estratégicos para la seguridad y operación continua. Conocer el

estado, la ubicación y el nivel de importancia de cada activo facilita la toma de decisiones para la protección, mantenimiento y renovación tecnológica, además de cumplir con normas internacionales y estándares de seguridad. A continuación, se detalla en la Tabla Nro. El inventario de activos de la Dirección de Seguridad Ciudadana y Gestión de Riesgos.

Tabla 10.

Inventario de Activos de la DSCGR

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_0001	Router Wifi (Usuarios)	Equipo de conexión a internet	Director de Seguridad	Servidor (físico)	Área de Gestión de Riesgos	Sí
ID_0002	Rack Swith	Distribución de red.	Dirección de TIC´S	Servidor (físico)	Área de Seguridad Ciudadana	SI
ID_0003	Servidor 01 (Web)	Servidor correo electrónico corporativa.	Dirección de TIC´S	Servidor (físico)	Direccion de TIC´S	NO

ID_0004	Base de Datos	Bases de datos para almacenamiento de mapas, puntos calientes del cantón	Dirección de Seguridad	Servidor (físico)	Area de Gestion de Riesgos	SI
ID_005	Equipos PC	Equipo de cómputo para uso del equipo técnico del área de Seguridad Ciudadana	Área de Seguridad Ciudadana	Servidor (físico)	Area de Seguridad Ciudadana	SI
ID_0006	Equipos PC	Equipo de cómputo para uso del equipo técnico del área de Gestión de Riesgos	Área de Gestión de Riesgos	Servidor (físico)	Area de Gestion de Riesgos	SI

ID_0007	Servidor 01 (Web)	Servicio para proveer de internet	Dirección de TIC´S	Servidor (físico)	Direccion de TIC´S	SI

4.3.1. Análisis de Riesgo

El análisis de riesgos es la acción a través de la cual la dirección, mediante el inventario de activos, el alcance, los objetivos del SGSI, puede obtener una visión global sobre los riesgos y amenazas a la que se enfrenta, para realizar esta evaluación, la Dirección de Seguridad Ciudadana y Gestión de Riesgos ha seguido la siguiente metodología:

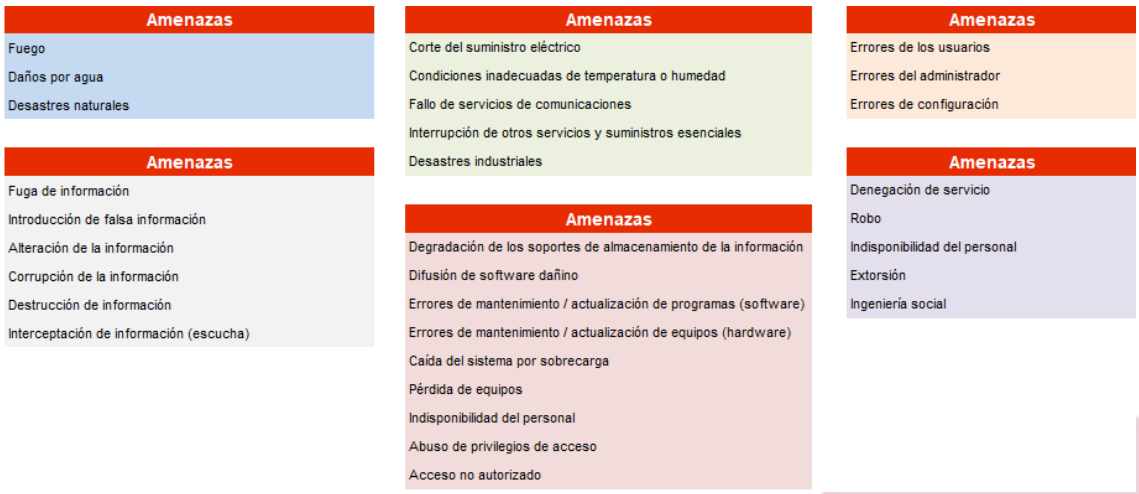
4.3.2. Identificación de activos susceptibles de sufrir amenazas

a fase siguiente implica reconocer todas las posibles amenazas a las que los activos previamente identificados podrían estar sometidos. Dada la gran cantidad y diversidad de amenazas existentes, es fundamental contar con experiencia y un profundo conocimiento del activo para detectar de manera precisa y práctica las amenazas relevantes. Tras esta identificación, es necesario proceder a la evaluación de las amenazas utilizando los siguientes criterios:

La siguiente figura recoge las principales amenazas a considerar en el ámbito de un análisis de riesgos. Se trata de un extracto ligeramente modificado del catálogo de amenazas de MAGERIT

Figura 3

Catalogo de amenazas



En la figura Nro. 3 se muestra la probabilidad de ocurrencia de la amenaza, clasificada en tres niveles: bajo, medio y alto. Este gráfico permite visualizar con claridad el valor que se asigna a cada nivel de probabilidad, facilitando la identificación y priorización de los riesgos asociados a la amenaza en cuestión.

Figura 4

Estimación de probabilidad

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Degradación: impacto que tiene la materialización de la amenaza en el activo, aplicable a las 3 dimensiones de la seguridad:

Figura 5

Impacto de las amenazas

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

La evaluación del impacto y de los riesgos residuales implica determinar el nivel de exposición real de la organización en el momento del análisis de riesgos. Este riesgo residual es aquel sobre el que se deben establecer criterios de aceptación y que servirán como base para diseñar un plan de acción destinado a reducir los riesgos críticos para la gestión. Al identificar estos riesgos residuales, se pueden reconocer las principales amenazas a los activos que podrían afectar significativamente los servicios ofrecidos a la ciudadanía si se llegaran a materializar. Tener una comprensión clara de estos riesgos permite enfocar de manera eficiente los recursos disponibles para la gestión de la seguridad de la información.

4.4. ANALISIS DE RIESGOS

La puesta en marcha de un Sistema de Gestión de Seguridad requiere, de manera fundamental, la ejecución de un análisis de riesgos. Este análisis facilita la identificación de los factores de riesgo que podrían afectar de forma significativa a la dirección, determinando

así los activos que requieren una gestión prioritaria. Para llevar a cabo este procedimiento, se ha elegido la metodología MAGERIT, tal como se especifica en el documento "Metodología de análisis de riesgo", la cual está diseñada para organizaciones que manejan información digital y sistemas informáticos**.**

En esta sección se identifica los activos de La Dirección de Seguridad y Ciudadana y Gestión de Riesgos presentados a continuación:

Tabla 11.

Identificación de activos susceptibles de sufrir amenazas -DSCGR

Tipo de Activo	Nombre	Descripción del Activo
Hardware	Router	Equipo de conexión a internet
Hardware	Sistema de video vigilancia	Sistema para control de seguridad y cámara
Hardware	Nodo 3	Rack Swith distribución de red
Redes	Firewall Cisco	Rack Swith distribución de red
Software	Carbonio	Correo electrónico

Software	Bases de datos de seguridad y gestión de riesgos	Bases de datos para almacenamiento de mapas, puntos calientes del cantón
Hardware	Equipos PC	Equipo de cómputo para uso del equipo técnico del área de Seguridad Ciudadana
Hardware	Equipos PC	Equipo de cómputo para uso técnico del área de Gestión de Riesgos
Hardware	Portátil	Portátil- administración de la Dirección de Seguridad Ciudadana y Gestión de Riesgos.
Software	Sistema Operativo W10	Instalado en los equipos de computo
Organización	Internet	Servicio para proveer de internet al Municipio

Organización	Impresiones	Impresiones (impresora y suministro como tóner)

Fuente: Municipio de Tena

El análisis de riesgo de los activos identificados junto con las amenazas, vulnerabilidad, probabilidad e impacto por cada activo de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Municipal del Tena a lo que están expuestos en la tabla.

Tabla 12.

Identificación de Amenaza, Vulnerabilidad Probabilidad Impacto -DSCGR

Tipo de Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo
Router	Robo	Falta de control físico adecuado y acceso inseguro	Media	Medio	4

Cámara de video vigilancia	Corte del suministro eléctrico	Ausencia de sistemas de energía de respaldo (UPS)	Media	Alto	6
Rack Swith distribución de red	Corte del suministro eléctrico	Dependencia de energía única sin respaldo adecuado	Media	Alto	6
Firewall Cisco	Corte del suministro eléctrico	Falta de redundancia y protección contra fallas eléctricas	Medio	Alto	6
Carbonio	Caída del sistema por sobrecarga	Limitada capacidad de escalabilidad	Bajo	Alto	3

		y balance de carga			
Bases de datos de seguridad y gestión de riesgos	Fuga de Información	Controles insuficientes de acceso y monitoreo de datos	Alto	Alto	9
Equipos informáticos y dispositivos móviles	Perdida de equipos	Falta de políticas estrictas de custodia y control físico	Media	Alto	6

Consecuencias

Las consecuencias ante las amenazas identificadas se detallan a continuación:

- Interrupción del tráfico de red, pérdida de conectividad, acceso no autorizado a la red, vulneración de datos.
- Pérdida de evidencia visual, incapacidad para monitorear áreas críticas, aumento

del riesgo de incidentes no detectados.

- Caída de la red interna, pérdida de comunicación entre segmentos, interrupción de servicios dependientes de la red.
- Exposición a ataques externos, pérdida de control y protección de la red, posible infiltración y compromisos de seguridad.
- Interrupción en la gestión de correos y comunicaciones, afectación de la productividad, posibles pérdidas de datos temporales.
- Divulgación de información confidencial, pérdida de confianza institucional, sanciones legales, impacto reputacional y financiero.
- Pérdida de información sensible, interrupción de labores, riesgo de acceso no autorizado si no están protegidos correctamente.

4.5. CLASIFICACION Y PRIORIZACION

La clasificación y priorización de iniciativas y riesgos es un proceso clave dentro de la gestión de la seguridad de la información, ya que permite organizar y asignar recursos de manera eficiente para mitigar las amenazas que afectan a la organización. Este proceso consiste en registrar cada amenaza identificada, describir detalladamente su naturaleza y

consecuencias, asignar responsabilidades para su gestión, y evaluar factores como el tipo y coste de la iniciativa necesaria para su mitigación.

Al clasificar y priorizar, se establecen criterios claros basados en la probabilidad de ocurrencia y el impacto potencial de cada riesgo, facilitando la toma de decisiones estratégicas y presupuestarias. De esta manera, la organización puede enfocarse primero en las amenazas más críticas, como la instalación de generadores para cortes de suministro eléctrico, la actualización de sistemas para prevenir fugas de información o la implementación de medidas físicas para proteger equipos informáticos contra robos.

Tabla 13.

REGISTRO, CLASIFICACIÓN Y PRIORIZACIÓN DE INICIATIVAS

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha
IN_0001	Corte del suministro eléctrico	colocación de un generador eléctrico que abarque a todas las direcciones del GAD Tena	Dirección de Administrativa / Dirección de TIC´S.	Técnica	90.000,00 $	marzo-01-2026

IN_0002	Fuga de información	actualizados los equipos, software, firewalls y parches de seguridad para evitar vulnerabilidades que puedan ser explotadas	Dirección de TIC´S	Técnica	2,000,00 $	marzo-01-2026
IN_0003	Perdida de equipos informáticos por robo	Implementar medidas de seguridad física como anclajes, cables de seguridad o lockers para fijar los dispositivos a escritorios o muebles.	Dirección Administrativa	Técnica	5,000,00 $	marzo-01-2026

4.6. CHECK LIST PDS

La evolución integral en la gestión de riesgos de seguridad de la información, desde un estado inicial sin registros ni procesos formales hasta un estado final estructurado con base en la metodología MAGERIT, refleja un cambio profundo y necesario para la robustez organizacional del GAD Tena.

Al inicio del proyecto, la ausencia de inventarios, análisis de amenazas, valoración de vulnerabilidades y riesgos implicaba una gestión reactiva y poco sistematizada, exponiendo a la institución a vulnerabilidades críticas sin control ni priorización. La implementación de MAGERIT permitió darle rigor científico y sistemático a la evaluación de riesgos, considerando los activos de información, sus interrelaciones, valores y su importancia para la continuidad operativa.

Gracias a este enfoque, el GAD Tena pudo identificar de manera categorizada los riesgos mediante análisis cuantitativos con bases numéricas para la probabilidad y el impacto, lo cual facilita la toma de decisiones estratégicas informadas en gestión de seguridad. Además, MAGERIT favorece la elaboración de estrategias de mitigación efectivas, asignación clara de responsabilidades y recursos, y la incorporación de controles técnicos y organizativos diseñados para mantener los riesgos en niveles aceptables.

Este progreso refleja la transformación hacia una gestión proactiva y sostenida, fundamentada en normativas internacionales (como ISO 31000) y herramientas específicas (como PILAR), que permiten además la monitorización continua y la revisión periódica del plan de seguridad, adaptándose a nuevos escenarios y amenazas emergentes.

Tabla 14

Check list pds

NIVEL	ALCANCE	CONTROL	
A	PRO	**Analizar la situación actual de la empresa** Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	X
A	PRO	**Alinear el PDS con la estrategia de la empresa** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	X
A	PRO	**Definir los proyectos a ejecutar** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	☐
A	PRO	**Clasificar y priorizar los proyectos** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios con relación a su coste.	X
A	PRO	**Aprobar el PDS**	☐

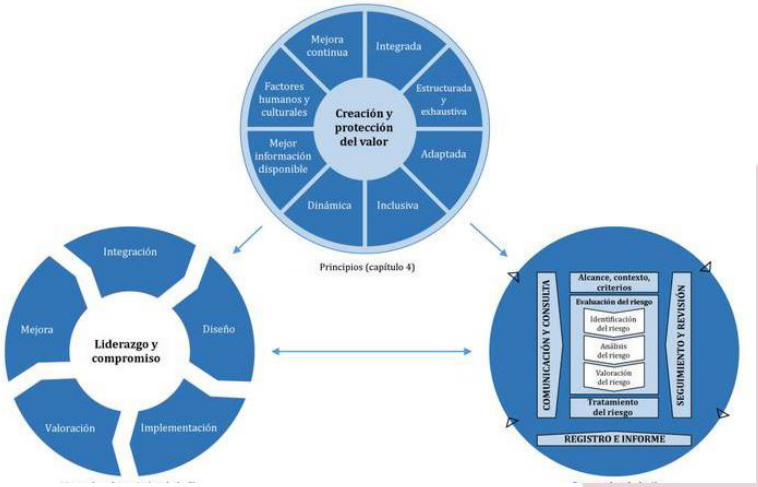
	Apruebas y publicas la versión definitiva del PDS.	
	Ejecución del PDS	X
RO	Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.	
	Certificación en seguridad	☐
RO	Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa.	

CAPITULO 5

Manual de gestión basado en la norma ISO 31000:2018

Figura 6

Principios, marco de referencia y proceso



5.1.Objeto y campo de aplicación

El propósito y el alcance del Sistema de Gestión de Riesgos, que se basa en la norma ISO 31000:2018 y fue creado para la Dirección de Seguridad Ciudadana y Gestión de Riesgos del Gobierno Autónomo Descentralizado Municipal del Tena, son objeto de este apartado.

El propósito del Sistema de Gestión de Riesgos es definir un enfoque integral, sistemático y estructurado para identificar, evaluar, analizar, gestionar, monitorear y revisar los riesgos que podrían poner en peligro el logro de las metas institucionales, la continuidad

operacional, la seguridad informativa y la prestación eficaz de servicios públicos a los ciudadanos.

El sistema tiene un campo de aplicación que abarca todos los procesos estratégicos, misionales y de apoyo que lleva a cabo la Dirección de Seguridad Ciudadana y Gestión de Riesgos. Esto incluye, entre otras cosas:

- La administración de la seguridad pública y la convivencia en armonía.
- La administración integral de riesgos en desastres a nivel cantonal.
- La gestión, el procesamiento y la salvaguarda de la información institucional y los datos privados.
- La utilización de recursos humanos, financieros, físicos y tecnológicos vinculados a los procesos directivos.
- La colaboración con otras dependencias del GAD Municipal del Tena, organismos públicos y privados y grupos comunitarios que participan en la gestión de riesgos y seguridad.

Este sistema es pertinente para todos los empleados de la dirección, los técnicos, los administrativos y el personal operativo que participen directa o indirectamente en los procesos de dirección. También se aplica a proveedores, contratistas y otras entidades que

tengan acceso a información, bienes o instalaciones institucionales, de acuerdo con la legislación vigente.

El establecimiento del Sistema de Gestión de Riesgos posibilitará el reforzamiento de la toma de decisiones, prever situaciones adversas, disminuir la probabilidad y el impacto de los riesgos detectados e impulsar una cultura organizativa enfocada en la mejora continua, la prevención y la resiliencia institucional. Todo esto ayudará a que se cumplan las metas estratégicas del GAD Municipal del Tena y a que se proteja a los ciudadanos.

5.2. Referencias Normativas

El Sistema de Gestión de Riesgos actual se basa en un compendio de leyes, regulaciones y normas técnicas que guían la gestión pública, la seguridad informativa y la gestión del riesgo dentro del marco institucional. Estas referencias normativas establecen el marco técnico y legal que se necesita para garantizar la aplicabilidad, validez y coherencia del sistema sugerido.

Las principales normas que se han tomado en cuenta son:

ISO 31000:2018 - Gestión del riesgo — Directrices: Estándar internacional que define los principios, el marco de referencia y el proceso para la gestión del riesgo. Es fundamental para establecer un enfoque sistemático y estructurado en la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos en la organización

SO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información (SGSI): Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Es crucial para proteger la confidencialidad, integridad y disponibilidad de la información en las organizaciones

Esquema Gubernamental de Seguridad de la Información (EGSI): Marco de referencia ecuatoriano, basado en ISO 27001 y emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), de cumplimiento obligatorio para las instituciones públicas en Ecuador. Proporciona directrices específicas para la seguridad de la información en el sector gubernamental

NIST Cybersecurity Framework (CSF): Conjunto de directrices, estándares y mejores prácticas publicadas por el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) para ayudar a las organizaciones a comprender y mejorar la gestión de sus riesgos de ciberseguridad. Aunque es un estándar estadounidense, es ampliamente adoptado a nivel global por su enfoque integral

COBIT (Control Objectives for Information and Related Technologies): Marco de trabajo para la gobernanza y gestión de TI que ayuda a las organizaciones a lograr sus objetivos estratégicos y a gestionar los riesgos relacionados con la información y la tecnología. Es fundamental para alinear la TI con los objetivos de negocio y asegurar el valor

de la información

Constitución de la República del Ecuador: La carta magna del país asegura el derecho a la seguridad, a la privacidad de los datos personales y a la información, sentando las bases para cualquier normativa específica en estas áreas

Ley Orgánica de Protección de Datos Personales del Ecuador: Esta ley establece las obligaciones y responsabilidades para las instituciones públicas y privadas en el tratamiento de datos personales, garantizando la protección de la información sensible de los ciudadanos

Reglamento del Sistema Nacional Descentralizado de Gestión de Riesgos: Establece las pautas para prevenir, mitigar y reaccionar ante sucesos desfavorables a nivel nacional y local, siendo un marco crucial para la gestión de riesgos en entidades públicas

Normativas internas, ordenanzas y el Estatuto Orgánico por Procesos del GAD Municipal del Tena: Documentos internos que establecen las funciones, responsabilidades y la estructura organizativa de la institución, adaptando los marcos normativos generales a la realidad específica del GAD.

5.3. Términos y definiciones

Con el propósito de este documento, se emplean los términos y definiciones establecidos en la norma ISO 31000:2018, que son complementados con conceptos importantes para la seguridad de la información y la gestión pública:

- **Riesgo:** Consecuencia de la incertidumbre en los objetivos institucionales.
- **Gestión de riesgos:** Conjunto de acciones coordinadas para gestionar y controlar una organización en relación con el riesgo.
- **Marco de referencia:** Conjunto de elementos que ofrecen las bases y disposiciones organizativas para diseñar, poner en práctica, supervisar y optimizar la gestión del riesgo.
- **Proceso de gestión de riesgos:** Implementación regular de políticas, procedimientos y prácticas para la comunicación, determinación del contexto, detección, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.
- **Probabilidad:** Es la posibilidad de que suceda un acontecimiento.
- **Impacto:** Efecto o consecuencia que puede tener un acontecimiento sobre las metas institucionales.
- **Partes interesadas:** Individuos o entidades que tienen la capacidad de influir, ser influenciados o sentirse influidos por una actividad o decisión.
- **Riesgo residual:** El riesgo que subsiste tras la implementación de medidas terapéuticas.

- **Mejora continua:** Tarea repetitiva para reforzar la capacidad de alcanzar los objetivos del sistema de gestión.
- **Parte interesada:** persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad
- **Fuente de riesgo:** elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias
- **Consecuencia:** resultado de un evento (3.5) que afecta a los objetivos
- **Control:** medida que mantiene y/o modifica un riesgo.

5.4.Principios

Los principios establecidos por la norma ISO 31000:2018 son los cimientos del manejo de riesgos del GAD Municipal del Tena. Estos garantizan que el manejo de riesgos sea eficiente, consistente y esté en consonancia con las metas institucionales.

5.4.1. Integrada

La gestión de riesgos está presente en todos los procesos, niveles y tareas de la Dirección de Seguridad Ciudadana y Gestión de Riesgos. Esta perspectiva asegura que los

riesgos vinculados sean tomados en cuenta de forma sistemática en el proceso de toma de decisiones, lo cual refuerza la planificación, la ejecución y el control institucional.

La gestión de riesgos estará intrínsecamente ligada a todos los procesos, niveles y funciones de la Dirección de Seguridad Ciudadana y Gestión de Riesgos. Esto implica que la evaluación de riesgos no será una actividad aislada, sino que se incorporará en la planificación estratégica anual, en la formulación de proyectos de seguridad ciudadana (ej. instalación de cámaras de vigilancia, programas de prevención del delito), en la adquisición de tecnología (ej. sistemas de monitoreo, equipos de comunicación) y en la toma de decisiones operativas diarias (ej. despliegue de personal, respuesta a emergencias). Se establecerán puntos de control de riesgo en los flujos de trabajo existentes para asegurar que las consideraciones de seguridad sean sistemáticamente evaluadas y abordadas desde el inicio de cualquier iniciativa.

5.4.2. Estructurada y exhaustiva

Se implementará un enfoque sistemático, documentado y consistente para la gestión de riesgos. Esto incluye la adopción de una metodología estandarizada para la identificación de riesgos (ej. talleres de lluvia de ideas, listas de verificación, análisis de incidentes pasados), el análisis (ej. matrices de probabilidad e impacto, análisis de causa raíz) y la evaluación de riesgos (ej. criterios de aceptación de riesgo definidos). Todos los pasos, desde la identificación hasta la evaluación, serán registrados y documentados en un sistema

centralizado, permitiendo la trazabilidad, la comparación de resultados a lo largo del tiempo y la toma de decisiones fundamentadas en datos objetivos. La exhaustividad garantizará que se consideren tanto los riesgos evidentes como los latentes, abarcando todas las dimensiones de la seguridad ciudadana y la gestión de riesgos institucionales.

5.4.3. Adaptada

El sistema de gestión de riesgos se elabora tomando en cuenta el marco legal, la estructura organizativa, las competencias técnicas y los requerimientos territoriales, así como el contexto interno y externo del GAD Municipal del Tena. Por lo tanto, el sistema se adecúa a la realidad de la institución y a los peligros particulares del ambiente.

El sistema de gestión de riesgos será diseñado y ajustado a las particularidades del GAD Municipal del Tena. Esto significa que se considerará el marco legal vigente en Ecuador y a nivel local (ej. ordenanzas municipales de seguridad, Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público - COESCOP), la estructura organizacional específica de la Dirección (ej. roles y responsabilidades del personal, organigrama), las capacidades técnicas y tecnológicas disponibles (ej. infraestructura de comunicaciones, sistemas de videovigilancia, personal capacitado), el contexto territorial del cantón Tena (ej. geografía, demografía, zonas de riesgo natural o social) y las dinámicas internas y externas (ej. presupuesto, políticas nacionales de seguridad, participación ciudadana). Esta adaptabilidad asegura que el plan sea relevante, práctico y eficaz frente a los

desafíos específicos de la institución y su entorno, evitando soluciones genéricas que no se ajusten a la realidad local.

5.4.4. Inclusiva

La gestión de riesgos impulsa la participación activa de las partes interesadas, tanto internas como externas, y propicia el diálogo, la consulta y la corresponsabilidad. La incorporación de diversos puntos de vista potencia la detección de riesgos y optimiza la aceptación de las decisiones tomadas.

Se promoverá la participación activa de todas las partes interesadas, tanto internas como externas. Internamente, se involucrará al personal de la Dirección de Seguridad Ciudadana y Gestión de Riesgos, otras direcciones del GAD Municipal, y el liderazgo político. Externamente, se buscará la colaboración con la Policía Nacional, el Cuerpo de Bomberos, organizaciones comunitarias, líderes barriales y la ciudadanía en general a través de mecanismos como mesas de seguridad ciudadana, talleres participativos, encuestas y canales de comunicación directa. Esta inclusión fomenta la corresponsabilidad en la gestión de riesgos, enriquece la identificación de amenazas y vulnerabilidades desde múltiples perspectivas, y mejora la aceptación y el compromiso con las decisiones y acciones de seguridad implementadas, asegurando que las soluciones sean pertinentes y sostenibles.

5.4.5. Dinámica

El sistema de gestión de riesgos admite que los riesgos tienen la posibilidad de cambiar con el tiempo a causa de elementos externos o internos. Por esta razón, se instituyen procesos de monitoreo y revisión constantes para poder prever, identificar y reaccionar a tiempo ante alteraciones en el contexto institucional.

Reconociendo que los riesgos evolucionan constantemente debido a factores internos (ej. cambios de personal, nuevas tecnologías) y externos (ej. fenómenos naturales, cambios en patrones delictivos, desarrollo urbano), el plan incluirá mecanismos robustos de monitoreo y revisión continua. Esto implica la realización de evaluaciones de riesgo periódicas (ej. semestrales o anuales), el seguimiento de indicadores clave de riesgo, el análisis de incidentes para identificar nuevas amenazas o la efectividad de los controles existentes, y la actualización proactiva de las estrategias y medidas de mitigación. La naturaleza dinámica del plan asegura que las respuestas a los riesgos se mantengan actuales, pertinentes y efectivas, permitiendo al GAD Municipal del Tena anticipar, identificar y reaccionar de manera oportuna a los cambios en el contexto de seguridad.

5.4.6. Mejor información disponible

Las decisiones que tienen que ver con la gestión de riesgos se fundamentan en información verificable, fidedigna y puntual, teniendo en cuenta datos del pasado, experiencia institucional y análisis técnicos. Además, se reconoce que la información disponible tiene limitaciones e incertidumbres.

Las decisiones relativas a la gestión de riesgos se basarán en la información más precisa, verificable y oportuna disponible. Esto incluye la recopilación y análisis de datos históricos de incidentes de seguridad, estadísticas delictivas, informes meteorológicos y geológicos (para riesgos naturales), análisis de vulnerabilidades de infraestructura crítica, experiencia institucional acumulada, y análisis técnicos especializados. Se establecerán procesos para validar la fiabilidad de las fuentes de información y se reconocerán explícitamente las limitaciones e incertidumbres inherentes a los datos disponibles. La Dirección invertirá en sistemas de información que permitan la centralización y el análisis de datos para generar inteligencia de seguridad accionable, garantizando que las decisiones sean informadas y basadas en evidencia.

5.4.7. Factores humanos y culturales

La gestión de riesgos tiene en cuenta la manera en que actúa el ser humano, la cultura de la organización y las habilidades del talento humano. Se fomenta una cultura institucional centrada en la prevención, la gestión proactiva del riesgo y la responsabilidad.

El plan considerará la influencia crítica del comportamiento humano, la cultura organizacional y las competencias del personal en la gestión de riesgos. Se implementarán programas de capacitación y sensibilización continuos para todo el personal del GAD Municipal, enfocados en la identificación de riesgos, la importancia de los protocolos de seguridad y la respuesta ante emergencias. Se fomentará una cultura institucional centrada en

la prevención, la gestión proactiva del riesgo y la responsabilidad individual y colectiva. Esto incluye el desarrollo de liderazgo en seguridad, la promoción de la comunicación abierta sobre riesgos y la creación de un entorno donde los errores sean vistos como oportunidades de aprendizaje, no de castigo, para fortalecer la resiliencia organizacional.

5.4.8. Mejora continua

La gestión de riesgos será concebida como un proceso de mejora constante y cíclica. Se establecerá un ciclo de Planificar-Hacer-Verificar-Actuar para la gestión de riesgos. Esto se traducirá en la realización de auditorías internas periódicas para evaluar la conformidad y eficacia del sistema de gestión de riesgos, evaluaciones de desempeño basadas en indicadores clave, y la implementación de acciones correctivas y preventivas derivadas de incidentes, auditorías o revisiones. El objetivo es asegurar que el sistema no solo cumpla con sus objetivos, sino que también evolucione y se fortalezca continuamente, contribuyendo de manera sostenida a los objetivos estratégicos de seguridad ciudadana y gestión de riesgos del GAD Municipal del Tena.

5.5. Marco de referencia.

La Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena propone la adopción de la norma ISO 31000 como marco de referencia para la gestión de riesgos, con el objetivo de fortalecer la capacidad institucional para identificar, analizar, evaluar y tratar los

riesgos que afectan la seguridad y el bienestar de la ciudadanía. Este marco busca integrar la gestión del riesgo en todos los procesos y niveles de la organización, alineándola con los objetivos estratégicos, la cultura institucional y las necesidades del contexto local.

La implementación de ISO 31000 permitirá al GAD Tena mejorar la toma de decisiones, proteger sus activos, optimizar la asignación de recursos y fortalecer la prevención y respuesta ante emergencias y amenazas. Además, facilitará la comunicación y consulta con las partes interesadas, promoviendo la transparencia, la participación ciudadana y la mejora continua de los servicios públicos.

Este marco de referencia constituye la base para desarrollar, implementar y mantener un sistema de gestión de riesgos eficaz, eficiente y sostenible, que contribuya a la seguridad integral, la resiliencia comunitaria y el cumplimiento de los objetivos institucionales del municipio.

5.5.1. Generalidades.

La Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena propone la adopción de la norma ISO31000 como marco de referencia para la gestión de riesgos, con el objetivo de integrar de manera sistemática y eficaz los procesos de identificación, análisis, evaluación y tratamiento del riesgo en todas las actividades institucionales. Este marco busca alinear la gestión del riesgo con los objetivos estratégicos y operativos del municipio,

garantizando la protección de la ciudadanía, la eficiencia en la asignación de recursos y la mejora continua de los servicios públicos.

El marco general de gestión de riesgos es el modelo de gobernanza que establece la forma en que el GAD Tena, a través de su Dirección, gestionará la incertidumbre para lograr sus objetivos.

- Propósito: El objetivo primordial del marco es crear y proteger el valor de la Dirección, lo que se traduce en mejorar la seguridad ciudadana y la capacidad de respuesta y resiliencia del cantón ante eventos adversos, a continuación, se detalla un análisis de principio a incorporar en el sistema de Gestión de Riesgos en la Dirección de Seguridad Ciudadana del GAD Tena.

Tabla 15

GAD tena

Área de Gestión	Objetivo del Área	Principios Clave de ISO 31000 Aplicados	Alcance del Proyecto de Implementación
Gestión de Riesgos	1. Prevención y Mitigación: Identificar, analizar y reducir las	Mejor Información Disponible: Uso de datos históricos, mapas de amenazas	Establecer el Proceso de Gestión de Riesgos (Identificación,

	amenazas y vulnerabilidades ante riesgos naturales (inundaciones, sismos, etc.) y antrópicos. 2. Preparación y Respuesta: Desarrollar, actualizar y mantener operativos los Planes de Respuesta a Emergencias y Desastres, y garantizar la activación eficiente del Comité de Operaciones de Emergencia (COE).	y pronósticos para la evaluación de riesgos. Dinámica: El marco permite anticipar y responder a los cambios en los patrones de riesgo (ej. cambio climático). Adaptada: El marco es proporcional al contexto geográfico y socioeconómico de Tena.	Análisis, Evaluación y Tratamiento) para la matriz de Riesgos Cantonales. Incluye la integración de la gestión del riesgo en la planificación territorial y en los planes de respuesta a emergencias (COE).
Seguridad Ciudadana	1. Control del Espacio Público: Controlar el uso del espacio público y	Integrada: La gestión del riesgo se incorpora en la rutina diaria y en la	Definir y estandarizar los Riesgos Operacionales

asegurar el cumplimiento de las ordenanzas municipales de seguridad y convivencia. 2. Prevención Social y Convivencia: Promover la convivencia social pacífica mediante la participación ciudadana y la prevención situacional del delito. 3. Operatividad Continua: Asegurar la prestación continua, profesional y efectiva de los servicios de seguridad y vigilancia ciudadana 24/7 (ej.	toma de decisiones operativas (ej. definir rutas de patrullaje). Estructurada y Exhaustiva: Unificación de protocolos de respuesta ante incidentes para lograr resultados consistentes. Inclusiva: Consulta y comunicación sistemática con la ciudadanía (partes interesadas) para entender la percepción del riesgo y las necesidades de seguridad.	Creación de protocolos y matrices de responsabilidades y comunicación para el personal

gestión de guardias).

Principios de la Gestión del Riesgo: La Dirección de Seguridad adoptará los siguientes principios de la ISO 31000, que guiarán todas las decisiones y acciones del marco, como se indica en la siguiente tabla:

Tabla 16.

Principios y aplicación en la Dirección de Seguridad Ciudadana y Gestión de Riesgos

Principio	Aplicación en la Dirección
Integrada	La gestión del riesgo es parte de la gobernanza, planificación y toma de decisiones, no una actividad separada (ej. cada plan de patrullaje considera los riesgos asociados).
Estructurada y Exhaustiva	Uso de una metodología uniforme (el proceso ISO 31000) para asegurar resultados consistentes en la evaluación de riesgos (ej. delitos vs. desastres naturales).
Adaptada	El marco es proporcional y se adapta al contexto específico de Tena (geografía, cultura amazónica, estructura del GAD).
Inclusiva	Involucra la participación de la ciudadanía, la Policía Nacional y otras dependencias del GAD en la identificación y evaluación de riesgos.

Dinámica	El sistema anticipa y responde a los cambios (ej. nuevas modalidades delictivas, cambio climático, nuevos riesgos tecnológicos).
Mejor Información Disponible	Las decisiones se basan en evidencia (datos de incidentes, pronósticos climáticos, estadísticas de riesgo).
Factores Humanos y Culturales	Considera la capacidad del personal, las percepciones de riesgo de la ciudadanía y la cultura organizacional en el diseño de controles.

Política de Gestión de Riesgos: Se establecerá una Política de Gestión de Riesgos aprobada por el Director de Seguridad Ciudadana y Gestión de Riesgos y el Alcalde del GAD Tena.

Declaración: La Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena se compromete a integrar de manera efectiva y eficiente la gestión del riesgo, basada en la norma ISO 31000:2018, en todas sus operaciones, con el fin de proteger la vida, el bienestar de la ciudadanía y los activos institucionales, garantizando el cumplimiento de sus objetivos de seguridad y resiliencia.

Esta política se guía por el compromiso de:

Liderazgo: Demostrar liderazgo y compromiso activo en la asignación de recursos y el apoyo al marco.

Rendición de Cuentas: Asignar roles y responsabilidades claras, asegurando que todos los servidores rindan cuentas por la gestión de los riesgos dentro de su área de competencia.

Mejora Continua: Revisar y mejorar periódicamente el marco y el desempeño de la gestión del riesgo.

- Organigrama: Conforme al organigrama de la Dirección de Seguridad Ciudad y Gestión de Riesgos establecido en el 2.1.8 Tamaño de la Organización se recoge las áreas que conforman la dirección.

- Alcance: El marco aplica a todas las actividades, funciones y procesos de la Dirección, desde la planificación estratégica y operativa como indica en el numeral

4.1.1.1 Alcance del proyecto.

Tala 17.

Alineación con Objetivos estratégicos

Tipo de Objetivo	Objetivo de la Dirección	Alineación del Marco ISO 31000
Estratégico	Contribuir a un Cantón Tena más seguro, ordenado y preparado para desastres.	La Gestión de Riesgos prioriza los recursos y acciones para minimizar amenazas (ej. delincuencia, inundaciones) y capitalizar oportunidades (ej. mejora de la percepción de seguridad, proyectos de resiliencia).
Operativo	Asegurar la respuesta efectiva e ininterrumpida ante emergencias 24/7.	El marco exige el diseño de protocolos claros de comunicación y responsabilidades para la operación continua (mitigando riesgos operativos como la falta de atención a llamadas de emergencia, como se sugiere en el contexto general de las operaciones de seguridad).
Cumplimiento	Cumplir con la normativa legal (LOSEP, COOTAD, ordenanzas) y regulatoria.	La gestión del riesgo identifica y evalúa el riesgo de incumplimiento legal, asegurando que los procedimientos internos

(incluyendo horarios y guardias) se ajusten a las leyes aplicables.

5.5.2. Liderazgo y compromiso.

La alta dirección del GAD Tena, a través de la Dirección de Seguridad Ciudadana y Gestión de Riesgos, asume el liderazgo y el compromiso activo en la implementación y mantenimiento del sistema de gestión de riesgos. Se promoverá una cultura organizacional proactiva hacia el riesgo, se asignarán los recursos necesarios, se comunicará la importancia de la gestión del riesgo a todos los niveles y se publicará una política institucional que refleje el compromiso con la seguridad ciudadana y la reducción de vulnerabilidades.

Compromiso de la Alta Dirección: El Director de la Dirección de Seguridad Ciudadana y Gestión de Riesgos debe demostrar un liderazgo activo mediante las siguientes acciones:

- Comunicar la Importancia: La Dirección debe emitir una comunicación formal a todo el personal y partes interesadas sobre el valor y la obligatoriedad de la gestión del riesgo como herramienta para el cumplimiento de la misión de seguridad y prevención.
- Aprobación y Alineación: Aprobar la Política de Gestión de Riesgos (establecida en 5.5.1) y asegurar que todos los objetivos de la gestión del riesgo estén directamente alineados con los objetivos estratégicos y operativos de la Dirección

(ej. asegurar la respuesta continua y efectiva 24/7).

- Asignación de Recursos: Garantizar que los recursos humanos (personal competente), financieros (presupuesto), tecnológicos (sistemas de monitoreo y comunicación) y de tiempo sean suficientes y se asignen efectivamente para el diseño, implementación y mantenimiento del marco.

A continuación, se detalla el compromiso específico que deben asumir los roles técnicos para garantizar que el marco de gestión de riesgos se implemente y opere correctamente, reforzando la cultura proactiva de la Dirección:

Tabla 18.

Compromiso de los Servidores Técnicos en la Gestión del Riesgo

Asignación	**Compromiso con la Gestión del Riesgo (ISO 31000)**	**Aplicación Operativa Específica**
Coordinador de Seguridad Ciudadana y Gestión de Riesgos	Liderazgo de la Integración y la Rendición de Cuentas. Asumir la responsabilidad de supervisar la correcta aplicación del marco ISO 31000 y garantizar la	1. Integración: Asegurar que los riesgos operativos de Seguridad Ciudadana (ej. rotación de guardias, fallas de comunicación) no comprometan la capacidad de respuesta de Gestión de Riesgos. 2. Supervisión

	comunicación efectiva entre ambas áreas.	Continua: Garantizar el cumplimiento de los protocolos de guardia y disponibilidad para emergencias fuera del horario laboral, actuando como punto de escalamiento primario y asegurando la asignación de recursos.
Técnico de Gestión de Riesgos	Estructura y Proceso Exhaustivo. Asumir la responsabilidad de aplicar el Proceso de Gestión del Riesgo de manera sistemática, asegurando que la evaluación de riesgos sea integral y basada en la mejor información disponible.	1. Análisis de Riesgo: Mantener actualizada la matriz de riesgos cantonales (naturales y antrópicos), incluyendo la probabilidad de ocurrencia y el impacto. 2. Tratamiento: Proponer y monitorear las acciones de mitigación y preparación necesarias, asegurando que los planes de emergencia sean adaptados y probados (simulacros).
Técnico de Seguridad Ciudadana	Integración y Dinamismo Operacional. Asumir la responsabilidad de	1. Identificación de Riesgos Operativos: Reportar inmediatamente riesgos que

	integrar la gestión del riesgo en la operación diaria, siendo un agente proactivo en la identificación de riesgos operativos y de servicio.	afecten la continuidad del servicio (ej. falta de insumos, fallas en vehículos, problemas de comunicación en campo o fuera de horario) para que puedan ser tratados. 2. Cumplimiento de Protocolos: Adherirse estrictamente a los protocolos de comunicación y respuesta en emergencias (incluyendo los procedimientos para la atención de requerimientos fuera de la jornada de 07h30 a 16h00) para garantizar que la incertidumbre sobre la respuesta sea mínima.

5.5.3. Integración.

La gestión del riesgo se integrará en todos los procesos de la Dirección de Seguridad Ciudadana y Gestión de Riesgos, desde la planificación estratégica hasta la operación diaria. Se capacitará al personal para que comprenda su rol en la identificación y manejo de riesgos, y se asegurará que la gestión del riesgo forme parte de la toma de decisiones, la planificación de proyectos y la ejecución de acciones preventivas y correctivas.

Para la Dirección, esto significa transformar la gestión del riesgo en una competencia transversal, haciendo que cada servidor público reconozca que su rol impacta directamente en la seguridad y la resiliencia cantonal.

Integración en los Niveles de Planificación y Operaciones

Se establecerán mecanismos formales para garantizar que la gestión del riesgo se incorpore en todos los niveles de planificación y ejecución:

Tabla 19.

Niveles de planificación

Nivel de Integración	Mecanismo de Inclusión del Riesgo	Ejemplo Operacional
Estratégico	Planificación Estratégica Institucional (PEI). El riesgo es un insumo para la definición de objetivos	El riesgo de desastre (Gestión de Riesgos) o el incremento de la delincuencia (Seguridad Ciudadana) justifican la priorización de proyectos de inversión y la asignación presupuestaria.
Táctico (Proyectos)	Fase de Diseño y Ejecución de Proyectos. Evaluación de riesgos de cada proyecto (ej.	Evaluar el riesgo de incumplimiento o falla en proyectos de infraestructura crítica (ej. el riesgo de que las

	instalación de cámaras, capacitaciones).	cámaras fallen fuera de horario, basado en el contexto de riesgo operacional identificado).
Operacional Diario	Procedimientos Operativos Estándar (POEs). El riesgo forma parte de las actividades cotidianas.	Definición de Protocolos 24/7: Formalizar las cadenas de comunicación y las responsabilidades para la atención de emergencias, asegurando la continuidad del servicio (mitigando directamente el riesgo de falta de respuesta fuera de la jornada laboral).

Desarrollo de la Conciencia de Riesgo y el Rol del Empleado: Para que la integración sea efectiva, se debe capacitar al personal para que comprenda cómo sus actividades diarias afectan el riesgo de la Dirección:

Se impartirá formación específica que vincule las tareas individuales con el riesgo general de la Dirección:

- Técnicos de Seguridad Ciudadana: Deben entender que el incumplimiento en el llenado de bitácoras o en el seguimiento de un protocolo de patrullaje no es solo una falta

administrativa, sino un riesgo de seguridad (riesgo de control) que puede llevar a incidentes o a la incapacidad de la Dirección para defenderse legalmente.

- Técnicos de Gestión de Riesgos: Deben entender que la falta de actualización de un mapa de amenazas es un riesgo de desastre directo para la ciudadanía, comprometiendo la vida y los bienes.
- Personal en Guardias: Debe comprender que la falta de atención a un requerimiento de emergencia fuera de horario (como se evidenció en el contexto operativo) constituye un riesgo de imagen institucional, legal y de vida, y que su compromiso es vital para la resiliencia del Cantón.

Se establecerá un plan de capacitación continuo para el personal:

- Módulo I: Introducción a la ISO 31000: Principios, terminología y la visión del riesgo como incertidumbre.
- Módulo II: El Riesgo en mi Proceso: Identificación de riesgos operativos específicos del área de trabajo (Seguridad o Riesgos) y el papel de cada servidor público como "dueño del riesgo" en su función.
- Módulo III: Comunicación de Riesgos y Protocolos Críticos: Enfatizar la importancia de los canales formales de comunicación y consulta para situaciones de emergencia, asegurando que el personal conozca cuándo y cómo escalar un riesgo o un requerimiento.

Todos los documentos y procedimientos clave de la Dirección (manuales de funciones, POEs, formularios de toma de decisiones) deberán incluir una sección obligatoria de "Consideración del Riesgo" para asegurar que la gestión del riesgo se mantenga como parte del ADN de la organización.

5.5.4. Diseño.

5.5.4.1.Comprensión de la organización y su contexto.

Se realizará un análisis detallado del contexto interno y externo de la Dirección de Seguridad Ciudadana y Gestión de Riesgos, considerando factores políticos, sociales, económicos, tecnológicos, ambientales y legales, así como las fortalezas, debilidades, oportunidades y amenazas del municipio. Se identificarán las partes interesadas y se definirá el propósito y alcance de la gestión del riesgo en función de los objetivos institucionales.

Se utiliza un análisis FODA para identificar los factores internos y externos que generan incertidumbre y que deben ser abordados por el diseño del marco ISO 31000.

Tabla 20.

Análisis del Contexto Interno y Externo FODA

Componente	Descripción y Factores Relevantes	Implicación Crítica para el Diseño del Marco

Fortalezas (F)	F1. Compromiso formal de la Alta Dirección (Director) para mejorar la gestión y demandar disponibilidad para asuntos críticos.	El marco debe aprovechar este liderazgo para impulsar la integración (5.5.3) y la asignación de recursos (5.5.4.4).
	F2. Personal técnico con conocimiento especializado en gestión de riesgos y seguridad ciudadana.	
	F3. Existencia de mecanismos de reporte formal (memorandos) para el manejo de fallas operativas.	
Debilidades (D)	D1. Riesgo Operacional Crítico de Continuidad (CRÍTICO): Falta de un protocolo formal, legal y compensado de disponibilidad y respuesta 24/7 para	El diseño del marco (5.5.4.2 y 5.5.4.5) debe atacar la D1 y D2 como las prioridades máximas, formalizando protocolos de guardia,

	personal clave fuera de la jornada laboral de 07h30-16h00. D2. Uso de canales de comunicación informales (ej. WhatsApp) para requerimientos de emergencia, generando ambigüedad y riesgos de control. D3. Posible falta de claridad sobre la jerarquía y autoridad en situaciones de emergencia fuera del horario habitual.	comunicación y rendición de cuentas.
Oportunidades (O)	O1. Mandato legal y político nacional (Sistema Nacional de Gestión de Riesgos) que respalda la necesidad de adoptar la ISO 31000. O2. Posibilidad de acceder a cooperación	Utilizar el respaldo legal y la cooperación para fortalecer el tratamiento del riesgo (recursos y alianzas).

	interinstitucional (Policía, SGR) para compartir recursos y capacidades de respuesta. O3. Avance tecnológico que permite implementar sistemas de gestión de incidentes y georreferenciación a costos razonables.	
Amenazas (A)	A1. Alta exposición a riesgos naturales (inundaciones, deslizamientos) específicos de la Amazonía. A2. Restricciones del marco legal (LOSEP) que dificultan la asignación de personal para guardias o la	El diseño debe mitigar las A1 (mediante el proceso de riesgo) y las A2/A3 (mediante protocolos formales que gestionen el riesgo de cumplimiento y reputacional).

	compensación por disponibilidad.
	A3. Alta expectativa ciudadana de respuesta inmediata, que magnifica el impacto negativo de cualquier falla operativa (vinculado a D1).

5.5.4.2.Articulación del compromiso con la gestión del riesgo.

Se elaborará y comunicará una política institucional de gestión de riesgos que refleje el compromiso de la Dirección de Seguridad Ciudadana y Gestión de Riesgos con la protección de la ciudadanía y la mejora continua de los servicios. Esta política será revisada periódicamente y se asegurará su difusión y comprensión en todos los niveles de la organización.

Este punto es la formalización del liderazgo y compromiso (5.5.2) a través de documentos oficiales, lo que garantiza que la gestión del riesgo se convierta en una obligación institucional y no en una iniciativa temporal.

Política de Gestión de Riesgos

La Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Tena establecerá una Política de Gestión de Riesgos que será aprobada por el Director y refrendada

por la máxima autoridad del GAD. Esta política es la declaración formal que guía todas las decisiones y acciones relativas al riesgo.

Tabla 21.

Política de Gestión de Riesgos

Componente	Declaración Específica
Propósito de la Política	La Dirección se compromete a proteger la vida, el bienestar de la ciudadanía y los activos institucionales, integrando la gestión del riesgo en la planificación, operación y toma de decisiones para garantizar la continuidad del servicio y la resiliencia cantonal.
Principios Fundamentales	La gestión del riesgo será: Integrada (parte de la operación diaria), Estructurada (basada en ISO 31000), Adaptada (al contexto geográfico de Tena y la normativa ecuatoriana) y Dinámica (proactiva ante los cambios).
Apetito de Riesgo y Criterio	La Dirección mantendrá un Apetito de Riesgo Bajo a Muy Bajo para cualquier riesgo que comprometa: 1) La vida o integridad física de las personas. 2) La capacidad de respuesta efectiva 24/7 ante emergencias (riesgo operacional). 3) El cumplimiento legal y la imagen institucional.
Obligación de Rendir Cuentas	La responsabilidad de la gestión del riesgo recae en todos los niveles. Los Coordinadores y Técnicos tienen la obligación explícita de rendir cuentas por la gestión

	de riesgos en sus áreas y por la adherencia a los protocolos de disponibilidad y respuesta de emergencia.
Mejora Continua	La Dirección se compromete a revisar, auditar y mejorar continuamente la eficacia del marco de gestión de riesgos.

Directrices Clave de la Política (Enfoque en Riesgo Crítico): La política debe traducir el compromiso en directrices que mitiguen la Debilidad D1 identificada en el FODA (falta de protocolo 24/7). Para ello, se establece formalmente el:

- Protocolo de Llamada Crítica Formal: Se implementará un procedimiento institucional obligatorio que definirá los canales formales de comunicación (reemplazando al WhatsApp personal para asuntos críticos) y la cadena de escalamiento para requerimientos de seguridad y emergencia fuera del horario ordinario (16h00).
- Definición de Asunto Crítico: La Dirección definirá taxativamente qué se considera un "asunto profesional, de seguridad y emergencia en temas de su competencia" para evitar ambigüedades, y obligará a la respuesta inmediata de los roles designados, respetando el marco legal (LOSEP) mediante la articulación con Talento Humano para establecer mecanismos de compensación, guardia o dedicación exclusiva formalizados.

Comunicación y Adhesión de la Política

La política debe ser comunicada y comprendida por todos los servidores para asegurar la Integración (5.5.3).

Tabla 22

Comunicación y adhesión de la política

Nivel de la Organización	Mecanismo de Comunicación	Objetivo de la Adhesión
Alta Dirección (Director)	Emisión del Memorando o Resolución de aprobación de la Política y divulgación en sesiones de trabajo.	Demostrar Liderazgo y asignar la autoridad para la implementación.
Nivel Coordinador/Técnico	Reuniones de capacitación y talleres de Articulación de Compromiso, donde se firman los acuerdos de responsabilidad individual.	Garantizar la comprensión del Riesgo Operacional Crítico y la aceptación de la obligación de respuesta en el marco del nuevo protocolo de llamada crítica.
Personal de Primera Línea	Sesiones de inducción, carteleras informativas y difusión digital.	Asegurar que todo el personal entienda que la gestión del riesgo es parte de su rol y que el

reporte de riesgos (dinamismo) es obligatorio.

5.5.4.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización.

Se definirán y comunicarán claramente los roles, autoridades, responsabilidades y obligaciones de rendir cuentas en la gestión del riesgo. Cada funcionario tendrá asignada una responsabilidad específica en la identificación, análisis, evaluación y tratamiento de riesgos, y se establecerán mecanismos de supervisión y seguimiento para garantizar la efectividad del sistema.

Políticas y Directrices para la Puesta en Marcha

Las políticas y directrices son los instrumentos que traducen el compromiso del Director (5.5.4.2) en acciones concretas y obligatorias, poniendo en marcha el sistema.

Política de Gestión de Riesgos (Ver Anexo): Es el documento marco que establece el Apetito de Riesgo (Bajo a Muy Bajo) y el compromiso con el servicio continuo.

Directriz de Continuidad Operativa 24/7: Esta directriz aborda directamente la Debilidad D1 identificada en el FODA (Falta de Protocolo de Disponibilidad). Define la obligación de los roles clave (Coordinador, Técnicos) de garantizar la respuesta efectiva ante requerimientos de emergencia fuera de la jornada ordinaria (16h00).

Protocolo de Llamada Crítica Formal (PLC): Es la herramienta operativa de la directriz anterior. Este protocolo establece:

- Canal Formal: Define el medio oficial y monitoreado para la notificación de emergencias, sustituyendo los canales informales (ej. WhatsApp).
- Cadena de Escalada: Define la secuencia de llamada (Agente de Guardia → Técnico de Turno → Coordinador → Director) con tiempos máximos de respuesta.
- Articulación Legal: Se establece que la obligación de disponibilidad debe estar formalizada con la Dirección de Talento Humano para asegurar el cumplimiento del marco legal (LOSEP), ya sea mediante guardias compensadas, disponibilidad de cargo o dedicación exclusiva, eliminando la ambigüedad sobre la respuesta fuera de horario.

Tabla 23.

Matriz de Roles, Responsabilidades y Obligación de Rendir Cuentas

Rol	Autoridad	Responsabilidad (Tareas Clave de Gestión de Riesgos)	Obligación de Rendir Cuentas (Accountability)
Director	Máxima Autoridad para	Dirigir la revisión gerencial del Marco.	Eficacia global del Marco y cumplimiento

	la asignación de recursos y la toma de decisiones sobre aceptación o tratamiento de riesgos "Extremos".	Aprobar la Política de Gestión de Riesgos.	de los objetivos estratégicos de seguridad y resiliencia.
Coordinador (Seg. Ciud. y G. Riesgos)	Autoridad para activar el Protocolo de Llamada Crítica y movilizar recursos interinstitucionales menores.	Supervisar la correcta ejecución de la matriz RARAO y la integración de ambas áreas.	Continuidad Operativa 24/7 y la adhesión de los técnicos a los protocolos críticos.

Técnicos (Seg. Ciud. y G. Riesgos)	Autoridad para iniciar planes de acción de riesgo preaprobados en una emergencia (ej. activar al COE local).	Identificación de Riesgos específicos de su área, Análisis de Causas y Consecuencias de incidentes y aplicación de controles.	Adherencia estricta al Protocolo de Llamada Crítica y a las directrices de disponibilidad fuera de horario.
Supervisor/Guardia	Autoridad para la toma de decisiones inmediatas en campo bajo procedimientos claros.	Ejecución de los controles diarios (ej. bitácoras, patrullaje) e identificación de riesgos de primera línea.	Reporte oportuno y veraz de incidentes, fallas de comunicación y "casi-accidentes" (Cultura Proactiva).

Comunicación de la Política y Directrices: La comunicación asegura la Integración (5.5.3) al trasladar el compromiso de la Dirección a una acción práctica y entendida por todos.

Comunicación Formal y Pública (A toda la Dirección):

- Medio: Emisión del Memorando o Resolución de Dirección que aprueba la Política de Gestión de Riesgos y la Directriz de Continuidad Operativa 24/7.
- Objetivo: Establecer formalmente el nuevo estándar de desempeño y la obligación institucional hacia el riesgo.

1. **Capacitación Específica y Talleres de Roles (Nivel Coordinador/Técnico):**
   Medio: Sesiones obligatorias y firmadas para revisar la Roles, Autoridades, Responsabilidades y Obligación de Rendir Cuentas y el Protocolo de Llamada Crítica Formal (PLC).
   - Objetivo: Asegurar la comprensión técnica de los roles, las nuevas responsabilidades y, fundamentalmente, la aceptación de la Obligación de Rendir Cuentas por la disponibilidad 24/7. Se debe destacar que la falla en la respuesta a una llamada crítica es ahora un incumplimiento de la Política de Gestión de Riesgos.
2. **Documentación Operativa:**
   - Medio: Inclusión de la Política y los roles del PLC en los Manuales de Procesos y Funciones de cada área.
   - Objetivo: Integrar el riesgo en la operación diaria, haciendo que el cumplimiento de los protocolos sea una tarea de gestión de riesgos.

5.5.4.4.Asignación de recursos.

La Dirección de Seguridad Ciudadana y Gestión de Riesgos asignará los recursos humanos, financieros y tecnológicos necesarios para la implementación y mantenimiento del sistema de gestión de riesgos. Se capacitará al personal en las herramientas y metodologías de gestión del riesgo y se asignará presupuesto para la adquisición de tecnologías y la realización de actividades de prevención y respuesta.

La Asignación de Recursos es un componente fundamental del diseño del marco, ya que el compromiso y la política (5.5.4.2) no son efectivos si no se les dota de los medios necesarios para su implementación. La Dirección debe garantizar que los recursos financieros, humanos y tecnológicos sean suficientes y estén alineados para mitigar los riesgos clave, especialmente la discontinuidad operativa 24/7.

1. Provisión de Recursos Necesarios

La Dirección debe identificar y asegurar la provisión de recursos esenciales para la implementación y el mantenimiento del marco.

A. Recursos Humanos y Financieros (Enfoque en Disponibilidad)

La principal necesidad financiera es formalizar la disponibilidad continua del personal clave, abordando la restricción legal (LOSEP) identificada en el FODA.

Tabla 24.

Asignación de recursos

Tipo de Recurso	Requerimiento Específico	Alineación con Riesgo Crítico (D1)
Recursos Financieros	Asignación Presupuestaria para Gestión de Riesgos: Fondo dedicado para el mantenimiento de equipos de emergencia, simulacros y, principalmente, la formalización de la disponibilidad.	Financiar los mecanismos de compensación (ej. horas extraordinarias formalizadas, régimen de guardia o dedicación exclusiva) para el personal (Técnicos, Coordinador) que opera bajo el Protocolo de Llamada Crítica Formal (PLC).
Recursos Humanos	Competencia y Dedicación: Garantizar la dedicación de tiempo del Coordinador y los Técnicos para tareas de gestión de riesgos (análisis, reporte, monitoreo).	Asegurar que el personal responsable del PLC no tenga cargas laborales que comprometan su disponibilidad y su capacidad de respuesta inmediata.

B. Recursos Tecnológicos y de Herramientas

La inversión tecnológica debe priorizar la eliminación de los canales de comunicación informales (ej. WhatsApp), lo cual es una debilidad crítica.

Tabla 25.

Recursos tecnológicos y herramientas

Requerimiento Específico	Descripción	Impacto en el Marco
Sistema de Comunicación	Implementación de un sistema de comunicación de emergencia dedicado (ej. radios, software de gestión de	Elimina la ambigüedad sobre la recepción de llamadas críticas fuera de

Formal (Tecnológico)	incidentes, o una línea institucional 24/7 monitoreada) para la notificación del Protocolo de Llamada Crítica (PLC).	horario, al ser un canal oficial que registra el evento y la respuesta.
Herramientas de Evaluación de Riesgos	Adquisición o desarrollo de software para el mapeo de riesgos (GIS), bases de datos de incidentes históricos y formatos estandarizados (matrices ISO 31000).	Permite al Técnico de Gestión de Riesgos realizar un Análisis de Riesgos estructurado y basado en la evidencia.

2. Capacitación y Desarrollo de Competencias

La capacitación es un recurso humano que asegura la Integración (5.5.3) del marco, permitiendo a los empleados entender su rol en el riesgo.

Tabla 26.

Capacitación y desarrollo de competencias

Nivel de Personal	Contenido de la Capacitación	Frecuencia
Alta Dirección/Coordinador	Gobernanza del Riesgo: Principios ISO 31000, Apetito de Riesgo y toma de decisiones estratégicas basadas en el riesgo.	Anual (Revisión del Marco)
Técnicos (Seguridad y Riesgos)	Proceso de Gestión de Riesgos: Identificación, Análisis, Evaluación, Tratamiento. Uso de las herramientas de mapeo y matrices de riesgo. Énfasis en el PLC.	Bianual (Refuerzo)

Personal Operativo/Guardias	Conciencia de Riesgo y Reporte: Identificación de incidentes, "casi-accidentes" y uso del nuevo Sistema de Comunicación Formal y del Protocolo de Llamada Crítica.	Inicial y al menos una vez al año.

3. Asignación del Presupuesto

La Dirección debe presentar una solicitud presupuestaria específica que incluya:

Tabla 27.

Asignación de presupuesto

	Componente Presupuestario	Justificación de Riesgo
(Compensación)	Talento Humano	Mitigación del Riesgo Operacional Crítico (D1): Financiamiento de horas de disponibilidad, guardias o dedicación exclusiva del personal clave para garantizar la respuesta 24/7.
	Tecnología	Adquisición e implementación del Sistema de Comunicación Formal (hardware/software), licencias de software de mapeo y gestión de incidentes.
	Capacitación	Contratación de expertos externos o asignación de recursos internos para el desarrollo de los módulos de formación y la realización de simulacros periódicos.

Mantenimiento	Presupuesto recurrente para el seguimiento y revisión del marco (ej. auditorías internas de riesgo) y el mantenimiento de equipos de emergencia.

La asignación de estos recursos demuestra el compromiso tangible de la Alta Dirección con la Política de Gestión de Riesgos, asegurando que los roles y responsabilidades críticos (RARAO) puedan cumplirse bajo un esquema operativo formalizado.

5.5.4.5.Establecimiento de la comunicación y la consulta.

Se desarrollará un plan de comunicación y consulta para informar y consultar a todas las partes interesadas sobre la gestión del riesgo. Se promoverá la participación activa del personal, la ciudadanía y las instituciones aliadas, asegurando la transparencia, la retroalimentación y la mejora continua del sistema.

La Comunicación y Consulta es fundamental para que la gestión de riesgos sea inclusiva y transparente, asegurando que la información relevante fluya en la Dirección, tanto en tiempos normales como en emergencias. El objetivo es compartir información y asegurar que las percepciones y expectativas de las partes interesadas sobre el riesgo se integren en la toma de decisiones.

1. Plan de Comunicación del Marco de Gestión de Riesgos

El plan de comunicación se estructura para difundir la Política de Gestión de Riesgos (5.5.4.2), la matriz RARAO (5.5.4.3) y, de manera crucial, el Protocolo de Llamada Crítica

Formal (PLC), que es la principal herramienta para mitigar el riesgo de discontinuidad operativa.

Tabla 28.

Plan de comunicación

Público Objetivo	Contenido Clave a Comunicar	Canal y Frecuencia
Interno - Personal Clave (Coordinador, Técnicos)	PLC y RARAO: Énfasis en las nuevas Obligaciones de Rendir Cuentas por la disponibilidad 24/7 y el uso del canal formal de comunicación para emergencias.	Taller Inicial Obligatorio (con firma de recepción del PLC), y refuerzo en reuniones operativas mensuales.
Interno - Personal Operativo (Guardias, Apoyo)	Conciencia de Riesgo y Reporte: Uso correcto del nuevo sistema de comunicación y la importancia de reportar fallas y riesgos de primera línea.	Sesiones de Inducción/Capacitación inicial y semestral. Carteleras Informativas y comunicación por correo electrónico oficial.
Externo - GAD (Alcaldía, Talento Humano)	Apetito de Riesgo y Asignación de Recursos: Justificación de la necesidad de formalizar	Informes de Dirección y Solicitudes Presupuestarias formales.

	legalmente los mecanismos de guardia/compensación para el personal de emergencia.	
Externo - Ciudadanía y Entes de Respuesta (Policía Nacional, Bomberos, SGR)	Capacidades y Protocolos Coordinados: Definición de los canales oficiales para reportar emergencias a la Dirección y el rol de la Dirección en el marco del COE.	Reuniones del COE, Foros de Seguridad Ciudadana y medios oficiales del GAD.

2. Mecanismos de Consulta Regular

La consulta es un proceso bidireccional que asegura que el marco de riesgos se mantenga relevante al capturar las perspectivas de las partes interesadas.

Tabla 29.

Mecanismo de consulta

Parte Interesada	Objetivo de la Consulta	Frecuencia y Metodología
Empleados (Técnicos/Operativos)	Comprender las barreras operativas para	Reuniones Operativas Mensuales: Uso de listas

		el cumplimiento de los protocolos (ej. fallas en el nuevo sistema de comunicación, sobrecarga laboral que compromete la disponibilidad).	de verificación de riesgos operativos y encuestas internas anónimas sobre la cultura de riesgo.
	Comunidad/Ciudadanía	Entender la percepción del riesgo (ej. ¿cuáles son las áreas de mayor inseguridad?, ¿la respuesta es efectiva en las noches o fines de semana?), y validar los criterios de priorización de riesgo.	Mesas de Seguridad Ciudadana/Barriales: Al menos dos veces al año. Uso de encuestas de percepción de seguridad.
	Entidades de Apoyo (SGR, Policía, Bomberos)	Evaluar la eficacia de la	Simulacros y Ejercicios de

	coordinación interinstitucional y la claridad del Protocolo de Llamada Crítica para asegurar que la ayuda se active correctamente en caso de desastre.	Mesa: Anuales. Revisión conjunta de la matriz de riesgos y los procedimientos de activación.

El proceso de consulta es dinámico; los resultados alimentan el proceso de Seguimiento y Revisión del marco, garantizando la mejora continua del sistema.

5.5.5. Implementación.

La Dirección de Seguridad Ciudadana y Gestión de Riesgos implementará el marco de referencia de gestión de riesgos mediante la ejecución de procesos definidos para la identificación, análisis, evaluación y tratamiento de riesgos. Se revisarán y ajustarán continuamente los procedimientos para asegurar su eficacia y alineación con los objetivos institucionales.

La implementación es el proceso mediante el cual se da vida al marco de referencia. Implica aplicar los recursos asignados (5.5.4.4) para ejecutar los procesos de gestión del riesgo y establecer mecanismos de seguimiento continuo que aseguren la eficacia del sistema.

1. Ejecución del Proceso de Gestión de Riesgos (Modelo ISO 31000)

La Dirección adoptará el Proceso de Gestión de Riesgos de la ISO 31000 como metodología obligatoria para todas sus actividades, proyectos y operaciones.

1.1. Identificación del Riesgo

El objetivo es encontrar, reconocer y describir todos los riesgos que pueden ayudar u obstaculizar los objetivos de la Dirección (seguridad y resiliencia).

Riesgos Externos/Estratégicos: Incluir la identificación de amenazas naturales (inundaciones, sismos, deslizamientos) por parte del Técnico de Gestión de Riesgos, y la identificación de tendencias delictivas y riesgos sociales (inseguridad, violencia) por parte del Técnico de Seguridad Ciudadana.

Riesgos Internos/Operacionales (Énfasis Crítico): Se formalizará la identificación del riesgo de discontinuidad operativa del servicio 24/7 y la falla en la comunicación como un riesgo inherente a la operación de emergencia.

1.2. Análisis y Evaluación del Riesgo

Los riesgos identificados se analizarán utilizando los Criterios de Riesgo definidos en la política (5.5.4.2).

Análisis: Se estimará la probabilidad y el impacto de cada riesgo. Para el riesgo de discontinuidad operativa 24/7, la probabilidad puede ser media (dada la jornada laboral) y la consecuencia se calificará como Extrema (debido al impacto en la vida, la reputación y el incumplimiento de la misión institucional).

Evaluación: Comparar los resultados del análisis con el Apetito de Riesgo Bajo a Muy Bajo de la Dirección. Dado que el riesgo de falta de respuesta 24/7 es extremo, este requerirá un Tratamiento del Riesgo (5.5.5.3) inmediato y prioritario.

1.3. Tratamiento del Riesgo

El tratamiento implica seleccionar e implementar opciones para modificar el riesgo.

Tratamiento del Riesgo Operacional Crítico: La opción seleccionada es la reducción del riesgo mediante la implementación obligatoria de:

El Protocolo de Llamada Crítica Formal (PLC) y la Directriz de Continuidad Operativa (5.5.4.2).

El Sistema de Comunicación Formal (Tecnológico) adquirido con el presupuesto (5.5.4.4).

La formalización legal de los mecanismos de guardia o disponibilidad con Talento Humano.

Tratamiento de Riesgos Estratégicos: Implementar planes de mitigación (ej. obras de infraestructura, patrullaje preventivo) y planes de transferencia de riesgo (ej. seguros, convenios interinstitucionales).

2. Monitoreo, Revisión y Ajuste Continuo (Mejora Continua)

La gestión de riesgos es un ciclo iterativo. La Dirección debe revisar y ajustar continuamente el marco y el proceso para asegurar su eficacia y alineación.

2.1. Seguimiento y Monitoreo (KPIs)

Se establecerán Indicadores Clave de Riesgo (KRI) y de desempeño para monitorear la efectividad de los controles:

KRI Crítico: Tasa de Cumplimiento del PLC: Porcentaje de cumplimiento del tiempo máximo de respuesta ante una Llamada Crítica fuera de la jornada laboral.

KPI Operacional: Número de incidentes/fallas reportadas internamente (para evaluar la cultura de reporte).

KPI Estratégico: Variación en la percepción de seguridad ciudadana (obtenida de la consulta 5.5.4.5) y reducción de daños por eventos naturales.

2.2. Revisión del Marco y Ajuste

La Dirección (liderada por el Director y el Coordinador) realizará revisiones periódicas formales del desempeño del marco.

Revisión del Director (Gerencial): Anual. Enfocada en la alineación del marco con los objetivos estratégicos y la suficiencia de los recursos asignados (5.5.4.4).

Revisión Operativa (Coordinador y Técnicos): Trimestral. Enfocada en la eficacia de los controles implementados y la necesidad de ajustar el Protocolo de Llamada Crítica Formal si se identifican fallas recurrentes.

Este enfoque asegura que el sistema de gestión de riesgos se mantenga dinámico, respondiendo a los cambios en el contexto de Tena y fortaleciendo continuamente la capacidad de la Dirección para cumplir con su misión 24/7.

5.5.6. Valoración.

Se establecerán indicadores clave de desempeño (KPIs) y se realizarán evaluaciones periódicas para medir la efectividad del sistema de gestión de riesgos. Se analizará el cumplimiento de los objetivos, la eficiencia en la asignación de recursos y la satisfacción de las partes interesadas, ajustando el sistema según los resultados obtenidos.

Para la Dirección, la valoración se centrará en medir la mitigación del riesgo operacional crítico (discontinuidad de servicio 24/7) y la eficacia de la respuesta ante los riesgos estratégicos (seguridad y desastres).

1. Establecimiento de Indicadores Clave de Desempeño (KPIs y KRIs)

Se establecerán indicadores que permitan una medición objetiva del cumplimiento de la política, los procedimientos (PLC) y los objetivos de reducción de riesgos.

Tabla 30.

Indicadores claves de desempeño

Tipo de Indicador	Indicador Específico	Fórmula / Criterio de Medición	Objetivo de la Medición
KRI Crítico (Riesgo Operacional)	Tasa de Cumplimiento del Protocolo de Llamada Crítica (PLC).	(N° de Llamadas Críticas Atendidas en el Tiempo Límite / N° Total de Llamadas Críticas) x 100. Meta: 98% de cumplimiento.	Evalúa la mitigación directa de la Debilidad D1 (Falta de Protocolo 24/7) y la efectividad del tratamiento del riesgo (PLC y Recursos).
KPI Operacional (Seguridad)	Tiempo Promedio de Respuesta a Incidentes de Seguridad.	Suma del Tiempo de Respuesta / N° de Incidentes Atendidos. Meta: Reducción del 10% anual.	Mide la eficacia de los controles operativos y la velocidad de reacción del personal.

KPI Estratégico (Gestión de Riesgos)	Nivel de Preparación Cantonal.	Porcentaje de cumplimiento de las acciones de mitigación y preparación definidas en la matriz de riesgos (ej. planes de evacuación actualizados, simulacros ejecutados).	Mide el avance en la reducción de la vulnerabilidad y el fortalecimiento de la resiliencia.
KPI de Conciencia de Riesgo	Tasa de Reporte de Riesgos y "Casi-Accidentes".	N° de reportes internos proactivos por mes.	Evalúa si la Cultura de Riesgo (promovida en 5.5.2) está mejorando.

2. Medición Regular de Resultados y Evaluación de la Efectividad

La medición será un proceso continuo, integrada en las rutinas de la Dirección.

Frecuencia de Medición:

Mensual: KPIs y KRIs Operacionales (ej. Tasa de Cumplimiento del PLC).

Trimestral: Revisión de la Matriz de Riesgos y los Tratamientos aplicados.

Anual: Informe de Valoración integral para la Dirección y las autoridades superiores del GAD.

Evaluación de la Efectividad: La valoración no es solo una medición, sino un juicio sobre el desempeño:

Cumplimiento de Objetivos: Se evaluará si el sistema de gestión de riesgos (SGR) está ayudando a la Dirección a cumplir sus objetivos estratégicos (ej. ¿Se ha reducido la percepción de inseguridad? ¿Se ha minimizado el impacto de las inundaciones?).

Alineación Continua: Se examinará si el SGR sigue siendo relevante para las necesidades del GAD, especialmente ante cambios en el contexto externo (ej. nuevas leyes, nuevos riesgos climáticos, o una nueva debilidad operativa). Si el KRI Crítico del PLC no alcanza su meta, el sistema no está alineado y debe ser ajustado (5.4.7).

5.8.2. Mejora.

5.8.2.1. Adaptación.

El marco de gestión de riesgos se adaptará a los cambios internos y externos del GAD Tena, revisando y ajustando el sistema ante nuevas amenazas, vulnerabilidades o modificaciones en la normativa. Se asegurará la alineación continua del sistema con los objetivos institucionales y las necesidades de la ciudadanía.

La revisión del Marco de Gestión de Riesgos y sus componentes se activará ante las siguientes condiciones:

A. Cambios Internos

Tabla 31.

Cambios internos

Cambio Interno	Impacto en el Marco	Acción de Adaptación Requerida
Bajo Desempeño (Falla del KRI)	El KRI Crítico (Tasa de Cumplimiento del PLC) cae por debajo de la meta del 98% en dos mediciones trimestrales consecutivas.	Reajuste de Controles: Revisar la RARAO (5.5.4.3), las Directrices Operativas y reevaluar si los Recursos (5.5.4.4) son insuficientes (ej. la compensación no es atractiva o el canal de comunicación formal está fallando).
Reestructuración Organizacional	Cambio en los roles, la autoridad o la estructura de la Dirección (ej. se crea una nueva unidad o se fusionan áreas).	Ajuste de la RARAO: Reasignar inmediatamente las responsabilidades de gestión de riesgos a los nuevos roles y actualizar la Matriz de Obligación de Rendición de Cuentas.

Adquisición de Nueva Tecnología	Implementación de un nuevo sistema de monitoreo o comunicación.	Actualización del PLC: El Protocolo de Llamada Crítica Formal debe ser ajustado para incorporar y operar bajo la nueva tecnología, eliminando las herramientas obsoletas.

B. Cambios Externos

Tabla 32

Cambios externos

Cambio Externo	Impacto en el Marco	Acción de Adaptación Requerida
Nuevas Tendencias de Riesgo	Aparición de un nuevo patrón delictivo o un cambio significativo en los riesgos climáticos (ej. sequías inusuales).	Actualización de la Matriz de Riesgos: El Técnico de Gestión de Riesgos debe identificar el nuevo riesgo,

			evaluarlo y proponer un Tratamiento que será integrado inmediatamente en los planes operativos.
	Cambio Regulatorio	Modificaciones en la LOSEP o en la normativa de la SGR que afecten la capacidad de respuesta (ej. nuevas restricciones en la jornada laboral).	Revisión de la Política y Directrices: Adaptar la Directriz de Continuidad Operativa 24/7 para asegurar el cumplimiento legal, trabajando con Talento Humano para formalizar nuevos esquemas de disponibilidad.
	Retroalimentación Externa	Resultados negativos en las consultas ciudadanas (5.5.4.5) sobre la percepción de inseguridad o la lentitud de la respuesta.	Revisión de la Estrategia: Ajustar los objetivos operacionales y estratégicos para responder a la percepción

ciudadana, lo que puede implicar un reajuste en los recursos o en los controles de seguridad.

2. Proceso de Ajuste y Mantenimiento de la Efectividad

La adaptación es un proceso formal que asegura que el marco mantenga su alineación con los objetivos de la Dirección.

Análisis de la Causa Raíz: Cuando los resultados de la Valoración (5.5.6) muestren una desviación, se debe realizar un análisis para identificar por qué el control falló (ej. ¿La falta de respuesta 24/7 se debió a que el protocolo no estaba claro, o a que el personal no estaba capacitado, o a que el recurso financiero no se formalizó?).

Diseño de la Acción Correctiva: En base al análisis, se diseña una acción de ajuste. Por ejemplo, si el problema fue el recurso, el Director debe priorizar la reasignación presupuestaria. Si el problema fue la claridad, el PLC debe ser reescrito y comunicado nuevamente.

Implementación Rápida: La acción correctiva se implementa siguiendo el mismo ciclo de la ISO 31000: se comunica (5.5.4.5), se dota de recursos (5.5.4.4) y se integra en los procedimientos.

Verificación y Re-Valoración: Tras el ajuste, se debe establecer un nuevo periodo de medición más corto para verificar que el cambio (la adaptación) ha sido efectivo y que el KRI vuelve a los niveles aceptables.

De esta manera, la Adaptación garantiza que la Dirección de Seguridad Ciudadana y Gestión de Riesgos mantenga su enfoque proactivo y resuelva los riesgos tan pronto como su tratamiento (controles) muestre signos de ineficacia.

3.4.1.1 Mejora continua.

La Dirección de Seguridad Ciudadana y Gestión de Riesgos implementará un proceso de mejora continua, realizando auditorías periódicas, revisiones y análisis de los resultados del sistema de gestión de riesgos. Se utilizarán los hallazgos para identificar áreas de mejora y aplicar acciones correctivas y preventivas, fortaleciendo la capacidad institucional para la gestión del riesgo.

1. Mecanismos de Revisión y Análisis

La Dirección implementará un sistema formal para analizar los resultados y detectar oportunidades de mejora en la Política, el Diseño y el Proceso de Gestión de Riesgos.

A. Auditorías Periódicas

Se realizarán auditorías internas para evaluar el cumplimiento y la eficacia del Marco de Gestión de Riesgos:

Auditoría de Cumplimiento (Anual): Verificar si el personal, especialmente los roles críticos, cumple con las responsabilidades definidas en la matriz RARAO (5.5.4.3) y, crucialmente, si se adhiere al Protocolo de Llamada Crítica Formal (PLC). Esto incluye la revisión de registros de llamadas, bitácoras y el uso del Sistema de Comunicación Formal.

Auditoría de Eficacia (Bienal): Evaluar si los controles y tratamientos de riesgo implementados realmente están logrando los objetivos. Por ejemplo, si el Tratamiento de Riesgo para las inundaciones ha reducido el impacto de los eventos.

B. Revisión Gerencial (Director y Coordinador)

El Director debe realizar una Revisión Gerencial del Marco al menos una vez al año, utilizando los siguientes insumos:

Resultados de los KPIs y KRIs (5.5.6).

Hallazgos de las auditorías internas y externas.

Resultados de las Consultas con Partes Interesadas (5.5.4.5) sobre la percepción del servicio.

Informes sobre incidentes graves o fallas críticas (ej. un incidente donde falló la respuesta 24/7).

2. Acciones Correctivas y Preventivas

Los hallazgos de las auditorías y las revisiones deben traducirse en acciones concretas que mejoren el sistema:

Tabla 33

Acciones correctivas y preventivas

Hallazgo (Oportunidad de Mejora)	Tipo de Acción	Ejemplo de Aplicación en la Dirección
Baja Tasa del KRI Crítico (Falla del PLC)	Acción Correctiva: Implementar una medida inmediata para solucionar la causa de la falla (ej. si fue por falta de conocimiento, se refuerza la capacitación).	Revisar el Mecanismo de Compensación y trabajar con Talento Humano para hacer más efectiva la Directriz de Continuidad Operativa 24/7 y asegurar la disponibilidad legal y motivada del personal clave.
Alto Nivel de Riesgo Residual	Acción Preventiva: Identificar la necesidad de un nuevo tratamiento de riesgo o de reforzar un control existente que no está funcionando de manera óptima.	Diseñar e implementar un nuevo sistema de alerta temprana comunitaria para inundaciones, o duplicar el recurso tecnológico de comunicación de emergencia.

Ineficiencia en la Comunicación (Resultado de la consulta)	Mejora del Proceso: Simplificar la forma en que se comunica la información para la gestión de riesgos.	Simplificar los formularios de reporte de incidentes para que sean más fáciles de usar por el personal operativo, fomentando una mayor Tasa de Reporte.

3. Fortalecimiento de la Cultura de Riesgo

La mejora continua debe enfocarse en fortalecer la cultura proactiva de la Dirección:

Lecciones Aprendidas: Establecer un proceso formal para documentar las "lecciones aprendidas" de cada incidente crítico y simulacro. Estas lecciones deben ser comunicadas a todos los niveles para prevenir la recurrencia de las fallas.

Reconocimiento: Reconocer y premiar al personal que demuestre una gestión de riesgos ejemplar, especialmente a quienes identifican y reportan proactivamente las debilidades operativas antes de que se conviertan en incidentes (Cultura de Reporte).

La mejora continua garantiza que el Marco de Gestión de Riesgos evolucione con el GAD Tena, manteniendo la seguridad ciudadana y la capacidad de respuesta como los objetivos centrales de su existencia.

5.5. Proceso.

5.5.1. Generalidades.

El proceso de gestión del riesgo, conforme a los lineamientos de la norma ISO 31000:2018, constituye el núcleo operativo del sistema propuesto para la Dirección de Seguridad Ciudadana y Gestión de Riesgos (DSCGR) del GAD Municipal de Tena. Este proceso es una aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto, y para la apreciación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Su naturaleza es iterativa y está diseñada para ser una parte integral de la gestión, la toma de decisiones y la cultura organizacional, en lugar de una actividad aislada (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 102).

La implementación de este proceso busca transformar la gestión reactiva, evidenciada en la ausencia inicial de inventarios y análisis formales, hacia un enfoque proactivo y estructurado. La adopción de metodologías robustas como MAGERIT, ya explorada en el análisis preliminar (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 97), sienta las bases para la aplicación rigurosa de las fases del proceso ISO 31000. A continuación, se detallan los pilares de este proceso

Apoyo a la toma de decisiones: La gestión del riesgo proporciona información estructurada para que la dirección tome decisiones informadas y basadas en evidencia, en lugar de en la intuición. Por ejemplo, al evaluar la asignación de recursos para patrullaje, el análisis de riesgos permite priorizar zonas con mayores índices delictivos (riesgo de seguridad ciudadana) o mayor vulnerabilidad a inundaciones (riesgo de desastre),

optimizando el uso de personal y vehículos. De igual forma, una decisión sobre invertir en un sistema de alerta temprana se justifica con datos sobre la probabilidad e impacto de un evento adverso, demostrando el retorno de la inversión en términos de vidas y bienes protegidos.

Alineación con los objetivos organizacionales: El proceso de gestión del riesgo no es un fin en sí mismo, sino una herramienta para alcanzar los objetivos de la DSCGR y del GAD Tena. Si un objetivo estratégico es "asegurar la respuesta efectiva e ininterrumpida ante emergencias 24/7" (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 104), la gestión de riesgos identifica amenazas como la "falta de un protocolo formal de disponibilidad" o la "dependencia de canales de comunicación informales" (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 112). El tratamiento de estos riesgos operacionales se convierte en una acción necesaria para garantizar el cumplimiento del objetivo.

Naturaleza dinámica, iterativa y adaptable: El riesgo no es estático; evoluciona con los cambios en el contexto interno y externo. El proceso debe ser dinámico para anticipar y responder a nuevas amenazas (ej. nuevas modalidades delictivas, efectos del cambio climático) y oportunidades. Es iterativo porque la evaluación y el tratamiento de riesgos se repiten cíclicamente, permitiendo el aprendizaje y la mejora continua. Por ejemplo, después de un simulacro de evacuación, se revisan los resultados, se identifican fallos en la comunicación o logística (nuevos riesgos) y se ajustan los planes de contingencia. Esta

adaptabilidad asegura que el sistema de gestión de riesgos siga siendo relevante y eficaz a lo largo del tiempo.

Estos componentes están soportados de manera transversal por el seguimiento y revisión, así como por el registro e informe, garantizando la mejora continua y la rendición de cuentas en todo el ciclo de vida del riesgo.

5.5.2. Comunicación y consulta.

La comunicación y consulta son actividades continuas e iterativas que la DSCGR debe llevar a cabo para asistir en la recopilación, intercambio y provisión de información relevante sobre la gestión del riesgo. Este proceso es fundamental para asegurar que las diferentes partes interesadas, tanto internas como externas, comprendan el riesgo, las bases sobre las cuales se toman las decisiones y las razones por las que se requieren acciones particulares (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 122).

El objetivo es fomentar la conciencia y la comprensión del riesgo, así como integrar las percepciones y expectativas de las partes interesadas en la toma de decisiones. Para la DSCGR, esto implica un diálogo bidireccional y transparente que fortalece la confianza y promueve la corresponsabilidad en la seguridad y resiliencia del cantón.

Se establecerá una combinación de métodos formales e informales para compartir la información de riesgos, adaptándose al público objetivo:

Tabla 34.

Métodos para Compartir Información con las Partes Interesadas

Tipo de Método	Descripción	Ejemplos Prácticos en la DSCGR
Reuniones y Talleres	Interacciones directas que permiten el diálogo, el debate y la retroalimentación inmediata.	Interno: Reuniones periódicas del Comité de Gestión de Riesgos. Externo: Talleres de socialización de mapas de riesgos con líderes barriales.
Informes y Documentación Formal	Documentos escritos y estructurados que presentan resultados, decisiones y planes.	Interno: Informe anual de rendimiento del SGR para la Alcaldía y la Dirección. Externo: Publicación del Plan de Respuesta a Desastres.
Plataformas Digitales y Medios	Uso de tecnología para la difusión masiva y rápida de información.	Interno: Uso de una intranet o sistema de gestión documental (SharePoint) para almacenar la matriz de

		riesgos. Externo: Alertas por redes sociales y mensajes de texto sobre el monitoreo de ríos y deslizamientos.
Campañas de Concientización	Actividades diseñadas para cambiar la percepción y el comportamiento del público.	Externo: Distribución de folletos sobre rutas de evacuación en zonas de inundación.

Las partes interesadas clave, identificadas en el perfil de la organización (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 37), son el foco de este proceso:

Partes Interesadas Internas: Autoridades municipales (Alcalde, Concejales), directores de otras áreas (TICs, Administrativa, Planificación), y todo el personal de la DSCGR (Director, Coordinadores, Técnicos, Agentes). La comunicación interna se formalizará mediante los canales establecidos en la Matriz de Comunicación (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 136), utilizando herramientas como el sistema Quipux para oficios, la red de radio troncalizada para operaciones y el correo institucional para informes técnicos.

Partes Interesadas Externas: La ciudadanía del cantón Tena, organizaciones sociales y barriales, Policía Nacional, Servicio Nacional de Gestión de Riesgos y Emergencias (SNGRE), Cuerpo de Bomberos, empresas locales e instituciones de cooperación. La consulta con estos grupos es vital para entender la percepción del riesgo en el territorio y alinear las estrategias de seguridad con las necesidades comunitarias.

Para mitigar la debilidad identificada del uso de canales informales como WhatsApp para emergencias (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 112), se implementará un Protocolo de Llamada Crítica Formal (PLC). Este protocolo definirá canales oficiales y monitoreados (línea institucional 24/7, sistema de gestión de incidentes) para asegurar la trazabilidad, la respuesta oportuna y la legalidad de las comunicaciones en situaciones de emergencia, reemplazando la ambigüedad actual por un sistema estructurado y auditable (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 116).

Tabla 35.

Roles y Responsabilidades en la Comunicación

Rol	Responsabilidad Principal
Director de la DSCGR	Aprobar la Estrategia de Comunicación y Consulta. Actuar como principal vocero para riesgos de alto impacto ante autoridades superiores y prensa.
Coordinador de Seguridad Ciudadana y Gestión de Riesgos	Coordinar las actividades de consulta. Garantizar que la información sea precisa y esté disponible para las partes interesadas internas.
Área de Gestión de Riesgos y Seguridad Ciudadana	Elaborar informes técnicos y materiales de comunicación basados en los datos de valoración del riesgo.
Personal de Cuerpo de Agentes de control Municipal	Participar en las consultas aportando su conocimiento de primera línea. Comunicar riesgos a nivel comunitario durante las operaciones.

5.5.3. Alcance, contexto y criterios.

5.5.3.1. Generalidades.

El propósito de esta etapa inicial del proceso de gestión del riesgo es personalizar y adaptar el enfoque a los objetivos y capacidades específicas de la Dirección de Seguridad Ciudadana y Gestión de Riesgos. Consiste en definir el alcance del sistema, comprender los contextos externo e interno en los que opera la organización y establecer los criterios con los cuales se evaluará la significancia del riesgo. Esta fase es fundamental, ya que proporciona la base y los límites para todo el proceso de apreciación y tratamiento del riesgo, asegurando que los esfuerzos se centren en los aspectos más relevantes para la misión institucional de proteger a la ciudadanía del cantón Tena.

5.5.3.2. Definición del alcance.

El alcance del sistema de gestión de riesgos se circunscribe a la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Municipal de Tena. Su objetivo es proteger la integridad, disponibilidad y confidencialidad de los procesos y sistemas clave que soportan la seguridad de la población y la gestión efectiva de emergencias (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 69).

El alcance abarca las siguientes áreas y procesos sustantivos de la Dirección, conforme a sus competencias y portafolio de productos (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, pp. 29, 69):

Gestión de la Seguridad Ciudadana: Incluye los procesos de planificación y ejecución del Plan de Seguridad Cantonal, coordinación con la Policía Nacional, control del

espacio público, supervisión de agentes de control municipal y fomento de la convivencia pacífica a través de comités barriales.

Gestión de Riesgos y Emergencias: Abarca los procesos de identificación, análisis y cartografía de amenazas y vulnerabilidades; elaboración de planes de contingencia y respuesta; activación y operación del Comité de Operaciones de Emergencia (COE) Cantonal; y coordinación de la ayuda humanitaria.

Sistemas de Información y Comunicación: Comprende la protección de los activos de información que soportan los procesos anteriores, tales como bases de datos de incidentes, sistemas de monitoreo (CCTV), sistemas de información geográfica (SIG), y las plataformas de comunicación (radios, telefonía) utilizadas para la coordinación de la respuesta.

Geográficamente, el alcance cubre la totalidad del territorio del cantón Tena, con una extensión de 3,897.41 km², incluyendo sus áreas urbanas y rurales (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 35).

El SGR se aplicará a los procesos misionales críticos de la DSCGR, aquellos cuyo fallo o interrupción tendría un impacto directo en la seguridad y la vida de la ciudadanía.

Tabla 36.

Proceso, actividades y Decisiones

Proceso Crítico	**Actividades Objeto de Gestión de Riesgos**	**Decisiones Objeto de Gestión de Riesgos**

A. Monitoreo y Alerta Temprana	Recolección, análisis e interpretación de datos hidrometeorológicos, geológicos y de amenazas antrópicas.	Declaración de niveles de alerta (amarilla, naranja, roja). Activación del COE Cantonal.
B. Preparación y Respuesta a Emergencias	Elaboración, socialización y simulacros de planes de emergencia y evacuación. Movilización y coordinación de recursos en la fase de respuesta.	Definición de las zonas de riesgo prioritarias para intervención. Asignación de recursos logísticos (albergues, equipos) durante una crisis.
C. Seguridad Ciudadana y Convivencia	Patrullajes preventivos y operativos conjuntos con la Policía Nacional. Intervención en conflictos comunitarios de riesgo.	Establecimiento de prioridades de vigilancia y distribución de personal en zonas de alta incidencia delictiva.
D. Logística y Mantenimiento Operacional	Adquisición y mantenimiento de equipos de comunicación, vehículos y herramientas de rescate. Gestión de los centros de operaciones.	Decisiones de inversión y descarte de equipos obsoletos o no funcionales.

Se establecen límites claros para enfocar los esfuerzos del proyecto:

	Límite	Descripción Específica
	Organizacional	Solo aplica a la DSCGR (personal directivo, técnico y operativo). La gestión de riesgos de otras direcciones (e.g., Obras Públicas, Financiero) queda excluida del alcance, aunque se mantendrá la coordinación interinstitucional.
(Geográfico)	Espacial	El SGR está diseñado para gestionar riesgos dentro del área de jurisdicción del Cantón Tena. Se incluirán los riesgos específicos de las zonas urbanas y rurales con mayor vulnerabilidad a inundaciones y deslizamientos.
	Temporal	El alcance del diseño se centra en la operación a mediano plazo (3 a 5 años) de la DSCGR. Se considera la revisión anual de la matriz de riesgos y la actualización bianual del Plan de Gestión de Riesgos Cantonal.

Recursos Disponibles y Necesarios

Recursos Disponibles (Identificados en el Contexto): La DSCGR cuenta con la siguiente base de recursos para iniciar el proceso de gestión de riesgos:

Talento Humano: Un equipo técnico con experiencia en respuesta a emergencias y operaciones de seguridad ciudadana.

Marco Legal: La existencia de una ordenanza municipal que faculta la acción en gestión de riesgos y seguridad.

Equipamiento Básico: Equipos de comunicación (radios) y vehículos operativos esenciales para la respuesta inicial.

Información Primaria: Mapas de amenazas cantonales básicos (ej. zonas propensas a inundación) y registros históricos de incidentes.

Recursos Necesarios No Existentes (Propuestos): Para que el SGR diseñado sea efectivo y cumpla con los estándares de la ISO 31000, se proponen los siguientes recursos adicionales:

Tabla 37.

Recursos necesarios

Tipo de Recurso	Recurso Específico Propuesto	Justificación y Objetivo
Tecnológico	Plataforma Digital de Gestión de Riesgos (Software)	Centralizar la Matriz de Riesgos, los planes de tratamiento y el registro de incidentes, permitiendo el

		monitoreo en tiempo real de indicadores clave de riesgo.
Humano/Competencia	Capacitación Especializada en ISO 31000 y Análisis de Riesgo	Formar al personal clave (Analistas de Riesgo y Comité) en la metodología específica de la norma para garantizar la consistencia y profesionalismo en la valoración.
Financiero	Partida Presupuestaria Específica para el SGR	Asegurar fondos dedicados anualmente para la implementación de tratamientos (ej. controles de riesgo, adquisición de equipos de mitigación) y el mantenimiento del sistema.

Información	Estudios Detallados de Vulnerabilidad y Capacidad	Ir más allá de los mapas de amenazas: cuantificar la vulnerabilidad social, económica e infraestructural de las zonas de riesgo para un análisis de riesgo más preciso.

5.5.3.3. Contextos externo e interno.

La comprensión de los contextos es crucial para identificar las fuentes de riesgo y definir criterios adecuados. Este análisis se basa en la información detallada de la organización y el análisis FODA presentado en el documento de investigación (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, pp. 22-38, 111-113).

Contexto Externo: El contexto externo incluye el entorno en el cual la DSCGR busca alcanzar sus objetivos. Los factores clave son:

Social y Demográfico: Una población cantonal de 80,816 habitantes con un crecimiento anual del 2.4%, superior al promedio nacional, lo que implica una creciente demanda de servicios de seguridad y una mayor exposición a riesgos (Gobierno Autónomo

Descentralizado Municipal de Tena, 2025, p. 35). A esto se suma la alta expectativa ciudadana de una respuesta inmediata ante incidentes, lo que magnifica el impacto reputacional de cualquier fallo operativo.

Legal y Regulatorio: La DSCGR opera bajo un marco legal estricto que incluye el COOTAD, la LOSEP y ordenanzas municipales. Las restricciones de la LOSEP, por ejemplo, dificultan la asignación flexible de personal para guardias, constituyendo una amenaza para la continuidad operativa 24/7 (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 113).

Ambiental y Geográfico: Ubicación en la región amazónica, con una alta exposición a riesgos naturales como inundaciones y deslizamientos, lo que requiere un enfoque especializado en la gestión de desastres.

Político e Interinstitucional: La existencia de un Sistema Nacional de Gestión de Riesgos y la posibilidad de cooperación con la Policía Nacional y el SNGRE representan una oportunidad para fortalecer capacidades y compartir recursos (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 112).

Tecnológico: El avance tecnológico ofrece oportunidades para implementar sistemas de gestión de incidentes y georreferenciación a costos razonables, mejorando la eficiencia de la respuesta.

Contexto Interno: El contexto interno se refiere al ambiente dentro de la organización. Los factores determinantes son:

Gobernanza y Estructura: La DSCGR está estructurada como un "Proceso Agregador de Valor" con unidades especializadas en seguridad y gestión de riesgos. Existe un compromiso formal de la alta dirección para mejorar la gestión, lo cual es una fortaleza clave (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, pp. 36, 111).

Cultura Organizacional y Capacidades: Se cuenta con personal técnico con conocimiento especializado. Sin embargo, se identifican debilidades críticas como la falta de un protocolo formal para la disponibilidad y respuesta 24/7 y el uso de canales de comunicación informales para emergencias, lo que genera ambigüedad y riesgos de control (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 112).

Políticas y Objetivos: La misión de la institución es "planear, implementar y sostener acciones institucionales para el servicio ciudadano del cantón" (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 22). Los objetivos del sistema de gestión de riesgos deben alinearse directamente con esta misión y con los objetivos estratégicos de seguridad y resiliencia.

Recursos y Activos de Información: La Dirección gestiona activos críticos como servidores, bases de datos de seguridad, sistemas de videovigilancia y equipos de comunicación. El análisis de riesgos preliminar identificó vulnerabilidades en estos activos, como la dependencia de una única fuente de energía y la falta de políticas estrictas de custodia (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 92).

La definición de los criterios de riesgo es el proceso de especificar la cantidad y el tipo de riesgo que la organización puede o no puede tomar en relación con sus objetivos. Estos criterios deben ser coherentes con el marco de referencia y el apetito de riesgo de la DSCGR, el cual se ha definido como Bajo a Muy Bajo para cualquier riesgo que comprometa la vida, la capacidad de respuesta 24/7 o el cumplimiento legal (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 114).

Para la valoración del riesgo, se adoptarán las escalas cualitativas y la matriz de riesgo basadas en la metodología MAGERIT, utilizadas en el análisis preliminar del Plan Director de Seguridad (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, pp. 88-89, 92).

Criterios de Probabilidad

La probabilidad se define como la posibilidad de que una amenaza se materialice en un período de tiempo determinado. Se utilizará la siguiente escala de tres niveles:

Tabla 38.

Probabilidad de evento

Valor	Nivel	Descripción
1	Bajo	La amenaza se materializa a lo sumo una vez cada año.

2	Medio	La amenaza se materializa a lo sumo una vez cada mes.
3	Alto	La amenaza se materializa a lo sumo una vez cada semana.

Fuente: Adaptado de Gobierno Autónomo Descentralizado Municipal de Tena (2025, p. 88).

Criterios de Impacto (Consecuencia)

El impacto evalúa la magnitud del daño que la materialización de una amenaza podría causar a la organización y sus objetivos. Se medirá en función de las consecuencias sobre las dimensiones de confidencialidad, integridad y disponibilidad de los activos y servicios.

Tabla 39.

Probabilidad impacto

Valor	Nivel	Descripción
1	Bajo	El daño derivado de la materialización de la amenaza no tiene

		consecuencias relevantes para la organización.
2	Medio	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
3	Alto	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.

Fuente: Adaptado de Gobierno Autónomo Descentralizado Municipal de Tena (2025, p. 89).

Matriz de Evaluación y Niveles de Riesgo

El nivel de riesgo se calculará multiplicando el valor de la probabilidad por el valor del impacto (Riesgo = Probabilidad × Impacto). El resultado se clasificará según la siguiente matriz, que define los niveles de riesgo y los criterios de aceptación.

Tabla 40.

Matriz de probabilidades

Probabilidad	Impacto		
Bajo (1)	Medio (2)	Alto (3)	
Alto (3)	3 (Medio)	(Alto)	9 (Extremo)
Medio (2)	2 (Bajo)	4 (Medio)	6 (Alto)
Bajo (1)	1 (Bajo)	2 (Bajo)	3 (Medio)

Los niveles de riesgo definen la acción requerida:

Riesgo Extremo (9): Inaceptable. Requiere tratamiento inmediato y la implementación de controles robustos. La actividad asociada no debe iniciarse o debe cesar hasta que el riesgo se reduzca.

Riesgo Alto (6): Inaceptable. Requiere atención prioritaria por parte de la dirección y un plan de tratamiento detallado con plazos definidos.

Riesgo Medio (3-4): Tolerable bajo supervisión. El riesgo debe ser monitoreado y gestionado mediante procedimientos de control estándar. Se deben considerar opciones de tratamiento costo-efectivas.

Riesgo Bajo (1-2): Aceptable. El riesgo se gestiona mediante los procedimientos de rutina y no requiere acciones de tratamiento adicionales, pero debe mantenerse bajo revisión periódica.

Estos criterios serán aplicados de manera consistente en todo el proceso de apreciación del riesgo para asegurar una valoración objetiva y facilitar la priorización de las acciones de tratamiento, tal como se demostró en la clasificación de iniciativas del Plan Director de Seguridad (Gobierno Autónomo Descentralizado Municipal de Tena, 2025, p. 95).

5.5.4. Evaluación del riesgo

La evaluación del riesgo es el núcleo analítico del sistema. En el contexto del GAD Tena, este proceso no es un ejercicio estático, sino una evaluación dinámica que debe responder a cambios en el entorno de seguridad, actualizaciones tecnológicas y modificaciones en el marco legal ecuatoriano.

5.5.4.1. Generalidades

El proceso de evaluación del riesgo comprende tres etapas secuenciales e interdependientes: identificación, análisis y valoración. La DSCGR adoptará un enfoque holístico que considere tanto los riesgos operativos tradicionales (físicos y naturales) como los riesgos emergentes relacionados con la seguridad de la información y la ciberseguridad, áreas identificadas como críticas en el análisis de activos.

La evaluación se realizará bajo los principios de:

- Exhaustividad: Se considerarán todas las fuentes de riesgo, tangibles e intangibles, que puedan afectar los objetivos de la Dirección.
- Basado en Evidencia: El análisis se fundamentará en datos históricos del cantón, estadísticas de incidentes del ECU911, registros de fallas tecnológicas internas y el conocimiento experto del personal técnico.
- Trazabilidad: Cada riesgo evaluado quedará registrado documentalmente, permitiendo auditar la racionalidad de las decisiones de tratamiento.

Para la seguridad de la información, se utilizará la metodología MAGERIT como marco de referencia específico, dada su robustez para analizar activos tecnológicos como los servidores HP Proliant y los sistemas de información geográfica QGIS utilizados por la Dirección.

5.5.4.2. Identificación del riesgo

La identificación del riesgo busca generar un inventario completo de los eventos que podrían impedir el logro de los objetivos institucionales. En la DSCGR, este proceso comienza con el reconocimiento detallado de los activos críticos y las amenazas asociadas.

Metodología de Identificación de Activos y Amenazas:

La identificación se basa en el levantamiento de inventarios de activos y la revisión de procesos. Según el diagnóstico institucional, se han identificado activos de información y tecnológicos que son el soporte de la operación de seguridad ciudadana.

Inventario de Activos Críticos Sujetos a Riesgo: El primer paso es reconocer qué se está protegiendo. En la DSCGR, los activos se clasifican en hardware, software, información y personal:

Infraestructura de Servidores y Virtualización: La Dirección depende críticamente de un servidor HP Proliant DL120 Gen9, el cual aloja servicios virtualizados mediante Proxmox. Este servidor ejecuta el sistema operativo Ubuntu Server LTS y soporta aplicaciones misionales como PostgreSQL (base de datos), Tomcat y GeoServer.

- *Riesgo Inherente:* La centralización de servicios en un único servidor físico representa un punto único de fallo. Si este activo colapsa, se detiene la capacidad de gestión de información geoespacial y catastral vinculada a riesgos.

Sistemas de Información y Aplicaciones:

- **SIGPro y QGIS:** Herramientas fundamentales para el análisis territorial y la cartografía de amenazas naturales.
- **Sistema Quipux:** Plataforma de gestión documental oficial.
- **Carbonio:** Sistema de correo electrónico institucional, vital para la comunicación formal.
- **Sistemas de Videovigilancia:** Cámaras de circuito cerrado que monitorean accesos y seguridad física.
- Equipos de Usuario Final:

- Computadoras de escritorio y portátiles asignadas al Director, Coordinadores y Analistas. Se ha identificado que estos equipos operan con Windows 10 y cuentan con antivirus (ESET/Kaspersky), pero carecen de políticas restrictivas de hardware.

Identificación de Amenazas y Vulnerabilidades: A partir de los activos, se han identificado amenazas específicas derivadas del contexto operativo y las debilidades de control existentes:

Amenaza de Interrupción del Suministro Eléctrico (R-TEC-01): El análisis de activos identifica el "Corte del suministro eléctrico" como una amenaza crítica para el router, el switch, el firewall Cisco y las cámaras de videovigilancia.

- Vulnerabilidad: Falta de generadores eléctricos de respaldo con capacidad suficiente para mantener la operatividad de toda la Dirección durante cortes prolongados. La dependencia exclusiva de la red pública en una zona con clima adverso aumenta la exposición.
- Amenaza de Fuga de Información y Acceso No Autorizado (R-INF-01):
- Se ha detectado el uso de cuentas personales de almacenamiento en la nube (Google Drive, etc.) para guardar información institucional y la ausencia de bloqueo de puertos USB en las estaciones de trabajo.
- Vulnerabilidad: Los funcionarios pueden extraer bases de datos sensibles

(catastros, mapas de riesgos, datos personales de ciudadanos) mediante memorias USB sin ningún control técnico, o subir documentos oficiales a nubes privadas fuera del control del GAD.

Amenaza de Obsolescencia y Fallo de Software (R-TEC-02): El uso de software que requiere renovación de licencias (como se evidencia en la contratación para mantenimiento del programa PUNIS) y la necesidad de reinstalación de sistemas operativos (Ubuntu Server) sugieren riesgos asociados a la continuidad del soporte técnico y la integridad de los datos durante migraciones.

Amenaza de Discontinuidad Operativa por Personal (R-OP-01):

La estructura organizacional define roles clave como el Director y Coordinadores, pero las limitaciones legales (LOSEP) y la falta de protocolos formalizados para la disponibilidad 24/7 generan el riesgo de que, ante una emergencia fuera de horario laboral, la cadena de mando no responda con la inmediatez requerida.

Amenaza Legal por Incumplimiento de Protección de Datos (R-LEG-01):

El sitio web institucional carece de una política de cookies clara y formularios de consentimiento adecuados para la recolección de datos, contraviniendo la Ley Orgánica de Protección de Datos Personales (LOPDP). Esto expone a la institución a sanciones y pérdida de reputación.

5.5.4.3. Análisis del riesgo

El análisis del riesgo busca comprender la naturaleza de las amenazas identificadas y determinar su nivel de riesgo mediante la estimación de la probabilidad de ocurrencia y la magnitud de las consecuencias.

Metodología de Análisis (Probabilidad x Impacto): La DSCGR utilizará una escala cualitativa de 1 a 3 para probabilidad e impacto, conforme a la metodología simplificada MAGERIT aplicada en el Plan Director de Seguridad.

Criterios de Análisis:

Probabilidad (P):

- 1 (Baja): Evento anual o menos frecuente.
- 2 (Media): Evento mensual o posible.
- 3 (Alta): Evento semanal o inminente.
- **Impacto (I):**
- 1 (Bajo): Sin consecuencias relevantes.
- 2 (Medio): Consecuencias reseñables, interrupción parcial.
- 3 (Alto): Consecuencias graves, interrupción total, daño legal o reputacional severo.

Desarrollo del Análisis para Escenarios Críticos del GAD Tena:

Escenario 1: Corte de Energía en la Sala de Monitoreo

- Activo: Servidores, Cámaras, Red.
- Amenaza: Fallo de suministro eléctrico regional.

- Análisis de Probabilidad: El contexto amazónico presenta frecuentes tormentas eléctricas e inestabilidad en la red. Se estima una probabilidad Media (2).
- Análisis de Impacto: La falta de energía apaga el "ojo" de la seguridad ciudadana y desconecta los servidores de gestión de riesgos (GeoServer). Esto impide la coordinación de emergencias en tiempo real. Se valora como impacto Alto (3).
- Cálculo del Riesgo: 2 x 3 = 6 (Alto).

Escenario 2: Exfiltración de Datos Sensibles vía USB

- Activo: Bases de datos de catastro y riesgos, PC de analistas.
- Amenaza: Fuga de información por empleado desleal o negligencia.
- Análisis de Probabilidad: Al no existir restricciones técnicas (puertos USB abiertos) ni controles de DLP, y dado el uso de nubes personales, la facilidad de ocurrencia es muy alta. Se estima una probabilidad Alta (3).
- Análisis de Impacto: La divulgación de datos personales de ciudadanos o vulnerabilidades estratégicas del cantón tendría consecuencias legales severas bajo la LOPDP y pérdida de confianza pública. Se valora como impacto Alto (3).
- Cálculo del Riesgo: 3 x 3 = 9 (Extremo).

Escenario 3: Pérdida de Datos por Fallo de Servidor Único

- Activo: Servidor HP Proliant DL120 (Virtualización Proxmox).
- Amenaza: Error de hardware o corrupción de software sin backup verificado.
- Análisis de Probabilidad: Aunque el servidor es robusto, la falta de políticas de backup verificadas regularmente (evidenciado por los "NO" en el Check List PDS) aumenta la probabilidad de pérdida definitiva ante un fallo. Se estima probabilidad **Media (2)**.

Análisis de Impacto*:* La pérdida de la configuración de GeoServer, PostgreSQL y los datos históricos de gestión de riesgos sería catastrófica para la planificación territorial. Impacto **Alto (3)**.

Cálculo del Riesgo: 2 x 3 = **6 (Alto)**.

5.6.4.4. Valoración del riesgo

La valoración implica comparar los resultados del análisis con los criterios de aceptación de riesgo de la institución para priorizar el tratamiento. La DSCGR, dada su misión crítica de protección ciudadana, mantiene un apetito de riesgo bajo para eventos que comprometan la disponibilidad operativa o la confidencialidad de datos sensibles.

Matriz de Priorización de Riesgos del GAD Tena: Utilizando los valores calculados, se clasifican los riesgos para la toma de decisiones:

Tabla 41.

Matriz de priorización de riesgos

Nivel de Riesgo (P x I)	Prioridad	Acción Requerida	Riesgos Identificados en este Nivel
9 (Extremo)	Crítica	Tratamiento Inmediato e Ineludible.	Fuga de Información (USB/Nube): La exposición de datos es inaceptable. Se requiere intervención técnica urgente.
6 (Alto)	Alta	Tratamiento Prioritario a Corto Plazo.	Corte Eléctrico: La discontinuidad del servicio compromete la misión. Requiere inversión en infraestructura. Pérdida de Equipos: Robo de laptops o dispositivos móviles sin cifrado.

3-4 (Medio)	Media	Gestión mediante Procedimientos.	Caída de Software (Carbonio): Interrupción temporal del correo. Gestión con soporte técnico.
1-2 (Bajo)	Baja	Aceptación y Monitoreo.	Fallos menores de hardware en estaciones no críticas.

La valoración concluye que los riesgos relacionados con la seguridad de la información (ciberseguridad) y la continuidad del negocio (infraestructura eléctrica) superan los niveles de tolerancia de la organización y deben ser objeto de planes de tratamiento específicos y financiados.

5.5.5. Tratamiento del riesgo

Una vez priorizados los riesgos, la DSCGR debe seleccionar e implementar opciones para modificarlos. Este proceso implica no solo decisiones técnicas, sino también la asignación de recursos financieros dentro del presupuesto municipal.

5.5.5.1. Generalidades

El tratamiento del riesgo en el sector público debe equilibrar el costo de la implementación con el beneficio social y operativo. Las opciones de tratamiento deben alinearse con la normativa legal (Ley de Contratación Pública) y técnica (Normas INEN, ISO 27001).

El enfoque general será:

- Protección de Activos Críticos: Priorizar inversiones que aseguren la disponibilidad de los servidores y la red.
- Fortalecimiento del Control Interno: Implementar políticas y procedimientos que reduzcan la vulnerabilidad humana sin costo financiero excesivo.
- Transferencia Financiera: Considerar seguros para bienes físicos, aunque el riesgo operativo debe ser mitigado internamente.

5.5.5.2. Selección de las opciones para el tratamiento del riesgo

Basado en la valoración, se seleccionan las siguientes opciones estratégicas para los riesgos principales:

Opción A: Reducción del Riesgo (Mitigación) para el Corte Eléctrico (Riesgo Alto)

- Análisis: No es posible "evitar" los cortes de luz regionales. La aceptación no es viable dado el impacto en seguridad.
- Opción Seleccionada: Implementar redundancia energética.
- Justificación: La adquisición de un generador eléctrico es la única medida que

garantiza la continuidad de la sala de monitoreo y los servidores Proliant. Aunque implica un costo alto, el beneficio en seguridad ciudadana lo justifica.

- Diferenciación: Un UPS estándar solo permite el apagado seguro; un generador permite la operación continua.

Opción B: Reducción del Riesgo para Fuga de Información (Riesgo Extremo)

- Análisis: El uso de USBs y nubes personales es una práctica cultural y técnica no controlada.
- Opción Seleccionada: Implementación de controles técnicos restrictivos y formalización de políticas.
- Justificación: Bloquear puertos USB y restringir el acceso web a nubes personales mediante el firewall son medidas de bajo costo y alta efectividad. Complementariamente, se deben cifrar los discos duros de las laptops (BitLocker) para mitigar el impacto en caso de robo.

Opción C: Evitar/Reducir el Riesgo Legal (Protección de Datos)

- Opción Seleccionada: Adecuación normativa del sitio web y gestión documental.
- Justificación: Implementar políticas de cookies y avisos legales en tena.gob.ec es obligatorio por ley. No hacerlo conlleva sanciones pecuniarias.

Opción D: Compartir el Riesgo de Obsolescencia Tecnológica

- Opción Seleccionada: Contratación de Soporte Especializado (Outsourcing).

- Justificación: El mantenimiento del servidor HP Proliant, la configuración de Ubuntu Server y Proxmox requieren conocimientos especializados que pueden no estar siempre disponibles in-house. Contratar empresas como la identificada en los antecedentes (PROACTINFO) transfiere el riesgo técnico de fallo al proveedor mediante SLAs (Acuerdos de Nivel de Servicio).

5.5.5.3. Preparación e implantación de los planes de tratamiento del riesgo

Para materializar las opciones seleccionadas, se estructuran planes de acción concretos con asignación presupuestaria y responsables, integrando los datos financieros identificados en la planificación institucional.

Tabla 42.

Plan de Acción Nro. 1: Continuidad Energética y Resiliencia

Componente	Detalle Operativo
Riesgo Atendido	Interrupción de servicios críticos por fallo eléctrico (Router, Switch, Servidores, Cámaras).
Acción	Adquisición, instalación y puesta en marcha de un Generador Eléctrico de alta capacidad con transferencia automática para el edificio de la DSCGR.

Recursos Financieros	$90,000.00 USD. Este monto debe incluirse en el Plan Anual de Contratación (PAC) y el presupuesto de inversión.
Responsable	Dirección Administrativa (Proceso de Compras) y Dirección de TICs (Validación Técnica).
Cronograma	Inicio: Enero 2026. Adjudicación: Marzo 2026. Instalación: Mayo 2026.
Beneficio Esperado	Autonomía operativa 24/7, garantizando que el sistema de videovigilancia y los datos de gestión de riesgos estén disponibles durante emergencias climáticas.

Tabla 43.

Plan de Acción Nro. 2: Fortalecimiento de la Ciberseguridad

Componente	Detalle Operativo
Riesgo Atendido	Fuga de información, acceso no autorizado, malware por USB.
Acciones	1. Implementación de políticas de grupo (GPO) para bloqueo de puertos USB de almacenamiento masivo. 2. Cifrado de discos duros en portátiles del Director y Analistas.

	3. Configuración de reglas en Firewall Cisco para bloquear nubes personales no autorizadas. 4. Actualización de licencias de software y parches de seguridad.
Recursos Financieros	$2,000.00 USD para licencias de software de seguridad o consultoría específica.
Responsable	Dirección de TICs (Ejecución técnica).
Cronograma	Implementación inmediata (Primer trimestre 2026).
Beneficio Esperado	Reducción drástica de la superficie de ataque y cumplimiento con principios de confidencialidad de la información.

Tabla 44.

Plan de Acción Nro. 3: Seguridad Física de Activos

Componente	Detalle Operativo
Riesgo Atendido	Robo de equipos informáticos (PC, Laptops) dentro de las instalaciones.

	Acción	Instalación de anclajes de seguridad (guayas), control de acceso biométrico a áreas sensibles (servidores/monitoreo) y lockers seguros.
	Recursos Financieros	$5,000.00 USD.
	Responsable	Dirección Administrativa.
	Cronograma	Ejecución hasta Marzo 2026.

5.6.6. Seguimiento y revisión

El entorno de riesgos en Tena es volátil. El seguimiento y la revisión aseguran que los planes de tratamiento implementados sigan siendo efectivos y que el análisis de riesgos se mantenga actualizado frente a cambios en el contexto (ej. nuevas amenazas cibernéticas o cambios en la legislación).

Mecanismos de Monitoreo:

Indicadores Clave de Riesgo (KRI): Se definirán métricas para monitorear la salud del sistema.

- KRI Disponibilidad: Tiempo de actividad (Uptime) del servidor HP Proliant y servicios asociados (GeoServer). Meta: 99.9%.
- KRI Seguridad: Número de intentos de conexión USB bloqueados por mes.

- KRI Incidencias: Número de cortes de energía gestionados exitosamente por el generador sin caída de servicios.
- Revisiones Periódicas de Seguridad: La Dirección de TICs realizará revisiones trimestrales de los logs de seguridad del Firewall Cisco y del servidor Ubuntu para detectar anomalías o intentos de intrusión no reportados. Asimismo, se verificará el estado de las copias de seguridad (Backups), una debilidad detectada en el diagnóstico inicial (Check List PDS marcó "NO" en verificación de backups).1
- Revisión por la Dirección: Semestralmente, el Director de la DSCGR revisará el estado de la implementación de los planes de tratamiento (ej. avance en la compra del generador) y la evolución del mapa de riesgos. Se evaluará si los recursos asignados ($90k, $5k, $2k) han sido ejecutados eficazmente o requieren ajustes presupuestarios.
- Integración de Cambios: Si se adquieren nuevos activos (ej. drones para monitoreo) o se implementan nuevos sistemas (ej. un nuevo ERP municipal), el proceso de evaluación de riesgos (5.6.4) debe activarse nuevamente para analizar las nuevas vulnerabilidades introducidas antes de su puesta en producción.

5.5.7. Registro e informe

La gestión de riesgos debe ser auditable y transparente. El registro adecuado de las actividades y decisiones es fundamental para la mejora continua y para demostrar la debida diligencia ante entes de control como la Contraloría General del Estado.

5.5.7.1. Medios de comunicación

La comunicación de los riesgos y las acciones de tratamiento debe fluir vertical y horizontalmente dentro del GAD Tena.

Tabla 45.

Matriz de Comunicación de Riesgos

Destinatario	Información a Comunicar	Medio / Canal	Frecuencia	Propósito
Alcaldía y Concejo	Informe Ejecutivo de Riesgos (Estado de riesgos críticos, avance de inversiones como el generador).	Oficio (Quipux) y Presentación en Sesión.	Semestral	Asegurar respaldo político y presupuestario.
Personal Técnico (Analistas)	Políticas de seguridad (ej. prohibición de USB), Alertas de	Correo Institucional (Carbonio),	Mensual / Por evento	Generar cultura de seguridad y cumplimiento.

	amenazas (phishing, virus), Procedimientos operativos seguros.	Reuniones de equipo, Intranet.		
Dirección de TICs	Requerimientos de configuración técnica, reportes de incidentes de ciberseguridad.	esa de Ayuda, Reuniones de Coordinación.	Permanente	Coordinar la implementación técnica de controles.
Ciudadanía	Políticas de privacidad, uso de datos, avisos legales en la web.	Sitio Web tena.gob.ec, Avisos Legales.	Permanente	Cumplimiento legal y transparencia.

5.6.7.2. Cronograma de actividades para la implementación de procesos de mejora

Basado en la priorización de iniciativas del Plan Director de Seguridad [1], se establece el siguiente cronograma maestro para la implementación de las mejoras críticas durante el primer semestre de 2026.

Tabla 46.

Cronograma de Implementación - Primer Semestre 2026

Actividad/Proyecto	Enero	Febrero	Marzo	Abril	Mayo	Junio	Responsable	Estado Inicial
1. Continuidad Elaboración de TDRs para Generador ($90k)	X						Admin.	Pendiente
Proceso de Licitación y Adjudicación		X	X				Compras	Pendiente
Instalación y Pruebas de Carga				X	X		Admin/TICs	Pendiente
2. Seguridad de la Información								
Auditoría de Activos y Accesos Actuales	X						TICs	En Proceso
Implementación de Bloqueo USB y Cifrado		X					TICs	Pendiente

Actualización de Licencias y Parches ($2k)		X		TICs	Pendiente
3. Seguridad Física					
Instalación de anclajes y seguridad física ($5k)		X		Admin.	Pendiente
4. Gestión Normativa					
Redacción y publicación Política de Cookies/Privacidad	X			Legal/TICs	Crítico
5. Auditoría Interna de Seguimiento			X	Auditoría	Planificado

5.5.8. Auditoría interna

La auditoría interna es el mecanismo de verificación independiente que asegura que el sistema de gestión de riesgos funciona según lo planificado y es conforme con la norma ISO 31000 y los requisitos internos del GAD Tena.

5.5.8.1. Objetivos de la Auditoría interna

El objetivo principal es proporcionar a la Alta Dirección (Alcalde y Director de la DSCGR) un aseguramiento objetivo sobre la eficacia de la gestión del riesgo.

Objetivos Específicos:

- Verificar la Conformidad: Determinar si los controles de seguridad implementados (bloqueos USB, backups, generador) cumplen con las políticas definidas en el Manual de Seguridad y el Plan Director.
- Evaluar la Eficacia: Comprobar si los planes de tratamiento han reducido efectivamente el nivel de riesgo residual. Por ejemplo, verificar si el generador realmente enciende ante un corte simulado.
- Identificar Brechas: Detectar activos no inventariados, vulnerabilidades no parcheadas o procedimientos no seguidos por el personal.
- Validar Datos: Asegurar que la información reportada en los inventarios de activos y matrices de riesgo corresponde a la realidad operativa (ej. verificar si el servidor HP Proliant tiene el sistema operativo Ubuntu actualizado como se declara).

5.5.8.2. Procesos de la Auditoría interna

El proceso de auditoría se estructurará en fases claras, utilizando como base las listas de verificación (Check List PDS) desarrolladas en el diagnóstico inicial.

Fase 1: Planificación de la Auditoría

- Alcance: Procesos de Seguridad Ciudadana, Gestión de Riesgos, Infraestructura Tecnológica de la DSCGR.
- Criterios: Norma ISO 31000:2018, Políticas Internas, LOPDP.
- Equipo Auditor: Personal competente e independiente (puede ser de la Unidad de Auditoría Interna del GAD o externo).

Fase 2: Ejecución (Trabajo de Campo): Se aplicarán pruebas de cumplimiento y sustantivas. Se utilizará el "Check List PDS" 1 para verificar el estado de los controles que fueron marcados como "NO" o deficientes en el diagnóstico previo.

Cuestionario de Auditoría (Muestra basada en hallazgos previos)

Tabla 47.

Cuestionario de auditoría

Control a Auditar	Pregunta de Verificación	Método de Prueba	Referencia Diagnóstico
Política de Seguridad	¿Se ha aprobado y difundido formalmente la política de seguridad?	Entrevista y revisión documental.	ID_0001 (Estaba NO)

Copias de Seguridad		¿Se realizan backups regulares según política? ¿Se han realizado pruebas de restauración?	Revisión de logs de backup y acta de prueba de restauración.	ID_0012, ID_0013 (Estaba NO)
Control de Acceso Físico		¿Están protegidos los equipos críticos (servidores) en áreas de acceso restringido?	Inspección visual de la sala de servidores.	ID_0010 (Estaba NO)
Incidentes	Gestión de	¿Existe un registro formal de los incidentes de seguridad ocurridos en el último periodo?	Revisión del libro de novedades o sistema de tickets.	ID_0023 (Estaba NO)
Web	Privacidad	¿El sitio web muestra el aviso de cookies y política de privacidad al ingresar?	Navegación en tena.gob.ec.	Análisis Web 3.11

Fase 3: Informe de Auditoría: El auditor elaborará un informe detallando los hallazgos, clasificándolos en Fortalezas, No Conformidades (Mayores/Menores) y Oportunidades de Mejora.

- **5.5.8.3. No conformidades y acciones correctivas**

La detección de una No Conformidad (NC) activa obligatoriamente un proceso de acción correctiva para eliminar la causa raíz del problema.

- Procedimiento de Gestión de No Conformidades:
- Identificación: El auditor documenta el hallazgo.
- Ejemplo de NC: "Se evidenció que tres funcionarios de la DSCGR utilizan memorias USB personales para transferir mapas de riesgos, a pesar de la política de prohibición. El control técnico de bloqueo de puertos no está activo en sus estaciones."
- Análisis de Causa Raíz: El responsable del proceso (Director de TICs / Director de Seguridad) debe investigar por qué ocurrió.
- Causa Raíz: La política de grupo (GPO) no se aplicó correctamente a esa unidad organizativa en el directorio activo, o los funcionarios desconocen la norma por falta de capacitación.

Plan de Acción Correctiva:

- Corrección Inmediata: Aplicar el bloqueo de puertos en las máquinas afectadas.

- Acción Correctiva (Largo Plazo): Revisar la configuración global de las GPO y realizar una campaña de re-inducción sobre seguridad de la información.
- Seguimiento y Cierre: En la siguiente auditoría, se verifica si el problema ha reaparecido. Si no, se cierra la NC.

Este ciclo de auditoría y mejora continua es lo que garantiza que la inversión realizada en planes de tratamiento (generadores, seguridad, etc.) se mantenga en el tiempo y aporte valor real a la seguridad de los ciudadanos de Tena.

6. CONCLUSIONES Y APLICACIONES

6.1. Conclusiones generales

El estudio demuestra que la Dirección de Seguridad Ciudadana y Gestión de Riesgos (DSCGR) del GAD Municipal del Tena operaba bajo un enfoque reactivo debido a la falta de un marco formal para proteger sus activos críticos. Se concluye que la identificación de activos sensibles, como el servidor HP Proliant y los sistemas de georreferenciación, es el pilar fundamental para asegurar la continuidad de los servicios de seguridad y respuesta ante emergencias en el cantón.

6.2. Conclusiones específicas

6.2.1. Análisis del cumplimiento de los objetivos de la investigación

- Identificación y evaluación: Se logró diagnosticar la situación actual mediante un Check List del Plan Director de Seguridad, identificando amenazas críticas como accesos no autorizados y fallas tecnológicas.
- Diseño de controles: Se diseñaron planes de acción específicos para mitigar riesgos, incluyendo el fortalecimiento de la ciberseguridad y la seguridad física de los activos.
- Mejora continua: Se estableció un proceso de seguimiento mediante

indicadores clave de desempeño (KRI) y un esquema de auditoría para garantizar la protección de datos personales a largo plazo

6.2.2. Contribución a la gestión empresarial

El estudio ayuda a optimizar la administración institucional del Gobierno Autónomo Descentralizado Municipal por medio de una estructura de gobernanza para la gestión del riesgo informático. El estudio propone una Matriz de Roles y Responsabilidades, que establece con claridad las tareas de cada área en la custodia, manejo y protección de la información institucional. Esto hace que haya menos ambigüedad en la toma de decisiones y en la distribución de responsabilidades.

Además, el estudio sugiere medidas para optimizar la distribución de recursos operativos y tecnológicos, así como la ejecución de planes de continuidad energética. Esto hace posible que la institución mejore su capacidad de reacción ante interrupciones del servicio eléctrico o incidentes tecnológicos.

6.2.3. Contribución a nivel académico

Desde el campo académico, la investigación ofrece un caso de estudio aplicado que analiza la aplicación de la norma ISO 31000 en entidades públicas de Ecuador, en particular en gobiernos autónomos descentralizados situados en la región amazónica.

La investigación muestra cómo se pueden adaptar las metodologías internacionales para la gestión de riesgos a la realidad de la administración pública local, teniendo en cuenta

restricciones normativas, organizacionales y tecnológicas. Además, el estudio combina la evaluación de los riesgos operativos con la protección de los datos personales. Esto puede ser útil como guía metodológica para futuros estudios que traten sobre la seguridad de la información en organizaciones públicas que gestionan información delicada de los ciudadanos.

6.2.4. Contribución a nivel personal

La realización de esta investigación posibilita que los autores robustecieran sus habilidades profesionales en la identificación, análisis y evaluación de riesgos informáticos al aplicar metodologías reconocidas como ISO 31000 y MAGERIT.

El proceso de investigación, además, ayuda a desarrollar competencias en el diseño de propuestas para mejorar la gestión institucional, así como en la planificación de controles y el análisis estratégico. Desde una perspectiva profesional, el proyecto fortalece la percepción de la seguridad de la información como un aspecto esencial para garantizar transparencia, eficacia administrativa y salvaguardar los datos del público.

6.3. Limitaciones a la Investigación

Restricciones de personal: La Ley Orgánica del Servicio Público (LOSEP), que es el marco legal en vigor, fija pautas rigurosas para la distribución y reasignación de los empleados al interior de las instituciones públicas. Esta regulación impide la opción de contar

con personal extra o reestructurar los turnos para asegurar una cobertura operativa continua (24/7), lo que limita el análisis de situaciones de continuidad operativa en condiciones óptimas.

Ausencia de datos históricos: La entidad no había tenido antes inventarios bien organizados de activos ni registros formales y sistemáticos de sucesos o incidentes riesgosos. La falta de información histórica dificulta la realización de análisis estadísticos rigurosos acerca de la probabilidad o frecuencia de ciertas amenazas, por lo que la valoración de riesgos tiene que basarse mayormente en criterios cualitativos y en la experiencia de expertos institucionales.

Dependencia tecnológica: La infraestructura tecnológica de la institución y las decisiones sobre el presupuesto tomadas por la Dirección de Tecnologías de la Información y Comunicación (TIC) son determinantes para que se pongan en marcha y sean eficaces diversas medidas propuestas en el sistema de gestión de riesgos. Como resultado, la implementación total de ciertos controles técnicos podría depender de la planificación tecnológica de dicha dependencia y de los recursos financieros disponibles.

7. Referencias

Asamblea Nacional del Ecuador. Código Orgánico de Organización Territorial Autonomía y Descentralización. Obtenido de Registro Oficial Suplemento 303 de 19 de octubre de 2010. https://www.cpccs.gob.ec/wp-content/uploads/2020/01/cootad.pdf.

De, D. L. 0. R. O. 449. (s/f). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008*. Oas.org. Recuperado el 29 de enero de 2026, de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf?utm_source=chatgpt.com

De, L. 0. R. O. S. 303. (s/f). *CODIGO ORGANICO DE ORGANIZACION TERRITORIAL, COOTAD*. Gob.ec. Recuperado el 29 de enero de 2026, de https://www.cpccs.gob.ec/wp-content/uploads/2020/01/cootad.pdf

De, L. 0. R. O. S. 488. (s/f). *LEY ORGÁNICA PARA LA GESTIÓN INTEGRAL DEL RIESGO DE DESASTRES*. Edu.ec. Recuperado el 29 de enero de 2026, de https://procuraduria.utpl.edu.ec/NormativaExterna/LEY%20ORG%C3%81NICA%20PARA%20LA%20GESTI%C3%93N%20INTEGRAL%20DEL%20RIESGO%20DE%20DESASTRES.pdf

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

ISO 31000:2018. (2024). ISO. https://www.iso.org/iso-31000-risk-management.html

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Montoro-Cazorla, D., & Pérez-Ocón, R. (2016). A warmstandby system under shocks and repair governed by MAPs. *Reliability Engineering & System Safety*, *152*, 331–338. https://doi.org/10.1016/j.ress.2016.03.023

Nacional, A., Ingeniero, S., Pozo Barrezueta, H. D., & Atentamente, D. J. (s/f). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Ley 0 Registro Oficial Suplemento 459 de 26-may.-2021 Estado: Vigente*. Gob.ec. Recuperado el 29 de enero de 2026, de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Reason, J. (2016). *Managing the risks of organizational accidents*. Routledge.

Renn, O. (2017). *Risk governance: Coping with uncertainty in a complex world*. https://doi.org/10.4324/9781849772440

Universidad Central del Ecuador, & Lahuasi Criollo, J. E. (2023). Aplicabilidad de la ISO 31000:2018 en la gestión del riesgo crediticio de los fondos complementarios previsionales

cerrados del sector público. *Revista Científica Retos de la Ciencia*, *7*(14), 28–38.

https://doi.org/10.53877/rc.7.14.202301010

ANEXOS

ANEXO 1

Borrador de la Política de Gestión de Riesgos del GAD Tena en la Dirección de Seguridad Ciudadana y Gestión de Riesgos

1. Propósito

Establecer los principios, el compromiso y las directrices que guiarán el diseño, la implementación, el mantenimiento y la mejora continua del Marco de Gestión de Riesgos en la Dirección de Seguridad Ciudadana y Gestión de Riesgos, de conformidad con la norma ISO 31000:2018.

2. Importancia y Razón de la Implementación

Importancia: La gestión de riesgos es vital para proteger y crear valor institucional, minimizando la incertidumbre ante amenazas que comprometen la vida, la integridad de los activos y la misión de servicio público.

Razón (Por qué se implementa): El GAD Tena, a través de su Dirección, busca migrar de una cultura reactiva a una proactiva, asegurando la continuidad del servicio 24/7 y la toma de decisiones informada, especialmente ante la alta exposición a riesgos naturales y la necesidad de una respuesta ininterrumpida de seguridad ciudadana.

3. Principios Fundamentales del Riesgo

La gestión de riesgos se regirá por los siguientes principios clave de la ISO 31000:

Principio	Aplicación
Integrada	La gestión del riesgo es parte intrínseca de la gobernanza, planificación estratégica y operaciones diarias.
Estructurada y Exhaustiva	Uso de metodologías uniformes (ISO 31000) para asegurar la consistencia en la evaluación y tratamiento de todos los riesgos.
Adaptada	El marco es proporcional y relevante al contexto geográfico, cultural y legal del cantón Tena.
Dinámica	El sistema anticipa, responde y se ajusta a los cambios (ej. nuevos riesgos delictivos, cambios climáticos o fallas operacionales).

Mejor Información Disponible	Las decisiones de riesgo se basan en datos verificables, estadísticas de incidentes y análisis profesionales.

Nota. Elaboración propia

4. Relación con la Gestión de Riesgos (Apetito y Criterios)

Apetito de Riesgo: La Dirección adopta un Apetito de Riesgo Bajo a Muy Bajo para todos los riesgos que puedan resultar en:

Pérdida de vidas humanas.

Interrupción del servicio de respuesta a emergencias (24/7).

Incumplimiento de la normativa legal (LOSEP, ordenanzas).

Compromiso Operacional: Se establece la obligación de implementar y adherirse estrictamente al Protocolo de Llamada Crítica Formal para garantizar la disponibilidad y la respuesta inmediata de los roles clave ante cualquier evento fuera de la jornada laboral que cumpla con los criterios de "asunto crítico profesional de seguridad y emergencia".

ANEXO 2

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)

Procedimientos relacionados:

- Manual del Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Norma Técnica de Gestión Documental y Archivo (Sector Público).
- Procedimiento de Control de Información Documentada.

Índice

Redactado por:	Revisado por:	Aprobado por:
Título y Nombre del Analista	Título y Nombre del Coordinador	Título y Nombre del Director
Analista de Riesgos	Coordinador de Unidad	Director de Seguridad Ciudadana

Nota. Elaboración propia.

1. OBJETIVO

Establecer la metodología estandarizada y los criterios técnicos para la redacción, revisión, aprobación, distribución y control de los Procedimientos Normalizados de Trabajo (PNT) dentro de la Dirección de Seguridad Ciudadana y Gestión de Riesgos del GAD Municipal de Tena.

El objetivo fundamental es garantizar la homogeneidad en la documentación del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST), facilitando la comprensión de las tareas críticas, minimizando la variabilidad en la ejecución de los procesos operativos y asegurando el cumplimiento de los requisitos de la norma ISO 45001:2018 y la normativa legal vigente. Este procedimiento busca orientar a los servidores públicos en la generación de documentos claros, útiles y auditables.

2. RESPONSABILIDAD DE APLICACIÓN Y ALCANCE

Responsabilidad:

La responsabilidad de aplicar este procedimiento recae sobre todo el personal de la Dirección (Técnicos, Analistas, Coordinadores y Administrativos) que tenga la tarea de documentar procesos o actividades.

- Redactores: Responsables de elaborar el contenido técnico veraz y conforme a este estándar.
- Revisores (Coordinadores): Responsables de verificar la idoneidad, coherencia técnica y transversalidad del documento.
- Aprobador (Director): Responsable final de autorizar la implementación del procedimiento y asignar los recursos necesarios para su ejecución.

Alcance:

Este procedimiento es de aplicación obligatoria para la elaboración de todos los documentos controlados del tipo "Procedimiento", "Instructivo", "Protocolo" o "Guía" que formen parte del SGSST de la Dirección de Seguridad Ciudadana y Gestión de Riesgos, abarcando tanto las actividades administrativas como las operaciones de campo en todo el territorio del cantón Tena.

3. DEFINICIONES

- Procedimiento: Documento que especifica la forma de llevar a cabo una actividad o un proceso. Responde a las preguntas: ¿Qué se hace?, ¿Quién lo hace?, ¿Cuándo se hace? y ¿Dónde se hace?.
- Procedimiento Normalizado de Trabajo (PNT): Documento escrito y aprobado que describe de forma específica, secuencial y detallada las operaciones a realizar en una tarea determinada, incorporando criterios de seguridad, calidad y eficiencia.

- Instructivo de Trabajo (IT): Documento técnico que describe detalladamente "cómo" realizar una tarea específica y limitada (ej. pasos para encender el generador eléctrico).
- Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas (ej. una lista de asistencia firmada).
- Revisión: Actividad emprendida para asegurar la conveniencia, adecuación y eficacia del tema objeto de la revisión.

4. DESCRIPCIÓN

Los procedimientos constituyen la base del conocimiento organizacional. Describen las actividades relacionadas directa o indirectamente con la gestión de riesgos, la seguridad ciudadana y la salud ocupacional.

Se distinguen los siguientes tipos de procedimientos según su naturaleza operativa:

- Procedimientos Generales (PG): Describen procesos transversales del sistema de gestión (ej. Control de Documentos, Auditorías, Gestión del Cambio, Revisión por la Dirección).
- Procedimientos Operativos de Seguridad (OS): Describen las tácticas y protocolos de actuación de la seguridad ciudadana (ej. Patrullaje Preventivo, Control de Espacio Público, Uso de la Fuerza Progresiva).
- Procedimientos de Gestión de Riesgos (GR): Describen las actividades técnicas de la Unidad de Riesgos (ej. Inspección Técnica de Amenazas, Elaboración de Informes de Vulnerabilidad, Monitoreo de Caudales).
- Procedimientos de Respuesta a Emergencias (PE): Protocolos de actuación inmediata ante eventos adversos (ej. Evacuación por Inundación, Primeros Auxilios, Conato de Incendio).

Todos los documentos tendrán el mismo formato gráfico e identidad visual, iniciando con una portada estandarizada (Página 1) y continuando con el desarrollo del contenido en las páginas subsiguientes.

Portada y Encabezado:

Como encabezamiento de todas las páginas debe aparecer una tabla (bloque) con la siguiente información:

- Logotipo: Escudo del GAD Municipal de Tena (Izquierda) y/o Dirección.
- Título: Nombre descriptivo y único del procedimiento.
- Código: Identificador alfanumérico único.
- Paginación: Número de página actual y total (Página X de Y).
- Revisión: Número de la versión vigente (Rev.: XX).
- Fecha de Edición: Mes y año de la aprobación.

Sistema de Codificación:

El número de código se construirá bajo la siguiente estructura lógica: GAD-DSCGR-SST--[NUM]-

- GAD: Gobierno Autónomo Descentralizado.
- DSCGR: Dirección de Seguridad Ciudadana y Gestión de Riesgos.
- SST: Sistema de Gestión de Seguridad y Salud.
- : PG, OS, GR, PE (según clasificación anterior).
- [NUM]: Número consecutivo de tres dígitos (001, 002,...).
- : Versión del documento (01, 02,...).

Ejemplo: GAD-DSCGR-SST-GR-005-01 (Quinto procedimiento de Gestión de Riesgos, versión 1).

Pie de Página (Primera Página):

Debe incluir obligatoriamente las firmas de responsabilidad que validan el documento, indicando Nombre, Cargo, Firma y Fecha para: Redactor, Revisor y Aprobador.

4.1. Apartados de los Procedimientos Normalizados de Trabajo

Para asegurar la completitud y utilidad de los documentos, todos los PNT deberán contener, como mínimo, los siguientes apartados numerados:

1. **Objetivo:** Explicar clara, breve y concisamente el propósito del procedimiento. Debe indicar qué se pretende lograr con su ejecución.
2. **Responsabilidad de aplicación y alcance:**
   - Definir taxativamente los cargos o roles responsables de cumplir y hacer cumplir el procedimiento.
   - Delimitar el ámbito de aplicación (áreas, procesos, ubicaciones geográficas).
3. **Definiciones:** Glosario de términos técnicos, siglas o acrónimos utilizados en el texto. Esto es vital para evitar interpretaciones erróneas, especialmente en temas técnicos de riesgos o legales.
4. **Descripción:** Es el núcleo del documento. Describe el desarrollo secuencial de las actividades.
   - Debe detallar los pasos lógicos del proceso.
   - Debe integrar las medidas de seguridad y salud (peligros y controles) en cada paso relevante.
   - Puede estructurarse mediante texto narrativo, viñetas o diagramas de flujo.
   - Debe mencionar las herramientas, equipos o software necesarios (ej. QGIS, Radio, Quipux).
5. **Registros:** Listado de los formatos (formularios, listas de chequeo, actas) que se generan como evidencia de la ejecución del procedimiento. Se debe indicar el código del formato y el lugar de archivo (físico o digital). Si el procedimiento no genera

registros, se indicará "No aplica".

6. **Control de copias y registro de lectura del procedimiento:** Tabla destinada a registrar la trazabilidad de la distribución del documento y la firma de los usuarios como constancia de haber leído, comprendido y aceptado el procedimiento (Toma de Conciencia).
7. **Anexos:** Información complementaria necesaria para la ejecución del procedimiento (ej. mapas, tablas de referencia, normativas legales, diagramas técnicos).
    - **Anexo I - Control de revisiones:** Obligatorio en todos los documentos para registrar el historial de cambios.

4.2. Redacción de los Procedimientos

- Claridad y Concisión: Los procedimientos se redactarán de forma clara, directa y sencilla. Se deben evitar frases ambiguas o excesivamente complejas. El objetivo es que sean comprensibles por todo el personal que los va a aplicar, independientemente de su nivel jerárquico.
- Estilo: Se recomienda usar el modo imperativo (ej. "Verifique la conexión") o infinitivo (ej. "Verificar la conexión"). Mantener la consistencia en todo el documento.
- Aplicabilidad: Cuando alguno de los apartados descritos no sea necesario para un procedimiento específico, se indicará "No procede" o "No aplica", pero no se eliminará el apartado para mantener la estructura uniforme.
- Disponibilidad: Los procedimientos son de lectura y cumplimiento obligatorio. Deben estar en todo momento a disposición del personal en los puntos de uso (físicos o digitales).

4.3. Distribución

- Control de Distribución: La distribución de los procedimientos aprobados se

realizará de manera controlada por el Responsable del SGSST o la Secretaría de la Dirección.

- Copias: Se emitirán tantas copias controladas como sean necesarias para las áreas operativas (ej. una copia para la Sala de Crisis, una para el Archivo Central, una para cada Unidad Técnica).
- Identificación: Las copias físicas controladas llevarán un sello de "COPIA CONTROLADA" en color rojo (o distintivo similar) para diferenciarlas de las copias no controladas o fotocopias no autorizadas.
- Toma de Conocimiento: Todas las copias distribuidas deben ir acompañadas del registro de lectura, donde el personal firmará confirmando su recepción y entendimiento.
- Retiro de Obsoletos: Al aprobarse una nueva versión, las versiones anteriores (obsoletas) deberán ser retiradas inmediatamente de los puntos de uso y destruidas o marcadas como "OBSOLETO" para evitar su uso involuntario, conservándose únicamente una copia maestra en el archivo histórico por razones legales.

4.4. Revisión y Control de Cambios

- Periodicidad: Los procedimientos serán revisados periódicamente (al menos una vez al año) para asegurar que siguen siendo adecuados y eficaces.
    - Causas de Revisión: También se revisarán cuando ocurran cambios en:
    - La normativa legal aplicable.
    - La estructura organizacional o las funciones.
    - La tecnología o equipos utilizados.
    - Los resultados de la investigación de accidentes o incidentes que sugieran fallas en el procedimiento.
- Registro: Se incluye obligatoriamente, como Anexo I, un registro para

documentar el control de cambios. En él se indicará la versión del procedimiento, una descripción resumen de los cambios realizados y la fecha de aprobación.

- Actualización: Cuando se actualice un PNT, este registro (Anexo I) se actualizará y permanecerá siempre adjunto a la nueva versión vigente.

5. REGISTROS

Los registros que se derivan de la aplicación de este procedimiento son fundamentales para demostrar la conformidad del sistema de gestión.

- **Anexo I:** Registro de Control de Cambios (parte integral del documento).
- **GAD-DSCGR-SST-FT-001**: Lista Maestra de Documentos Internos (Registro donde se indexan todos los procedimientos vigentes).
- **GAD-DSCGR-SST-FT-002**: Registro de Distribución de Documentos (Control de entrega de copias).

6. CONTROL DE COPIAS Y REGISTRO DE LECTURA DEL PROCEDIMIENTO

Esta sección documenta la distribución del procedimiento y la toma de conciencia del personal. La firma en este registro implica que el servidor público ha sido capacitado o ha leído el documento y se compromete a cumplirlo.

Copia Número	Nombre del Servidor	Cargo / Área	Firma	Fecha
01 (Maestra)	Archivo Central	Secretaría Dirección		
02		[Nombre] Coord. Gestión Riesgos		

03	[Nombre]	Coord. Seguridad C.
04	[Nombre]	Analista de Riesgos
05	[Nombre]	Analista de Monitoreo
06	[Nombre]	Técnico de Campo
07	[Nombre]	Técnico de Campo
08	[Nombre]	Administrativo
09	[Nombre]	Chofer / Conductor
10	[Nombre]	Guardia de Turno
11	[Nombre]	Guardia de Turno

Nota. Elaboración propia.

Este espacio se reserva para continuar con el listado de personal en caso de que el número de servidores exceda el espacio de la página anterior, o para incluir observaciones específicas sobre la distribución (ej. restricciones de acceso a copias confidenciales).

Instrucciones de llenado:

1. El responsable de la distribución debe llenar el número de copia, nombre y cargo.
2. El servidor receptor debe firmar y fechar al momento de recibir la copia física o la notificación digital.

3. Este registro debe ser archivado por el Responsable del SGSST como evidencia de comunicación.

REGISTRO DE CONTROL DE CAMBIOS

Este anexo es obligatorio y debe acompañar a la última página de todos los procedimientos. Permite auditar la evolución del documento y entender las razones de las modificaciones.

PNT Código	Versión N°	Descripción de los Cambios Realizados	Motivo del Cambio	Fecha de Aprobación
GAD-DSCGR-SST-PG-001	01	Emisión Inicial del Documento. Establecimiento del estándar documental para el SGSST del GAD Tena.	Implementación inicial del Sistema de Gestión ISO 45001.	Diciembre 2025

Nota. Elaboración propia