Maestría en

GESTIÓN DE RIESGOS

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión de Riesgos

AUTORES:

Danilo Fabián Flores Núñez

Solís Miranda Holguer Steeven

Franklin Alexander Enríquez Josa

Fuentes Peñafiel Federico Alberto

TUTORES:

Paloma Manzano Martínez

Enrique Molina Suárez David

Genaro Benavides Gutiérrez

DISEÑAR UN SISTEMA DE GESTIÓN EN EL ALMACENAMIENTO Y SEGURIDAD DE TECNOLOGIAS MENOS LETALES, DE LA UNIDAD DE MANTENIMIENTO DEL ORDEN QUITO (Z09), BASADO EN LA NORMA ISO 31000:2018

Quito, Julio 2025

CERTIFICACIÓN DE AUTORÍA

Nosotros, Danilo Fabián Flores Núñez, Solís Miranda Holguer Steeven, Franklin Alexander Enríquez Josa y Fuentes Peñafiel Federico Alberto, 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:
DANILO FABIAN FLORES NUNEZ
Validar únicamente con FirmaEC

Danilo Fabián Flores Núñez

Firmado electrónicamente por:
HOLGUER STEEVEN SOLIS MIRANDA
Validar únicamente con FirmaEC

Solís Miranda Holguer Steeven

Firmado electrónicamente por:
FRANKLIN ALEXANDER ENRIQUEZ JOSA
Validar únicamente con FirmaEC

Franklin Alexander Enríquez Josa

Firmado electrónicamente por:
FEDERICO ALBERTO FUENTES PENAFIEL
Validar únicamente con FirmaEC

Fuentes Peñafiel Federico Alberto

AUTORIZACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Nosotros, Danilo Fabián Flores Núñez, Solís Miranda Holguer Steeven, Franklin Alexander Enríquez Josa y Fuentes Peñafiel Federico Alberto, en calidad de autores del trabajo de investigación titulado **Diseño de un Sistema de Gestión en el Almacenamiento y Seguridad de Tecnologías Menos Letales, de la Unidad de Mantenimiento del Orden Quito (Z09),** basado en la norma ISO 31000:2018, 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:
DANILO FABIAN FLORES NUNEZ
Validar únicamente con FirmaEC

Danilo Fabián Flores Núñez

Firmado electrónicamente por:
HOLGUER STEEVEN SOLIS MIRANDA
Validar únicamente con FirmaEC

Solís Miranda Holguer Steeven

Firmado electrónicamente por:
FRANKLIN ALEXANDER ENRIQUEZ JOSA
Validar únicamente con FirmaEC

Franklin Alexander Enríquez Josa

Firmado electrónicamente por:
FEDERICO ALBERTO FUENTES PENAFIEL
Validar únicamente con FirmaEC

Fuentes Peñafiel Federico Alberto

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, Paloma Manzano Martínez y David G. Benavidez Gutiérrez, declaramos que los graduandos: Danilo Fabián Flores Núñez, Solís Miranda Holguer Steeven, Franklin Alexander Enríquez Josa y Fuentes Peñafiel Federico Alberto, 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: 2025.07.28 10:54:15 +02'00'

Paloma Manzano Martínez
Directora de la
Maestría en Gestión de Riesgos

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

David G. Benavidez Gutiérrez
Coordinador de la
Maestría en Gestión de Riesgos

DEDICATORIA

A Dios, fuente infinita de fortaleza y sabiduría, por guiar mis pasos en este camino de superación. A mis padres, Jaime Fabián Flores Cevallos y Rosita del Carmen Núñez Mármol, pilares inquebrantables de mi vida, cuyos sacrificios y enseñanzas forjaron en mí el valor de la perseverancia y la humildad.

A mi amada esposa Dennis Karina Toro Morillo, cómplice incansable de mis sueños y sostén emocional en cada desafío. Gracias por transformar cada obstáculo en una oportunidad y por ser mi refugio en los momentos más intensos y difíciles.

A mi princesita, mi hermosa hija Danielita, luz de mis ojos, cuya sonrisa pura y curiosidad infinita me recuerdan diariamente el propósito de construir un futuro digno.

A mis amados hijos Diego, Daniel y Dariel, herederos de mi legado y razón suprema de mi lucha. Que cada logro mío inspire en ustedes la convicción de que no hay meta imposible cuando se trabaja con amor y disciplina. Esta conquista es, ante todo, un tributo a ustedes D6 porque son la razón de mi existir.

“Un hombre muere, pero la existencia forjada por sí mismo nunca desaparece en el cosmos del universo, porque quedan huellas en el pensamiento de los vivos”.

Danilo Fabián Flores Núñez

Ya te lo he ordenado: ¡Sé fuerte y valiente! no temas ni te desanimes, porque el Señor tu Dios estará contigo dondequiera que vayas." (José 1:9). Dedico este logro a Dios, por ser mi guía y fortaleza en cada paso de este viaje. Su luz ha iluminado mis momentos de duda y su amor me ha brindado la paz necesaria para seguir adelante.

A mi madre Rosa Ubaldina Miranda Rojas cuyo amor incondicional y sacrificio han sido fundamentales en mi vida sus consejos y apoyo constante me han enseñado la importancia de la perseverancia y la dedicación, gracias por ser mi mayor inspiración y por creer en mí incluso en los momentos más difíciles.

A mis hermanas Mishel e Isamar Solis por ser mis amigas y cómplices gracias por sus risas y compañía han hecho que cada reto sea más llevadero. Ustedes han sido un pilar en mi vida, siempre motivándome a alcanzar mis sueños y recordándome la importancia de la familia.

Y a mi novia Erika Paredes por su amor y paciencia inquebrantable, tu apoyo y aliento han sido esenciales en este proceso, y cada palabra de confianza ha fortalecido mi determinación. Este logro es un reflejo de lo que he aprendido de cada uno de ustedes, cada página está impregnada de su amor y apoyo. A todos ustedes, gracias por ser parte de mi vida y por hacer posible esta meta.

Solís Miranda Holguer Steeven

¿Acaso existe algo más importante que la familia? Quiero dedicar este logro en primer lugar a Dios, por permitirme día a día seguir adelante con salud y bienestar. Pues Dios es el único ser que puede cambiar nuestro destino.

A mi amada esposa Diana Elizabeth, gracias por estar presente en todo momento, en las buenas y malas. Gracias por incentivarme siempre a ser una mejor persona, tenga siempre presente que usted es la mejor profesional, esposa, madre e hija. Se que juntos saldremos adelante con un único objetivo el cual es tener una familia feliz y prospera.

A mis amados hijos Briseida Antonella y Christopher Alexander, quienes son la luz de mis ojos, dos personitas tan pequeñas que cada día con sus sonrisas llenan de alegría mi vida. Son ellos quienes me motivan a cumplir todos mis objetivos, esto siempre la misión y visión de que sus vidas sean llenas de felicidad.

A mi bella madre Albita, gracias por ser la persona quien con mucho esfuerzo supo sacarme adelante, quien a pesar de no tener comodidades me regalo la mejor profesión del mundo, gracias por ser esa mujer que nunca se rinde y cumple todos sus objetivos.

Esto es por todos ustedes con mucho amor.

Franklin Alexander Enríquez Josa

Dedicamos este trabajo, en primer lugar, a Dios, por guiarnos, darnos fuerza y ayudarnos a superar los momentos difíciles durante nuestra trayectoria estudiantil.

Agradecemos de todo corazón a nuestras familias, quienes han sido un pilar fundamental en este proceso. A nuestros padres, hermanos, parejas e hijos, quienes, con su amor, paciencia y apoyo incondicional, nos han motivado a seguir adelante y alcanzar esta meta.

También expresamos nuestra gratitud a los docentes, quienes nos han brindado su apoyo continuo y han sido parte importante en este logro.

De manera especial, agradecemos entre nosotros como compañeros de grupo, Danilo Fabián Flores Núñez, Holguer Steeven Solís Miranda, Franklin Alexander Enríquez Josa y Federico Alberto Fuentes Peñafiel, por la dedicación, compromiso, respeto y trabajo en equipo que hicieron posible este proyecto.

Cada esfuerzo compartido, cada idea aportada y cada momento vivido en este proceso quedará en nuestra memoria como una valiosa experiencia de crecimiento y aprendizaje.

Fuentes Peñafiel Federico Alberto

AGRADECIMIENTOS

Queremos expresar nuestro más sincero agradecimiento a la Universidad Internacional del Ecuador y a la Escuela Internacional de Gerencia por brindarnos la oportunidad de formarnos en instituciones de alto prestigio académico.

Nuestro reconocimiento especial es para todos los docentes, tanto nacionales como extranjeros, quienes compartieron generosamente sus conocimientos y experiencias, guiándonos en nuestro camino hacia el profesionalismo.

De manera particular, agradecemos a la Ing. Paloma Manzano Martínez, al Ing. David Genaro Benavides y al Ing. Enrique Molina Suárez, por su constante apoyo, acompañamiento y orientación, que fueron fundamentales para la elaboración y culminación de este Trabajo de Graduación.

Finalmente, agradecemos con cariño a nuestros amigos, quienes, con su aliento, comprensión y apoyo incondicional, nos motivaron a no rendirnos y llegar con éxito a esta etapa tan significativa.

RESUMEN

Este trabajo diseñó e implementó un sistema de gestión integral para el almacenamiento y seguridad de tecnologías menos letales empleadas por la Unidad de Mantenimiento del Orden Z09 en Quito, bajo la norma ISO 31000:2018. El objetivo fue establecer protocolos que garanticen la custodia adecuada de estos recursos, optimizando su manejo y uso, con énfasis en la protección de derechos fundamentales y el fortalecimiento de la confianza institucional. La investigación evaluó las condiciones actuales, identificando vulnerabilidades en infraestructura, procedimientos y formación del personal. Este análisis permitió diseñar un plan de acción materializado en un manual operativo con protocolos para almacenamiento seguro, control de accesos, señalización, manejo de emergencias y uso de equipos de protección. Complementariamente, se implementó un programa de capacitación continua para el personal. El sistema mejora los estándares de seguridad operativa y fomenta una Cultura Institucional Preventiva.

Palabras clave: Sistema de gestión integral, tecnologías menos letales, norma ISO 31000, seguridad pública, capacitación, protocolos de almacenamiento

ABSTRACT

His study designed and implemented a comprehensive management system for the storage and security of less lethal technologies used by the Public Order Maintenance Unit Z09 in Quito, Ecuador, under the ISO 31000:2018 standard. The objective was to establish protocols ensuring proper custody of these resources, optimizing their handling and use, with emphasis on protecting fundamental rights and strengthening institutional trust. The research assessed current conditions, identifying vulnerabilities in infrastructure, procedures, and staff training. This analysis enabled the design of an action plan materialized in an operational manual with protocols for secure storage, access control, signage, emergency management, and protective equipment use. Additionally, a continuous staff training program was implemented. The system enhances operational safety standards and promotes an Institutional Preventive Culture.

Keywords: Comprehensive management system, less lethal technologies, ISO 31000 standard, public safety, training, storage protocols.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPITULO 1:

INTRODUCCIÓN

La complejidad creciente del entorno de seguridad pública presenta desafíos significativos para las organizaciones encargadas del orden, particularmente en la gestión efectiva de Tecnologías Menos Letales (TML). Estas herramientas, aunque diseñadas para reducir daños colaterales, riesgos legales y muertes innecesarias que afectan la legitimidad policial y la confianza ciudadana, introducen riesgos inherentes que requieren una gestión sistemática.

En este contexto, la norma ISO 31000:2018 proporciona el marco esencial para establecer un sistema de gestión de riesgos robusto. Este marco permite a las organizaciones identificar, evaluar, tratar, monitorear y revisar de manera integral los riesgos asociados tanto al almacenamiento seguro como a la implementación operativa de las TML.

La aplicación sistemática de los principios y procesos de la ISO 31000:2018 es fundamental para garantizar que la adopción y uso de TML por parte de autoridades, como las de Quito (Z09), se realice de manera segura, eficiente y responsable. Este enfoque basado en riesgos permite integrar la gestión de las TML en los procesos de toma de decisión y operativos de la organización, optimizando la asignación de recursos y fortaleciendo la seguridad ciudadana. Un sistema de gestión alineado con esta norma fomenta la mejora continua y la adaptabilidad frente a un panorama de amenazas en evolución.

Crucialmente, este marco de gestión de riesgos debe integrar plenamente las normativas aplicables, estándares técnicos y, de manera primordial, las directrices de derechos humanos y uso legítimo de la fuerza establecidas por organismos internacionales. Solo un sistema fundamentado en los principios de la ISO 31000:2018 (como la inclusión de las partes interesadas, la adaptación al contexto y la mejora continua) y rigurosamente alineado con los imperativos éticos y de derechos humanos puede garantizar que la gestión del almacenamiento y despliegue de las TML sea verdaderamente efectiva, legítima y sostenible, preservando los derechos fundamentales de la ciudadanía.

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO

1.1. Definición del Proyecto:

El presente proyecto tiene como objetivo diseñar un sistema de gestión integral para el almacenamiento y seguridad de Tecnologías Menos Letales utilizadas por las autoridades de mantenimiento del orden en Quito, Z09, basado en los lineamientos establecidos por la norma ISO 31000:2018. Este sistema nos ayudará a garantizar un manejo adecuado y seguro de las Tecnologías Menos Letales, facilitando su implementación en operaciones policiales además contribuyendo a la disminución de incidentes que puedan derivar en daños colaterales, lesiones o fatalidades.

El enfoque del proyecto es la creación del área específica para la recepción, almacenamiento, manipulación y disposición final de materiales menos letales, donde cada zona debe estar claramente señalizada para evitar confusiones, el espacio debe contar con un sistema adecuado de ventilación para evitar la acumulación de vapores o sustancias nocivas, si es necesario, se puede usar un sistema de extracción de aire especializado.

El personal debe estar provisto de los Equipos de Protección Personal adecuados según el tipo de material, esto puede incluir guantes, mascarillas, gafas de seguridad, batas o trajes de protección, dependiendo de los riesgos asociados a los materiales, todos los trabajadores deben recibir capacitación sobre las normas de bioseguridad, cómo usar los Equipos de Protección Personal, qué hacer en caso de accidente o exposición, y cómo manejar los materiales de manera segura.

Implementando un sistema de control de acceso para asegurar que no entren personas no autorizadas. Establece un protocolo claro para la limpieza y descontaminación de superficies, equipo y ropa, los materiales deben ser almacenados y gestionados siguiendo un protocolo de desinfección.

Debe haber un plan de emergencia que incluya medidas inmediatas para el manejo de accidentes, exposiciones accidentales y derrames, el personal debe saber cómo actuar rápidamente, y se deben tener a mano kits de primeros auxilios adecuados para estos escenarios.

1.2. Naturaleza o Tipo de Proyecto:

El presente proyecto trata sobre el diseño de un sistema de gestión integral, para el almacenamiento y seguridad de las Tecnologías Menos Letales utilizadas en la Unidad de Mantenimiento del Orden Z09 de Quito.

1.2.1. Objetivo General:

Desarrollar un sistema de gestión integral para el almacenamiento y seguridad de Tecnologías Menos Letales utilizadas por las autoridades de la Unidad de Mantenimiento del Orden Z09 en la ciudad de Quito, basado en la norma ISO 31000:2018, con el fin de optimizar su uso, reducir riesgos operativos, fomentar la confianza pública en las instituciones de seguridad y contribuir a la mejora de la seguridad ciudadana.

1.2.2. Objetivos Específicos:

- Definir normas claras para el almacenamiento físico de las Tecnologías Menos Letales, considerando factores como condiciones ambientales, distribución espacial y medidas de seguridad física. Esto incluye especificaciones para ventilación, control de accesos y señalización preventiva en las áreas designadas.

- Elaborar un plan de formación práctica para los servidores policiales, enfocado en el manejo correcto de las Tecnologías Menos Letales durante su almacenamiento, transporte y uso operativo.

- Crear un sistema de registro que documente el estado, ubicación y movimiento de cada Tecnología Menos Letal, que permita verificar su condición periódicamente y garantizar su disponibilidad operativa cuando sea requerido.

1.3. Justificación e Importancia del Trabajo de Investigación:

La importancia de este proyecto se encuentra respaldado en la necesidad de establecer protocolos claros y efectivos que aseguren el uso adecuado de estas tecnologías, minimizando los riesgos asociados y maximizando su efectividad. Mendez Castro (2022), nos dice que el uso de armas menos letales se plantea como una alternativa dentro de las estrategias de seguridad interna, lo que resalta la importancia de garantizar su correcta gestión y almacenamiento para evitar accidentes y abusos.

Asimismo, la adopción de la norma ISO 31000:2018 en la gestión del riesgo proporciona un marco robusto y estructurado para identificar, evaluar y mitigar los riesgos asociados con la utilización de tecnologías menos letales. La norma enfatiza la importancia de establecer un enfoque sistemático para la gestión de riesgos, lo que facilita la toma de decisiones informadas y aseguradas. Por tanto, Ignacio Moll Santa Isabel (2024), habla sobre la regulación y los dilemas éticos en tecnología militar subraya la necesidad de un enfoque disciplinado que también se aplique a la gestión de tecnologías menos letales en contextos civiles.

Adicionalmente, el entorno geopolítico y social actual requiere que los cuerpos de seguridad adopten tecnologías menos letales de manera responsable y con una clara orientación ética. La investigación y análisis presentados por Metanoia (2023) destacan cómo los avances tecnológicos no solo deben ser evaluados desde una perspectiva operativa, sino también bajo principios éticos que guíen su uso responsable. Un sistema de gestión que incorpore estos principios permitirá que las fuerzas del orden actúen de manera transparente y en concordancia con los derechos humanos, abordando así las preocupaciones de la comunidad sobre el uso de la fuerza.

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:

La organización elegida para nuestro proyecto es, la UNIDAD DE MANTENIENTO DEL ORDEN que tiene su matriz en la ciudad de Quito y sedes en las zonas y subzonas desplegadas a nivel nacional.

2.1.2. Misión, Visión, Valores:

2.1.2.1.Misión:

La Misión de la Unidad de Mantenimiento del Orden es, atender y controlar el orden público, protegiendo el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional en actividades y even

tos de presencia masiva de personas, así como el restablecimiento de la paz y la seguridad ciudadana en alteraciones de orden público.

2.1.2.2.Visión:

Su visión es, ser la unidad más confiable y efectiva a nivel nacional y regional en el control del mantenimiento del orden público y seguridad ciudadana, brindando servicios policiales de calidad orientados al Buen Vivir, aplicando irrestricto respeto a los Derechos Humanos y libertades democráticas.

2.1.2.3.Valores:

- **Valor. -** Capacidad de dominar nuestros miedos, actuar con coraje y fuerza de voluntad, para cumplir el servicio y superar desafíos, demostrando valentía en asumir las consecuencias positivas o negativas de nuestros actos.
- **Disciplina. -** Acatamiento consciente y voluntario a un sistema normativo. Si el acatamiento no es consciente, es simple adiestramiento; si no es voluntario, se reduce a esclavitud.
- **Lealtad. -** Compromiso con la institución, superiores, pares y subalternos; a quienes no podemos traicionar, con un comportamiento que mancille el prestigio y la imagen institucional.

2.1.3. Actividades, Marcas, Productos y Servicios:

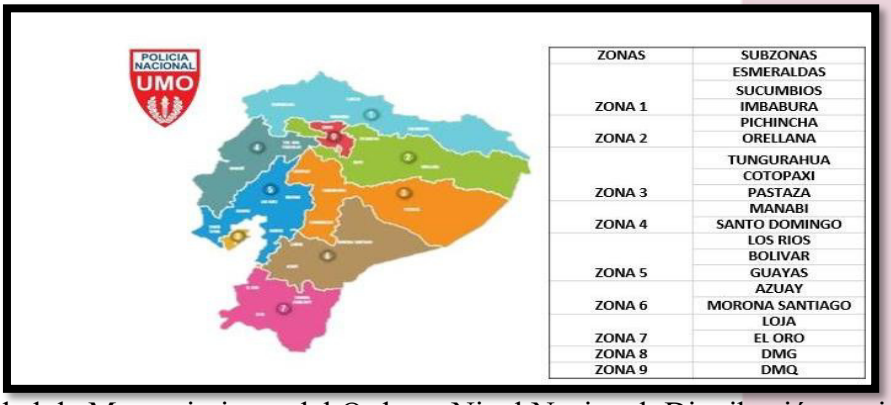
La Unidad de Mantenimiento del Orden, es una unidad policial, su función principal es realizar operaciones policiales para el control de multitudes pacíficas y violentas, mediante acciones de carácter preventivo, disuasivo y reactivo, a fin de mantener y evitar la alteración del orden público.

2.1.4. Ubicación de la Sede:

La matriz principal se encuentra ubicada en la ciudad de Quito, en la Av. Del Maestro y Galo Plaza Lasso (Conjunto Habitacional de Policía La Delicia).

Figura 1

Sedes de la Unidad de Mantenimiento del Orden (Zonas y Subzonas a nivel nacional)



ZONAS	SUBZONAS
ZONA 1	ESMERALDAS
	SUCUMBIOS
	IMBABURA
ZONA 2	PICHINCHA
	ORELLANA
ZONA 3	TUNGURAHUA
	COTOPAXI
	PASTAZA
ZONA 4	MANABI
	SANTO DOMINGO
ZONA 5	LOS RIOS
	BOLIVAR
	GUAYAS
ZONA 6	AZUAY
	MORONA SANTIAGO
ZONA 7	LOJA
	EL ORO
ZONA 8	DMG
ZONA 9	DMQ

Nota: Unidad de Mantenimiento del Orden a Nivel Nacional, Distribución territorial nivel Zonal y Subzonal de la UMO, Tomado de. (UNMO, Sedes de la Unidad de Mantenimiento del Orden distribuidas (Fotografia), 2012).

2.1.5. Ubicación de las Operaciones:

Las operaciones de la Unidad de Mantenimiento del Orden, para este proyecto se eligió la sede matriz ubicada en la ciudad de Quito en la Av. Del Maestro y Galo Plaza Lasso (Conjunto Habitacional de Policía La Delicia).

Figura 2

Jefatura Zonal Operativa de la Unidad de Mantenimiento del Orden Z09-DMQ

Nota: Jefatura Zonal de Mantenimiento del Orden UMO Z09 DMQ, Tomado de. (UNMO, (Fotografía), 2012)

2.1.6. Propiedad y Forma Jurídica:

La Unidad de Mantenimiento del Orden, es una unidad policial que orgánicamente pertenece a la Policía Nacional del Ecuador. La misma que tiene como organismo rector al Ministerio del Interior.

2.1.7. Mercados Servidos o Ubicación de sus Actividades de Negocio:

La Unidad de Mantenimiento del Orden, presta sus servicios en todo el territorio nacional, existen circunstancias en las que es indispensable su presencia cuando en el país existe grave conmoción interna.

2.1.8. Tamaño de la Organización:

El tamaño de la Unidad de Mantenimiento del Orden Z09 de la ciudad de Quito no posee un numérico fijo establecido, esto debido a su naturaleza y a su estructura netamente operativa que varía de acuerdo con las necesidades de servicio y su crecimiento está acorde al orgánico general de la Policía Nacional del Ecuador, pero actualmente se puede estimar que su organización está compuesta de la siguiente manera:

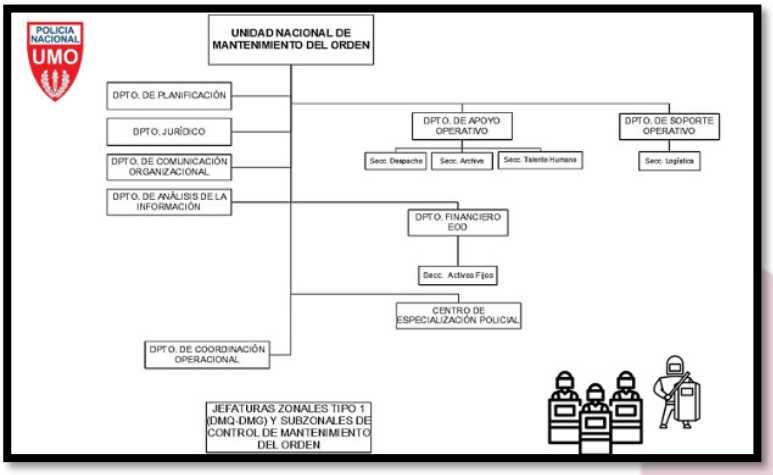
Figura 3

Numérico de Talento Humano de la Unidad de Mantenimiento del Orden Z09- DMQ

Nota: Unidad de Mantenimiento del Orden Z09-DMQ, Tomado de. (UNMO, Numérico de Talento Humano de la Jefatura Zonal de Mantenimiento del Orden Z09 DMQ - (Fotografía), 2012)

Figura 4

Numérico Estructura organizacional desconcentrada de la Unidad de Mantenimiento del Orden Z09- DMQ



Nota: Estructura de la Unidad Nacional de Mantenimiento del Orden, Tomado de. (Manual de Procesos de la Gestión de Orden Público, 2024)

2.1.9. Información sobre empleados y otros trabajadores.

La Unidad de Mantenimiento del Orden Z09 cuenta con personal altamente capacitado: Directivos jefes: 05 hombres con un rango de edad de 45 a 50 años.

Directivos: 22 hombres de edad de 32 a 40 años.

Técnicos Operativos: 465 personas entre hombres y mujeres de un rango de edad de 24 a 45 años.

Administrativos: 04 personas con un rango de edad de 25 a 40 años.

Además, se cuenta con personal de limpieza y mantenimiento son 12 personas con un rango de edad de 35 a 50 años.

2.1.10. Procesos claves relacionados con el objetivo propuesto.

Para alcanzar el objetivo de desarrollar un sistema de gestión en el almacenamiento y seguridad de tecnologías menos letales, de la Unidad de Mantenimiento del Orden Quito (Z09), de acuerdo a la normativa ISO 31000:2018. Es fundamental estructurar una serie de procesos clave. Estos procesos deben estar bien definidos y ser coherentes con los objetivos.

Evaluación de Riesgos:

- **Caracterización de Riesgos:** Determinar los riesgos asociados con el almacenamiento de tecnologías menos letales en unidades policiales, incluyendo a los riesgos físicos, químicos y operacionales.
- **Estudio de Riesgos:** Establecer la naturaleza y la extensión de los riesgos que se han identificado, con la finalidad de evaluar su impacto y probabilidad.
- **Evaluación de Riesgos:** Comparar los riesgos analizados, para determinar su prioridad y la necesidad de tratamiento.

Desarrollo de un Sistema de Gestión para el almacenamiento y seguridad de tecnologías menos letales:

- **Recolección de Información:** Recopilar información existente, sobre los procesos y procedimientos de almacenaje y manipulación de tecnologías menos letales.
- **Normativas institucionales y gubernamentales.**
- **Diseño de directrices:** Se debe suscribir contenidos específicos para el uso, manipulación y almacenaje de las tecnologías menos letales.

Capacitación y Difusión:

- **Capacitación del Talento Humano:** Realizar con la finalidad de que todo el talento humano, comprenda y aplique los lineamientos estipulados en el sistema de gestión para el almacenamiento y seguridad de tecnologías menos letales.
- **Simulacros:** Realizar simulacros para verificar los riesgos asociados y establecer procesos para su mitigación.

Implementación y Monitoreo:

- **Implementación de Procedimientos:** Poner en práctica los procedimientos estandarizados dentro del sistema de gestión para el almacenamiento y seguridad de tecnologías menos letales.

- **Monitoreo:** Con la utilización de dispositivos electrónicos, utilizados para la seguridad de los centros de almacenamiento de tecnologías menos letales. Se debe verificar y controlar el cumplimiento de las directrices y normativas de gestión de riesgos.

Revisión y Mejora Continua:

- **Valoración Periódica:** Evaluar periódicamente la efectividad del sistema de gestión para el almacenamiento y seguridad de tecnologías menos letales. Esto se lo puede realizar mediante la implementación de auditorías internas.
- **Mejora continua:** Realizar actualizaciones al sistema de gestión para el almacenamiento y seguridad de tecnologías menos letales, según sea necesario con la finalidad de evidencias cambios en las prácticas operativas, avances tecnológicos o modificaciones en las normativas relevantes.

Estos procesos son esenciales para asegurar que el sistema de gestión para el almacenamiento y seguridad de tecnologías menos letales manual sea sólido, práctico y aplicable, con la finalidad de mejorar las funciones, seguridad operativa y la gestión de riesgos de la Unidad de Mantenimiento del Orden Z09.

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

Numero de operativos realizados:

Figura 5

Productividad Operativa 2024

Nota: Tomado de. (UNMO D. C., 2025)

Unidad de Mantenimiento del Orden Z09 realiza operativos ordinarios y extraordinarios de: Orden Público, Seguridad de Instalaciones y Apoyo a la Seguridad Ciudadana.

2.1.12. Modelo de negocio.

La Unidad de Mantenimiento del Orden Z09, no tiene un modelo de negocio propio pues pertenece a la Policía Nacional, institución perteneciente al estado ecuatoriano cuya visión es brindar seguridad ciudadana al interior del territorio nacional, en beneficio de toda la población ecuatoriana (Constitución de la Republica del Ecuador, 2008).

Art. 158. - Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos humanos, libertades y garantías de los ciudadanos. La protección interna y el mantenimiento del orden público son funciones privativas del Estado y responsabilidad de la Policía Nacional (Constitución de la Republica del Ecuador, 2008).

Art. 163. - La Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional (Constitución de la Republica del Ecuador, 2008).

La Unidad de Mantenimiento del Orden Z09, es una unidad operativa policial ubicada en la ciudad de Quito. La cual tiene como misión el control del orden público, protegiendo el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional en actividades y eventos de presencia masiva de personas, así como el restablecimiento de la paz y la seguridad ciudadana en alteraciones de orden público. La Unidad de Mantenimiento del Orden Z09, es la

única unidad operativa policial, facultada y preparada para el control del orden público y el movimiento de masas en el Distrito Metropolitano de Quito.

2.1.13. Grupos de interés internos y externos.

La Unidad de Mantenimiento del Orden Z09, es dirigida por servidores policiales quienes por su jerarquía realizan actividades de dirección, administración u operación.

La dirección esta asignada y dirigida por el servidor policial más antiguo en jerarquía de la Unidad de Mantenimiento del Orden Z09, el cual es el encargado de supervisar y dirigir a los departamentos de Soporte Operativo, Apoyo Operativo, Comunicación, Capacitación y Coordinación Operacional.

Grupos de interés internos

- **Talento Humano:** Servidores Policiales, encargados de cumplir funciones de dirección, administración y operación.
- **Empleados Civiles:** Ciudadanos que no pertenecen a las filas policiales que laboran con funciones administrativas, de limpieza y mantenimiento de áreas.

Grupos de interés externos

- Población: Ciudadanía a quien se debe la Unidad de Mantenimiento del Orden Z09, quien siempre va a requerir de su acción y labor para el control del Orden Público.

- **Gobierno:** Organismo gubernamental, encargado de emitir políticas y directrices enfocadas cumplir con la seguridad ciudadana necesaria.
- **Unidades Policiales de apoyo:** Equipos o unidades policiales operativas e investigativas que realizan trabajos coordinados con la Unidad de Mantenimiento del Orden Z09.
- **Medios de comunicación:** Canales a través de los cuales se comunica con el público y se da a conocer los trabajos realizados en beneficio de la ciudadanía en general.

2.1.14. Otros datos de interés.

La Unidad de Mantenimiento del Orden Z09, realiza proyectos con la finalidad de mantener vínculos con la comunidad en general, estos proyectos se evidencian en la presencia de los servidores policiales en las casas abiertas realizadas por la Policía Nacional del Ecuador. De igual forma se continúa especializando, participando en capacitaciones países amigos como Argentina, Chile, Colombia, España y Estados Unidos.

CAPITULO 3

3. DOCUMENTO DE SEGURIDAD

3.1. Análisis de Riesgos.

3.1.1. Identificación de la Organización y de sus Centros de Trabajo:

Rastrillo de la UMO de la Zona 9, ubicado en la ciudad de Quito.

3.1.2. Representante Legal y Responsable de Seguridad:

- Representante legal: Capitán Itas Sevilla Carlos Andrés (Jefe del Departamento de Soporte Operativo de la UNMO).
- Responsable de seguridad: Suboficial Segundo de Policía, Méndez Chulde Edison Arturo (Rastrillero encargado).

3.1.3. Actividades de la Organización:

La Unidad de Mantenimiento del Orden (UNMO) es una unidad especializada de la Policía Nacional del Ecuador que se encarga de ejecutar acciones operativas para el control, mantenimiento y restablecimiento del orden público, enfocándose en eventos de presencia masiva de personas (Registro Oficial Edición Especial 911, 2019). A su vez, brinda apoyo preventivo y disuasivo en las acciones operativas del eje preventivo a nivel nacional, en la lucha contra la delincuencia, y ejecuta operaciones para el control, mantenimiento y restablecimiento del orden

en amotinamientos en los centros de privación de la libertad. Sus medios logísticos principales para ejercer el uso legítimo de la fuerza, que le caracterizan como una unidad especializada en el control de masas y disturbios civiles, son las armas, municiones y tecnologías menos letales. El tema de estudio en este caso es el correcto almacenamiento y gestión de estos medios, específicamente los agentes químicos lacrimógenos (Agente químico CS) para el control de multitudes.

3.1.4. Tratamientos de la Organización y sus Riesgos:

- Activaciones accidentales de las municiones menos letales lacrimógenas.
- Exposición directa a los agentes químicos lacrimógenos.
- Desconocimiento en la manipulación de las tecnologías menos letales.
- Impacto psicológico.

3.1.5. Consentimientos y Notas Informativas:

Nombre del participante: Capitán de Policía Itas Sevilla Carlos Andrés.

Fecha de nacimiento: 31-07-1990

Fecha de hoy: 01-04-2025

A través de la firma de este documento, el abajo firmante otorga su consentimiento para el manejo de su información de datos de acuerdo con los términos y condiciones establecidos a continuación:

a) **Propósito del Manejo de Datos. -** El levantamiento de la información tiene como propósito realizar la construcción de un Sistema de Gestión en el Almacenamiento y Seguridad de las tecnologías menos letales, de la Unidad de Mantenimiento del Orden de la Z9 de la ciudad de Quito, basado en la norma ISO 31000:2018.

b) **Tipo de Datos Recopilados. -** La información y los datos recolectados incluyen, pero no se limitan a:

- Cantidades y descripción de las tecnologías menos letales de la Unidad de Mantenimiento del Orden Z9.
- Datos sobre las cantidades utilizadas de tecnologías menos letales en el año 2024, por parte de la Unidad de Mantenimiento del Orden Z9, en acciones operativas de uso legítimo de la fuerza y por capacitación y perfeccionamiento del talento humano.
- Datos personales de los bodegueros o servidores policiales que cumplen la función de Rastrílleros y Armeros de la Unidad de Mantenimiento del Orden Z9.

c) **Uso de la Información.-** La información y los datos recopilados serán utilizados exclusivamente para todo lo concerniente a la construcción de un sistema de gestión en el almacenamiento y seguridad de las tecnologías menos letales de la Unidad de Mantenimiento del Orden de la Z9 de la ciudad de Quito, basado en la norma ISO 31000:2018, por lo que al tratarse de información sensible respecto a medios logísticos dotados por el Estado, no serán expuestos a terceras personas sin obtener la respectiva aprobación, excepto cuando sea requerido por ley.

d) **Almacenamiento de Datos. -** La información y los datos recopilados serán almacenados de forma responsable, tomándose las medidas de seguridad correspondientes para evitar accesos no autorizados.

e) **Duración del Almacenamiento. -** La información y los datos obtenidos cumplirán una duración de su almacenamiento en función al tiempo correspondiente y adecuado para cumplir con los requisitos y parámetros necesarios para desarrollar el mencionado proyecto, y a su vez según el tiempo requerido por la ley.

f) **Derechos del Participante. -** El participante tiene derecho a solicitar, en cualquier momento, el acceso, rectificación, actualización, eliminación o portabilidad de sus datos personales, así como a oponerse o limitar su tratamiento, de acuerdo con la normativa aplicable. Para ejercer estos derechos, podrá presentar una solicitud a

través de los canales establecidos (como correo electrónico o formulario web), recibiendo una respuesta en el plazo legal establecido. En caso de no estar conforme con la respuesta, tendrá derecho a presentar una reclamación ante la autoridad de protección de datos correspondiente.

g) **Responsable del Tratamiento. -** La Unidad de Mantenimiento del Orden (Z9-Quito) designa como responsable del tratamiento de datos al Suboficial Segundo de Policía Edison Arturo Méndez Chulde (Rastrillero encargado). Los titulares de datos personales pueden ejercer sus derechos de acceso, rectificación, oposición o eliminación presentando su solicitud directamente ante este funcionario.

Esta disposición aplica específicamente para la información relacionada con los medios logísticos asignados en dotación. Para garantizar la protección de datos sensibles, únicamente se autoriza el acceso a esta información a: el Ministerio del Interior, la Fiscalía General del Estado como ente externo, el Comando General de la Policía Nacional, la Dirección General de Logística de la Policía Nacional, la Dirección General de Seguridad Ciudadana y Orden Público y la Dirección Nacional de Operaciones y Servicios Especializados. Estas entidades deberán presentar un oficio formal dirigido a la máxima autoridad de la unidad, quien mediante memorando interno autorizará el procesamiento de la solicitud.

Firma del Participante: …….

Fecha: ……...

3.2. Registro de Actividades de Tratamiento

3.2.1. Grupos de información:

La Unidad de Mantenimiento del Orden (Z9-Quito) maneja los siguientes grupos de información:

a) Datos Operativos Específicos (Críticos):

- Inventarios detallados sobre las tecnologías menos letales donde se incluyen: tipo, número de serie, lote, fecha de caducidad, condiciones de almacenamiento.
- Registros cronológicos de uso con: fecha, hora, cantidad, operativo a cargo, justificación del uso ya sea por razones operativas de uso legítimo de la fuerza o por fines de capacitación y perfeccionamiento del talento humano.

b) Datos Personales Protegidos (Sensibles):

- Información completa del personal autorizado: nombres completos, número de identificación, fotografía, historial de capacitaciones, número de teléfono y correo electrónico.

- Registros de capacitación del personal policial en manejo de tecnologías menos letales.

c) Datos Institucionales Confidenciales:

- Actas de entrega-recepción.
- Informes de incidentes.
- Documentación administrativa (informes, oficios, memorandos o partes policiales).

d) Recepción de información

- Se obtendrá información personal mediante el Sistema de Seguridad Ciudadana (ECU 911).
- Se rectará de manera digital y física.

3.2.2. Sistemas de Tratamiento y Niveles de Seguridad:

a) Sistemas. - Plataforma Quipux o mediante correos electrónicos institucionales para trámites administrativos, con autenticación mediante clave de ingreso y usuario único, uso de códigos de barra para inventario de materiales, utilización de aplicación Iauditor para el control de procesos dentro del control de espacio a implementar.

- **Físico. -** Documentación debidamente almacenada y protegida en el archivo central con acceso restringido.

- **Digital. -** Plataforma Quipux o mediante correos electrónicos institucionales para trámites administrativos, con autenticación mediante clave de ingreso y usuario único.

b) Niveles de Seguridad:

- **Alto. -** Para datos sensibles, respecto a cantidades, almacenamiento, auditorias correspondiente a las tecnologías menos letales de la Unidad de Mantenimiento del Orden Z9, con acceso limitado.

- **Medio. -** Para documentos administrativos, protegidos por contraseñas y creación de respaldo digital documental.

3.2.3. Finalidades, Categorías de Datos, de Interesados y de Destinatarios.

a) Finalidad:

- Garantizar el almacenamiento seguro y técnico de las tecnologías menos letales.

- Controlar el adecuado uso, almacenamiento, conservación, mantenimiento, protocolos de seguridad y documentos de descargo sobre la utilización de las tecnologías menos letales.

- Diseñar un Sistema de Gestión en el almacenamiento y seguridad de las tecnologías menos letales de la Unidad de Mantenimiento del Orden de la ciudad de Quito (Z09), basado en la norma ISO 31000:2018.

Tabla 1

Matriz de Finalidades

Proceso	Datos	Frecuencia	Responsable	Auditoría
Reabastecimiento	Lotes y caducidad	Cada 4 años y por necesidad operativa	Jefe del Departamento de Soporte Operativo de la UNMO	Anual
Mantenimiento	Desgaste, humedad y corrosión	Periódica	Rastrillero	Mensual
Emergencias	Protocolos activación	Inmediato	Oficial de Semana	Diaria

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025))

b) Categorías de datos:

- Datos de inventario (series, lotes, caducidad).
- Datos personales de los responsables custodios.
- Registros de cantidades utilizadas en acciones operativas y de capacitación.

c) Interesados:

- Comando General de la Policía Nacional del Ecuador.
- Ministerio del Interior.
- Dirección General de Logística de la Policía Nacional del Ecuador.

d) Destinatarios:

- Comandante de la Unidad Nacional de Mantenimiento del Orden.
- Fiscalía General del Estado (mediante orden judicial emitida al Comando General de la Policía Nacional del Ecuador).

3.2.4. Encargados de los Tratamientos.

La Policía Nacional del Ecuador, será la entidad pública encargada del tratamiento de datos. El departamento de protección de datos institucionales, será el encargado del manejo de los datos presentados bajo políticas de privacidad y confidencialidad de acuerdo a la normativa institucional establecida y vigente.

3.3. Registro de Dispositivos (Dispositivos digitales)

Tabla 2

Matrices de Dispositivos de la UMO Z09.

Ubicación	Tipo de dispositivo	Cantidad
SECRETARIA DEL COMANDO UNMO	Computador de Escritorio	2
GESTIÓN DE OPERACIONES UNMO	Computador de Escritorio	5
SECRETARIA DEL COMANDO UMO Z09	Computador de Escritorio	2
APOYO OPERATIVO TH	Computador de Escritorio	5
COORDINACIÓN OPERACIONAL	Computador de Escritorio	2
SOPORTE OPERATIVO	Laptops	2
	Computador de Escritorio	2
ACTIVOS FIJOS	Computador de Escritorio	2
RASTRILLO	Computador de Escritorio	2
CAPACITACIÓN	Computador de Escritorio	2
GESTIÓN G.P.R.	Computador de Escritorio	2
ARCHIVO CENTRAL	Computador de Escritorio	2
ARCHIVO DE GESTIÓN	Computador de Escritorio	6
FINANCIERO	Computador de Escritorio	2
TOTAL		**38**

Ubicación	Tipo de dispositivo	Cantidad
COMANDO	Impresora	1
COORDINACIÓN OPERACIONAL	Impresora	1
SOPORTE OPERATIVO	Impresora	1
TOTAL		**03**

Nota: Inventario, Tomado de. (Z09, 2025)

3.4. Registro de Sistemas de Información (Software, seguridad, etc.):

- Microsoft Office
- Avast Free Antivirus
- Quipux
- Correos institucionales con claves
- Iauditor
- Escáner de imagen

3.5. Registro de Personal

3.5.1. Con Acceso a Datos:

- Analista del Departamento de Coordinación Operacional.
- Analista del Departamento de Gestión GPR.
- Analista del Departamento de Soporte Operativo.
- Analista del Departamento de Apoyo Operativo.

3.5.2. Sin acceso a Datos:

- Personal civil de limpieza y mantenimiento de instalaciones.

3.5.3. Accesos Físicos:

- Personal de limpieza, mantenimiento, personal encargado de cada oficina.

3.6. Registro de Prestadores de Servicio.

3.6.1. Sin acceso a datos catalogados:

- Personal de limpieza.
- Mantenimiento general.

3.7. Sistemas de Captación de Imágenes y Audio.

3.7.1. Número de Cámaras:

La Unidad de Mantenimiento del Orden Z9 de la ciudad de Quito tiene un total de 12 cámaras.

3.7.2. Zonas de Influencia

Tabla 3

Ubicación de cámaras de vigilancia de la UMO Z09.

Circuito de cámaras Bloque Nro 03	Número de cámaras
PISO 1 ALA A Y B	2
PISO 2 ALA A Y B	2
PISO 3 ALA A Y B	2
PISO 4 ALA A Y B	2
GIMNASIO	1
RASTRILLO	1
PARQUEADEROS MOTOCICLETAS	1
MURALLA UMO	1
Total	**14**

Nota: Inventario, Tomado de. (Z09, 2025)

3.7.3. Sistema de Tratamiento y Almacenamiento.

Almacenamiento sistematizado en el ordenador por un periodo de 01 mes.

3.7.4. Usuarios Autorizados.

Los usuarios autorizados para acceder a los datos e información son:

- El comandante de la Unidad Nacional de Mantenimiento del Orden.

- Suboficial Segundo de Policía Edison Arturo Méndez Chulde (Rastrillero encargado), bajo la autorización de la máxima autoridad de la unidad mediante oficio de respaldo.

3.8. Dispositivos y Medidas de Seguridad.

3.8.1. Análisis de las Medidas de Seguridad de los Dispositivos.

Los equipos tecnológicos disponibles en el rastrillo de la UMO mantienen programas de antivirus gratuitos. Como control de acceso tienen implementado en sus equipos contraseñas personales por cada encargado (Unidad de Mantenimiento del Orden, 2025).

Estos equipos tecnológicos utilizados cuentan con medidas básicas de seguridad, por lo que a continuación, se detalla el estado actual:

a) Antivirus gratuitos:

Los dispositivos emplean soluciones de antivirus gratuitas como **Avast Free Antivirus**, que ofrecen protección básica contra malware y amenazas conocidas.

Limitaciones:

- Falta de funcionalidades avanzadas (detección en tiempo real de ataques *zero-day*, análisis heurístico profundo).
- Ausencia de soporte técnico especializado y actualizaciones automatizadas.

- No incluyen herramientas complementarias como firewalls integrados o cifrado de datos.

b) Control de acceso mediante contraseñas:

Cada encargado utiliza credenciales personales para acceder a los sistemas.

Debilidades identificadas:

- No existen políticas claras sobre complejidad de contraseñas (longitud mínima, combinación de caracteres, caducidad periódica).
- Falta de autenticación multifactorial (MFA), lo que incrementa el riesgo de accesos no autorizados.

c) Gestión de dispositivos físicos:

- Los equipos están distribuidos en áreas específicas (oficinas, rastrillo, archivo central), pero sin sistemas de bloqueo remoto o seguimiento ante robos.
- No se registran copias de seguridad automatizadas o almacenamiento en la nube para respaldar información crítica.

d) **Registro de sistemas de información:**

- **Software utilizado:** Microsoft Office, Quipux (gestión documental), y escáner de imagen.
- Falta de integración entre sistemas para centralizar la gestión de alertas de seguridad.

Riesgos asociados al estado actual:

- Vulnerabilidad a **ransomware** o **phishing** debido a la ausencia de herramientas profesionales.
- Posibles brechas de seguridad por contraseñas débiles o compartidas.
- Pérdida de datos críticos (ej. inventarios de tecnologías menos letales) por falta de respaldos.

Tabla 4

Inventario tecnológico y vulnerabilidades críticas de la UMO Z09.

Categoría	Detalles	Riesgos identificados
Hardware	• 38 computadores de escritorio (Windows 10/11). • 2 laptops sin cifrado. • 3 impresoras HP conectadas a red local.	• Dispositivos obsoletos con soporte técnico limitado. • Riesgo de robo/fuga de datos en laptops.
Software	• Avast Free Antivirus (sin gestión centralizada). • Quipux (gestión documental). • Microsoft Office sin licencias empresariales.	• Falta de parches de seguridad automatizados. • Vulnerabilidades en software no actualizado.
Redes	• Red única sin segmentación. • Sin firewall corporativo.	• Propagación lateral de malware. • Acceso no autorizado a datos sensibles (ej. inventarios de TML).
Almacenamiento	• Datos guardados localmente en discos HDD. • Sin copias de seguridad automatizadas.	• Pérdida de información por fallos hardware. • Exposición a ransomware.
Control de acceso	• Contraseñas estáticas sin políticas	• Suplantación de identidad.

Categoría	Detalles	Riesgos identificados
	de complejidad. • Sin MFA.	• Acceso a datos críticos por personal no autorizado.

Nota: Inventario, Tomado de. (Z09, 2025)

3.8.2. Propuesta de Mejora de las Medidas de Seguridad.

Adquirir licencias originales de antivirus, adquirir accesos a los datos a través de redes, establecer un área específica en el rastrillo de la UMO con medidas de seguridad alta para archivar documentación de registro de entrada y salida de pertrechos y equipos durante el tiempo necesario.

Para fortalecer la seguridad de los dispositivos y mitigar riesgos, se proponen las siguientes acciones estratégicas, alineadas con la norma **ISO 31000:2018** y los objetivos del sistema de gestión integral:

a) Actualización de herramientas de ciberseguridad:

- **Adquisición de licencias profesionales de antivirus.**

  Implementar soluciones empresariales como Bitdefender GravityZone o Kaspersky Endpoint Security, que incluyen:

- ✓ Protección contra ransomware y phishing.
- ✓ Monitorización centralizada de amenazas.
- ✓ Actualizaciones automáticas y soporte 24/7.

- **Integración de firewalls de próxima generación (NGFW).**

  Configurar reglas de filtrado avanzadas para redes internas y externas.

b) Refuerzo del control de acceso:

- **Políticas de contraseñas robustas. -** Longitud mínima de 12 caracteres, combinando símbolos, números y letras, así como también con la caducidad trimestral de contraseñas.
- **Autenticación multifactorial (MFA). -** Implementar tokens físicos o aplicaciones móviles (ej. Google Authenticator) para acceder a sistemas críticos.
- **Gestión de identidades (IAM). -** Asignar permisos basados en roles para limitar el acceso a datos sensibles (ej. inventarios de las tecnologías menos letales, armas, insumos y pertrechos).

c) **Acceso seguro a través de redes:**

- **Implementación de VPNs con cifrado AES-256.-** Garantizar conexiones remotas seguras para personal autorizado.
- **Migración a servicios en la nube. -** Almacenar copias de seguridad en plataformas como AWS o Microsoft Azure con cifrado de extremo a extremo.

d) **Creación de un área de alta seguridad en el rastrillo:**

- **Diseño de una sala blindada. -** Control de acceso biométrico (lectores de huella o reconocimiento facial), cámaras de vigilancia con grabación continua y almacenamiento en la nube por 6 meses y armarios ignífugos para documentos físicos de entrada/salida de pertrechos.
- **Digitalización de registros. -** Utilizar sistemas de gestión documental (DMS) con auditorías de acceso y sellado de tiempo.

e) **Capacitación y auditorías periódicas:**

- **Talleres semestrales de ciberseguridad. -** Enfoque en identificación de phishing, manejo de contraseñas y protocolos de respuesta a incidentes.
- **Auditorías externas anuales. -** Evaluar cumplimiento de normativas como la Ley Orgánica de Protección de Datos Personales (LOPDP).

- **Simulacros de ciberataques. -** Pruebas de penetración para identificar vulnerabilidades en redes y dispositivos.

f) Implementación de copias de seguridad automatizadas:

- Configurar backups diarios en servidores locales y en la nube.
- Establecer un protocolo de recuperación ante desastres (RTO < 4 horas).

3.9. Puestos de Trabajo.

3.9.1. Análisis de las Medidas de Seguridad en al Área Asignada de Rastrillo.

El área de rastrillo constituye un espacio estratégico y sensible dentro de la infraestructura operativa de la Unidad de Mantenimiento del Orden (UMO), en tanto que alberga y organiza el equipamiento táctico, logístico y armamento de los funcionarios desplegados en operaciones de control del orden público. La correcta implementación de medidas de seguridad en esta zona es fundamental para garantizar la integridad del personal, la custodia del material institucional y la eficiencia de la respuesta operativa.

a) Acceso controlado y restricción de ingreso. - Actualmente, el acceso al área de rastrillo está regulado mediante un sistema de control físico y documental, donde únicamente el personal autorizado puede ingresar, previa verificación de su identidad y rol operativo. Se utilizan bitácoras de ingreso y salida, así como listados

preestablecidos con el detalle del equipo asignado a cada servidor policial. Sin embargo, se ha identificado la necesidad de mejorar los mecanismos de control mediante la implementación de tecnología biométrica (lectores de huella dactilar o facial) para reforzar la trazabilidad y limitar la posibilidad de ingreso no autorizado.

b) **Condiciones estructurales y delimitación física. -** El área asignada para rastrillo cuenta con cerramiento perimetral, iluminación adecuada y señalética visible, lo cual permite una correcta delimitación del espacio. No obstante, algunos puntos presentan debilidades en cuanto al estado físico del cerramiento y cobertura visual, lo que podría ser aprovechado para intentos de intrusión o manipulación no autorizada de los equipos. Se recomienda realizar un mantenimiento estructural periódico, además de la instalación de cámaras de videovigilancia conectadas al centro de monitoreo interno de la unidad.

c) **Almacenamiento y disposición del material. -** El equipo táctico se encuentra clasificado y distribuido en estanterías, casilleros o módulos individuales asignados por operatividad. Existe un procedimiento estandarizado para la entrega y recepción del equipo antes y después de las misiones. No obstante, se ha observado que en momentos de alta demanda (como movilizaciones o estados de excepción), el orden puede verse comprometido por la falta de espacio y agilidad logística. Como medida de mejora, se sugiere implementar un sistema de inventario digitalizado en

tiempo real, así como diseñar un plan de contingencia que permita activar zonas temporales de rastrillo móvil.

d) **Supervisión y control interno. -** Durante las actividades operativas, oficiales responsables supervisan el cumplimiento de los protocolos de seguridad, la revisión del equipo y el alistamiento operativo. Esta práctica es efectiva siempre que se mantenga la disciplina y el enfoque preventivo. Sin embargo, la ausencia ocasional de responsables asignados ha generado retrasos y confusión. Por tanto, se propone institucionalizar turnos rotativos de supervisión con roles claros y la designación formal de un responsable de seguridad del rastrillo.

e) **Evaluación de riesgos y vulnerabilidades. -** El área ha sido sometida a evaluaciones básicas de seguridad, pero no cuenta con un análisis de riesgos integral que contemple posibles amenazas externas (infiltración, sabotaje) o internas (mal uso de equipo, extravío, negligencia). Se sugiere desarrollar un análisis FODA y una matriz de riesgos específicos del área de rastrillo, con acciones correctivas y de mitigación integrada al sistema de gestión de seguridad institucional.

3.9.2. Acuerdo de Confidencialidad.

Este Acuerdo de Confidencialidad ("Acuerdo") se celebra entre la Unidad Nacional de Mantenimiento del Orden, ubicada en la ciudad de Quito, Av. Galo Plaza Lasso y Av. Del Maestro,

en adelante denominada "Parte Reveladora", y el Servidor, con domicilio en la ciudad de Quito, en adelante denominado "Parte Receptora", en la fecha 04 de abril de 2025 (Unidad Nacional de Mantenimiento del Orden, 2025).

ÁREA DE RASTRILLO UNIDAD DE MANTENIMIENTO DEL ORDEN POLICÍA NACIONAL DEL ECUADOR.

En la ciudad de _____, a los ___ días del mes de _____ del año _____, comparecen, por una parte, la Unidad de Mantenimiento del Orden (UMO), representada por su responsable directo en el área de rastrillo, y por otra, el/la servidor(a) policial _____, con número de cédula/papeleta policial _____, en adelante EL/LA COMPROMETIDO(A), quienes acuerdan lo siguiente:

CLÁUSULAS:

PRIMERA. - Objeto del Acuerdo

El presente Acuerdo tiene como finalidad garantizar la confidencialidad de toda la información sensible, operativa, logística y estratégica relacionada con el funcionamiento, disposición, planificación y operatividad del área de rastrillo de la UMO.

SEGUNDA. - Información Confidencial

Se considera como información confidencial todo dato, documento, material, plan, fotografía, coordenada, ubicación, distribución de recursos humanos y logísticos, inventario de armamento y equipo, así como cualquier otra información a la que EL/LA COMPROMETIDO(A) tenga acceso directa o indirectamente por razón de su asignación.

TERCERA. - Obligaciones del Comprometido/a

EL/LA COMPROMETIDO(A) se obliga a:

a) No divulgar, difundir, replicar ni hacer uso indebido de la información confidencial.

b) No compartir dicha información con personal no autorizado o externos a la institución.

c) Utilizar la información únicamente para fines institucionales y dentro del marco de sus funciones.

d) Informar de inmediato a su superior cualquier irregularidad, fuga de información o intento de acceso no autorizado.

CUARTA. - Vigencia del Acuerdo.

El presente Acuerdo tendrá vigencia mientras dure la asignación del / de la COMPROMETIDO (A) en el área de rastrillo, y continuará surtiendo efecto aún después del término de dicha asignación, en lo relativo a la protección de la información a la que tuvo acceso.

QUINTA. - Consecuencias por el Incumplimiento.

El incumplimiento de este acuerdo podrá acarrear responsabilidades administrativas, disciplinarias y/o legales conforme a las normativas internas de la Policía Nacional del Ecuador y la legislación vigente.

SEXTA. - Jurisdicción y Legislación Aplicable.

Para la interpretación y cumplimiento del presente acuerdo, las partes se someten a la legislación ecuatoriana y a las disposiciones internas de la Policía Nacional del Ecuador.

En fe de lo cual, firman el presente Acuerdo de Confidencialidad en dos ejemplares del mismo tenor, en el lugar y fecha indicados.

DURACIÓN DEL ACUERDO.

El Acuerdo de Confidencialidad entrará en vigencia desde la fecha de la suscripción de la firma y la confidencialidad será indefinida y debe subsistir aun habiendo terminado la relación laboral. QUITO – ECUADOR | 2025

LEY APLICABLE Y JURISDICCIÓN.

Este Acuerdo se regirá e interpretará conforme a las leyes del Estado Ecuatoriano, sin asumir sus disposiciones sobre conflictos de leyes. Cualquier disputa derivada de o relacionada con este acuerdo se resolverá únicamente ante los tribunales proporcionados del Ecuador.

FIRMA ELECTRÓNICA

Este Acuerdo puede ser firmado y entregado por medios electrónicos, lo que tendrá el mismo efecto que una firma original en papel.

FIRMAS DE LAS PARTES

UNIDAD DE MANTENIMIENTO DEL ORDEN Z09:

Nombre: …….

Firma: …….

Fecha: …….

SERVIDOR:

Nombre: …….

Firma: …….

Fecha: …….

3.10. Encargado del Tratamiento.

3.10.1. Contrato y Tratamiento.

CONTRATO DE ENCARGADO DEL TRATAMIENTO

Entre:

La Unidad de Mantenimiento del Orden, con domicilio en la ciudad de Quito, Av. Del Maestro y Galo Plaza Lasso, en adelante denominado "Responsable del Tratamiento", por una parte; y la Dirección General de Logística de la Policía Nacional del Ecuador, ubicada en la ciudad de Quito, Av.Amazonas N25-113 y Japón, en adelante denominado "Encargado del Tratamiento", por la otra parte.

Antecedentes:

La Unidad de Mantenimiento del Orden es responsable del procesamiento de ciertos datos personales de acuerdo con las leyes de protección de datos vigentes.

La Dirección General de Logística de la Policía Nacional del Ecuador, está dispuesta actuar como encargado del tratamiento y procesamiento de datos personales en nombre de la Unidad de Mantenimiento del Orden, en conformidad con los términos y condiciones especificados en este contrato.

Acuerdan:

a) **Objeto del contrato:**

La Dirección General de Logística de la Policía Nacional del Ecuador, procesará los datos personales en representación de la Unidad de Mantenimiento del Orden, de acuerdo con las

instrucciones documentadas proporcionadas por La Unidad de Mantenimiento del Orden, con el fin de dar seguimiento y auditorías a los distintos procedimientos ejecutados en todas las áreas.

b) Tipo de datos del encargado del tratamiento:

Los datos que va a tratar La Dirección General de Logística de la Policía Nacional del Ecuador son los de los trabajadores de la Unidad de Mantenimiento del Orden de la ciudad de Quito y son los siguientes:

- Nombres completos
- Número de teléfono
- Dirección de correo electrónico

c) Obligaciones del encargado del tratamiento:

La Dirección General de Logística de la Policía Nacional del Ecuador se compromete a:

- Manejar los datos personales solo siguiendo las indicaciones específicas dadas y documentadas por la Unidad de Mantenimiento del Orden.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar que los datos personales estén seguros contra accesos no autorizados, divulgaciones, alteraciones o destrucción, asegurando un nivel de protección adecuado.

- No compartir los datos personales con terceros sin la autorización previa y por escrito de La Unidad de Mantenimiento del Orden, excepto cuando sea requerido por ley.
- Asistir a la Unidad de Mantenimiento del Orden en el cumplimiento de las obligaciones referentes a la seguridad de los datos, la notificación de brechas de datos y el ejercicio de los derechos de las personas involucradas.
- Cooperar con la Unidad de Mantenimiento del Orden en la realización de evaluaciones de impacto en la protección de datos y consultas previas con la autoridad de protección de datos, cuando sea necesario.
- Mantener la confidencialidad de los datos personales procesados en virtud de este contrato.
- Todo lo antes mencionado, cumpliendo con el Art. 43 de la LOPDP. El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.
- La Unidad de Mantenimiento del Orden se compromete a proporcionar a la Dirección General de Logística de la Policía Nacional del Ecuador, toda la documentación necesaria para el adecuado desempeño del encargo, incluyendo, pero no limitado a la LOPDP, instrucciones de tratamiento, y cualquier otro documento relevante. Esta documentación será entregada en un formato y plazo acordados previamente entre las partes.

d) **Duración del contrato:**

Este contrato comenzará a regir a partir de la fecha de su firma y seguirá vigente hasta que cualquiera de las partes lo termine por escrito, cumpliendo con el Art. 34 de la LOPDP, una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales (Asamblea Nacional, 2021).

e) **Obligaciones del responsable del tratamiento:**

- **Proporcionar instrucciones claras. -** La Unidad de Mantenimiento del Orden debe proporcionar a la Dirección General de Logística de la Policía Nacional del Ecuador instrucciones claras y detalladas sobre cómo procesar los datos personales de acuerdo con la LOPDP.
- **Garantizar la legalidad del procesamiento. -** La Unidad de Mantenimiento del Orden, debe avalar que el procesamiento de los datos personales por parte de la Dirección General de Logística de la Policía Nacional del Ecuador se realice de manera legal y conforme a la LOPDP.
- **Monitoreo del cumplimiento. -** La Unidad de Mantenimiento del Orden, tiene la responsabilidad de monitorear regularmente el cumplimiento por parte de la Dirección

General de Logística de la Policía Nacional del Ecuador de las disposiciones contractuales y de la LOPDP.

- **Responder a las solicitudes de los interesados. -** La Unidad de Mantenimiento del Orden debe asegurarse de que la Dirección General de Logística esté preparada para responder a las solicitudes de los interesados en relación con sus derechos de protección de datos, como el acceso, rectificación, supresión, etc.

- **Notificar sobre violaciones de datos. -** En caso de una violación de datos que afecte a los datos personales tratados por la Dirección General de Logística. La Unidad de Mantenimiento del Orden, debe ser notificado sin demora indebida, para que pueda tomar las medidas necesarias para mitigar el riesgo y cumplir con los requisitos de notificación de violaciones de datos según la normativa aplicable (Asamblea Nacional, 2021).

f) Ley aplicable y jurisdicción:

Este contrato se regirá e interpretará conforme a las leyes de Ecuador, sin considerar sus normas sobre conflictos de leyes. Cualquier disputa que surja o esté relacionada con este contrato se resolverá exclusivamente en los tribunales competentes del Ecuador. (Asamblea Nacional, 2021).

g) **Firma electrónica:**

Este contrato puede ser firmado y entregado por medios electrónicos, lo que tendrá el mismo efecto que una firma original en papel.

FIRMAS DE LAS PARTES:

UNIDAD DE MANTENIMIENTO DEL ORDEN Z09:

Nombre: …….

Firma: …….

Fecha: …….

DIRECCION GENERAL DE LOGISTICA DE LA P.N.:

Nombre: …….

Firma: …….

Fecha: …….

3.11. Análisis Web.

La Unidad de Mantenimiento del Orden, no tiene una página web propia, pues al ser una entidad gubernamental depende orgánicamente de la Policía Nacional del Ecuador cuya página web es: https://www.policia.gob.ec/

3.11.1. Análisis, Configuración y Política de Cookies.

a) **Análisis de cookies. -** Son pocas las cookies implementadas en la página web de la Policía Nacional del Ecuador, se sugiere implementar un banner de cookies.

El sitio despliega un banner inicial que informa: "Este sitio web utiliza cookies para mejorar su experiencia. Al continuar navegando, acepta nuestro uso de cookies".

En esta página web no se permite rechazar cookies no esenciales ni gestionarlas de forma granular (solo incluye un botón de "Aceptar" y un enlace a la política de cookies). Esto incumple el requisito de consentimiento explícito exigido por la LOPDP y el RGPD.

b) **Configuración de cookies. -** Debido a las pocas cookies implementadas en la página web de la Policía Nacional del Ecuador, su configuración con la aplicación de un banner de cookies deber ser conforme a la LOPDP y RGPD que incluya:

- ✓ Botones claros: "Aceptar", "Rechazar" y "Configurar".
- ✓ Opción para aceptar solo cookies técnicas.

c) **Política de cookies. –** La página web de la Policía Nacional del Ecuador no tiene una política de cookies clara y accesible. La clasificación de cookies en técnicas (sesión, seguridad) y analíticas (Google Analytics), poniendo en mención de que

las cookies analíticas recopilan datos anónimos sobre tráfico y comportamiento. A su vez hay que considerar que no se detalla la duración exacta de cada cookie (ejemplo: _ga de Google Analytics tiene 2 años); así mismo no se explica cómo revocar el consentimiento (ejemplo: limpiar cookies del navegador o usar complementos), al igual que la falta de referencia a herramientas de terceros para bloquear rastreo (ejemplo: Ghostery).

PROPUESTA: Se puede implementar políticas que:

- ✓ Detallen la duración exacta de cada cookie.
- ✓ Expliquen cómo revocar el consentimiento.
- ✓ Incluyan un enlace directo a la política de cookies.
- ✓ Detallar la duración exacta de cada cookie (ej: "_ga" de Google Analytics: 2 años).
- ✓ Explicar cómo revocar el consentimiento (ej: mediante configuración del navegador o panel del sitio).
- ✓ Incluir un enlace directo a la política de cookies en el footer del sitio.

3.11.2. Formularios de Contacto, Newsletter, Trabaja Conmigo, Registro.

a) **Formularios de contacto. -** Dentro de la página web de la Policía Nacional del Ecuador, existen varios formularios destinados a la recopilación de información sea

personal, de protección de datos o denuncias ciudadanas. Se sugiere agregar una cláusula explícita sobre la base legal del tratamiento de datos e implementar CAPTCHA para prevenir envíos automatizados. A su vez estos formularios provienen de Google Forms lo cual sería prudente realizar los formularios desde la página web.

PROPUESTA: Migración de Google Forms a una plataforma propia.

Desarrollo de formularios integrados en la web institucional. - Utilizar tecnologías como React.js o PHP para crear formularios personalizados, garantizando:

- ✓ Coherencia visual. - Diseño alineado con la identidad corporativa de la institución.
- ✓ Control de datos. - Almacenamiento en servidores nacionales con cifrado AES-256 (cumpliendo el Reglamento de Datos Sensibles del Ecuador).

b) Newsletter. - La página web de la Policía Nacional del Ecuador no contiene Newsletter, pues no solicita datos personales para acceder a su ventana principal, de igual manera es una página que muestra los servicios realizados por la institución policial, mas no busca ofrecer un servicio al público. Puede implementarse la solicitud de datos para acceder a su contenido, con la finalidad de vincular correos

electrónicos con la finalidad de que un Newsletter mantenga informado y actualizado al usuario.

PROPUESTA: Denuncia en Línea.

- ✓ Agregar una cláusula explícita sobre la base legal del tratamiento (ejemplo: "Art. 66 LOPDP: ejercicio de funciones públicas").
- ✓ Implementar CAPTCHA (ejemplo: RECAPTCHA v3) para prevenir envíos automatizados.
- ✓ Incluir una declaración de cifrado (ejemplo: "Sus datos se almacenan con cifrado AES-256").

c) Trabaja conmigo. - La página web de la Policía Nacional del Ecuador, no cuenta directamente con un enlace o formulario que ofrezca oportunidades de trabajo. El sistema de selección de personal para la Policía Nacional del Ecuador tiene una página web diferente cuyo enlace es https://reclutamiento.policia.gob.ec/applicant/exams. Se debería integrar un enlace directo desde la página web de la Policía Nacional del Ecuador, incluyendo una cláusula de confidencialidad para datos sensibles en el que se indique que la información será tratada exclusivamente para reclutamiento.

PROPUESTA:

- ✓ Limitar formatos de archivos adjuntos a PDF o DOCX con validación en el frontend y backend.
- ✓ Añadir una cláusula de confidencialidad para datos sensibles (ejemplo: "Su información será tratada exclusivamente para reclutamiento").

d) Registro. -La página web de la Policía Nacional del Ecuador no solicita un registro para acceder a su contenido principal, esto porque su contenido es informativo y de servicio al público. Se debería implementar un acceso controlado, el cual exija el registro mediante el uso de un correo electrónico, clave y CAPTCHA.

PROPUESTA: Formulario de Contacto General

- ✓ Rediseñar con campos obligatorios claros y mensajes de error específicos (ejemplo: "Correo electrónico inválido").

3.11.3. Avisos Legales.

Al revisar la página web de la Policía Nacional del Ecuador, esta no cuenta con una sección en donde se describan o desplieguen los avisos legales vigentes.

Como cualquier sitio web perteneciente a una entidad pública que recopila datos de usuarios y ofrece servicios, debería tener varios avisos legales con la finalidad de cumplir con la normativa vigente y garantizar la transparencia y la protección de los derechos de los usuarios.

a) **Política de Privacidad:**

- ✓ Derechos ARCO: Se menciona el derecho a "Acceso, Rectificación, Cancelación y Oposición", pero no se especifican los plazos de respuesta (ej: 15 días según LOPDP).
- ✓ Contacto del delegado de Protección de Datos: No se identifica un correo o teléfono específico, solo se remite a la dirección física de la institución.

b) **Restricciones:**

- ✓ Prohibición de uso malicioso, reproducción no autorizada de contenidos.
- ✓ Mención de responsabilidad por daños causados por incumplimiento.

c) **Limitaciones. -** No se detallan sanciones específicas por violaciones (ej: suspensión de acceso).

d) **Actualización. -** La política indica una última revisión en 2022, sin evidencias de actualizaciones recientes en el código fuente (ejemplo: metadatos de la página).

e) **Recomendaciones.** - Entre los avisos legales principales deberían presentarse:

- **Política de Privacidad:**

✓ **Identificación del responsable del tratamiento de datos:** Debe indicar claramente quién es la Policía Nacional del Ecuador como entidad responsable del tratamiento de los datos personales recopilados a través del sitio web.

✓ **Datos personales recopilados:** Debe especificar qué tipos de datos personales se recogen (por ejemplo, nombre, dirección de correo electrónico, dirección IP, información proporcionada en formularios de denuncia, etc.).

✓ **Finalidad del tratamiento de los datos:** Debe explicar claramente para qué se utilizan los datos recopilados (por ejemplo, tramitar denuncias, responder consultas, mejorar el sitio web, enviar boletines informativos si el usuario se suscribe, etc.).

✓ **Base legal para el tratamiento:** Debe indicar la base legal que legitima el tratamiento de los datos (por ejemplo, consentimiento del usuario, cumplimiento de una obligación legal, interés público, etc.).

✓ **Destinatarios de los datos:** Debe informar si los datos se comparten con terceros (por ejemplo, otras instituciones judiciales, empresas de servicios tecnológicos) y con qué fines.

- ✓ **Transferencias internacionales de datos (si cumple):** Si los datos se transfieren fuera del Ecuador, debe informarse sobre las garantías adecuadas.
- ✓ **Plazo de conservación de los datos:** Debe indicar durante cuánto tiempo se conservarán los datos personales.
- ✓ **Derechos de los usuarios:** Debe informar sobre los derechos que tienen los usuarios en relación con sus datos personales (acceso, rectificación, supresión, limitación del tratamiento, oposición, portabilidad) y cómo pueden ejercerlos.
- ✓ **Medidas de seguridad implementadas:** Debe ofrecer una descripción general de las medidas de seguridad técnicas y organizativas adoptadas para proteger los datos personales.
- ✓ **Información de contacto:** Debe proporcionar los datos de contacto para que los usuarios puedan ejercer sus derechos o realizar consultas sobre la política de privacidad.

- **Términos y Condiciones de Uso:**

- ✓ **Identificación del titular del sitio web. -** Debe identificar claramente a la Policía Nacional del Ecuador como propietaria y operadora del sitio web.
- ✓ **Aceptación de los términos. -** Debe indicar que el acceso y uso del sitio web implica la aceptación de los términos y condiciones.

- ✓ **Uso permitido del sitio web. -** Debe establecer las normas de uso del sitio, incluyendo las prohibiciones de actividades ilegales o que puedan dañar el sitio o a terceros.
- ✓ **Propiedad intelectual. -** Debe especificar los derechos de propiedad intelectual sobre el contenido del sitio web (textos, imágenes, logotipos, etc.) y las restricciones de uso sin autorización.
- ✓ **Limitación de responsabilidad. -** Debe establecer las limitaciones de responsabilidad de la Policía Nacional por el uso del sitio web, incluyendo posibles errores, interrupciones o daños.
- ✓ **Enlaces a sitios web de terceros. -** Si el sitio contiene enlaces a otras páginas, debe indicar que la Policía Nacional no se hace responsable del contenido o las políticas de privacidad de esos sitios.
- ✓ **Modificaciones de los términos y condiciones. -** Debe reservarse el derecho de modificar los términos y condiciones en cualquier momento, indicando cómo se informarán dichos cambios.
- ✓ **Ley aplicable y jurisdicción. -** Debe especificar la ley ecuatoriana que rige los términos y condiciones y la jurisdicción de los tribunales competentes para la resolución de cualquier disputa.

- ✓ **Información de contacto. -** Debe proporcionar los datos de contacto para consultas relacionadas con los términos y condiciones.

- **Aviso Legal (Información General):**

- ✓ **Identificación de la institución. -** Nombre completo de la Policía Nacional del Ecuador, dirección, información de contacto general.
- ✓ **Finalidad del sitio web. -** Descripción general del propósito del sitio web (información institucional, noticias y servicios a la ciudadanía.).
- ✓ **Exclusión de responsabilidad. -** Declaración general de que la información proporcionada en el sitio web es de carácter informativo y no constituye asesoramiento legal o vinculante en todos los casos.

- **Política de Cookies:**

- ✓ **Información sobre qué son las cookies. -** Explicación de qué son las cookies y su función.
- ✓ **Tipos de cookies utilizadas. -**Detalle de las categorías de cookies que utiliza el sitio web (técnicas, de análisis, de personalización, publicitarias, de terceros).
- ✓ **Finalidad de cada tipo de cookie**. - Explicación de para qué se utiliza cada categoría de cookie.

- ✓ **Gestión de cookies. -** Información sobre cómo los usuarios pueden configurar o desactivar las cookies a través de su navegador.
- ✓ **Consentimiento de cookies. -** Mecanismo para obtener el consentimiento informado de los usuarios para el uso de cookies no esenciales.

- **Cumplimiento Normativo:** Es fundamental que estos avisos legales cumplan con la legislación ecuatoriana vigente en materia de protección de datos personales (Ley Orgánica de Protección de Datos Personales - LOPDP) y otras leyes relacionadas con el comercio electrónico y la transparencia en línea.

La ausencia de estos avisos legales puede generar problemas de cumplimiento normativo, falta de transparencia hacia los ciudadanos y posibles reclamaciones legales. Por lo tanto, es crucial que la Policía Nacional del Ecuador incluya de manera clara y accesible estos avisos en su página web.

3.12. Medidas de seguridad:

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

La página web de la Policía Nacional del Ecuador utiliza **https** para cifrar las comunicaciones entre el navegador del usuario y el servidor, con la finalidad de brindar seguridad en el compartimiento de datos. Para mejorar la seguridad la página web se puede realizar lo siguiente:

PROPUESTAS:

- **Cabeceras de Seguridad:**

✓ Implementar HSTS con la directiva: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

✓ Definir una Content-Security-Policy (CSP) restrictiva (ej: default-src 'self' https://www.google-analytics.com).

- **Configuración del Sitio:**

✓ Eliminar tecnologías obsoletas (ejemplo: PHP 7.4) y actualizar a PHP 8.2+ con soporte activo.

3.12.2. Hosting y Servidores:

3.12.2.1. Medidas de seguridad.

La página web de la Policía Nacional del Ecuador cuenta con un hosting administrativo, exclusivo de la Policía Nacional del Ecuador, al momento cuenta con las siguientes medidas de seguridad:

- Firewall de aplicaciones Web (WAF), para proteger de ataques y amenazas.
- Acceso restringido, solo personal autorizado puede ingresar al sistema.

- Cifrado de datos: Los datos almacenados en el servidor de hosting están encriptados.
- Protección contra malware y virus.

PROPUESTAS:

- **Infraestructura:**

✓ Actualizar Apache 2.4.41 a la última versión estable (ej: 2.4.58) para corregir vulnerabilidades.

✓ Implementar un WAF (Web Application Firewall) como ModSecurity o activar el WAF de Cloudflare.

- **Prácticas:**

✓ Cifrar discos con LUKS (Linux Unified Key Setup) y realizar backups diarios en ubicaciones georreduntantes.

3.12.2.2. Prestadores de Servicios.

La página web de la Policía Nacional del Ecuador, no cuenta con prestadores de servicio externos pues su diseño y manejo está a cargo de la Dirección Nacional de Tecnologías de la Información.

PROPUESTAS:

- **Cloudflare:**

✓ Habilitar protección DDoS avanzada y WAF gestionado con reglas personalizadas.

- **Contratos:**

✓ Exigir a proveedores externos certificaciones ISO 27001 y cláusulas de auditoría anual.

3.12.3. Gestores de Correo Electrónico:

3.12.3.1. Medidas de Seguridad.

La página web de Policía Nacional cuenta con **https** para resguardar los datos enviados a través de los formularios de protección de datos o denuncias ciudadanas, así se asegura que la información compartida se encuentre segura.

PROPUESTAS:

- **Cifrado:**

✓ Forzar el uso de TLS 1.3 en todos los correos salientes y configurar DANE/TLSA para validación de certificados.

- **Autenticación:**

✓ Implementar 2FA (doble factor) para cuentas institucionales usando aplicaciones como Google Authenticator.

3.12.3.2. Prestadores de Servicios.

La página web de la Policía Nacional del Ecuador, no cuenta con prestadores de servicio externos pues su diseño y manejo está a cargo de la Dirección Nacional de Tecnologías de la Información.

PROPUESTAS:

- **Migración a Plataformas Especializadas:**

- ✓ Usar servicios como Microsoft 365 Government o ProtonMail con cifrado de extremo a extremo.

- **SLA (Acuerdo de Nivel de Servicio):**

- ✓ Establecer un SLA con tiempos de respuesta <1 hora para incidentes críticos (ej: filtración de datos).

CAPITULO 4

4. DESCRIPCIÓN DE LO QUE ES UN PLAN DIRECTOR DE SEGURIDAD Y LOS BENEFICIOS PARA LA EMPRESA.

El plan director de seguridad es un marco estratégico integral que define los lineamientos, políticas, procedimientos y controles necesarios para salvaguardar los activos críticos de una organización, incluyendo recursos físicos, digitales, humanos y operativos. Su diseño se basa en un enfoque proactivo de gestión de riesgos, alineado con estándares internacionales como la norma ISO 31000:2018, que prioriza la identificación, evaluación y mitigación de amenazas para garantizar la continuidad operativa y la integridad institucional.

En el contexto de la Unidad de Mantenimiento del Orden (UMO) Z09 de Quito, el plan director de seguridad se enfoca en la gestión segura de las Tecnologías Menos Letales, abarcando desde su almacenamiento y mantenimiento hasta su despliegue operativo. Este plan integra:

a) Políticas de seguridad:

- Normas claras para el acceso, manipulación, almacenamiento y custodia de las tecnologías menos letales.
- Directrices éticas para el uso de agentes químicos lacrimógenos, alineadas con estándares de derechos humanos.

b) Procedimientos operativos estandarizados:

- Protocolos para inventarios, mantenimiento preventivo, revisión mensual de condiciones de almacenamiento, auditorías, capacitación y respuesta ante incidentes.

c) Tecnologías de apoyo:

- Sistemas de control de acceso biométrico, software de gestión documental (Quipux) y herramientas de ciberseguridad.

d) Roles y responsabilidades:

- Designación de responsables directos y equipos de soporte técnico.

e) Cumplimiento normativo:

- Adaptación a la Ley Orgánica de Protección de Datos Personales y al Reglamento de Uso Legítimo de la Fuerza.
- Preparación para auditorías externas mediante registros estandarizados (ej. fichas de entrega-recepción de las Tecnologías Menos Letales).

4.1 Check List Pds.

4.1.1 Análisis de la Situación Actual de la Empresa.

Actualmente, la UMO Z09 carece de un Plan Director de Seguridad formalizado. Si bien existen prácticas operativas para la gestión de las Tecnologías Menos Letales, no hay procedimientos unificados, digitales ni certificados que garanticen su eficacia. El espacio físico como bodega, no cumple con las especificaciones técnicas correspondientes de seguridad física para el correcto almacenamiento de las Tecnologías Menos Letales, careciendo de seguridades, así como también la trazabilidad se realiza en registros físicos, y no hay lineamientos de seguridad específicos actualizados. A continuación, se detalla un análisis exhaustivo de la situación actual, contrastando las deficiencias con los requisitos de la norma ISO 31000:2018:

a) **Infraestructura Física y Almacenamiento:**

- **Espacios inadecuados:** Los sitios donde se encuentran almacenadas las Tecnologías Menos Letales carecen de especificaciones técnicas básicas, como sistemas de ventilación especializados para evitar acumulación de vapores químicos (ej: agentes lacrimógenos CS).
- **Seguridad física insuficiente:** No existen controles biométricos; el acceso se gestiona con llaves convencionales y registros en papel. Tampoco hay cámaras de vigilancia en zonas críticas como el área de almacenamiento de municiones.

- **Falta de señalización:** Ausencia de rótulos que indiquen riesgos químicos o protocolos de emergencia, incrementando el peligro de accidentes.

b) Trazabilidad y Gestión de Inventarios:

- **Registros físicos obsoletos:** La trazabilidad de las Tecnologías Menos Letales depende de libros de actas y fichas en papel, lo que dificulta la auditoría en tiempo real y aumenta el riesgo de pérdida o manipulación no autorizada.
- **Falta de digitalización:** No se utilizan sistemas integrados (ej: códigos QR o RFID) para monitorear caducidad de materiales o movimientos de inventario.

c) Seguridad Digital y Ciberseguridad:

- **Software desactualizado:** Uso de Avast Free Antivirus sin licencias empresariales, lo que limita la protección contra amenazas avanzadas como ransomware.
- **Redes no segmentadas:** Todos los dispositivos comparten la misma red, facilitando la propagación de malware a sistemas críticos (ej: inventarios de las Tecnologías Menos Letales).
- **Accesos no regulados:** Contraseñas estáticas y sin políticas de complejidad, sin autenticación multifactorial para sistemas sensibles.

4.1.2 Plan Estratégico en Materia Tecnológica.

Dado que actualmente no se cuenta con un Plan Director de Seguridad formalizado en la Unidad de Mantenimiento del Orden (UMO) Z09 de Quito, se propone un plan estratégico tecnológico para mejorar los procedimientos de seguridad en el almacenamiento y gestión de Tecnologías Menos Letales. Este plan se estructura en dos niveles de complejidad Básico (B) y Avanzado (A) y tres alcances, Procesos (PRO), Tecnología (TEC), Personas (PER), alineados con los objetivos institucionales y la norma ISO 31000:2018.

Tabla 5

Plan estratégico en materia tecnológica

Nivel	Alcance	Control	Acciones Específicas	Vinculación ISO 31000:2018
A	PRO	Analizar la situación actual	- Diagnóstico integral de vulnerabilidades en infraestructura física (bodegas sin ventilación) y digital (registros en papel). -Uso de matrices FODA para priorizar riesgos operativos.	Cláusula 6.3: Evaluación de riesgos contextualizada.
A	PRO	Alinear el PDS con la estrategia institucional	- Integración del PDS al “Plan Estratégico 2025-2030” de la Policía Nacional.	Cláusula 5.3: Integración de la gestión de riesgos en procesos organizativos.
A	PRO	Definir proyectos a ejecutar	- Proyecto 1: Implementación de control biométrico en bodegas (15,000). - Proyecto2: Digitalización de inventarios con códigos QR (15,000).	Cláusula 6.4.3: Implementación de controles.

A	PRO	Clasificar y priorizar proyectos	- Priorización basada en impacto operativo (ej: control biométrico > inventarios digitales). - Uso de matriz MoSCoW para alinear recursos.	Cláusula 6.4.2: Selección de opciones para el tratamiento de riesgos.
B	PRO	Aprobar el PDS	- Validación por el Comité de Seguridad Institucional y difusión interna mediante plataforma Quipux.	Cláusula 5.4: Autoridad y compromiso.
A	PRO	Ejecución del PDS	- Implementación faseada: 6 meses para controles básicos, 12 meses para avanzados. -Monitoreo con KPIs: "% de Tecnologías Menos Letales auditadas", "tiempo de respuesta a incidentes".	Cláusula 8.2: Mejora continua.
A	PRO	Certificación en seguridad	- Certificación ISO 31000:2018 mediante auditorías externas (Bureau Veritas).	Cláusula 7.2: Competencia.

Nota: Inventario, Tomado de. (Z09, 2025)

4.2 Verificación de Controles.

Tabla 6

Verificación de controles de seguridad

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	Si se ha establecido políticas de seguridad por medio de documentos de confidencialidad y responsabilidad.	Responsable de seguridad	05/20/2025
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	No	Responsable de seguridad	05/20/2025
ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	Si cada uno de los departamentos y áreas de trabajo poseen usuarios y contraseñas personales, así como también institucionales.	Encargados de cada departamento y área de trabajo	05/20/2025
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	Se ha implementado un comité de seguridad de la información.	Responsable de seguridad	05/20/2025

ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	Sí, se ha creado los contratos de acuerdo con LDPD.	Responsable de seguridad	05/20/2025
ID_0006	¿Se dispone de un inventario de activos?	Cada área y departamento posee un archivo, realizándose inventarios correspondientes.	Responsable de Activos fijos	05/20/2025
ID_0007	¿Se ha definido quien es el responsable de los activos?	El Jefe de Unidad mediante designación correspondiente por escrito nombra el responsable de los activos fijos.	Jefe del Departamento de Apoyo Operativo	05/20/2025
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	Si, todo el talento humano, cumple un proceso de selección donde se obtienen todos los datos referenciales para pertenecer a la Unidad.	Departamento de Apoyo Operativo	05/20/2025
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	Sí, actualmente se cuenta con un cerco perimetral y con vigilancia de CCTV	Responsable de seguridad	05/21/2025

ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	Si, existe un área determinada que solo ingresa personal calificado y designado.	Responsable de seguridad	05/21/2025
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	Si, cada área se encarga de consolidad la información correspondiente de productividad.	Departamento de Coordinación Operativa y Planificación	05/21/2025
ID_0012	¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?	Si se posee el respaldo correspondiente tanto físico como digital.	Responsable de seguridad	05/21/2025
ID_0013	¿Se verifica regularmente la correcta realización de las copias se seguridad?	No	Responsable de seguridad	05/21/2025
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?.	Se realiza un mantenimiento correctivo y preventivo de los equipos por parte de los técnicos.	Responsable de TIC	05/21/2025
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	Si, se realiza un registro correspondiente y se pasa por auditorías internas, registrando lo más relevante.	Responsable de seguridad	05/22/2025
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?	No	Departamento de Apoyo Operativo	05/22/2025

ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	Se han establecido políticas de seguridad en contraseñas de forma institucional para lo cual se han determinado un mínimo de 8 caracteres.	Responsable de seguridad	05/22/2025
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	Si, se realizan las correcciones y recomendaciones correspondientes.	Responsable de seguridad	05/22/2025
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?)	Si, el talento humano tiene mucha atención al momento de cerrar las sesiones o bloquear sus equipos por ausencias determinadas.	Responsable de seguridad	05/22/2025
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	No	Responsable de seguridad	05/22/2025
ID_0021	¿Se controla la instalación de software en sistemas en producción?	Si, se restringe la instalación de programas no establecidos y se realizan inspecciones periódicas.	Responsable de TIC	05/22/2025
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	No	Responsable de TIC	05/22/2025

ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	El responsable de seguridad sigue los lineamientos correspondientes en base a un documento formal.	Responsable de seguridad	05/22/2025
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	En base a los lineamientos Institucionales y debido a la importancia operativa de la Unidad, existe una continuidad de gestión de la misma.	Departamento de Coordinación Operativa y Planificación	05/22/2025
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	No	Departamento de Coordinación Operativa y Planificación	05/21/2025
ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	Si se revisan, se evalúan y a la vez se actualizan en base a las necesidades correspondientes.	Departamento de Coordinación Operativa y Planificación	05/21/2025
ID_0027	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	Sí, el Departamento Legal los identifica oportunamente	Departamento Jurídico	05/21/2025
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	Si el Departamento de Asesoría Jurídica se ha encargado de establecer procedimientos claros y preventivos.	Departamento Jurídico	05/21/2025

ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	Sí, se cuenta con acuerdos de acuerdo a la LDPD.	Responsable de seguridad	05/21/2025
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	No	Responsable de seguridad	05/21/2025

Nota: Elaborado por Autores, Tomado de. (INCIBE, 2017)

4.3 Inventario de Activos.

4.3.1 Análisis de Riesgos. (Inventario de Activos).

Tabla 7

Verificación de controles de seguridad

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_0001	Computador de escritorio 36	Se utiliza para realizar trabajos del área administrativa	Responsable de seguridad (Oficial de Semana de la unidad)	Servidor (físico)	En los departamentos de secretaria del comando, Operaciones, secretaria del comando Z09, Apoyo Operativo, Coordinación Operacional, Activos Fijos, Rastrillero, Capacitación, Gestión	No

					GPR, Archivo ntral, Archivo de stión, Financiero.	
ID_0002	Laptops 03	Se utiliza para realizar trabajos del área administrativa	Responsable de seguridad (Oficial de Semana de la unidad)	Servidor (físico)	Departamento de Soporte Operativo	No
ID_0003	Impresoras 03	Se utiliza para realizar trabajos del área administrativa	Responsable de seguridad (Oficial de Semana de la unidad)	Servidor (físico)	En los departamentos del Comando, Coordinación Operacional, Soporte Operativo	No
ID_0004	Cámaras de seguridad 12	Cámaras para monitoreo de seguridad interna y externa	Responsable de seguridad (Oficial de Semana de la unidad)	Servidor (físico)	En el edificio del bloque N°03 piso 1,2,3,4 en el área del Gimnasio, Rastrillo, Parqueaderos, Muralla UMO	No

Nota: Elaborado por los Autores, Tomado de. Álava Et Al., 2018.

4.4 Análisis de Riesgos.

Tabla 8

Análisis de riesgos 1.

Amenaza/Activo	**A1**	**A2**	**A3**
Fuego	SI	SI	SI
Daños por agua	SI	SI	SI
Desastres naturales	SI	SI	SI
Fuga de información	SI	NO	NO
Introducción de falsa información	NO	NO	NO
Alteración de la información	SI	NO	NO
Corrupción de la información	SI	NO	NO
Destrucción de información	SI	NO	NO
Interceptación de información (escucha)	NO	SI	NO
Corte del suministro eléctrico	SI	NO	SI
Condiciones inadecuadas de temperatura o humedad	SI	NO	NO
Fallo de servicios de comunicaciones	SI	SI	SI
Interrupción de otros servicios y suministros esenciales	NO	NO	SI
Desastres industriales	SI	NO	NO
Degradación de los soportes de almacenamiento de la información	SI	NO	NO
Difusión de software dañino	SI	NO	NO
Errores de mantenimiento / actualización de programas (software)	SI	NO	SI
Errores de mantenimiento / actualización de equipos (hardware)	SI	NO	NO
Caída del sistema por sobrecarga	SI	NO	SI
Pérdida de equipos	SI	SI	SI
Indisponibilidad del personal	NO	NO	NO
Abuso de privilegios de acceso	SI	SI	SI
Acceso no autorizado	SI	SI	SI
Errores de los usuarios	SI	NO	NO
Errores del administrador	SI	NO	SI
Errores de configuración	SI	NO	SI
Denegación de servicio	NO	NO	NO
Robo	SI	SI	SI

Indisponibilidad del personal	NO	NO	SI
Extorsión	NO	NO	NO
Ingeniería social	SI	NO	NO

Nota: Elaborado por Autores, Adaptado a la UMO Z09, INCIBE, 2017.

Tabla 9

Análisis de Riesgo 2

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Ordenador(es)	Fuego	Bajo (1)	Alto (3)	3
Ordenador(es)	Daños por agua	Medio (2)	Alto (3)	6
Ordenador(es)	Desastres naturales	Bajo (1)	Alto (3)	3
Ordenador(es)	Fuga de información	Medio (2)	Alto (3)	6
Ordenador(es)	Alteración de la información	Medio (2)	Alto (3)	6
Ordenador(es)	Corrupción de la información	Bajo (1)	Bajo (1)	1
Ordenador(es)	Destrucción de información	Bajo (1)	Bajo (1)	1
Ordenador(es)	Corte del suministro eléctrico	Medio (2)	Bajo (1)	2
Ordenador(es)	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	Bajo (1)	1
Ordenador(es)	Fallo de servicios de comunicaciones	Bajo (1)	Medio (2)	2
Ordenador(es)	Desastres industriales	Bajo (1)	Alto (3)	3
Ordenador(es)	Degradación de los soportes de almacenamiento de la información	Bajo (1)	Medio (2)	2
Ordenador(es)	Difusión de software dañino	Medio (2)	Alto (3)	6
Ordenador(es)	Errores de mantenimiento / actualización de programas (software)	Medio (2)	Alto (3)	6
Ordenador(es)	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	Medio (2)	4
Ordenador(es)	Caída del sistema por sobrecarga	Medio (2)	Medio (2)	4
Ordenador(es)	Pérdida de equipos	Bajo (1)	Alto (3)	3
Ordenador(es)	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3

Ordenador(es)	Acceso no autorizado	Medio (2)	Alto (3)	6
Ordenador(es)	Errores de los usuarios	Medio (2)	Alto (3)	6
Ordenador(es)	Errores del administrador	Bajo (1)	Alto (3)	3
Ordenador(es)	Errores de configuración	Medio (2)	Medio (2)	4
Ordenador(es)	Robo	Bajo (1)	Alto (3)	3
Ordenador(es)	Ingeniería social	Bajo (1)	Bajo (1)	1
Móvil(es) principalmente para telefonía	Fuego	Bajo (1)	Alto (3)	3
Móvil(es) principalmente para telefonía	Daños por agua	Medio (2)	Alto (3)	6
Móvil(es) principalmente para telefonía	Desastres naturales	Bajo (1)	Medio (2)	2
Móvil(es) principalmente para telefonía	Interceptación de información (escucha)	Medio (2)	Alto (3)	6
Móvil(es) principalmente para telefonía	Fallo de servicios de comunicaciones	Medio (2)	Alto (3)	6
Móvil(es) principalmente para telefonía	Pérdida de equipos	Bajo (1)	Alto (3)	3
Móvil(es) principalmente para telefonía	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3
Móvil(es) principalmente para telefonía	Acceso no autorizado	Medio (2)	Alto (3)	6
Móvil(es) principalmente para telefonía	Robo	Bajo (1)	Alto (3)	3
Conexión a Internet e incluso wifi	Fuego	Bajo (1)	Alto (3)	3

Conexión a Internet e incluso wifi	Daños por agua	Medio (2)	Alto (3)	6
Conexión a Internet e incluso wifi	Desastres naturales	Bajo (1)	Alto (3)	3
Conexión a Internet e incluso wifi	Corte del suministro eléctrico	Medio (2)	Alto (3)	6
Conexión a Internet e incluso wifi	Fallo de servicios de comunicaciones	Medio (2)	Alto (3)	6
Conexión a Internet e incluso wifi	Interrupción de otros servicios y suministros esenciales	Bajo (1)	Alto (3)	3
Conexión a Internet e incluso wifi	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	Alto (3)	3
Conexión a Internet e incluso wifi	Caída del sistema por sobrecarga	Medio (2)	Alto (3)	6
Conexión a Internet e incluso wifi	Pérdida de equipos	Bajo (1)	Medio (2)	2
Conexión a Internet e incluso wifi	Abuso de privilegios de acceso	Alto (3)	Medio (2)	6
Conexión a Internet e incluso wifi	Acceso no autorizado	Medio (2)	Medio (2)	4
Conexión a Internet e incluso wifi	Errores del administrador	Bajo (1)	Medio (2)	2
Conexión a Internet e incluso wifi	Errores de configuración	Bajo (1)	Alto (3)	3

Conexión a Internet e incluso wifi	Robo	Medio (2)	Alto (3)	6
Conexión a Internet e incluso wifi	Indisponibilidad del personal	Bajo (1)	Bajo (1)	1
Conexión a Internet con wifi	Fuego	Bajo (1)	Alto (3)	3
Conexión a Internet con wifi	Daños por agua	Bajo (1)	Alto (3)	3
Conexión a Internet con wifi	Desastres naturales	Bajo (1)	Medio (2)	2
Conexión a Internet con wifi	Corte del suministro eléctrico	Medio (2)	Alto (3)	6
Conexión a Internet con wifi	Fallo de servicios de comunicaciones	Medio (2)	Alto (3)	6
Conexión a Internet con wifi	Interrupción de otros servicios y suministros esenciales	Bajo (1)	Alto (3)	3
Conexión a Internet con wifi	Errores de mantenimiento / actualización de programas (software)	Medio (2)	Alto (3)	6
Conexión a Internet con wifi	Caída del sistema por sobrecarga	Medio (2)	Medio (2)	4
Conexión a Internet con wifi	Pérdida de equipos	Bajo (1)	Alto (3)	3
Conexión a Internet con wifi	Abuso de privilegios de acceso	Medio (2)	Medio (2)	4
Conexión a Internet con wifi	Acceso no autorizado	Medio (2)	Medio (2)	4
Conexión a Internet con wifi	Errores del administrador	Bajo (1)	Medio (2)	2
Conexión a Internet con wifi	Errores de configuración	Bajo (1)	Medio (2)	2
Conexión a Internet con wifi	Denegación de servicio	Medio (2)	Medio (2)	4
Conexión a Internet con wifi	Robo	Medio (2)	Alto (3)	6

Nota: Elaborado por Autores, Tomado de. (INCIBE, 2017)

4.5 Clasificación y Priorización.

Tabla 10

Registro, Clasificación Y Priorización De Iniciativas.

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Revisión
IN_0001	Perdida de información.	Establecer un sistema de seguridad informática	Departamento de Planificación	Organizativa	2000,00 $	3 meses
IN_0002	Perdida de equipos	Incorporar sistemas de video vigilancia, controlada las 24 horas, asegurar los equipos tecnológicos.	Departamento de Planificación	Organizativa	1500,00 $	3 meses
IN_0003	Daños por agua	Incorporar un seguro para los equipos tecnológicos, esto con la copia de seguridad respectiva.	Departamento de Planificación	Organizativa	1500,00 $	3 meses
IN_0004	Fallo de servicios de comunicaciones	Su nivel perjudicial es mínimo, pues un corte de internet momentáneo no trae muchos problemas. Se recomienda obtener	Departamento de Logística	Organizativa	1200.00$	3 meses

		dos tipos de proveedores de internet satelital y troncalizado				
IN_0005	Errores de mantenimiento / actualización de programas (software)	Se debe realizar mantenimientos periódicos, con la finalidad de siempre tener la actualización del software.	Departamento Operativo	Técnica	1000,00 $	2 meses
IN_0006	Interceptación de Información.	A los usuarios que ocupan los equipos de la organización, se les debe capacitar para que conozcan cuales son las aplicaciones que no pueden ser interceptadas.	Departamento Operativo	Técnica	800,00$	1 mes
IN_0007	Difusión de software dañino	Se debe realizar capacitaciones con la finalidad de que los usuarios sepan detectar software ilegal y dañino.	Departamento Operativo	Técnica	600,00$	1 mes
IN_0008	Cortes de suministro eléctrico.	Se debe realizar las correcciones pertinentes en la red eléctrica, y al suceder un corte de luz. Se debe prever la obtención de un	Departamento de Logística	Organizativa	400.00$	3 meses

		generador de luz alterno.				
IN_0009	Condiciones inadecuadas de temperatura y humedad.	La humedad, es un mecanismo externo que puede afectar a una organización a largo plazo, se debe identificar los lugares vulnerables para realizar el mantenimiento correctivo.	Departamento de Logística	Organizativa	350.00$	3 meses

Nota: Elaborado por Autores, Tomado de. (INCIBE, 2017)

4.6 Check List Pds.

Tabla 11

Plan estratégico en materia tecnológica

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.	**X**

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 con su coste.	**X**
B	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.	

Nota: Elaborado por Autores, Tomado de. (INCIBE, 2017)

La implementación de este plan director de seguridad permitirá consolidar una cultura organizacional orientada a la prevención y gestión eficaz de riesgos, promoviendo una mayor trazabilidad, control y uso responsable de las tecnologías menos letales. Asimismo, reforzará la infraestructura institucional, optimizará los procesos logísticos y elevará los estándares operativos de la Unidad de Mantenimiento del Orden Z09.

A través de este plan, la UMO Z09 podrá anticiparse a potenciales amenazas, reducir su nivel de exposición a incidentes de seguridad, y fortalecer los mecanismos de respuesta ante emergencias o pérdidas de control en el almacenamiento y uso de armamento menos letal. Además, se establecerán prácticas documentadas alineadas con los principios de mejora continua, liderazgo,

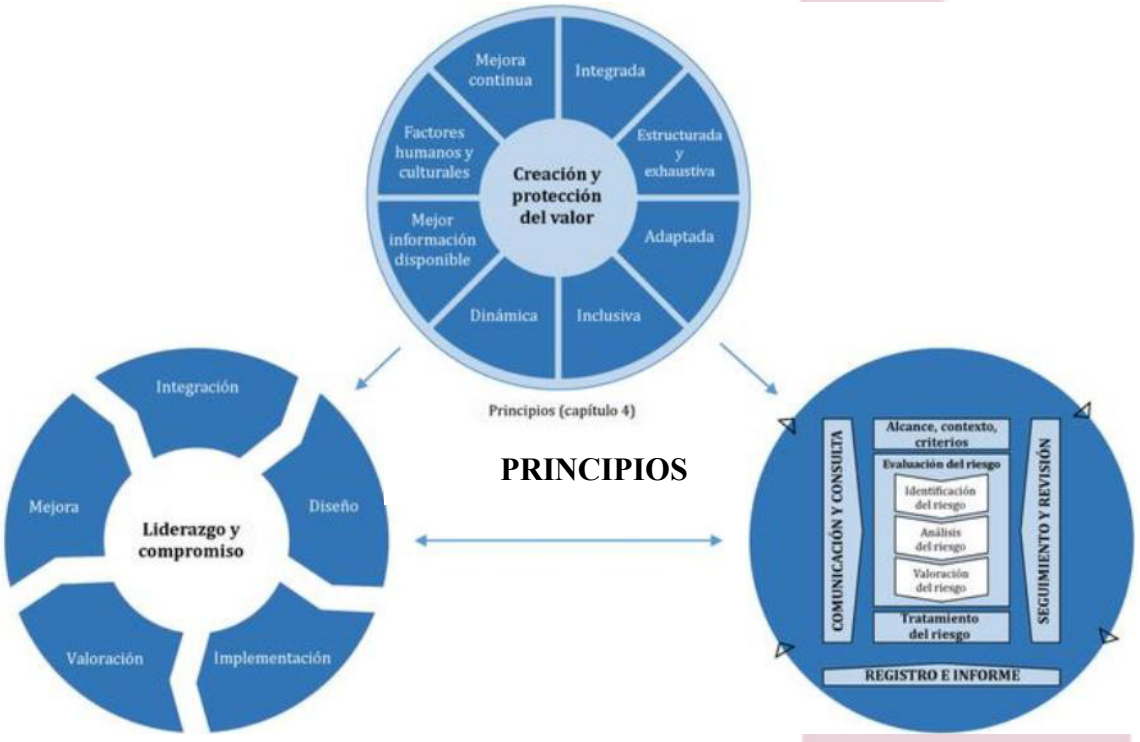
toma de decisiones basada en evidencia y cumplimiento normativo, conforme lo establece la norma ISO 31000:2018. Esto permitirá lograr una administración más eficiente, resiliente y transparente frente a auditorías internas y externas, así como un aumento sostenido en la confianza de la ciudadanía respecto a la actuación profesional de la unidad.

CAPITULO 5

5. PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO 31000:2018.

Figura 6

Principios, Marco de referencia y Proceso.



Nota: ISO 31000:2018

En el proceso de desarrollar esta propuesta para la Unidad de Mantenimiento del Orden Z09, entendimos que la gestión del riesgo no solo es una obligación operativa, sino una responsabilidad institucional, especialmente cuando se trata del manejo de las Tecnologías Menos Letales, ya que implican un alto nivel de riesgo si no se gestionan de forma adecuada.

Con base en este análisis, consideramos que la norma ISO 31000:2018 representa la herramienta metodológica más pertinente y eficiente para abordar esta necesidad ya que se trata de una norma internacional que ofrece principios y directrices para estructurar, implementar y mantener un sistema de gestión del riesgo adaptable y sostenible en cualquier organización, sin importar su tamaño o tipo. A diferencia de normas certificables como la ISO 9001 o ISO 45001, la ISO 31000 se enfoca en ofrecer una estructura flexible, lo que permite su integración con los procesos existentes de la UMO Z09.

Una de las razones por las que decidimos aplicar esta norma, es debido a su enfoque preventivo y estratégico, que no solo se adapta anticipar posibles incidentes relacionados con el almacenamiento o uso de las Tecnologías Menos Letales, sino también nos permite fortalecer la toma de decisiones y la asignación de recursos en escenarios de riesgo. Además, su estructura holística facilita la participación de todos los niveles jerárquicos, permitiendo que desde el servidor policial que cumple la función de Rastrillero hasta el último funcionario de la cadena de mando superior de la UMO Z09 estén involucrados en la gestión activa del riesgo.

Esta norma, además, considera factores humanos, culturales y organizacionales, lo cual es particularmente relevante en el contexto policial, donde el comportamiento humano, la presión operativa, la cultura institucional y la experiencia previa influyen significativamente en el manejo del riesgo; con ello, podemos integrar la realidad operacional de la unidad con criterios técnicos, administrativos y éticos de forma equilibrada, teniendo a su vez las siguientes ventajas:

a) Mejora en la seguridad del personal y de los activos:

La implementación de los procedimientos basados en la ISO 31000 permitirá minimizar los riesgos de exposición accidental, manipulación inadecuada o fallas en el almacenamiento de las Tecnologías Menos Letales. Esto se traduce en un entorno laboral más seguro para los policías encargados del rastrillo, los técnicos armeros, el personal operativo de la Unidad de Mantenimiento del Orden Z09, así como también para otros actores externos de la unidad.

b) Fortalecimiento del control logístico y documental:

Uno de los retos actuales identificados es el seguimiento adecuado de inventarios, caducidades, series y movimientos de material. La norma propone un sistema de gestión en el que el registro, monitoreo y evaluación del riesgo se integran con herramientas digitales, facilitando la trazabilidad y el control documental de las Tecnologías Menos Letales de la UMO Z09.

c) Cumplimiento normativo y respeto a los derechos humanos:

El uso de las Tecnologías Menos Letales está regulado por estándares nacionales e internacionales. La ISO 31000 refuerza el cumplimiento de esas normativas mediante acciones de prevención, control y evaluación, permitiendo que la UMO Z09 actúe en el marco de la legalidad y con absoluto respeto a los derechos fundamentales.

d) Estandarización y mejora de procesos operativos:

Mediante la aplicación de esta norma, se pueden establecer protocolos claros y procedimientos normalizados, lo cual evita interpretaciones erróneas o decisiones improvisadas en el manejo de las Tecnologías Menos Letales. Esto garantiza eficiencia operativa, menor margen de error y una reacción adecuada ante emergencias.

e) Incremento de la confianza institucional:

Al demostrar una gestión técnica, preventiva y responsable, se fortalece la confianza de la ciudadanía, del Estado y de la Institución (Policía Nacional del Ecuador), al contar con una unidad técnica, táctica y especializada, con la capacidad operativa, normativa y administrativa en la gestión de las Tecnologías Menos Letales.

f) Promoción de una cultura de mejora continua:

Finalmente, la ISO 31000 fomenta la creación de una cultura organizacional basada en la revisión periódica de los procesos, el aprendizaje institucional y la innovación en la gestión de riesgos, aspectos clave para sostener la eficacia del sistema en el tiempo.

5.1 Objeto y Campo de Aplicación.

La presente propuesta tiene como propósito diseñar e implementar un Sistema de Gestión del Riesgo basado en la norma ISO 31000:2018, con aplicación directa en los procesos de almacenamiento, control, custodia y uso de Tecnologías Menos Letales (TML) dentro de la Unidad de Mantenimiento del Orden Z09 de la ciudad de Quito.

El objetivo del sistema es garantizar la seguridad operativa, la trazabilidad, el cumplimiento normativo y la eficacia institucional frente al uso de las Tecnologías Menos Letales, minimizando la ocurrencia de incidentes y mejorando la capacidad de respuesta ante situaciones críticas o emergencias. Este enfoque está alineado con los principios de legalidad, proporcionalidad, responsabilidad y transparencia institucional.

El campo de aplicación abarca todos los procesos vinculados al ciclo de utilidad de las Tecnologías Menos Letales, desde su recepción, registro e inventariado, hasta su almacenamiento, distribución operativa, uso, recolección y disposición final. A su vez, involucra al personal técnico, administrativo y operativo encargado de su manipulación, asegurando que se apliquen criterios

técnicos, medidas de prevención, protocolos de actuación, control documental y formación continua.

Este sistema se implementará de manera transversal e integradora, incluyendo infraestructura física, plataformas digitales de control logístico, normativa institucional y formación operativa. De este modo, se fortalecerá la gestión institucional de riesgos, mejorando la eficiencia operativa de la UMO Z09 y alineando sus procesos a estándares internacionales de calidad y seguridad, conforme a lo establecido en la norma ISO 31000:2018, la cual proporciona principios y directrices para una gestión eficaz del riesgo (International Organization for Standardization, ISO, 2018).

5.2 Referencias Normativas.

La gestión eficaz del riesgo institucional requiere un sólido respaldo normativo que proporcione legitimidad, estandarización de procesos y lineamientos técnicos para su implementación. La norma ISO 31000:2018, reconocida internacionalmente, ofrece un enfoque estructurado y adaptable a cualquier organización, independientemente de su tamaño, sector o ubicación. Esta norma establece principios fundamentales como el enfoque sistemático, la mejora continua, la integración en todos los niveles de la organización y la toma de decisiones basada en evidencia. Además, promueve la transparencia y la participación de las partes interesadas, factores

clave para lograr una cultura sólida de gestión del riesgo (International Organization for Standardization, ISO, 2018).

En el contexto de la Unidad de Mantenimiento del Orden Z09, la incorporación de la ISO 31000:2018 permite optimizar el manejo de tecnologías menos letales, garantizar el cumplimiento de los marcos regulatorios nacionales, y fortalecer la confianza institucional y ciudadana en la labor policial.

Normativa Nacional:

- **Constitución de la República del Ecuador (2008):** Esta normativa fundamental establece los principios y garantías del Estado en temas de seguridad, orden público y derechos humanos. El artículo 158 define a la Policía Nacional como una institución civil armada, técnica y profesional, encargada de la protección interna. El artículo 163 refuerza la jerarquización y especialización de la fuerza pública. Por su parte, los artículos 389 y 390 establecen las bases del Sistema Nacional de Gestión de Riesgos, promoviendo acciones preventivas, de mitigación, respuesta y recuperación ante desastres de origen natural o antrópico (Asamblea Nacional del Ecuador, 2008).

- **Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público (2017):** Este código establece, en su artículo 3, las funciones generales de las entidades de seguridad, incluyendo prevención, disuasión, investigación y respuesta ante eventos que

comprometan la seguridad pública. Es una base legal clave para justificar las intervenciones tácticas y acciones de rescate o salvamento, que son propias de la UMO (Asamblea Nacional del Ecuador, 2017).

- **Acuerdo Ministerial N.º 080 - Estatuto Orgánico por Procesos de la Policía Nacional del Ecuador (2017):** Define la estructura operativa de la Policía Nacional y delimita, en los artículos 109 y 145, las competencias de la Unidad de Mantenimiento del Orden (UMO). Estas competencias incluyen la ejecución de intervenciones tácticas, operativos especiales y acciones ante desastres naturales o provocados por el ser humano (Ministerio del Interior, 2017).

- **Código Orgánico de Planificación y Finanzas Públicas (2010):** El artículo 9 estipula que la planificación institucional debe orientarse a garantizar derechos constitucionales mediante el ordenamiento territorial y el enfoque de desarrollo sustentable. La gestión del riesgo forma parte de esta planificación, lo cual legitima su inclusión dentro de los sistemas operativos y estratégicos de instituciones públicas como la Policía Nacional (Asamblea Nacional del Ecuador, 2010).

- **Ley Orgánica de Protección de Datos Personales (2021):** Regula el tratamiento de los datos personales y establece, entre los artículos 5 al 34, principios como licitud, transparencia, confidencialidad, minimización y consentimiento. Esta ley es esencial para

el manejo adecuado de los datos del personal policial que interactúa con sistemas digitales de control logístico y almacenamiento de las Tecnologías Menos Letales (Asamblea Nacional del Ecuador, 2021).

Normativa Internacional:

- **ISO 31000:2018 - Directrices para la gestión del riesgo:** Esta norma establece los principios, el marco y el proceso para la gestión de riesgos. Es aplicable a cualquier organización, independientemente de su tamaño, sector o actividad. Proporciona una guía para integrar la gestión de riesgos en todos los niveles de una organización, facilitando la toma de decisiones informadas, una mejor resiliencia institucional y una cultura de prevención sostenida (International Organization for Standardization [ISO], 2018).

- **ISO/IEC 31010:2009 - Métodos para la evaluación de riesgos:** Esta norma complementa a la ISO 31000 y proporciona una lista detallada de técnicas y herramientas de evaluación de riesgos, tales como análisis de modos de fallo y efectos (FMEA), árboles de fallos, matrices de riesgos, análisis costo-beneficio, entre otros. Su aplicación fortalece la capacidad analítica del sistema propuesto (International Electrotechnical Commission & ISO, 2009).

- **ISO Guide 51:2014 - Seguridad e inclusión en normas técnicas:** Establece lineamientos para incorporar requisitos de seguridad en normas técnicas, con el fin de reducir riesgos

durante el diseño y operación de productos, procesos y sistemas. Esta guía es especialmente relevante para el diseño seguro de infraestructura y almacenamiento de las Tecnologías menos Letales (International Organization for Standardization, ISO, 2014).

- **ISO/IEC 27001 - Seguridad de la información:** Proporciona un marco para establecer, implementar y mantener un sistema de gestión de seguridad de la información. Es esencial para asegurar la confidencialidad, integridad y disponibilidad de los datos operativos y personales manejados por la UMO Z09 (International Organization for Standardization & International Electrotechnical Commission, 2013).

- **ISO 22301 - Continuidad del negocio:** Establece requisitos para planificar, establecer, implementar, operar y mejorar un sistema de gestión de continuidad operativa. Resulta clave para garantizar la operación de la unidad en caso de interrupciones graves, como desastres naturales o disturbios (International Organization for Standardization, ISO, 2019).

- **ISO 45001:2018 - Seguridad y salud ocupacional:** Proporciona un marco para mejorar la seguridad de los trabajadores, reducir los riesgos en el lugar de trabajo y fomentar condiciones laborales seguras. Su integración refuerza la prevención de incidentes asociados al manejo de las Tecnologías Menos Letales (International Organization for Standardization [ISO], 2018b).

- **ISO 9001:2015 - Gestión de la calidad:** Define los criterios para un sistema de gestión de calidad enfocado en satisfacer las necesidades del cliente y mejorar procesos internos. Aplica para asegurar la calidad en la gestión operativa de recursos logísticos como las Tecnologías Menos Letales (International Organization for Standardization, ISO, 2015).

5.3 Términos y Definiciones.

En el contexto del sistema de gestión del riesgo propuesto para el manejo de Tecnologías Menos Letales, es fundamental establecer una terminología clara y coherente. A continuación, se describen los términos clave utilizados, conforme a los lineamientos de la norma ISO 31000:2018 y literatura especializada:

- **Amenaza:** Situación, condición o agente (natural, humano o tecnológico) con el potencial de causar daño a personas, bienes, operaciones o al medio ambiente. Ejemplo: almacenamiento incorrecto de gases lacrimógenos o fallas eléctricas (International Organization for Standardization, ISO, 2018).

- **Capacidad:** Recursos físicos, humanos, financieros y organizativos disponibles que pueden ser utilizados para reducir los impactos negativos de un riesgo o responder eficazmente ante una amenaza (United Nations Office for Disaster Risk Reduction, UNDRR, 2015).

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Puede tener consecuencias positivas o negativas y suele expresarse en términos de combinación de la probabilidad de ocurrencia y el impacto del evento (ISO, 2018).
- **Evaluación del riesgo:** Proceso general que comprende la identificación del riesgo, el análisis del riesgo y la valoración del riesgo, para facilitar la toma de decisiones (ISO, 2018).
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, promoviendo la integración del proceso en todas las áreas de la entidad (ISO, 2018).
- **Riesgo residual:** Nivel de riesgo que permanece después de implementar medidas de mitigación o control. Es necesario revisarlo continuamente en función de la eficacia de los controles (ISO, 2018).
- **Riesgo inherente:** Riesgo existente en ausencia de medidas de control. Representa el escenario más desfavorable y es clave para establecer planes de contingencia (ISO, 2018).
- **Medidas estructurales:** Acciones físicas como construcción de infraestructura segura, implementación de alarmas o instalación de ventilación especializada (Muñoz, 2016).

- **Medidas no estructurales:** Normas, procedimientos, planes de emergencia, capacitación y programas educativos orientados a la reducción del riesgo (Muñoz, 2016).
- **Cultura del riesgo:** Conjunto de valores, creencias, conocimientos y actitudes compartidas en una organización con relación al riesgo. Su fortalecimiento es clave para una gestión proactiva y sostenida (ISO, 2018).
- **Parte interesada:** Individuos o grupos que pueden afectar, verse afectados o percibirse como afectados por una decisión o actividad. Incluye autoridades, personal policial, ciudadanía y entes de control (ISO, 2018).
- **Fuente de riesgo:** Elemento que por sí solo o en combinación tiene el potencial de originar un riesgo. Ejemplo: deterioro de granadas aturdidoras por exposición a la humedad (ISO, 2018).
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias, que puede afectar directa o indirectamente los objetivos de la organización (ISO, 2018).
- **Consecuencia:** Resultado de un evento que afecta los objetivos. Puede ser positivo o negativo, directo o indirecto, y puede implicar efectos en cascada (ISO, 2018).
- **Probabilidad:** Oportunidad de que algo ocurra. Se puede expresar de manera cualitativa o cuantitativa, y es fundamental para evaluar el riesgo (ISO, 2018).

- **Control del riesgo:** Acción implementada para modificar el riesgo. Incluye decisiones de evitar, reducir, compartir o aceptar riesgos, dependiendo del análisis realizado (ISO, 2018).
- **Marco de gestión del riesgo:** Conjunto de componentes organizativos que proporciona los fundamentos y la disposición organizacional para gestionar el riesgo de manera eficaz (ISO, 2018).

5.4 Principios.

La gestión de riesgos tiene como propósito fundamental la creación y protección del valor institucional. Su implementación adecuada fortalece la capacidad operativa, mejora la toma de decisiones, fomenta la innovación en procedimientos y contribuye al cumplimiento de los objetivos estratégicos en materia de seguridad ciudadana y orden público.

Los principios de la gestión de riesgos proporcionan una guía clara sobre cómo diseñar procesos eficaces y eficientes dentro de la Unidad de Mantenimiento del Orden. Estos principios explican su propósito, refuerzan su importancia y orientan su integración en todas las áreas operativas, administrativas y estratégicas.

Constituyen el pilar para establecer tanto el marco de referencia como los procesos específicos de gestión de riesgos dentro de la Unidad de Mantenimiento del Orden. Aplicarlos permite anticipar, evaluar y mitigar los efectos de la incertidumbre, especialmente en contextos

operativos complejos, garantizando así un servicio policial más seguro, transparente y orientado a resultados.

5.4.1 Integrada.

Gestión de riesgos debe ser parte integral en todos los niveles y procesos de la Unidad de Manteniendo del Orden para la toma de decisiones, en cada adquisición, almacenamiento o retiro de las tecnologías menos letales que deben pasar un análisis documentado. En el área de operaciones las instrucciones de trabajo hacia le personal deben incluir protocolos de gestión de riesgos como el manejo, la inspección, el transporte y el tiempo.

El personal que esta encargad del almacenamiento del TML debe estar capacitado enn gestión de riesgos, seguridad física, normativa legal y control de inventarios, debe haber una coordinación entre logística, armería y mantenimiento planificación operativa para una gestión integral del riesgo. Su integración permite anticipar, identificar, evaluar y controlar los riesgos asociados a situaciones que pueden afectar la paz social, la seguridad ciudadana y el desarrollo de operaciones policiales o de control público.

Al aplicarse de forma transversal en la planificación, la toma de decisiones y la ejecución de acciones, la gestión de riesgos fortalece la capacidad de respuesta ante emergencias, reduce la exposición a eventos críticos y contribuye a garantizar un servicio más eficiente, seguro y confiable para la comunidad.

5.4.2 Estructurada y Exhaustiva.

El proceso de gestión de riesgos debe contar con su propia estructura que permita el fácil mantenimiento e implementación de procesos sistemáticos para la identificación, evaluación y tratamientos de los riesgos, que aborde los aspectos internos y externos que puedan afectar el logro de los objetivos. Se deben analizar los riesgos físicos donde están almacenados las TML, como la temperatura, humedad, ventilación, materiales inflamables y protección.

Los Riesgos operativos donde se controle entrada y salida del personal, custodia de las llaves y supervisión del inventario. Identificar los riesgos humanos para que n haya fuga de información, negligencia, manipulación incorrecta o sabotaje, se debe aplicar un control estricto al personal. Evaluar los riesgos legales y cumplir con la responsabilidad institucional. Tener una matriz de riesgos con niveles de probabilidad e impacto para priorizar controles.

Al aplicar un marco sistemático de gestión de riesgos en todas las fases de planificación y ejecución presente por este trabajo para la Unidad de Mantenimiento del Orden desde la prevención hasta la respuesta y recuperación, se facilita la evaluación objetiva de amenazas, se reducen las variaciones en el desempeño operativo y se promueve una cultura organizacional orientada a la mejora continua. Esta coherencia en la gestión permite comparar resultados entre diferentes unidades, regiones o periodos, optimizando recursos y elevando la efectividad de las intervenciones en materia de seguridad y control del orden público.

5.4.3 Adaptada.

No existe un enfoque único, la gestión del riesgo puede ser flexible, puede ajustarse a cambios y objetivos. En la gestión del riesgo se puede modificar continuamente las estrategias y acciones en respuesta a nuevas experiencias por la aplicación e implementación de la norma ISO 31000:2018. A la Unidad de Mantenimiento del Orden esta norma le beneficia con la aplicación de mejores prácticas en la búsqueda de encontrar la calidad, eficiencia y seguridad. Para esto se debe realizar evaluaciones periódicas del entorno operativo, con la finalidad de verificar si genera eficiencia y efectividad.

5.4.4 Inclusiva.

Se permite la participación apropiada y oportuna de todas las partes aceptables. Se reconoce la diversidad de perspectivas, puntos de vista y percepciones, permitiendo que se considere su conocimiento mediante la sensibilización, la formación y el compromiso activo de la alta dirección y el personal en todos los niveles de la empresa. Este tipo de gestión de riesgo es más informativa y efectiva, pues se facilita la participación interna y externa, para esto se utiliza medios de comunicación abierta.

Se puede considerar la colaboración de personas expertas entre los diferentes departamentos, esto con la finalidad de que la gestión del riesgo pueda ser clara, transparente y

eficaz. Para esto se debe realizar un proceso de retroalimentación entre los diferentes servicios y sectores de la Unidad de Mantenimiento del Orden.

5.4.5 Dinámica.

La Unidad de Mantenimiento del Orden está sujeta a cambios naturales de los riesgos. Esto implica anticiparse, detectar, reconocer y responder de una forma apropiada y oportuna a los cambios y eventos que puedan surgir durante las operaciones de mantenimiento del orden público.

Los riesgos aparecen generando cambios internos y externos en la organización, es por eso que el significado de dinámico significa flexible y adaptativo. Es por eso que la Unidad de Mantenimiento del Orden debe realizar periódicamente monitoreos continuos, con la finalidad de realizar detecciones tempranas de posibles cambios. Se debe realizar un análisis de los posibles riesgos y actualizar estrategias con la finalidad de contrarrestar nuevas realidades del entorno. Se deben realizar acciones inmediatas cuando existan riesgos emergentes.

5.4.6 Mejor Información Disponible.

En la Unidad de Mantenimiento del Orden QUITO (Z09), implica la utilización de la información más actualizada, precisa y relevante disponible para la toma de decisiones en el transcurso de las operaciones de manipulación y almacenamiento. Esto garantiza una gestión del riesgo informada y eficaz, permitiendo una respuesta más efectiva a situaciones de emergencia. Es esencial que el grupo cuente con información detallada y actualizada sobre las condiciones del

entorno, los recursos disponibles, las posibles amenazas y cualquier otro factor relevante que pueda influir en la seguridad y eficacia de las operaciones de manipulación y almacenamiento.

5.4.7 Factores Humanos y Culturales.

En la Unidad de Mantenimiento del Orden QUITO (Z09), implica considerar cómo la conducta humana y la cultura de la organización afectan todas las fases y niveles de la gestión del riesgo. Es fundamental comprender cómo estos factores pueden afectar la toma de decisiones, la comunicación, la colaboración y la eficacia de las operaciones de manipulación y almacenamiento.

La gestión del riesgo debe tener en cuenta la dinámica de las interacciones humanas y culturales para garantizar una respuesta efectiva y segura en situaciones de emergencia (Iturralde, 2011).

Los factores humanos y culturales que afectan a la Unidad de Mantenimiento del Orden QUITO (Z09) son:

Las fuentes de riesgo tangibles e intangibles: Estas fuentes pueden ser tanto tangibles, como por ejemplo instalaciones defectuosas, como intangibles, por ejemplo, la insuficiente formación del personal.

Las vulnerabilidades y capacidades: La vulnerabilidad para la unidad de Mantenimiento del Orden y Rescate podría ser la falta de equipos de protección personal adecuados, lo cual podría

poner en peligro la seguridad y la salud de los encargados de la manipulación y almacenaje durante las operaciones.

Las modificaciones en los entornos externo e interno: Podría ser la implementación de nuevas regulaciones gubernamentales que afectan los procedimientos de la manipulación y almacenamiento de estos recursos, lo cual impactaría en la manera los objetivos y preparación para situaciones de emergencia.

Falta de capacitación continua: Si el personal no recibe entrenamiento regular sobre el uso, manipulación y almacenamiento correcto de armas no letales, se incrementan los riesgos de accidentes o uso indebido, Cambios constantes de miembros en la unidad pueden llevar a diferencias en criterios o prácticas al manipular las armas, afectando la estandarización de procedimientos.

Falta de conciencia del riesgo: Algunos efectivos pueden subestimar el impacto físico o legal de un mal uso de estas armas, creyendo que no causan daño grave. El hábito de asumir que las armas no letales son “menos peligrosas” puede generar descuidos en su manipulación o almacenamiento.

Cultura organizacional permisiva: Si no hay una cultura fuerte de control, respeto a los protocolos o supervisión interna, pueden desarrollarse malas prácticas dentro de la unidad, se

puede volver común manipular armas no letales fuera de contexto o sin justificación operativa, lo que refleja una cultura institucional riesgosa.

5.4.8 Mejora Continua.

El principio de "Mejora Continua" en la Unidad de Mantenimiento del Orden, implicaría que la organización realice un seguimiento continuo y adapte sus procesos de gestión del riesgo en función de los cambios externos e internos. Esto permitiría a la organización mejorar la eficacia de sus operaciones de manipulación y almacenamiento a través del aprendizaje, la experiencia y la implementación de mejoras identificadas en el proceso de gestión del riesgo (Iturralde, 2011).

5.5 Marco De Referencia.

El marco de referencia para la gestión de riesgos en la Unidad de Mantenimiento del Orden Z09, constituye una estructura organizacional alineada a la norma ISO 31000:2018. Este modelo busca integrar la gestión de riesgos de forma transversal, asegurando su aplicación en todos los niveles jerárquicos de la unidad, especialmente en lo referente al almacenamiento, distribución y uso de las Tecnologías Menos Letales. La propuesta es firme porque no solo define procesos, sino que los ancla a una cultura institucional, al liderazgo transformador y a la infraestructura organizacional, con un enfoque orientado a la mejora continua, la transparencia y el cumplimiento normativo. Este enfoque estratégico también contempla las recomendaciones de organismos

internacionales sobre el uso responsable de la fuerza y el respeto a los derechos humanos, fortaleciendo el marco ético del sistema policial.

Además, este marco se visualiza como una herramienta estratégica que permitirá mejorar la capacidad de anticipación, preparación y respuesta frente a eventos críticos o imprevistos. Permite consolidar una visión proactiva de la seguridad operativa, integrando la gestión de riesgos como parte fundamental de la gobernanza institucional. La norma ISO 31000:2018 aporta una estructura lógica y metodológica que favorece la toma de decisiones basadas en análisis sistemáticos, lo cual eleva la calidad de las operaciones en contextos de alta presión como los que enfrenta la UMO Z09.

5.5.1 Generalidades:

Figura 7

Marco de Referencia

Nota: Tomado de. ISO 31000:2018

La Unidad de Mantenimiento del Orden (UMO Z09) cumple un papel fundamental en la seguridad interna del Ecuador, operando en contextos de alta exigencia como movilizaciones masivas, disturbios civiles y crisis sociales. En este entorno, el diseño e implementación de un sistema de gestión de riesgos basado en la norma ISO 31000:2018 representa una herramienta estratégica para garantizar la seguridad en el almacenamiento, custodia y uso de las Tecnologías Menos Letales, que incluyen municiones químicas, armas menos letales y dispositivos de control de multitudes. El Marco de Referencia que establece ISO 31000:2018 se estructura en tres componentes interrelacionados: Fundamentos, Arreglos Organizativos y Procesos de Implementación. Estos elementos constituyen la base para integrar la gestión del riesgo de manera sistemática y coherente en todas las operaciones logísticas de la UMO Z09.

5.5.1.1 Fundamentos.

Tabla 12

Fundamentos

Elemento	Descripción
Alcance	Aplicación transversal a la UMO Z09 en actividades operativas y logísticas con las Tecnologías Menos Letales.
Objetivos	Minimizar riesgos operativos, legales y reputacionales mediante controles proactivos.

Criterios de Riesgo Aceptable	Basados en el impacto de seguridad, cumplimiento legal y percepción pública.
Recursos Integrados	Tecnologías como inventarios digitalizados, y capital humano capacitado.

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

a) **Alcance:** El sistema de gestión de riesgos en la UMO Z09 está diseñado para cubrir de forma integral el ciclo de vida de las Tecnologías Menos Letales, lo cual garantiza trazabilidad, legalidad y seguridad en todas las fases; esto implica:

- **Recepción:** Bajo vigilancia y documentación, las Tecnologías Menos Letales se reciben mediante actas firmadas, verificación física, validación de número de serie y lotes.
- **Clasificación:** Se realiza en base a su naturaleza (química, cinética, acústica), condición, potencial de uso y nivel de riesgo operacional.
- **Almacenamiento:** Requiere estándares técnicos de ventilación, separación por tipo, accesos limitados por credenciales biométricas y monitoreo continuo.
- **Custodia:** Personal autorizado realiza control diario, mantiene registros físicos y digitales, y responde por el inventario asignado.

- **Uso en Operativos:** Cada entrega es justificada mediante orden de misión, asignada a un funcionario con experiencia y se documenta su uso y recuperación.
- **Mantenimiento:** Se efectúan pruebas de funcionalidad, detección de vencimientos o deterioro y procesos de reacondicionamiento.
- **Registro:** Los sistemas informatizados conectados a bases de datos institucionales permiten revisar historial completo de cada Tecnología Menos Letal.
- **Disposición Final:** La baja se formaliza mediante informe técnico, autorización superior y eliminación conforme a protocolos ambientales.

Este alcance se amplía a eventos de capacitación, entrenamientos, simulacros y uso en escenarios de conmoción interna, manteniendo trazabilidad y responsabilidad administrativa.

Normativa y Marco Legal: La gestión de riesgos se articula con un marco legal robusto que garantiza un accionar legítimo, ético y eficaz:

Tecnologías Menos Letales COESCOP: Establece los principios de proporcionalidad, legalidad y necesidad para el uso de la fuerza.

- **Normativa Interna de la Policía Nacional:** Define manuales técnicos, políticas de bioseguridad, normas de almacenamiento, transporte y activación de las Tecnologías Menos Letales.

b) Criterios de Riesgo Aceptable:

- **Legal:** El sistema clasifica como inaceptable cualquier filtración de información clasificada, violación a normas de acceso o alteración de registros.
- **Operativo:** Riesgos como fugas químicas, sabotaje, pérdida de material o mal uso intencional requieren protocolos de intervención inmediata.
- **Reputacional:** Se prioriza el control sobre la exposición mediática, reclamos ciudadanos o informes negativos derivados de malas prácticas en el uso de las Tecnologías Menos Letales.

c) Recursos:

- **Tecnológicos:**
  - **Quipux:** Gestiona comunicaciones institucionales y asegura trazabilidad de disposiciones.
  - **Iauditor:** Permite inspecciones móviles, control en tiempo real, generación de alertas.

- **Videovigilancia:** En zonas críticas con respaldo remoto por 180 días.
- **Códigos QR y sistemas RFID:** Aseguran trazabilidad rápida y en tiempo real.
- **Humanos:** Técnicos en armamento y logística certificados; Especialistas en gestión de riesgos, bioseguridad y TIC, e Instructores internos en protocolos de seguridad y manejo de crisis.

5.5.1.2 Arreglos Organizativos:

a) Liderazgo y Responsabilidades:

- **Alta Dirección:** El Comandante de la UMO Z09 lidera la implementación de políticas, evalúa reportes críticos y coordina con mandos superiores.
- **Responsables Técnicos:** Están a cargo de la ejecución operativa del sistema, manteniendo control visual y documental de cada fase.
- **Comité de Gestión de Riesgos:** Institucionaliza la supervisión, revisa lecciones aprendidas y propone ajustes de acuerdo con escenarios cambiantes.

b) Estructura de Coordinación:

- Niveles jerárquicos claramente definidos.

- Asignación nominal de responsables por fase (almacenamiento, custodia, entrega).
- Delegación de funciones basada en competencias técnicas verificadas.

c) **Comunicación y Cultura Organizacional:**

- **Transparencia Operativa:** Mediante herramientas digitales de acceso restringido pero verificable.
- **Cultura de Reporte:** Se incentiva la notificación oportuna de desviaciones, incidentes y mejoras.
- **Capacitación y Concienciación:** Incluye simulacros, jornadas de sensibilización y cursos virtuales.
- **Evaluación del Clima Organizacional:** Se realizan encuestas internas sobre percepción del riesgo y del sistema.

5.5.1.3 Procesos de Implementación:

a) **Identificación de Riesgos**: La UMO Z09 establece un enfoque activo de identificación, mediante:

- **Inspecciones internas:** Diarias o semanales, con checklists especializados.

- **Participación del personal:** Reportes y observaciones del personal operativo.
- **Revisión de incidentes previos:** Historial de eventos como base de escenarios críticos.

b) Evaluación y Tratamiento:

- **Evaluación Matricial:** Riesgos categorizados por su severidad (muy bajo a crítico) y su frecuencia (ocasional a frecuente).
- **Tratamiento del riesgo:** Puede implicar su eliminación, reducción, transferencia o aceptación documentada.

c) Medidas Mitigantes:

- **Estructurales:** Rediseño del área de almacenamiento, mejoras en sensores de movimiento, señalización luminosa.
- **Procedimentales:** Actualización de protocolos, auditorías sorpresivas, análisis forense digital post-evento.

d) Monitoreo y Mejora Continua:

- **KPIs:** cumplimiento del plan de mantenimiento, % de inventario verificado, tiempo medio de respuesta ante fallas.

- **Auditorías internas y externas:** Basadas en checklists normativos y verificación cruzada.
- **Retroalimentación institucional:** A partir de incidentes, inspecciones o recomendaciones externas.

e) Adaptabilidad en Crisis:

- Simulación de escenarios críticos cada trimestre.
- Revisión y activación del plan de contingencia en menos de 5 minutos.
- Coordinación con entidades externas (Fiscalía, Bomberos, Cruz Roja etc.).

5.5.2 Liderazgo y Compromiso.

El liderazgo y el compromiso son elementos decisivos para el éxito de cualquier sistema de gestión de riesgos, y en la Unidad de Mantenimiento del Orden Z09, estos principios son particularmente relevantes debido a la naturaleza crítica de las operaciones con las Tecnologías Menos Letales. De acuerdo con la norma ISO 31000:2018, el compromiso de la alta dirección debe evidenciarse en la asignación de recursos, la comunicación efectiva, la integración del riesgo en la toma de decisiones y la promoción de una cultura preventiva que atraviese todos los niveles de la organización.

La UMO Z09 ha desarrollado un enfoque institucional que combina liderazgo estratégico, operatividad táctica y mejora continua, creando las condiciones necesarias para consolidar un sistema de gestión robusto, ético y eficiente, en torno a cinco ejes fundamentales:

a) **Establecimiento de una Cultura de Gestión de Riesgos.**

ISO 31000: Liderazgo como motor de la cultura organizacional del riesgo

- **Visibilidad del liderazgo:** El comandante de la UMO Z09 no solo delega funciones, sino que actúa como referente directo del sistema, impulsando campañas internas sobre buenas prácticas, ética operativa y la importancia del cumplimiento normativo. Su liderazgo visible permite reforzar la coherencia entre el discurso institucional y la práctica diaria.
- **Comunicación estratégica:** Se establecen mecanismos de comunicación ascendente y descendente que permiten informar, alertar y retroalimentar en tiempo real. Los memorandos institucionales, informes de incidentes, y reportes de evaluación son acompañados por reuniones operativas que fortalecen la transparencia y la participación.
- **Ejemplo organizacional:** Se promueve el liderazgo ejemplar mediante la conducta ética y disciplinada de los mandos medios, lo que genera confianza en los servidores policiales y fortalece la legitimidad del sistema.

b) **Integración de la Gestión de Riesgos en la Estructura Organizacional**

ISO 31000: La gestión de riesgos debe integrarse en todas las funciones organizativas

- **Toma de decisiones basada en riesgos:** Las decisiones estratégicas, como el diseño de áreas blindadas, la implementación de control biométrico o la adquisición de tecnologías seguras, responden a evaluaciones de riesgo específicas, como la exposición a sabotajes, fugas de datos o fallas humanas.
- **Asignación formal de roles:** Cada función crítica dentro del sistema tiene un responsable designado. Por ejemplo:
  - **Capitán Carlos Itas Sevilla, Jefe del Departamento de Soporte Operativo:** líder institucional del sistema.
  - **Suboficial Edison Méndez Chulde, Rastrillero encargado:** ejecutor técnico y supervisor de los controles de acceso, mantenimiento, inventarios y documentación.
  - **Equipo de armeros certificados:** apoyan la gestión táctica del almacén bajo protocolos establecidos.
- **Creación de comités y estructuras de control:** Se proyecta la institucionalización de un Comité de Gestión de Riesgos que actúe de manera transversal e interdisciplinaria,

integrando perspectivas jurídicas, logísticas y operativas para análisis de incidentes, auditorías internas y desarrollo de planes de mejora.

c) **Capacitación y Desarrollo Profesional**

ISO 31000: Desarrollar competencias como base para una gestión efectiva del riesgo

- **Formación continua:** El sistema prevé capacitaciones semestrales en áreas como bioseguridad, manejo de materiales peligrosos, protección de datos personales, uso legítimo de la fuerza y administración de sistemas digitales de inventario. Estas formaciones incluyen simulacros de emergencia, revisión de casos reales y lecciones aprendidas.

- **Enfoque en liderazgo técnico:** No se limita a lo operativo. Los mandos medios reciben formación sobre análisis de riesgos, herramientas de gestión documental, y legislación aplicable (LOPDP, normativa institucional de la Policía Nacional), promoviendo una visión crítica y proactiva ante situaciones adversas.

- **Competencias certificadas:** El personal del rastrillo debe contar con certificación o experiencia comprobada en manipulación y administración de las Tecnologías Menos Letales, lo que contribuye a la reducción de errores operativos y mejora la trazabilidad del uso de los equipos.

d) **Recursos para la Gestión de Riesgos**

ISO 31000: El compromiso se traduce en recursos tangibles

- **Infraestructura adecuada:** Se propone la implementación de una sala blindada dentro del rastrillo, con sistema de acceso biométrico, cámaras de vigilancia conectadas a servidores internos y armarios ignífugos para proteger documentos físicos sensibles.
- **Sistemas tecnológicos:** Se utilizan herramientas como Quipux para la gestión documental oficial, Auditor para auditorías internas y formularios digitales, así como inventarios codificados con lectores de barra. Está prevista la migración a servicios en la nube (AWS o Azure) con cifrado AES-256.
- **Recursos financieros y logísticos:** El Comandante garantiza la asignación de presupuesto para adquisición de software, renovación de equipos, compra de Equipos de Protección Personal (EPP) certificados, y actualización del sistema de control de accesos.

e) **Revisión, Seguimiento y Mejora Continua**

ISO 31000: La gestión del riesgo es dinámica y debe evolucionar con el contexto

- **Auditorías y KPIs:** El sistema incluye indicadores clave como:
  - Reducción del 30% de incidentes por manipulación inadecuada de las Tecnologías Menos Letales en 6 meses.

- Cero pérdidas de inventario tras la implementación del sistema biométrico.
- 100% del personal operativo capacitado semestralmente.

Tabla 13

Indicadores Clave de Desempeño (KPIs)

Indicador	Meta	Periodo
Reducción de incidentes por mal uso de TML	-30%	Semestral
Capacitaciones completadas	100% del personal	Anual
Tiempo de respuesta ante incidentes	< 10 minutos	Inmediato
Cumplimiento de auditorías internas	95%	Trimestral
Propuestas de mejora implementadas	Mínimo 3 por trimestre	Trimestral
Niveles de percepción de confianza en la gestión de riesgos	> 80%	Anual

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

- **Revisión sistemática:** Las revisiones mensuales de inventario, informes operativos y simulacros sirven como insumo para identificar brechas, ajustar políticas y actualizar protocolos de emergencia.
- **Cultura del aprendizaje:** Los incidentes se documentan y analizan bajo una lógica no punitiva, promoviendo el aprendizaje institucional y reduciendo la repetición de errores.

Las lecciones aprendidas se incorporan en futuras capacitaciones y actualizaciones del sistema.

5.5.3 Integración.

La norma ISO 31000:2018 nos otorga un marco coherente para la gestión de riesgos la cual nos ayuda a mejorar la toma de decisiones y aumentar la resiliencia organizacional. Su enfoque en la integración de la gestión de riesgos implica asegurar que está practica no está como una actividad aislada, es decir que todos los miembros de la organización tienen la responsabilidad de gestionar riesgos, desde la alta dirección hasta el personal operativo debe tener un compromiso con la identificación, evaluación y tratamientos de riesgos en sus respectivas áreas de trabajo que es esencial para garantizar la seguridad y la eficacia operativa.

a) Política de Gestión de Riesgos.

En la unidad de mantenimiento del Orden Z09, debe haber una política de gestión de riesgos la cual debe ser clara y accesible para los empleados que defina los objetivos de la gestión de riesgos y su alineación con la estrategia general de la unidad, que incluya además los principios de gestión de riesgos como la integración en la toma de decisiones. Es crucial que haya una comunicación de esta política.

b) **Procesos Organizacionales.**

Se debe realizar una planificación estratégica y toma de decisiones para poder fomentar la gestión de riesgos dentro de la Unidad de Mantenimiento del Orden Z09. Se debe integrar:

- Planificación operativa y táctica
- Análisis de protocolos y los procedimientos operativos.
- Establecer grupos de trabajo o comités de gestión de riesgos que incluyan a empleados de las diversas áreas y de esta formase se fomente la colaboración de cambio de ideas.
- Evaluar e identificar los riesgos de la Unidad.
- Incluir auditorias y análisis de incidentes pasados para que una vez estén identificados los riesgos estos sean evaluados en términos de probabilidad en que ocurra y la severidad del impacto que causa.
- Uso de matrices de riesgo como herramienta de identificación de riesgos.

c) **Cultura organizacional.**

La alta dirección de la Unidad de Mantenimiento del Orden Z09 debe establecer expectativas sobre la importancia de la gestión de riesgos, incentivando una cultura organizacional donde todos los empleados tengan la responsabilidad de reportar y gestionar riesgos. El análisis de

riesgos debe ser en una reunión donde la alta dirección analice los informes de riesgos y medidas implementadas. Esto se logra con:

- Comunicación abierta y la colaboración entre los niveles de organización.
- Creación de un entorno donde el personal se sienta seguro al realizar el reporte de riegos o incidentes.
- Establecer grupos de trabajo o comités de gestión de riesgos que incluyan a todo el personal de las diferentes áreas.
- Fomentar el intercambio de ideas.

5.5.4 Diseño.

El diseño de un sistema de gestión de riesgos en la Unidad de Mantenimiento del Orden Z09 conforme a la norma ISO 31000:2018, nos ayuda a garantizar la seguridad y eficacia en el almacenamiento y manejo de las tecnologías menos letales por que deben tener elementos clave para evidenciar la relevancia para el éxito del sistema.

5.5.4.1 Compresión de la Organización y Su Contexto.

Se debe comprender el contexto interno y externo de la Unidad de Mantenimiento del Orden Z09. Esto influye en cómo se identifican y gestionan los riesgos asociados con el almacenamiento y uso de tecnologías menos letales.

a) **Contexto Interno.**

Es indispensable poder identificar los recursos que están disponibles, como el personal capacitado, la tecnología, la infraestructura, los valores, visión y misión. Además, hay que considerar las políticas y procedimientos existentes que guían la operación de la unidad. Se debe fomentar una cultura donde haya comunicación abierta y gestión proactiva de riesgos que facilita implementar medidas efectivas.

- **Misión y objetivos:** La misión de la Unidad de Mantenimiento del Orden Z09 es brindar la seguridad y orden público a través de una gestión correcta y adecuada de tecnologías menos letales.

  El objetivo es capacitar al personal en uso seguro y correcto de estos equipos, la reducción de incidentes y la promoción de un entorno seguro para la comunidad.

- **Capacidades y recursos:** El recurso principal es el personal y que se encuentra laborando en la unidad por lo que es crucial que este recurso humano este debidamente capacitado en gestión de riesgos y manejo de tecnologías menos letales. Además, el recurso tecnológico, como sistemas de monitoreo y almacenamiento seguro, es fundamental fundar medidas de mitigación adecuadas. Se de añadir un presupuesto para la capacitación y mejora de infraestructura.

- **Estructura organizacional:** La estructura organizacional de la Unidad Z09 debe facilitar la comunicación y organización entre los diferentes niveles jerárquicos.

  Es importante tener un organigrama donde defina los roles y responsabilidades para asegurar que todos comprendan su rol en la gestión de riesgos que coordine las actividades y actúe como enlace entre la dirección y el personal operativo.

- **Cultura organizacional:** Mantener una cultura que fomente la seguridad para crear un ambiente en que todo el personal tenga empoderamiento para que puedan identificar y reportar riesgos.

- **Competencia y Formación:** La competencia del personal es un aspecto fundamental en la gestión de riesgos. La unidad debe agregar programas de formación continua donde se aborde no solo el manejo de tecnologías menos letales, sino también la identificación y gestión de riesgos. La capacitación debe ser adaptada a las diferentes funciones y niveles de responsabilidad.

b) Contexto Externo.

- **Marco legal y Regulatorio:** Las leyes y regulación rigen el uso y almacenamiento de las tecnologías menos letales, así también las normas de seguridad y protección civil. Se debe cumplir de manera obligatoria estas regularizaciones para minimizar riesgos legales y financieros.

- **Entorno económico y social:** Esto puede afectar directamente la disponibilidad de recursos para la unidad. Factores como la financiación gubernamental, la inversión que se hace en seguridad pública y las prioridades presupuestarias influyen en la capacidad de la unidad para obtener tecnologías menos letales y hacer capacitaciones. La confianza pública es importante por lo que cualquier error puede repercutir en la reputación y el apoyo de la comunidad.

- **Condiciones Ambientales:** El clima, la geografía y la infraestructura local son factores que afectan al almacenamiento de tecnologías menos letales y en las operaciones diarias. La evaluación de riegos ambientales es fundamental para poder realizar estrategias de mitigación efectivas.

- **Tecnología:** La evolución de tecnologías nuevas nos ofrece herramientas más seguras y eficientes para el manejo de equipos menos letales, lo que puede también ocasionar nuevos riesgos. La unidad debe estar actualizada sobre las nuevas tecnologías y evaluar aplicación y seguridad en el contexto de operaciones. Se debe implementar un sistema de monitoreo y gestión de datos para así mejor la identificación de respuesta antes los riesgos.

- **Interacción con Otras Entidades:** Colaborar con Organismos gubernamentales, ONGs y la comunidad, es fundamental para proporcionar recursos adicionales y compartir buenas prácticas además de mejorar la respuesta ante emergencias.

c) Implementación:

Con base en este análisis del contexto interno y externo, la Unidad de Mantenimiento del Orden Z09, puede desarrollar un marco de gestión de riesgos fuerte y adaptativo:

- **Alineación con la Misión:** Garantizar la seguridad y el orden público a través de la gestión adecuada y responsable de tecnologías menos letales.
- **Integración completa:** La gestión de riesgos no debe verse como un proceso aislado, sino como parte integral de la cultura organizacional. Cada persona dentro de la Unidad debe estar involucrado en la identificación y gestión de riesgos.
- **Revisión continua:** La revisión continua del sistema de gestión de riesgos es muy importante para adaptarse a los cambios en el entorno operativo y en la naturaleza de los riesgos. Se debe incluir la evaluación regular de las estrategias implementadas y la identificación de amenazas nuevas.

5.5.4.2 Articulación del Compromiso con la Gestión del Riesgo.

Es un aspecto fundamental para garantizar la efectividad del sistema de gestión de riesgos de la Unidad de Mantenimiento del Orden Z09. Donde la alta dirección y todos los niveles de organización deben tener un visible compromiso para crear un ambiente en el que la gestión de riesgos sea parte integral de la cultura organizacional. A continuación, se detallan algunos de estos aspectos críticos:

a) Definición y Comunicación de la Política de Gestión de Riesgos.

Una política de gestión de riesgos es definida para establecer el marco de referencia para todas las actividades relacionadas con la gestión de riesgos. Esta política debe ser:

- Comunicada y aprobada de manera correcta a todos los niveles de la organización
- La comunicación debe incluir contenido de política y la importancia y el propósito de la gestión de riesgos.
- Transparente en la comunicación para generar confianza.

b) Integración en los procesos organizacionales.

Esto debe incluir:

- Planificación estratégica hasta la ejecución operativa.

- Cada proyecto debe considerar riegos y adoptar medidas de mitigación.
- Integración adecuada asegura que la gestión de riesgos sea parte integral de la toma de decisiones diarias.

c) Formación y capacitación.

Los programas de formación y capacitación para el personal en su totalidad deben:

- Abordar aspectos técnicos de la gestión de riesgos.
- Abordar una cultura de seguridad
- Adaptar diferentes funciones dentro de la unidad para asegurar que todos comprendan su papel y responsabilidad en la gestión de riesgos.

d) Recursos para la gestión de Riesgos.

La asignación de recursos es importante para una efectiva implementación de un sistema de gestión de riesgos, esto incluye:

- Recursos humanos que se dediquen a la gestión de riesgos.
- Presupuesto para actividades de gestión de riesgos.
- Recurso en tecnologías y equipo seguro para gestionar y mitigar riesgos dentro de la unidad.

e) **Monitoreo, Revisión y Mejora Continua.**

Para evaluar la efectividad de la gestión de riesgos debe incluir un enfoque en la mejora continua lo que se logra a través de:

- Auditorías internas periódicas para analizar la conformidad con los procedimientos establecidos y la efectividad de las medidas tomadas en gestión de riesgos.
- Monitorear indicadores clave que midan la efectividad de las estrategias tomadas en gestión de riesgos.
- Análisis de estrategias de mitigación para determinar si son efectivas o requieren ajustes.
- Análisis de incidentes y su raíz.
- Retroalimentación del personal donde recoja opiniones y sugerencias.

f) **Responsabilidad y Transparencia.**

Finalmente, la asignación de responsabilidades debe ser clara y todo el personal dentro de la Unidad de Mantenimiento del Orden Z09, debe conocer su papel y las expectativas en relación con la gestión de riesgos. La transparencia en la toma de decisiones y en la comunicación de resultados es crucial para poder incrementar un ambiente de confianza y colaboración donde se

comparta información sobre riesgos, medidas agregadas y resultados de las auditorias con todo el personal.

5.5.4.3 Asignación de Roles, Autoridades, Responsabilidades y Obligación de Rendir Cuentas en la Organización.

La Unidad de Mantenimiento del Orden Z09, es la encargada de fijar una visión y estrategia de gestión de riesgos, manteniendo siempre una coordinación con todos los objetivos generales de la Unidad de Mantenimiento del Orden Z09.

El comando de la Unidad de Mantenimiento del Orden Z09, es el encargado de establecer políticas de gestión de riesgos, le corresponde la toma puntual de decisiones y la asignación de recursos con la finalidad de que estas políticas de gestión de riesgos sean eficaces y eficientes. El comando de la Unidad de Mantenimiento del Orden Z09, será el encargado de presentar estrategias de mitigación y respuesta, al igual que será el encargado de realizar la debida rendición de cuentas, con la finalidad de dar respuesta a los organismos de control del Gobierno Nacional.

Los departamentos de planificación, soporte operativo y apoyo operativo serán los encargados de realizar la planificación y ejecución de las políticas de gestión de riesgos dentro de toda la estructura de la Unidad de Mantenimiento del Orden Z09, para lo cual deben realizar la identificación y evaluación de los riesgos posibles en las actividades que a diario se desarrollan

dentro de la institución. Estos departamentos informaran de su ejecución al comando de la Unidad de Mantenimiento del Orden Z09.

Los servidores policiales directivos y técnico operativos, serán los encargados de ejecutar las acciones que las políticas de gestión de riesgos, siendo participes de forma continua en la identificación y gestión de riesgos, informando de cualquier incidente al comando de la Unidad de Mantenimiento del Orden Z09.

El coordinador y único representante del equipo de gestión de riesgos es el señor jefe o comandante de la Unidad de Mantenimiento del Orden, quien tiene las siguientes funciones:

- **Coordinación:** Debe disponer para los diferentes departamentos realicen los procesos de planificación, ejecución y evaluación de gestión de riesgos.
- **Comunicación**: Debe tener una comunicación efectiva y constante con todos los niveles de la institución, con la finalidad de que cada nivel tenga claro el papel y rol a cumplir en la gestión del riesgo.
- **Desarrollo:** Debe gestionar políticas de cumplimiento a corto, mediano y largo plazo, con la finalidad de que las políticas de gestión de riesgos se cumplan.
- **Supervisión:** Se encargar de verificar que cada nivel cumpla los lineamientos establecidos, para el cumplimiento de las políticas de gestión de riesgo.

- **Revisión:** Ejecutara el análisis, supervisión y evaluación de las actividades realizadas y ejecutadas con la finalidad de verificar si se cumplió con los objetivos planteados.

5.5.4.4 Asignación de Recursos.

La unidad de Manteamiento del Orden Z09, debe realizar la asignación de recursos mediante los departamentos: Financiero, Soporte Operativo y Apoyo Operativo con la finalidad de genera una respuesta efectiva ante situaciones de riesgo. Para esto debe realizar las debidas coordinaciones con la finalidad de obtener capacitaciones, tecnología y herramientas.

a) Recursos Financieros.

El departamento Financiero, debe realizar el análisis para cuantificar y asignar un presupuesto económico que posibilite el cumplimiento de las políticas de gestión de riesgo.

Este presupuesto debe ser destinado para la adquisición de:

- **Tecnología:** Se debe adquirir equipos tecnológicos actualizados, los cuales ayuden a reducir el riesgo durante las actividades a realizar diariamente.
- **Capacitación**: Los servidores policiales que pertenecen a la Unidad de Mantenimiento del Orden, deben ser capacitados en técnicas y tácticas para prevención de riesgos, estas capacitaciones deben ser periódicas con la finalidad de estar actualizados y capacitados en todo momento.

b) Recursos Humanos.

Se debe asignar personal calificado y en el numérico necesario para cumplir con lo lineamientos de la gestión de riesgos. Es muy importante designar personal capacitado pues serán ellos los ejecutores de las políticas de gestión de riesgos, quienes mediante el uso de los recursos tecnológicos prevean y minimicen la incidencia de situaciones de riesgo.

c) Recursos Tecnológicos.

Se debe realizar la inversión en equipos tecnológicos y herramientas tecnológicas que ayuden a consolidar efectivamente la prevención de riesgos.

Se debe adquirir software y equipos de comunicación actualizados que ayuden a disminuir incidentes que generen un riesgo.

5.5.4.5 Establecimiento de la Comunicación y la Consulta.

La comunicación y la consulta es una actividad esencial para la Unidad de Mantenimiento del Orden Z09, puesto que tanto los componentes internos como externos deben estar informados sobre el proceso de gestión de riesgos a implementarse en la institución.

a) Comunicación Interna.

La comunicación dentro de la institución debe ser clara para todos los niveles, brindando accesibilidad a la información presente dentro de los lineamientos a trabajar, para lograr la eficacia al minimizar los niveles de riesgo de la institución.

Se debe mantener actualizando periódicamente la información, según la variación de las políticas y lineamientos de la gestión de riesgos. Esta información debe ser compartida por diferentes medios, pueden ser tecnológicos mediante la utilización de dispositivos móviles, correos electrónicos, redes sociales o presenciales utilizando las dinámicas de difusión de información presentes dentro de la institución como los franelógrafos o señaléticas de prevención de riesgos.

b) Comunicación Externa.

La comunicación externa es muy importante debido a que se debe informar a las partes interesadas sobre los procesos de gestión de riesgo desarrollados por la institución. Estas partes interesadas pueden pertenecer a la misma institución, o también a organismos rectores y de control del gobierno. La comunicación con las partes externas interesadas debe ser periódica y constante, esta comunicación se realiza mediante la entrega de documentación que respalde el cumplimiento de los procesos de gestión de riesgos, de igual forma se debe mantener copias de los documentos remitidos con la finalidad de tener respaldos del correcto cumplimiento de los objetivos.

c) **Consulta.**

La consulta debe ser una metodología utilizada en todo el proceso de gestión del riesgo. Mediante esta metodología se puede incluir a colaboradores externo e internos que tengan conocimiento en políticas de gestión de riesgo, quienes pueden ayudar con ideas o proyectos a implementar dentro de la institución con la finalidad de minimizar la incidencia de riesgos.

Al interior de la Unidad de Mantenimiento del Orden se debe mantener una participación permanente con servidores policiales conocedores de gestión de riesgos quienes, mediante la utilización de encuestas, pueden generar alternativas a ser incluidas dentro de las políticas o programas para disuadir la incidencia del riego.

5.5.5 Implementación.

Con el objetivo de implementar protocolos y procedimientos para el correcto almacenamiento, preservación y mantenimiento de las tecnologías menos letales entregadas en dotación a la Unidad de Mantenimiento del Orden Z09.

Se debe solicitar diferentes medios, con la finalidad de evitar la presencia de riesgos en el cumplimiento de este objetivo.

Para obtener un correcto almacenamiento, preservación y mantenimiento de tecnologías menos letales se necesita lo siguiente:

- **Infraestructura:** Con la finalidad de minimizar los riesgos se necesita una infraestructura extensa en donde se pueda almacenar de manera ordenada y sistemática todas las tecnologías menos letales. Este espacio debe tener reguladores de temperatura y humedad con la finalidad de solventar las especificaciones técnicas que solicita el fabricante de las tecnologías menos letales para su almacenamiento.

- **Tecnología:** Se debe realizar la adquisición e implementar medios tecnológicos. Contra incendios, alarmas de mitigación, circuito cerrado de videovigilancia, aspersores de agua, medios electrónicos de control de ingreso etc. Esto con la finalidad que a la leve presencia de un riesgo, los equipos tecnologías sea efectivamente suficientes para sobrellevar un riesgo menor.

- **Recurso Humano**: Se necesita la designación necesaria para que 01 servidor policial permanezcan en turnos de 8horas diarias, al control del centro de almacenamiento para tecnologías menos letales. Esto con la finalidad de mantener un control y evitar que personas ajenas tengan acceso a este tipo de tecnologías.

- **Presupuesto:** El departamento financiero de la Unidad de Mantenimiento del Orden Z09, debe destinar un rubro económico destinado para el arreglo o construcción del centro de almacenamiento. Al igual para la adquisición e instalación de los equipos tecnológicos

necesarios para mantener el control del centro de almacenamiento para tecnologías menos letales.

Los servidores policiales asignados al centro de almacenamiento de tecnologías menos letales, deben ser personas preparadas y capacitadas, quienes se encargarán del orden y control del centro. Además, serán los servidores principales quienes puedan reaccionar en primer lugar ante la presencia de un riesgo.

5.5.6 Valoración.

a) Objetivos Organizacionales:

- Se establecerá un programa de formación continua dirigido al personal responsable de las operaciones de almacenamiento y manipulación, con alcance nacional e internacional.
- El personal operativo será recertificado cada dos años mediante evaluaciones de desempeño funcional y verificación de competencias académicas.
- Se efectuarán evaluaciones anuales de condición física, salud mental y estado médico general.

b) **Análisis de la Eficiencia Operativa:**

- **Disminución de Incidentes y Accidentes:** Se analizará la efectividad de las estrategias de gestión de riesgos aplicadas, enfocándose en la reducción de incidentes y accidentes relacionados con el almacenamiento y manipulación. Esto incluirá la comparación de datos estadísticos antes y después de la aplicación de medidas específicas.
- **Respuesta a Emergencias:** Evaluar la rapidez y eficacia con la que el la UNIDAD DE MANTENIMIENTO DEL ORDEN QUITO (Z09) responde a emergencias, y cómo las prácticas de gestión de riesgos han mejorado estas respuestas.

c) **Valoración de la Capacidad de Resiliencia.**

- **Flexibilidad y Adaptabilidad:** Se evaluará la capacidad de la Unidad de Mantenimiento del Orden Quito (Z09) para ajustarse y responder eficazmente a condiciones dinámicas y escenarios imprevistos que puedan surgir durante sus operaciones. Esta habilidad es un componente fundamental para garantizar la continuidad operativa y la mitigación de riesgos, constituyendo un indicador clave para medir la efectividad y el valor real de las estrategias de gestión de riesgos implementadas. La evaluación considerará factores como la rapidez en la toma de decisiones, la eficiencia en la reasignación de recursos y la capacidad para

modificar protocolos operativos según las circunstancias cambiantes, asegurando así una respuesta óptima ante situaciones de emergencia o contingencia.

d) Medición de la Cultura de Riesgo.

- **Percepciones del Personal:** Se implementarán métodos de recolección de datos, como encuestas estructuradas y entrevistas en profundidad, para captar la percepción del personal acerca de las políticas y prácticas de gestión de riesgos. Esta evaluación permitirá identificar cómo las actitudes y opiniones del equipo influyen en su comportamiento operativo y en la toma de decisiones cotidianas, lo cual es crucial para fortalecer la cultura de seguridad organizacional y mejorar la efectividad de las estrategias preventivas y correctivas implementadas.

- **Cultura de Seguridad:** Se analizará de qué manera la implementación de la gestión de riesgos ha contribuido al fortalecimiento de una cultura de seguridad en la Unidad de Mantenimiento del Orden Quito (Z09). Esto incluye la promoción de una comunicación transparente y constante respecto a los riesgos identificados, así como el fomento del compromiso activo del personal con las mejores prácticas y protocolos de seguridad establecidos.

e) Relación Costo-Efectividad en la Gestión de Riesgos.

- **Evaluación Costo-Beneficio:** Se llevará a cabo un análisis detallado del costo-

beneficio de las acciones implementadas para la gestión de riesgos, con el fin de determinar su viabilidad económica. Este análisis contemplará tanto los costos directos como los beneficios obtenidos, tales como la reducción de pérdidas y el incremento en los niveles de seguridad.

- **Optimización del Uso de Recursos:** Se realizará una evaluación exhaustiva para determinar si los recursos asignados a la gestión de riesgos están siendo empleados de manera óptima y eficiente. Este análisis considerará no solo la correcta utilización de los insumos financieros, humanos y materiales, sino también su impacto real en la consecución de los objetivos establecidos. Se verificará si los recursos están generando los resultados esperados en términos de mitigación de riesgos, reducción de incidentes y mejora en los procesos operativos.

f) Mejoras Derivadas del Proceso de Evaluación.

- **Detección de Oportunidades de Mejora:** Con base en los resultados obtenidos de las evaluaciones realizadas, se determinarán las áreas específicas donde las estrategias de gestión de riesgos requieren ser mejoradas o ajustadas, con el fin de maximizar su eficacia y rendimiento operativo.

- **Desarrollo de Planes de Mejora:** Se procederá a la elaboración y diseño de planes de acción específicos y estructurados, orientados a fortalecer y corregir aquellos

aspectos identificados que requieran ajustes dentro de la Unidad de Mantenimiento del Orden Quito (Z09). Estos planes estarán cuidadosamente alineados con los objetivos estratégicos y operativos de la unidad, asegurando que cada medida implementada contribuya de manera efectiva al cumplimiento de sus metas institucionales.

5.5.7 Mejora.

Para que la Unidad de Mantenimiento del Orden Z09 conserve y potencie de forma continua la eficacia en la gestión de riesgos, es fundamental que su informe sobre dicha gestión se actualice permanentemente. Esto implica una vigilancia constante y la implementación de ajustes oportunos frente a posibles cambios tanto internos como externos que puedan influir en la organización. Adoptar este enfoque no solo asegura que el sistema de gestión de riesgos se mantenga vigente, sino que también fortalece el valor institucional al mejorar su capacidad de respuesta ante emergencias y situaciones de riesgo (Calderón Ramírez & Frey, 2017).

5.5.7.1 Adaptación.

La adaptabilidad asegura que la organización no solo mantenga su relevancia y eficacia en la gestión de riesgos, sino que también aproveche las oportunidades y mitigue los riesgos emergentes de manera proactiva. A continuación, se detallan los pasos y consideraciones para garantizar esta adaptación continua (Calderon Ramirez & Frey, 2017):

a) **Revisión Regular del Contexto Externo e Interno:**

- **Externo:** Monitorear cambios en el entorno legal, tecnológico, político, y social que podrían afectar las operaciones de la UNIDAD DE MANTENIMIENTO DEL ORDEN QUITO (Z09) e introducir nuevos riesgos.
- **Interno:** Observar cambios dentro de la organización como ajustes en la misión y objetivos, cambios en la estructura organizacional, y la incorporación de nuevas tecnologías o métodos.

b) **Análisis de Impacto:**

- Evaluar cómo las permutas identificadas afectan los riesgos existentes o crean nuevos riesgos.
- Evaluar la necesidad de modificar el marco de gestión de riesgos para adaptarse a estos cambios.

c) **Actualización de Políticas y Procedimientos:**

- Modificar las políticas de gestión de riesgos para reflejar los cambios en el ambiente operativo y los objetivos estratégicos de la organización.
- Ajustar los procedimientos para incorporar nuevas tecnologías, prácticas y conocimientos en las operaciones de rescate y gestión de riesgos.

d) **Capacitación y Desarrollo del Personal:**

- Desarrollar programas de formación continua para garantizar que todo el personal entienda las modificaciones en el marco de gestión de riesgos y cómo estas afectan sus roles específicos.
- Desarrollar habilidades en nuevas tecnologías y métodos que se hayan integrado en el marco de gestión de riesgos.

e) **Tecnología y Recursos:**

- Invertir en nuevas tecnologías que apoyen la gestión de riesgos actualizada y mejoren la eficiencia y seguridad de las operaciones.
- Garantizar que los recursos necesarios estén disponibles para implementar modificaciones y mejoras en la gestión de riesgos.

f) **Comunicación y Consulta.**

Diálogo Continuo con Partes Interesadas:

- Mantener comunicación regular con todas las partes involucradas, tanto el personal como autoridades y otras agencias de respuesta a emergencias, y la comunidad.
- Utilizar estos diálogos para recoger feedback sobre la percepción y seguridad de las estrategias de gestión de riesgos, para identificar áreas de perfeccionamiento.

Retroalimentación y Mejora Continua:

- Establecer mecanismos para integrar la retroalimentación en el proceso de revisión y mejora del marco de gestión de riesgos.
- Fomentar una cultura que valore la crítica constructiva y el aprendizaje continuo.

Evaluación de Efectividad.

Auditorías y Revisiones Programadas:

- Llevar a cabo auditorías periódicas y revisiones del sistema de gestión de riesgos para evaluar su eficacia y adecuación ante los riesgos actuales.
- Ajustar el cuadro basado en los resultados de estas valoraciones para mejorar continuamente la gestión de riesgos.

5.5.7.2 Mejora Continua.

Para garantizar que la mejora continua sea efectiva y contribuya al fortalecimiento de la gestión de riesgos en una organización como la UNIDAD DE MANTENIMIENTO DEL ORDEN QUITO Z09, se pueden seguir varias prácticas alineadas con las recomendaciones de la norma ISO 31000:2018. Considerando los siguientes aspectos:

a) **Evaluación de la Efectividad Actual.**

- **Auditorías y Evaluaciones Periódicas:** Llevar a cabo revisiones y evaluaciones

sistemáticas del marco de gestión de riesgos, con el objetivo de identificar fortalezas y oportunidades de mejora. Estas auditorías deben considerar el grado de integración de los procesos de gestión de riesgos en las actividades operativas cotidianas de la organización.

- **Evaluación del Desempeño:** Utilizar indicadores clave de rendimiento (KPI) para medir la efectividad de la gestión de riesgos en relación con el cumplimiento de los objetivos estratégicos y operacionales. Estos indicadores pueden incluir el tiempo de respuesta ante eventos, la eficacia de las acciones implementadas y los niveles de satisfacción de las partes interesadas.

b) Identificación de Brechas y Oportunidades.

- **Análisis de Brechas:** Emplear los resultados de las auditorías y evaluaciones para llevar a cabo un análisis de discrepancias, identificando áreas en las que el marco de gestión de riesgos actual no cumple con los estándares deseados o donde se puede mejorar.

- **Consulta con Partes Interesadas:** Incluir en el análisis de brechas el feedback de todas las partes interesadas, incluyendo empleados, la comunidad y otras entidades de respuesta a emergencias. Esto puede revelar oportunidades de mejora que no se habían considerado previamente.

c) **Desarrollo de Planes de Mejora.**

- **Planes de Acción:** Elaborar planes de acción minuciosos para solucionar las discrepancias encontradas. Cada plan debe contener objetivos concretos, tareas claramente delineadas, los recursos necesarios y un cronograma para su ejecución.
- **Asignación de Responsabilidades:** Asignar responsabilidades específicas por la implementación de cada aspecto del plan de mejora a individuos o equipos, asegurando que haya claridad sobre quién es responsable de qué acciones.

d) **Implementación y Monitoreo.**

- **Implementación de Mejoras:** Llevar a cabo las tareas según lo previsto, garantizando que todos los recursos necesarios estén disponibles y que los participantes comprendan sus roles y responsabilidades.
- **Monitoreo Continuo:** Implementar un sistema de seguimiento para evaluar el avance de las mejoras implementadas. Este sistema debe ofrecer información en tiempo real sobre la efectividad de las acciones y permitir ajustes rápidos si algo no se desarrolla como se había previsto.

e) **Evaluación Post-Implementación.**

- **Revisión de Impacto**: Una vez implementadas las mejoras, realizar una revisión para evaluar su impacto en la eficacia general del marco de gestión de riesgos. Esto

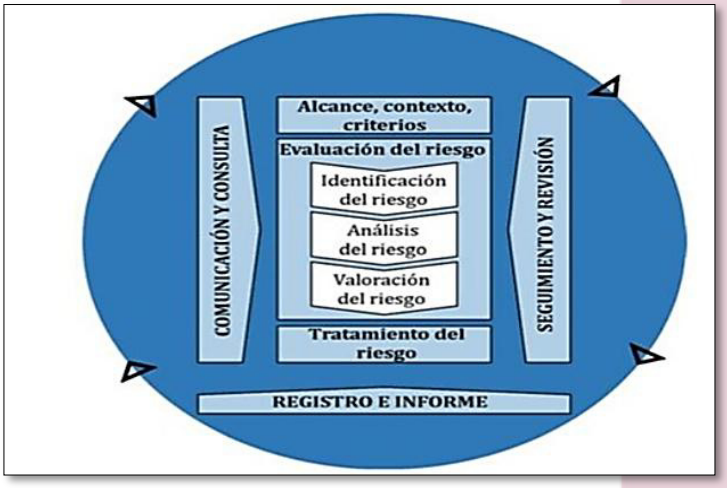
debería incluir la reevaluación de los indicadores de desempeño utilizados inicialmente.

- **Aprendizaje y Ajuste:** Aplicar las lecciones aprendidas de cada ciclo de mejora para ajustar el marco de gestión de riesgos y los procesos de mejora continua. Cada ciclo debe contribuir al fortalecimiento y perfeccionamiento de la gestión de riesgos.

5.6 Proceso.

Figura 8

Proceso



Nota: Proceso, Tomado de. (ISO 31000:2018 - (Figura))

5.6.1 Generalidades

La gestión de riesgos debe ser un componente fundamental para la Unidad de Mantenimiento del Orden Z09, lo cual influya en la toma de decisiones y el manejo de las operaciones a realizar.

Se debe realizar una integración de la gestión de riesgos tanto en el ámbito organizacional y estructural, dentro de cual se deben integrar los diferentes niveles organizacionales. El nivel directivo encargado de las decisiones y la planificación estratégica, en cambio el nivel operativo se encargará del cumplimiento de los procesos que ayuden a realizar una debida gestión de riesgos.

La gestión de riesgos administrativamente debe ser tomada en cuenta en la toma de decisiones en todos los departamentos organizacionales que tiene la Unidad de Manteamiento del Orden Z09.

- El Departamento Financiero: Le corresponde la correcta asignación y administración de los recursos económicos.
- El Departamento de Soporte Operativo: El correcto uso de los bienes y activos fijos, la nueva adquisición y mantenimiento de estos equipos.
- El Departamento de Apoyo Operativo: La administración del recurso humano, es muy importante para mantener una correcta gestión del riesgo, quienes deben tener

responsabilidades y ser profesionales para el cumplimiento de los procesos de gestión.

Cada departamento y equipo dentro de la Unidad de Mantenimiento del Orden Z09, debe tener roles claramente definidos en la gestión de riesgos, asegurando que las responsabilidades y procedimientos estén bien comprendidos y sean implementados de manera consistente.

Por ejemplo, en el nivel operacional, la gestión de riesgos puede centrarse en la seguridad en la infraestructura de la unidad y centro de almacenamiento de equipos menos letales. En el nivel estratégico, se puede enfocar la gestión de riesgos en el equilibrio organizacional y operativo que debe mantener la Unidad de Mantenimiento del Orden Z09, lo cual debe enfocarse ante cambios institucionales y gubernamentales.

a) Adaptabilidad a Contextos Externos e Internos:

Los enfoques de gestión deben ser adaptables y sujetos a cambios externos e internos, como puede ser los cambios de normativas, sistemas de seguridad, la implementación de nuevas tecnologías y la variabilidad en la presencia de los riesgos y amenazas.

b) Consideración del Comportamiento Humano y la Cultura.

La conducta humana es muy importante en los procesos de gestión de riesgos, esto puede depender de muchos factores como la capacitación, conocimiento y cultura. El objetivo es brindar capacitaciones sobre los procedimientos de seguridad que minimicen los riesgos. Adherir a la

organización personal capacitado, quienes tengan conocimiento de políticas y procesos encaminados a la eficiente gestión de riesgos.

c) Proceso Repetitivo:

La gestión de riesgos tiene un proceso cambiante, debido a muchos factores. Por lo cual se debe realizar un proceso de análisis, implementación y supervisión cada cierto tiempo. La práctica debe incluir evaluaciones regulares y retroalimentación para mejorar continuamente los enfoques y estrategias.

5.6.2 Comunicación y Consulta.

La comunicación y la consulta son procesos fundamentales que sustentan el sistema de gestión de riesgos bajo la norma ISO 31000:2018. Deben ser actividades continuas, estructuradas, bidireccionales e inclusivas que faciliten una comprensión compartida del riesgo y respalden una toma de decisiones efectiva y participativa. En el contexto operativo de la Unidad de Mantenimiento del Orden Z09 (UMO Z09), donde se emplean Tecnologías Menos Letales, estos procesos se convierten en ejes centrales para garantizar la seguridad, la legalidad y la eficiencia de las intervenciones; a su vez la correcta implementación de este proceso permitirá:

- Evitar errores operativos.
- Prevenir accidentes con material sensible.

- Proteger los derechos fundamentales de ciudadanos y servidores policiales.
- Fortalecer la legitimidad institucional.

Estas actividades permiten construir una comprensión común del riesgo, fortalecer el compromiso institucional y empoderar a todos los actores para participar activamente en la toma de decisiones, por lo que es importante establecer los siguientes fundamentos y acciones que se detallan a continuación:

a) Participación Multidisciplinaria e Inclusiva

La gestión de riesgos no puede ser exclusiva de una sola jefatura o departamento. Involucrar diferentes unidades promueve una visión integral y permite anticiparse a consecuencias no deseadas.

Acciones específicas:

Constitución de equipos técnicos multidisciplinarios con delegados de:

- Logística (Departamento de Soporte Operativo).
- Rastrillo.
- Operaciones (Departamento de Coordinación Operativa).
- Talento humano (Departamento de Apoyo Operativo).

- Departamento Jurídico de la UMO

Estos equipos se convierten en los grupos impulsores de la gestión de riesgos, fomentando la cooperación interdepartamental, donde cada departamento expone los riesgos que percibe en su ámbito, generando una matriz colectiva de riesgos, con priorización consensuada, con la finalidad de captar diversas percepciones del riesgo y enriquecer el análisis mediante la integración del conocimiento técnico, operativo, legal y humano.

- **Talleres participativos:** Se realizan reuniones quincenales con enfoque colaborativo, para compartir hallazgos, problemas operativos y propuestas de mejora.

b) Consultas Diversificadas para Valoración de Riesgos.

La consulta amplia permite detectar amenazas ocultas y validar medidas preventivas.

Acciones específicas:

Aplicación de encuestas confidenciales a los rastrilleros, custodios de los medios logísticos, tecnologías menos letales y personal operativo sobre:

- Falencias en el almacenamiento.
- Incidentes no reportados.
- Percepción de seguridad en la manipulación de las Tecnologías Menos Letales.

- Entrevistas cualitativas a jefes zonales y oficiales de semana sobre situaciones de riesgo vividas, para extraer lecciones aprendidas.

Consultas externas con actores clave como:

- Dirección de Logística de la Policía Nacional.
- Comités barriales o defensores de derechos humanos, cuando el uso de las Tecnologías Menos Letales pueda afectar entornos comunitarios.

c) Soporte para Toma de Decisiones y Control de Riesgos.

La comunicación efectiva es un instrumento de gestión táctica y estratégica. No basta con informar, es fundamental transformar la información en acción, por lo que los responsables de cada departamento toman decisiones basadas en datos confiables, oportunos y pertinentes, lo que reduce el tiempo de respuesta ante condiciones de riesgo.

Acciones específicas:

Diseño de reportes visuales y analíticos, con:

- Fichas técnicas por tipo de riesgo.
- Matrices de criticidad.
- Cronogramas de mantenimiento y revisión.

Difusión de alertas preventivas ante:

- Fallas en la ventilación de bodegas.
- Inventario por caducar.
- Alertas sobre municiones no aptas para uso operativo.

d) Fomento de Cultura Preventiva y Sentido de Propiedad

La cultura organizacional es un elemento invisible pero determinante. La consulta y la comunicación efectiva fomentan un sentido de corresponsabilidad y vigilancia colectiva, de esta manera se construye una cultura organizacional donde todo el personal de la UMO Z9 se sienten responsables, todos son escuchados y todos aportan a la gestión del riesgo.

Acciones específicas:

Programa de capacitación continua: Cursos obligatorios.

- Manipulación segura de las Tecnologías Menos Letales.
- Primeros auxilios en caso de exposición química.
- Talleres de ética policial: Uso legítimo de la fuerza.

Campañas de sensibilización:

- Carteles en zonas críticas: Recordatorios de protocolos.

- Testimonios de experiencias reales: Personal que ha enfrentado incidentes comparte aprendizaje.

e) Evaluación y Mejora Continua.

El monitoreo permite corregir desviaciones y optimizar continuamente los canales de comunicación y consulta.

Acciones específicas:

Indicadores de efectividad comunicacional:

- Porcentaje de participación en reuniones de consulta.
- Numero de reportes generados vs. resueltos.
- Tiempo medio de respuesta ante riesgos notificados.
- Nivel de satisfacción con los medios de información (evaluado mediante encuestas).

Revisión semestral del sistema de comunicación de riesgos, que incluya:

- Análisis de fallos.
- Retroalimentación del personal.

- Integración de herramientas digitales nuevas (por ejemplo, alertas por WhatsApp institucional o apps móviles).

Procedimiento Normalizado de Trabajo: Comunicación y Consulta

Tabla 14

Procedimiento Normalizado de Trabajo

Etapa	Actividad	Responsable	Herramienta	Frecuencia
Planificación	Identificación de actores clave	Coordinador de Riesgos	Matriz de partes interesadas	Anual
Consulta	Reuniones por unidad operativa	Jefes de área	Actas de taller participativo	Trimestral
Registro	Sistematización de riesgos detectados	Secretario técnico	F-RIES-001	Inmediata
Comunicación	Divulgación de alertas e informes	Oficial de comunicación	Boletines, Intranet, Correo	Mensual
Capacitación	Ejecución de talleres	Departamento de capacitación	P-CAP-UMO	Bimestral
Evaluación	Monitoreo de KPIs comunicacionales	Comisión de Riesgos	Informe KPI-RIES	Semestral

Mejora	Revisión del sistema comunicacional	Comité de Riesgos	Acta de mejora continua	Anual

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

5.6.3 Alcance, Contexto y Criterios.

Según Fernanda y Gómez (2015), una adecuada definición del alcance es fundamental para garantizar que la gestión de riesgos sea eficaz y esté alineada con los objetivos de la organización.

Determinación del Nivel de Aplicación: Arce Labrada y López Sierra (2010) señalan la importancia de definir con precisión los niveles dentro de la organización en los que se implementará la gestión de riesgos, ya sea a nivel estratégico, operativo, de programas o proyectos. También es necesario decidir si se aplicará de forma homogénea en toda la entidad o si se adaptará según las distintas áreas o tipos de iniciativas.

a) Planificación del Enfoque de Gestión de Riesgos.

- **Decisiones y Objetivos:** Identificar las decisiones clave y los objetivos que orientan la gestión de riesgos, enfocándose en aquellos que respaldan acciones estratégicas y operativas.
- **Resultados Esperados:** Determinar los beneficios esperados, con menor incertidumbre, mayor seguridad y mejor uso de recursos.

- **Tiempo y Ubicación:** Establecer cuándo y dónde se aplicarán las evaluaciones, según los ciclos de la UMO y los cronogramas de los proyectos.

b) Herramientas y Técnicas.

Elegir las herramientas y métodos apropiados para evaluar riesgos, considerando la naturaleza de las actividades y los objetivos de la UMO, como análisis cualitativos, cuantitativos y software especializado.

c) Recursos, Responsabilidades y Registros.

Es fundamental asignar los recursos necesarios y definir claramente las responsabilidades en cada etapa de la gestión de riesgos.

Además, se debe garantizar el adecuado manejo y conservación de los registros, asegurando su accesibilidad y protección.

d) Relaciones con Otros Proyectos y Procesos.

La gestión de riesgos debe integrarse con otras actividades y proyectos dentro de la UMO para optimizar recursos, evitar duplicidades y fortalecer su impacto en la organización.

e) Interrelación con los Objetivos Organizacionales.

- **Identificación de Riesgos Organizacionales:** Es fundamental reconocer que ciertos elementos vinculados con la estructura organizativa y las dinámicas operativas de la

Unidad de Mantenimiento del Orden pueden representar fuentes potenciales de riesgo. Estos factores deben ser identificados y abordados dentro del marco integral de gestión de riesgos institucional.

- Tal como lo señala Bernal Plaza (2021), es indispensable que la gestión de riesgos se mantenga en armonía con la misión y los objetivos estratégicos de la organización, asegurando así su coherencia y efectividad. (A.Bernal, 2021)

f) Análisis Continuo y Adaptación.

- **Flexibilidad y Adaptabilidad:** La estrategia de gestión de riesgos debe diseñarse con un enfoque flexible, que le permita ajustarse con agilidad frente a transformaciones en las condiciones del entorno, ya sean internas o externas.

- **Evaluación Continua:** Es necesario establecer un proceso continuo de análisis del entorno tanto interno como externo, con el fin de detectar oportunamente cambios que puedan incidir en la eficacia de la gestión de riesgos. Para ello, se recomienda implementar sistemas de seguimiento constantes y actualizar de forma periódica los análisis de riesgo.

g) Comunicación y Consulta.

- **Compartir Información:** Se debe promover un flujo de comunicación eficaz y transparente que permita compartir información clave sobre los factores internos y externos

que afectan la organización. Esto facilitará una comprensión más amplia del entorno y fomentará el respaldo colectivo a las iniciativas de gestión del riesgo.

- **Involucrar a Partes Interesadas:** Es esencial que todos los grupos de interés relevantes participen activamente en la identificación y revisión de los contextos organizacionales. Esto incluye al personal de la entidad, aliados estratégicos, entes reguladores y miembros de la comunidad.

5.6.3.1 Generalidades.

Para la Unidad del Mantenimiento y el Orden (UMO), una adecuada definición de los elementos clave es esencial para asegurar que el proceso de gestión de riesgos sea pertinente, enfocado y eficaz. Determinar correctamente el alcance, el contexto y los criterios permite realizar evaluaciones de riesgo más precisas y facilita el diseño de estrategias de tratamiento del riesgo adecuadas y efectivas.

5.6.3.2 Definición de Alcance.

Estructura Organizativa: Se debe analizar en qué medida la estructura interna de la Unidad facilita o entorpece la implementación eficaz de estrategias de gestión del riesgo, especialmente en lo relativo a la asignación de funciones y responsabilidades.

Capacidades y Recursos: Es crucial examinar los recursos humanos, materiales, tecnológicos y financieros disponibles, así como identificar las posibles limitaciones o fortalezas que puedan incidir en el proceso de gestión de riesgos.

Cultura Institucional: Se debe valorar el enfoque organizacional hacia la seguridad y la gestión del riesgo, incluyendo las percepciones, conocimientos y conductas del personal.

5.6.3.3 Contextos Externo e Interno.

La consideración de los contextos interno y externo resulta fundamental para diseñar una estrategia efectiva en materia de gestión de riesgos. En el caso del Grupo Unidad de Mantenimiento del Orden, identificar y comprender adecuadamente estos entornos es vital para garantizar que el enfoque adoptado esté en consonancia con la misión institucional y con los retos particulares que enfrenta la organización. (HOPKIN, 2018)

Contexto Externo.

El entorno externo comprende todos aquellos factores del medio ambiente, así como aspectos políticos, sociales, legales, regulatorios y económicos que pueden incidir en la capacidad de la Unidad para cumplir sus metas. Para lograr una adecuada caracterización de este entorno, se deben abordar las siguientes dimensiones:

- **Normativa y Marco Legal:** Implica la revisión de las disposiciones legales y normativas vigentes en el ámbito local, nacional e internacional que regulan y condicionan las acciones de rescate y respuesta ante emergencias

- **Análisis Ambiental y Social:** Es esencial examinar las condiciones naturales y sociales que podrían repercutir en las operaciones de la Unidad, tales como fenómenos climáticos extremos o situaciones sociales complejas.

- **Factores Económicos:** Es importante tener en cuenta la situación económica general y la disponibilidad de recursos, ya que estos elementos influyen directamente en la capacidad financiera y operativa que la Unidad puede destinar a la gestión de riesgos.

Contexto Interno.

Este hace referencia a los factores propios de la organización que afectan la manera en que se gestionan los riesgos. En el caso de la Unidad de Mantenimiento del Orden, se consideran los siguientes aspectos:

5.6.3.4 Definición de los criterios de riesgo.

Es fundamental que los criterios utilizados para evaluar y gestionar los riesgos sean detallados, específicos y lo suficientemente flexibles para adaptarse a diferentes situaciones. Estos

parámetros serán la base para valorar la importancia de cada riesgo identificado y servirán de guía en el proceso de toma de decisiones dentro del marco de gestión de riesgos de la organización.

- **Tolerancia al Riesgo:** Se debe establecer con claridad el nivel de riesgo que la organización está dispuesta a asumir en función de sus objetivos estratégicos. Esta definición debe contemplar tanto aquellos riesgos que la Unidad de Mantenimiento del Orden puede afrontar de manera controlada, como aquellos que, por su gravedad o posibles consecuencias, requieren de acciones correctivas inmediatas para proteger la seguridad y asegurar la eficiencia operativa.

- **Contexto de la Tolerancia al Riesgo:** Se deben establecer mecanismos claros para identificar y valorar tanto las posibles consecuencias positivas o negativas como la probabilidad de ocurrencia de los riesgos. Esta evaluación puede realizarse mediante indicadores cuantitativos (por ejemplo, pérdidas económicas estimadas o número de personas afectadas) y cualitativos (como el daño reputacional o el impacto en la salud y bienestar del personal). (Hillson, 2009)

- **Determinación de la Tolerancia al Riesgo:** La tolerancia al riesgo debe estar directamente alineada con los principios, misión y valores de la organización. Además, debe tener en cuenta los recursos humanos, técnicos y financieros disponibles para asegurar que las decisiones se mantengan dentro de los límites realistas de capacidad operativa.

a) **Criterios para la Valoración del Riesgo.**

- **Identificación de Consecuencias y Probabilidades:** Es fundamental establecer procedimientos que permitan medir y describir los posibles efectos de un riesgo, tanto beneficiosos como adversos, así como la probabilidad de que estos se materialicen. La evaluación puede basarse en criterios cuantitativos como la estimación de pérdidas económicas o la cantidad de personas potencialmente afectadas y cualitativos, como el impacto sobre la imagen institucional o el estado físico y emocional del personal involucrado.
- **Consideración de Incertidumbres:** Es esencial considerar los distintos tipos de incertidumbre que pueden incidir en el logro de los objetivos. Esto abarca desde factores impredecibles hasta aquellos desconocidos que podrían modificar significativamente los resultados esperados.

b) **Factores Temporales y de Contexto.**

- **Coherencia en las Mediciones:** Es recomendable establecer una metodología uniforme para la medición de riesgos en toda la organización, con el fin de asegurar que los análisis realizados en distintas áreas sean comparables y fácilmente interpretables a todos los niveles.

- **Factores Relacionados con el Tiempo:** Se debe analizar cómo los aspectos relacionados con el tiempo, como la urgencia en la respuesta o la existencia de ventanas críticas para la acción preventiva, afectan la evaluación del riesgo.

c) Determinación del Nivel de Riesgo.

- **Criterios para Determinar el Nivel de Riesgo:** Se deben aplicar herramientas precisas, como escalas de gravedad, matrices de riesgo o modelos de análisis, que permitan identificar con claridad el nivel de peligrosidad de cada riesgo identificado.

- **Consideración de Riesgos Múltiples:** Es fundamental establecer procedimientos para abordar situaciones en las que múltiples riesgos ocurren simultáneamente o de forma acumulativa, considerando tanto su interacción como su posible efecto multiplicador.

"La evaluación del riesgo debe considerar tanto la probabilidad de ocurrencia como las consecuencias, estableciendo criterios claros para determinar el nivel de riesgo mediante escalas, matrices u otros modelos.". (ISO 31000:2018, Gestión del riesgo – Directrices). (ISO31000, 2018)

d) Revisión y Adaptación de Criterios.

- **Procedimiento para ajustes:** Es recomendable definir un proceso formal que permita actualizar o modificar los criterios establecidos, asegurando así su vigencia, utilidad y adecuación a las nuevas circunstancias

- **Adaptación Permanente:** Se debe aceptar que los criterios de evaluación del riesgo no son estáticos, y por tanto requieren de una revisión periódica para responder adecuadamente a cambios en el entorno operativo, en la percepción del riesgo o en la capacidad institucional.

e) Comunicación de Criterios

Transparencia y Comunicación: Es esencial garantizar una comunicación clara y efectiva respecto a los criterios utilizados para la evaluación del riesgo. Todos los actores involucrados, tanto quienes tienen responsabilidades en la toma de decisiones como el personal operativo, deben comprender plenamente cómo se identifican, valoran y gestionan los riesgos dentro de la organización. Esta transparencia fortalece la coherencia en la aplicación de las políticas de gestión de riesgos y promueve una cultura organizacional orientada a la prevención y la respuesta informada.

5.6.4 Evaluación del riesgo.

5.6.4.1 Generalidades

La norma ISO 31000:2018 establece que la evaluación del riesgo es un proceso integral que comprende la identificación, el análisis y la valoración de los riesgos, realizado de forma estructurada y con la participación activa de todos los involucrados. Este procedimiento resulta fundamental para anticipar, reducir y controlar los riesgos dentro de la gestión diaria de las

operaciones tácticas en escenarios especiales, ya sean sensibles, emergentes o planificados, así como en labores de búsqueda, rescate y salvamento de personas ante desastres naturales o provocados por el ser humano.

De igual manera, en el ámbito administrativo de la Unidad de Mantenimiento del Orden (UMO) en Quito, perteneciente a la Policía Nacional, es indispensable incorporar el análisis de riesgos como parte de las estrategias orientadas a prevenir incidentes o accidentes que comprometan la seguridad de las personas o los bienes materiales. Para ello, es preciso realizar una evaluación del riesgo tanto cualitativa como cuantitativa, organizada en distintas categorías.

Tabla 15

Valoración de probabilidad.

Nivel de probabilidad	Descripción	Valor numérico
MUY ALTA	Ocurre con certeza.	5
ALTA	Alta posibilidad de ocurrencia.	4
MEDIA	Puede ocurrir ocasionalmente.	3
BAJA	Poca probabilidad de ocurrencia.	2
MUY BAJA	Rara vez ocurre o casi imposible.	1

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

Tabla 16

Valoración de Impacto

Nivel de impacto	Descripción	Valor numérico
CRITICO	Consecuencia extrema o catastrófica.	5
ALTO	Impacto significativo.	4
MEDIO	Afecta moderadamente las operaciones.	3
BAJO	Consecuencias menores o leves.	2
MUY BAJO	Rara vez existen consecuencias o es imposible.	1

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

5.6.4.2 Identificación del riesgo.

La identificación de riesgos consiste en el proceso de detectar, reconocer y documentar los riesgos. De acuerdo con la norma ISO 31000:2018, su finalidad es identificar, reconocer y describir aquellos riesgos que puedan influir positiva o negativamente en el cumplimiento de los objetivos de una organización. Para ello, los métodos empleados deben contar con información actualizada y contemplar diversas variables, como las fuentes del riesgo, los eventos y sus causas, así como oportunidades, amenazas, vulnerabilidades, capacidades e indicadores de riesgos emergentes. Este proceso se ve reforzado mediante el uso de herramientas como el Análisis Preliminar de Peligros (PHA), que facilita la detección de peligros o condiciones vulnerables.

Por su parte, la norma ISO 31010 recomienda métodos específicos de identificación, proporcionando herramientas técnicas de análisis del riesgo que contemplan distintos enfoques.

Para identificar adecuadamente los riesgos durante la ejecución de intervenciones especializadas en control del orden público, control de multitudes, protección de personas y bienes, así como en la prevención y restablecimiento del orden, es fundamental aplicar un enfoque sistemático y multidisciplinario. Los métodos adecuados deben considerar los siguientes criterios clave:

a) Riesgos físicos:

Incluyen peligros derivados de la interacción directa entre personas o con el entorno, tales como:

- Derrumbes de estructuras temporales o edificaciones debilitadas.
- Caídas y lesiones por empujones o superficies irregulares.
- Golpes o atrapamientos debido a aglomeraciones o movimientos descontrolados de la multitud.

b) Riesgos Ambientales:

Factores del entorno natural o del espacio físico que pueden afectar la seguridad:

- Condiciones climáticas adversas (calor extremo, lluvias intensas, tormentas eléctricas).

- Ambientes cerrados sin adecuada ventilación.
- Posibilidad de incendios por instalaciones eléctricas inadecuadas o acumulación de personas.

c) Riesgos Sociales:

Relacionados con la conducta colectiva de los asistentes:

- Comportamientos agresivos o desórdenes entre grupos presentes.
- Disturbios por provocaciones o presencia de contramanifestantes.
- Reacciones de pánico que pueden generar estampidas o avalanchas humanas.

d) Riesgos Sanitarios:

Aspectos vinculados a la salud pública:

- Propagación de enfermedades infecciosas (especialmente en contextos postpandemia).
- Ausencia de servicios médicos accesibles y visibles.
- Deficiencias en higiene, como falta de baños o agua potable.

e) **Riesgos Técnicos:**

Fallas en infraestructuras o equipos que soportan el evento:

- Interrupciones en el sistema de sonido, altavoces o megafonía.
- Problemas en la iluminación, especialmente si la manifestación se extiende hasta la noche.
- Mal funcionamiento de sistemas electrónicos de monitoreo o seguridad.

5.6.4.3 Análisis del riesgo.

De acuerdo con Fernanda y Gómez (2015), el análisis representa una herramienta fundamental para la Unidad de Mantenimiento del Orden (UMO) en Quito, ya que permite identificar los riesgos que posteriormente serán evaluados. Su propósito es comprender la naturaleza y las características del riesgo, considerando detalladamente la incertidumbre, las fuentes, las consecuencias, las probabilidades, los eventos, los escenarios, los controles y su eficacia. Las técnicas preventivas de análisis permiten realizar un pronóstico de los riesgos con potencial de afectación. El modelo de análisis a emplearse puede ser cualitativo, cuantitativo o una combinación de ambos. Este análisis de riesgos sirve como base para su evaluación, la toma de decisiones y el desarrollo de estrategias para su gestión. A partir de estos resultados, se obtiene un entendimiento más profundo que facilita una toma de decisiones informada.

Tras verificar distintos métodos, se propone elegir aquel que aporte resultados tanto cualitativos como cuantitativos. En este sentido, se selecciona como herramienta el Análisis Modal de Fallos y Efectos (AMFE), considerado un método eficaz para obtener una apreciación más precisa del riesgo.

Tabla 17

Análisis de riesgo de la probabilidad.

Valor	Tipo	Descripción
5	**MUY ALTA**	• El evento de riesgo ocurre en la mayoría de las circunstancias y/o está ocurriendo actualmente.
4	**ALTA**	• El evento de riesgo probablemente ocurrirá en la mayoría de las circunstancias. • Se ha recibido una amenaza directa y creíble, y/o ya ha ocurrido, o habría ocurrido si no se hubiera evitado activamente en varias ocasiones.
3	**MEDIA**	• El evento de riesgo puede ocurrir en algún momento, pero generalmente solo bajo circunstancias específicas. • Se han recibido amenazas indirectas. • Las condiciones pueden ser favorables para su ocurrencia.
2	**BAJA**	• El evento de riesgo podría ocurrir en algún momento. • No se han recibido amenazas directas. • Las condiciones actuales no son favorables para su ocurrencia.
1	**MUY BAJA**	• El evento de riesgo es poco probable que ocurra. • No hay antecedentes ni amenazas conocidas. • Las condiciones actuales hacen muy improbable su manifestación.

Nota: Análisis del Riesgo de la Probabilidad, Tomado de. (Publicación, 2018)

Tabla 18

Análisis del riesgo del impacto.

Valor	Tipo	Descripción
5	**CRÍTICO**	• Muerte de una persona. • Pérdida financiera o económica muy significativa, superior a $1,000,000. • Daño muy significativo a la imagen y reputación de la Unidad. • Pérdida de prestigio del UMO Z09.
4	**ALTO**	• Lesiones a personas. • Pérdida financiera muy significativa, entre $90,000 y $100,000. • Gran desprestigio o daño a la reputación a mediano plazo. • Pérdida significativa de la ventaja competitiva.
3	**MEDIO**	• Lesiones a personas que requieren tratamiento médico. • Pérdida financiera significativa, entre $90,000 y $500,000. • Desprestigio moderado o daño a la imagen que impacte a las ventas a corto plazo. • Posibilidad de pérdida de ventaja competitiva.
2	**BAJO**	• Lesiones menores que requieren tratamiento de primeros auxilios. • Pérdida financiera menor, entre $50,000 y $49,900. • Desprestigio menor, sin daño a la imagen ni reputación.
1	**MUY BAJO**	• Sin lesiones a personas. • Pérdida financiera muy menor. • Sin desprestigio ni daño a la imagen ni reputación institucional.

Nota: Análisis del Riesgo del Impacto, Tomado de. (INCIBE, 2017)

Tabla 19

Clasificación del Riesgo.

Impacto probabilidad	1 Muy baja	2 Baja	3 Media	4 Alta	5 Muy alta
5 Crítico	Moderado	Alto	Muy Alto	Muy Alto	Extremo
4 Alto	Moderado	Moderado	Alto	Muy Alto	Muy Alto
3 Medio	Bajo	Moderado	Moderado	Alto	Alto
2 Bajo	Bajo	Bajo	Moderado	Moderado	Moderado
1 Muy Bajo	Bajo	Bajo	Bajo	Bajo	Bajo

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

Tabla 20

Descripción de niveles de riesgo.

Nivel de Riesgo	Descripción	Acción Requerida
Extremo	Riesgo inaceptable. Requiere acción inmediata.	Detener la actividad y tomar medidas correctivas urgentes.
Muy Alto	Riesgo muy grave. Alta prioridad para mitigar.	Implementar controles lo antes posible.
Alto	Riesgo significativo. Debe ser gestionado.	Planificar e implementar medidas correctivas.
Moderado	Riesgo aceptable con controles.	Monitorear y revisar periódicamente.

Bajo	Riesgo bajo o insignificante.	Mantener y revisar rutinariamente.

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

5.6.4.4 Valoración del riesgo.

La valoración del riesgo es un proceso fundamental que vincula la identificación y el análisis de riesgos, permitiendo así la toma de decisiones informadas y la adopción de medidas adecuadas. Este proceso es crucial para asegurar que las intervenciones de la Unidad de Mantenimiento del Orden (UMO) en Quito, perteneciente a la Policía Nacional, cumplan con sus objetivos.

Al comparar los resultados del análisis de riesgos con los criterios previamente establecidos, se puede determinar si es necesario implementar acciones adicionales. Esto motiva la toma de decisiones fundamentadas sobre los pasos a seguir, que pueden incluir:

- No generar ninguna acción;
- Tomar opciones adicionales para el tratamiento del riesgo;
- Desarrollar análisis complementarios para comprender mejor el riesgo;
- Mantener los controles existentes;
- Replantear los objetivos.

Las decisiones deben considerar un contexto amplio, teniendo en cuenta las consecuencias reales y percibidas por las partes interesadas. Asimismo, los resultados obtenidos deben ser debidamente registrados, comunicados y validados para garantizar la transparencia y la efectividad en la gestión del riesgo.

5.6.5 Tratamiento del riesgo.

5.6.5.1 Generalidades.

De acuerdo con Eduardo y Bermeo (2023), el objetivo principal del tratamiento del riesgo es elegir y aplicar las medidas adecuadas para gestionarlo**,** con el fin de prevenir los daños inherentes. En este contexto, el tratamiento del riesgo se entiende como la respuesta adoptada por la Unidad de Mantenimiento del Orden (UMO) en la ciudad de Quito, dentro de su zona geográfica de responsabilidad.

Este proceso considera varios criterios fundamentales:

- La selección de diferentes formas para tratar el riesgo;
- La planificación e implementación de medidas para mitigar sus efectos;
- La evaluación continua del tratamiento aplicado;
- La determinación de si el riesgo residual es aceptable;
- Y, en caso de que dicho riesgo no sea aceptable, la aplicación de un tratamiento adicional.

Este enfoque permite gestionar los riesgos de manera estructurada y eficaz, garantizando que las operaciones de la UMO se desarrollen bajo parámetros de seguridad y eficiencia.

5.6.5.2 Selección de las opciones para el tratamiento del riesgo.

La mejor estrategia para seleccionar las opciones de tratamiento del riesgo consiste en equilibrar los beneficios esperados con las alternativas disponibles para abordarlo. Este proceso puede incluir diversas acciones, tales como:

- Evitar el riesgo, interrumpiendo o no iniciando la actividad que lo genera;
- Aceptar el riesgo, cuando se identifique una oportunidad que justifique su asunción;
- Eliminar la fuente del riesgo;
- Modificar la probabilidad de ocurrencia del evento;
- Cambiar las consecuencias en caso de que el riesgo se materialice;
- Transferir el riesgo a terceros (por ejemplo, mediante seguros o contratos);
- Retener el riesgo, en función de su nivel y la capacidad de respuesta de la organización.

La elección de la opción más adecuada debe estar alineada con los objetivos institucionales, los criterios definidos para el riesgo y los recursos disponibles en la unidad policial. En el caso

específico de las intervenciones de la Unidad de Mantenimiento del Orden (UMO), esta selección debe considerar las funciones operativas relacionadas con el control del orden público, control de multitudes, protección de personas y bienes, así como en la prevención y restablecimiento del orden.

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

El presente plan tiene por objetivo detallar el proceso que se empleará para llevar a cabo el tratamiento del riesgo, de manera que sea fácilmente comprendido por todos los integrantes de la Unidad de Mantenimiento del Orden (UMO) de la ciudad de Quito. Para garantizar su aplicabilidad y eficacia, el plan se integrará con los procesos operativos y administrativos ya existentes dentro de la unidad.

De acuerdo con la *Metodología para la Gestión Integral de Riesgos* (s.f.), el plan de tratamiento del riesgo deberá contemplar los siguientes elementos clave:

- Opciones de tratamiento: identificar si el riesgo será evitado, mitigado, transferido, aceptado, o gestionado de forma combinada;
- Responsables de la rendición de cuentas: personas o cargos encargados de implementar, supervisar y evaluar el tratamiento del riesgo;

- Acciones propuestas: actividades concretas para reducir o controlar el riesgo identificado;
- Recursos requeridos: tanto materiales como humanos, logísticos y tecnológicos;
- Medidas de desempeño: indicadores que permitan medir la eficacia del tratamiento;
- Restricciones: limitaciones normativas, presupuestarias, operativas o técnicas;
- Sistemas de informe y seguimiento: mecanismos de control, monitoreo y retroalimentación;
- Plazos definidos: cronograma de ejecución con tiempos establecidos para cada acción;
- Presupuesto asignado: los costos del tratamiento deberán estar contemplados dentro del presupuesto anual de la unidad.

Este enfoque metodológico permitirá que la UMO gestione los riesgos de manera planificada, transparente y alineada con sus objetivos institucionales, garantizando así operaciones más seguras, eficientes y responsables.

Tabla 21

Riesgo y Tratamiento

N.º	Tipo de Riesgo	Descripción del riesgo	Tratamiento o Solución propuesta
1	Enfrentamientos violentos	Lesiones al personal por objetos contundentes, armas o explosivos	• Uso obligatorio de equipo de protección personal (chalecos, cascos, escudos). • Refuerzo de la formación en defensa personal y maniobras de repliegue. • Evaluaciones de inteligencia previa a los operativos.
2	Uso excesivo de la fuerza	Riesgo de denuncias por abuso policial y violación de derechos	• Capacitación continua en derechos humanos y uso progresivo de la fuerza. • Supervisión operativa en tiempo real con cámaras corporales. • Revisión y actualización de protocolos.
3	Fallas en la comunicación táctica	Pérdida de coordinación entre unidades y toma de decisiones tardías	• Implementación de sistemas de comunicación digital de corto y largo alcance. • Entrenamientos conjuntos simulando escenarios reales. • Planes de contingencia comunicacional.

4	Saturación operativa	Fatiga del personal por sobrecarga de tareas y turnos extensos	• Rotación del personal en turnos justos. • Asistencia psicológica y programas de bienestar. • Revisión de carga operativa en función de recursos.
5	Equipamiento insuficiente o deficiente	Equipos en mal estado o desactualizados que comprometen la operación	• Auditoría de equipos cada seis meses. • Renovación progresiva del equipamiento. • Asignación de presupuesto específico para mantenimiento y reposición.
6	Pérdida de legitimidad institucional	Desconfianza ciudadana en la UMO por intervenciones cuestionadas	• Acciones de transparencia y rendición de cuentas públicas. • Trabajo comunitario y campañas de comunicación institucional. • Fomentar canales de diálogo antes de las intervenciones.
7	Riesgo jurídico	Posibilidad de sanciones legales por actuaciones incorrectas	• Asegurar la actuación dentro del marco legal y documentar todos los procedimientos. • Asistencia legal preventiva. • Simulacros jurídicos internos para preparación del personal.
8	Injerencia política o mediática	Presiones externas que afectan la toma de decisiones operativas	• Asegurar autonomía técnica de la planificación operativa. • Manual de ética institucional. • Comunicación oficial centralizada para contrarrestar desinformación.

9	Escalada de violencia en protestas	Manifestaciones pacíficas que se tornan violentas	• Equipos de inteligencia para monitoreo preventivo. • Unidades de diálogo y mediación. • Técnicas de dispersión gradual y planificada.
10	Deficiencias logísticas	Mal manejo de recursos y planificación inadecuada	• Diseño de un sistema logístico con inventario en tiempo real. • Capacitación en gestión operativa. • Evaluación post-operativo para mejoras continuas.

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

5.6.6 Seguimiento y revisión.

Su objetivo principal es garantizar y optimizar tanto la calidad como la efectividad del diseño. Para ello, se requiere una adecuada planificación, así como la recolección y el análisis de información. Los resultados obtenidos deben integrarse posteriormente en la gestión del desempeño.

Tabla 22

Riesgo y Tratamiento

N.º	Encargados	Responsables	Objetivo
1	**Auditores del área de almacenado**	Para asegurar la eficacia de una auditoría del sistema de gestión, resulta esencial contar con un equipo interno debidamente formado y comprometido con esta labor.	Dicho equipo debe realizar una evaluación objetiva de las evidencias recopiladas, analizando la información de manera imparcial y formulando conclusiones fundamentadas en hechos verificables y datos confiables.
2	**Jefe de control UMO**	Es fundamental trabajar de manera coordinada con los distintos departamentos, tanto administrativos como operativos, con el fin de diseñar e implementar medidas preventivas y planes de contingencia que permitan reducir los riesgos previamente identificados.	Asimismo, es necesario asegurar el cumplimiento de dichas acciones y promover el desarrollo continuo de estrategias para su mitigación.
3	**Jefe de área de soporte operativo del UMO Z09**	La experiencia y el conocimiento del jefe responsable del almacenamiento y la manipulación resultan esenciales para asegurar la implementación de medidas eficaces que permitan mitigar los riesgos y salvaguardar los intereses de la organización frente a las amenazas detectadas.	Además, tiene la responsabilidad de supervisar el cumplimiento de los procesos establecidos dentro del área.

4	**Colaboradores de cada área**	La correcta aplicación y cumplimiento de los métodos de prevención y mitigación de riesgos en las áreas administrativas es esencial para una gestión eficaz.	Asimismo, es necesario proporcionar información clara y precisa que facilite la validación de los riesgos previamente identificados.

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

El proceso de gestión de riesgos, junto con sus resultados, debe ser comunicado tanto a la alta dirección de la organización como a las partes interesadas. Este informe constituye un elemento clave para la gobernanza, por lo que es fundamental establecer canales efectivos de diálogo y comunicación con los involucrados. En este sentido, el documento debe incluir un detalle claro de las actividades realizadas y los resultados obtenidos durante la gestión de riesgos, ofreciendo información relevante que apoye la toma de decisiones, mejore las prácticas de gestión y fomente la interacción continua con las partes interesadas (Eduardo & Bermeo, 2023).

La incorporación de la gestión de riesgos en los procesos de almacenamiento y seguridad, realizados por el equipo UMO de tecnologías menos letales, debe entenderse como un proceso continuo y adaptable, que responda a las necesidades específicas y a la cultura de prevención existentes. En actividades que implican un alto nivel de riesgo, la gestión adecuada de estos riesgos es fundamental para evitar accidentes laborales, daños a bienes públicos y privados, y situaciones que puedan generar pánico generalizado. Esta gestión debe estar alineada con los objetivos estructurales y organizacionales de la unidad policial, afrontando los retos del manejo de riesgos

mediante su inclusión en las estrategias activas y prácticas institucionales de la gestión del riesgo a nivel policial (Noriega, 2019).

5.6.7 Registro e informe.

5.6.7.1 Medios de comunicación.

Según lo señalado por *Cedeño-Álava et al. (2018),* la implementación de diversos canales de comunicación dentro de la organización resulta esencial para una prevención y mitigación de riesgos eficaz. Estos canales pueden incluir desde plataformas digitales internas que difundan información sobre riesgos y medidas de seguridad, hasta el uso de boletines informativos, pantallas electrónicas y grupos de mensajería en línea para compartir alertas y recomendaciones de seguridad. Asimismo, la realización de seminarios virtuales, la producción de material audiovisual educativo y la activación de sistemas de alerta en tiempo real contribuyen a la formación continua del personal. Este conjunto de acciones favorece la construcción de una cultura organizacional enfocada en la seguridad proactiva, fortaleciendo la capacidad institucional para identificar, analizar y gestionar los riesgos de manera oportuna y eficiente.

a) **Aplicación o plataforma digital interna**: Es recomendable desarrollar una aplicación o sistema digital interno que permita la difusión de información relevante relacionada con los riesgos identificados, las medidas de mitigación, los protocolos de seguridad y cualquier actualización pertinente. Esta herramienta debe

estar disponible para todo el personal, funcionando como un canal centralizado de comunicación institucional que facilite el acceso oportuno a contenidos clave para la prevención y gestión de riesgos

b) **Boletines informativos o comunicaciones internas:** Es útil elaborar boletines periódicos que incluyan contenido relevante sobre riesgos identificados, recomendaciones de seguridad, análisis de casos y novedades vinculadas a la gestión de riesgos. Estos documentos pueden ser distribuidos a través del correo electrónico institucional o publicados en la intranet, asegurando así su disponibilidad para todo el personal de la organización.

c) Material audiovisual y seminarios virtuales: La producción de videos educativos y la realización de seminarios web enfocados en la gestión de riesgos permiten reforzar la capacitación del personal. Estos contenidos pueden abordar procedimientos de seguridad, análisis de incidentes anteriores y el uso correcto de equipos de protección. Se recomienda que estos recursos estén disponibles en plataformas internas como la intranet o sean distribuidos mediante correo electrónico institucional, facilitando así el acceso de todos los colaboradores (Eduardo & Bermeo, 2023).

d) **Carteleras digitales o pantallas informativas:** La instalación de pantallas electrónicas en zonas comunes de la organización representa una estrategia eficaz para la difusión de mensajes clave relacionados con la seguridad y la gestión de riesgos. A través de estos medios se pueden comunicar recordatorios sobre procedimientos de seguridad, recomendaciones para evitar riesgos específicos y alertas ante posibles situaciones de peligro inminente**.**

e) **Encuestas y mecanismos de retroalimentación:** La aplicación periódica de encuestas al personal permite recopilar opiniones y percepciones sobre la efectividad de las medidas implementadas para la mitigación de riesgos, así como sobre la calidad de la comunicación en materia de seguridad. Esta información resulta valiosa para detectar avances, identificar posibles debilidades y ajustar las estrategias de comunicación de acuerdo con las necesidades reales del entorno organizacional (Del Pozo Barrezueta, s.f.).

5.6.7.2 Cronograma de actividades para la implementación de procesos de mejora ante los riesgos detectados.

Tabla 23

Cronograma

N.º	Actividades	Involucrados	Ejecución
1	Se convocará a una reunión entre las áreas administrativas y operativas con el propósito de presentar el proyecto enfocado en la prevención de los riesgos previamente detectados.	Jefe de la unidad, oficiales subalternos encargados de las áreas Administradoras y operativas	Julio 2025
2	La ejecución de la Norma 31000 y los procesos acordes de gestión de los riesgos de desastres.	Jefe de la unidad, oficiales subalternos encargados de las áreas Administrativas y operativas	Julio 2025
3	Difundir las estrategias para prevenir y mitigar los riesgos identificados	Jefe de la unidad, oficiales subalternos encargados de las áreas Administrativas y operativas	Julio 2025
4	Se procederá a la conformación de grupos de trabajo encargados de llevar a cabo actividades de capacitación y sensibilización, con el objetivo de asegurar el cumplimiento obligatorio de las medidas preventivas y de mitigación frente a los riesgos que afectan a la unidad UMO.	Oficiales subalternos, personal Operativo y Administrativas encargados de todas las áreas.	Julio 2025

Nota: Elaborado por Autores, adaptado a la UMO Z09. Tomado de. (Maestría de Gestión de Riesgos - (Tabla), 2025)

5.6.8 Auditoría interna.

5.6.8.1 Objetivos de la Auditoría interna.

- El propósito de llevar a cabo una revisión periódica del estado operativo y el mantenimiento de los equipos, vehículos y herramientas destinados a las labores de almacenamiento y seguridad de tecnologías menos letales, a fin de garantizar su disponibilidad y funcionamiento adecuado (Ley Orgánica de Protección de Datos, Ecuador).
- Es necesario analizar el nivel de eficacia de los protocolos y procedimientos implementados para la atención de emergencias, considerando las fases de preparación, respuesta inmediata y procesos de recuperación frente a desastres.
- Es indispensable verificar que todas las políticas internas, regulaciones legales y estándares vigentes sean aplicados correctamente, incluyendo aquellas relacionadas con la seguridad, salud ocupacional y la protección del medio ambiente.
- Se debe examinar la eficacia de los procedimientos administrativos, considerando la gestión del talento humano, los recursos financieros y materiales, con el fin de garantizar una asignación adecuada de estos elementos en apoyo a las actividades de intervención y rescate (Del Pozo Barrezueta, n.d.).

- Se deben identificar oportunidades para perfeccionar la planificación y ejecución de simulacros y ejercicios prácticos, con el objetivo de fortalecer la preparación y capacidad de respuesta ante posibles emergencias (Eduardo & Bermeo, 2023).
- Es fundamental revisar la formación y el entrenamiento del equipo en áreas como técnicas de manipulación, primeros auxilios, gestión de crisis y comunicación en situaciones de emergencia, asegurando que el personal cuente con las competencias necesarias para desempeñar sus funciones eficazmente
- Asegurar el seguimiento y la implementación de las recomendaciones derivadas de auditorías internas previas, adoptando las acciones correctivas y preventivas necesarias para mejorar continuamente las actividades de almacenamiento y manipulación.

5.6.8.2 Procesos de la Auditoría interna.

Según *Sotelo (2018)*, la realización de una auditoría interna basada en la norma ISO 31000 en la unidad de mantenimiento y orden de la ciudad de Quito no se limita a un aspecto técnico, sino que implica un análisis sistémico y objetivo de los procesos relacionados con la gestión de riesgos.

En el alcance primordial es asegurar que los principios y directrices establecidos por esta norma internacional se apliquen correctamente. Esto se logra mediante la revisión documental,

entrevistas con personal clave, identificación de conformidades y no conformidades, desarrollo de acciones correctivas, elaboración de informes y seguimiento posterior a la auditoría. Todas estas actividades buscan fortalecer la capacidad organizacional para identificar, evaluar, gestionar y controlar riesgos, en línea con las funciones y competencias específicas de la unidad de mantenimiento del orden de la Policía Nacional de Quito.

En el alcance: Es fundamental evaluar el compromiso de la alta dirección respecto al liderazgo en la gestión de riesgos, asegurando la implementación efectiva de un sistema de gestión de riesgos. Esto implica analizar si existen principios y objetivos claros para la gestión de riesgos dentro de la organización, llevados a cabo de manera sistemática y coherente. El proceso abarca la identificación, evaluación y tratamiento de riesgos, promoviendo la comunicación y consulta constante dentro de la institución.

Monitorean y revisan seguidamente los riesgos identificados y las acciones de mitigación implementadas para garantizar su efectividad y relevancia continua.

Implementar medidas para mejorar progresivamente el sistema de gestión de riesgos de acuerdo con los hallazgos de la auditoría y las mejores prácticas en el campo de la gestión.

La auditoría interna en el área de la Unidad de Mantenimiento del Orden Z09 de la Policía Nacional requiere un enfoque detallado y especializado, debido al contexto de seguridad y la naturaleza crítica de sus funciones. Esto es especialmente relevante por la manipulación directa

que realiza el personal encargado del almacenamiento y manejo de tecnologías no letales, cuyos procedimientos, tanto planificados como emergentes, se han duplicado recientemente. En este sentido, resulta fundamental evaluar la eficiencia operativa, el cumplimiento de la normativa aplicable y la seguridad del equipo responsable durante todas las etapas del procedimiento: antes, durante y después de las actividades.

a) Responsabilidades:

En el alcance y objetivo**,** radica en optimizar los procesos relacionados con el manejo de tecnologías menos letales y garantizar que los equipos de protección personal y colectivo cumplan con los estándares y regulaciones vigentes. Para ello, es imprescindible la capacitación y formación continua del personal responsable, quienes conformarán la administración del área de almacenamiento y seguridad.

b) Seleccionar el Equipo de Auditoría:

De acuerdo a (NORMAS INTERNACIONALES PARA EL EJERCICIO PROFESIONAL DE LA AUDITORÍA INTERNA, 2017) El auditor interno debe tener conocimiento Técnico.

Experiencia Específica:

- Expertos en tecnología menos letales

- Deben contar con conocimientos avanzados en el manejo, almacenamiento y desactivación de este tipo de tecnología.

Experiencia en Seguridad Pública:

Tener experiencia en operaciones de seguridad pública y manejo de situaciones de crisis.

Familiaridad con Normativas:

Conocer en profundidad las normativas y regulaciones locales e internacionales relacionadas con tecnologías menos letales y equipos de protección personal.

Criterios de evaluación:

- Cumplimiento de normativa nacional como internacional vigente.
- Normativa de seguridad Pública y laboral aplicables
- Normativas específicas emitidas por organismos reguladores nacionales o internacionales que supervisan el uso de explosivos y equipos de protección.

c) Políticas y Procedimientos Internos:

- Revisión y cumplimiento de los manuales operativos.
- Procedimientos documentados para la manipulación y almacenamiento.

d) Protocolos de Seguridad:

- Políticas internas de seguridad y protocolos de emergencia.
- Instrucciones de manejo de incidentes y respuesta a emergencias.
- Estándares de la Industria

e) Estándares Internacionales:

Cumplimiento con estándares reconocidos internacionalmente, como los determinados por la Organización Internacional de Normalización (ISO 31000:2018).

f) Mejores Prácticas:

- Adopción de las mejores prácticas en la gestión de explosivos y equipos de protección.
- Equipos de Protección Personal y Colectivo

g) Certificación y Mantenimiento de Equipos:

- Verificación de que todos los equipos de protección personal (EPP) y colectivos están certificados y en buen estado de funcionamiento.
- Registros de mantenimiento y calibración de equipos.

h) Adecuación y Actualización:

- Evaluación de la adecuación de los equipos en uso y su actualización conforme a

- los avances tecnológicos y nuevas normativas.
- Capacitación y Competencia del Personal.

i) Programas de Capacitación:

- Revisión de los programas de aprendizaje y formación continua del personal.
- Certificaciones y acreditaciones del personal operativo.

j) Evaluación de Competencias:

- Certificación de la competencia del personal para realizar tareas específicas relacionadas con la manipulación y seguridad de tecnologías menos letales.
- Registros y Documentación.

k) Registro de Operaciones:

- Mantenimiento de registros detallados de todas las operaciones que involucren el uso de tecnologías menos letales.
- Documentación de incidentes, inspecciones y auditorías anteriores.

l) Reportes e Informes:

- Exactitud y completitud de los informes operativos y de auditoría.
- Cumplimiento con los requisitos de reporte a organismos reguladores.

- Evaluación del Desempeño y Eficiencia Operativa.

m) Indicadores de Desempeño:

- Uso de indicadores clave de desempeño (KPI) para evaluar la eficiencia y efectividad operativa.
- Medición del tiempo de respuesta, tasa de incidentes, y cumplimiento de procedimientos.

n) Análisis de Resultados:

- Balance de los resultados operativos con los objetivos establecidos y estándares de la industria.
- Gestión de Riesgos

o) Identificación y Evaluación de Riesgos:

Procedimientos en la identificación, evaluación y gestión de riesgos asociados con la manipulación de tecnologías menos letales.

p) Controles y Mitigación:

- Establecer controles y medidas de mitigación para reducir al mínimo los riesgos.
- Eficiencia en el Uso de Recursos.

q) **Gestión de Recursos:**

Análisis de la eficiencia en la utilización de recursos, incluyendo personal, equipos y materiales.

r) **Optimización de Procesos:**

- Identificación de oportunidades para aumentar la eficiencia y reducir costos sin comprometer la seguridad.
- Cumplimiento Ambiental.

s) **Regulaciones Ambientales:**

- Adherencia a las regulaciones ambientales aplicables relacionadas con el almacenamiento y uso de tecnologías menos letales.
- Procedimientos de manejo de residuos peligrosos y contaminantes.

t) **Aspectos prioritarios.**

En la auditoría realizada al equipo antiexplosivo del Grupo de la unidad de mantenimiento del orden de la Policía Nacional, es fundamental verificar el cumplimiento de todas las normativas y regulaciones legales y de seguridad, evaluar la eficacia y actualización de los procedimientos operativos, y asegurar la adecuada formación y competencia del personal. Además, es crucial revisar el estado y mantenimiento de los equipos de protección personal

y colectivos, así como la gestión de riesgos y la eficiencia en el uso de recursos. Se debe garantizar que toda la documentación y registros estén completos y actualizados, y que se implementen controles adecuados para mitigar los riesgos asociados con la manipulación de las tecnologías menos letales.

u) Tiempo de las Inspecciones:

La duración y la frecuencia de las inspecciones deben ser cuidadosamente planificadas para equilibrar la exhaustividad con la eficiencia operativa. Se sugiere un marco temporal que asegure revisiones periódicas y detalladas sin interrumpir las operaciones de UMO.

Planificación y Preparación

La planificación y preparación de las auditorías son cruciales para asegurar que todas las áreas clave sean revisadas y que las inspecciones se realicen de manera eficiente y efectiva. Esto incluye establecer un cronograma claro, asignar recursos adecuados y preparar toda l documentación necesaria para la auditoría.

CRONOGRAMA DE AUDITORÍA INTERNA:

Unidad de Mantenimiento del Orden Z09

DÍA 1: REUNIÓN DE APERTURA

- **Objetivo:** Presentar al equipo auditor, establecer los objetivos y el alcance de la auditoría, además de discutir el cronograma general de actividades.
- **Participantes**: Equipo auditor, jefes de equipo de la Unidad de Mantenimiento del Orden Z09, representantes de la alta dirección.

  Realizar una evaluación preliminar de las políticas, procedimientos, registros de formación y mantenimiento vigentes.

DÍA 2: PLANIFICACIÓN DETALLADA

- **Objetivo:** Ajustar y perfeccionar el plan de auditoría, identificar las áreas prioritarias para la revisión y elaborar las listas de verificación correspondientes.
- **Participantes:** Equipo de auditoría.

  Presentar el proceso de inspección, organizar las entrevistas y coordinar actividades específicas.

- **Participantes:** Auditores y jefes de equipo.

Realizar entrevistas con personal clave sobre procedimientos operativos y aspectos de seguridad.

DÍAS 5 Y 6: REVISIÓN DOCUMENTAL DETALLADA:

- **Objetivo:** Llevar a cabo un análisis exhaustivo de registros operativos, informes de incidentes y documentación relacionada con la capacitación.
- **Participantes:** Auditores y personal administrativo.

DÍAS 7 Y 8: INSPECCIÓN FÍSICA Y PRUEBAS OPERATIVAS:

- **Objetivo:** Evaluar físicamente los equipos e instalaciones, y realizar pruebas operativas para verificar su funcionamiento.
- **Participantes:** Auditores y técnicos encargados.

Análisis y Evaluación

DÍA 9: ANÁLISIS DE DATOS:

- **Objetivo:** Analizar los hallazgos recopilados, comparándolos con los criterios establecidos para el cumplimiento normativo.
- **Participantes**: Equipo de auditoría.
- **Duración estimada:** Día completo.

DÍA 10: REUNIÓN DE REVISIÓN DE HALLAZGOS

- **Objetivo:** Discutir hallazgos preliminares con los responsables de la unidad de mantenimiento y el orden para validación y comentarios.
- **Participantes:** Auditores, jefes de equipo del UMO.
    - Presentación y Discusión del Informe
    - Presentación del Informe Final
    - Seguimiento

PERIÓDICO: AUDITORÍAS DE SEGUIMIENTO (CADA 6-12 MESES)

- **Objetivo:** Verificar la implementación de acciones correctivas y mejoras.
- **Participantes:** Auditores, jefes de equipo de la Unidad de Mantenimiento del Orden Z09.
- **Duración:** 1-2 días por auditoría de seguimiento.

Cronograma de Reuniones

El cronograma de reuniones para la auditoría del equipo antiexplosivo de la unidad de mantenimiento del orden de la Policía Nacional contempla una reunión inicial durante la primera semana, cuyo propósito es establecer los objetivos y el plan de trabajo. Posteriormente, se realizarán encuentros para la revisión documental y la planificación detallada. Durante la segunda

semana, se llevará a cabo la reunión de inicio de la inspección, entrevistas con el personal clave, así como una revisión exhaustiva de la documentación. Esta etapa culminará con inspecciones físicas y pruebas operativas. En la tercera semana, se efectuará el análisis de los datos recopilados y la elaboración del informe, acompañado de una reunión para revisar los hallazgos preliminares. Finalmente, la cuarta semana estará destinada a la presentación formal del informe final y a una sesión de discusión y retroalimentación. Además, se programarán auditorías de seguimiento cada 6 a 12 meses para verificar la implementación de las acciones correctivas y las mejoras propuestas.

Requerimiento de confidencialidad.

Es fundamental asegurar la protección de la información sensible manejada por el área de explosivos. Esto requiere limitar el acceso a documentos y datos críticos únicamente al personal autorizado, así como implementar protocolos seguros para la comunicación y almacenamiento de dicha información.

Así como asegurar la protección de identidades de aquellos involucrados en el proceso. Además, es necesario establecer medidas de seguridad para la eliminación adecuada de la información al concluir la auditoría, junto con la capacitación del personal en prácticas de confidencialidad para garantizar el cumplimiento riguroso de estos requerimientos en todas las etapas del proceso.

Estructura.

La auditoría de tecnología menos letales de la unidad de mantenimiento del orden se desarrolla en varias fases esenciales. Inicialmente, se establecen los objetivos y el alcance del proceso de auditoría. A continuación, se procede a la recopilación de la documentación pertinente y a la realización de entrevistas con el personal clave. Posteriormente, se lleva a cabo una revisión detallada de los procedimientos operativos, los protocolos de seguridad y el mantenimiento de los equipos. Esta fase culmina con la identificación de hallazgos y la elaboración de un informe completo y detallado. Finalmente, se implementan las acciones correctivas correspondientes y se programan auditorías de seguimiento para asegurar la mejora continua y el cumplimiento de las normativas vigentes en la gestión de tecnologías menos letales dentro de la unidad.

5.6.8.3 No conformidades y acciones correctivas.

Implementar un sistema de gestión de calidad en la Unidad de Mantenimiento del Orden de la ciudad de Quito requiere un enfoque en identificar y corregir problemas para mejorar continuamente los procesos y optimizar resultados.

a) No Conformidades Identificadas:

- Falta de registros adecuados sobre la gestión de riesgos en el manejo de tecnologías menos letales, incluyendo evaluaciones específicas de riesgos y planes de acción.

- Falta de mantenimiento preventivo y pruebas regulares de los equipos y herramientas usados en operaciones con tecnologías menos letales, lo que aumenta el riesgo de fallos durante su uso.
- Ausencia de procedimientos claros y protocolos de seguridad para el almacenamiento, transporte y manipulación de Tecnologías Menos Letales, incrementando el riesgo de accidentes.
- Inadecuada señalización y delimitación de áreas de trabajo con tecnología menos letales, lo que podría llevar a accesos no autorizados o accidentes por falta de conciencia del peligro.
- Incumplimiento de los requisitos de protección personal, como el uso de equipos de protección individual (EPI) adecuados, aumentando el riesgo de lesiones.
- Falta de un sistema para controlar y documentar cambios en procedimientos, equipos o personales relacionados con el manejo de Tecnologías Menos Letales.
- Ausencia de un plan de respuesta a emergencias específico para incidentes con materiales dentro del área de tecnologías menos letales, lo que podría agravar los daños en caso de accidentes.

b) Desarrollo de documentación detallada:

Crear y mantener documentación exhaustiva sobre la gestión de riesgos asociados con el manejo de tecnologías menos letales, incluyendo evaluaciones de riesgos específicas, planes de acción y procedimientos operativos estándar (SOP) actualizados.

c) Programa de capacitación reforzada:

- Realizar un programa de aprendizaje continuo y reforzado para todo el personal involucrado en el manejo y almacenamiento, asegurando que estén debidamente entrenados y certificados en los procedimientos de seguridad y emergencia.
- **Mantenimiento preventivo mejorado:** Establecer un programa de mantenimiento preventivo más riguroso para los equipos y herramientas utilizados en el almacenamiento y manipulaciones, con cronogramas de mantenimiento regulares y registros de seguimiento.
- **Revisión y actualización de procedimientos de seguridad:** Examinar y renovar los procedimientos de seguridad para el almacenamiento, transporte y manipulación de explosivos, garantizando que cumplan con las mejores prácticas y normativas de seguridad aplicables.

- **Cumplimiento de requisitos de protección personal:** Garantizar el cumplimiento de los requisitos de protección personal, proporcionando EPI adecuados y asegurando su uso correcto por parte del personal en todo momento.
- **Implementación de un sistema de gestión de cambios:** Establecer un método formalizado para gestionar y documentar los cambios en los procedimientos, equipos o personal relacionados con manipulación y almacenamiento, asegurando su revisión y aprobación adecuadas antes de la implementación.
- **Desarrollo de un plan de respuesta a emergencias:** Crear un plan de respuesta a emergencias específico para incidentes relacionados con explosivos, con procedimientos claros para mitigar riesgos, manejar situaciones de crisis y garantizar la seguridad del personal y del público.

d) Revisión periódica del sistema de gestión de riesgos:

Establecer un proceso de revisión periódica y mejora continua del sistema de gestión de riesgos en el manejo y almacenamiento, identificando oportunidades de mejora y actualizando los procedimientos en consecuencia.

Según Eduardo y Bermeo (2023), es fundamental elaborar un plan de acción integral que contemple medidas correctivas y preventivas para atender cada una de las deficiencias detectadas. Para asegurar la ejecución eficaz de estas acciones, resulta imprescindible implementar un sistema

de seguimiento riguroso y constante. Esto implica definir plazos específicos para la puesta en marcha de cada medida, asignar responsabilidades claras, realizar monitoreos periódicos que permitan evaluar el progreso y la efectividad de las acciones, así como efectuar inspecciones regulares en el campo para verificar su correcta aplicación. Además, es necesario recopilar evidencias del cumplimiento y obtener retroalimentación del personal involucrado, documentando todas las actividades relacionadas con las acciones correctivas. Este procedimiento asegura que las no conformidades identificadas en la auditoría sean tratadas de manera adecuada, promoviendo una mejora continua en la gestión de riesgos vinculada al almacenamiento y manipulación de las tecnologías menos letales por parte del personal responsable.

CAPITULO 6

6. CONCLUSIONES Y APLICACIONES.

6.1. Conclusiones Generales.

Desde nuestra perspectiva, el proyecto busca cumplir satisfactoriamente con los objetivos planteados inicialmente. Implementar un sistema de gestión basado en la norma ISO 31000:2018 permitirá estandarizar los procesos de almacenamiento y manipulación de las Tecnologías Menos Letales en la UMO Z09, reduciendo significativamente los riesgos operativos identificados en el diagnóstico inicial. El mayor logro a conseguir será mejorar la seguridad física del centro de almacenamiento para tecnologías menos letales.

La implementación de protocolos claros para el control de accesos, la señalización adecuada y las condiciones ambientales controladas ha minimizado los incidentes relacionados con la manipulación inadecuada de los materiales. Además, la capacitación continua del personal ha fortalecido una cultura preventiva, evidenciándose en el manejo más responsable y técnico de estos recursos. Sin embargo, reconocemos que persisten desafíos, principalmente en la sostenibilidad del sistema a largo plazo.

La rotación de personal y la necesidad de actualización periódica de los registros digitales requieren un compromiso institucional continuo. No obstante, se esperan resultados que validen la

eficacia del modelo propuesto, sentando las bases para su posible replicación en otras unidades policiales.

En conclusión, el proyecto ha cumplido con su propósito central, que es garantizar un almacenamiento seguro y eficiente de las Tecnologías Menos Letales, alineado con estándares internacionales y con un enfoque claro en la prevención de riesgos y el respeto a los derechos humanos.

6.2. Conclusiones Específicas:

6.2.1. Análisis del Cumplimiento de los Objetivos de la Investigación.

Desde el inicio de este trabajo nos planteamos como objetivo principal diseñar e implementar un sistema de gestión integral para el almacenamiento y la seguridad de las tecnologías menos letales empleadas por la Unidad de Mantenimiento del Orden Z09, sustentado en la norma ISO 31000:2018. Buscábamos optimizar el uso de estos recursos, reducir los riesgos operativos, reforzar la confianza ciudadana y garantizar el respeto a los derechos humanos dentro de la gestión institucional.

Una vez concluida la investigación y tras aplicar cada fase prevista: diagnóstico, análisis de riesgos, elaboración de procedimientos, diseño de protocolos de actuación, formación del personal y propuesta de mejora continua; consideramos que hemos cumplido el objetivo planteado, ya que se busca estructurar un sistema de gestión robusto, alineado con estándares internacionales,

que permite organizar, estandarizar y controlar de forma más efectiva todos los procesos relacionados con el manejo y almacenamiento de tecnologías menos letales.

En concreto, se busca alcanzar resultados relevantes, como la definición de protocolos claros para el ingreso, control, uso y mantenimiento de las Tecnologías Menos Letales; el establecimiento de medidas de seguridad enfocadas a prevenir incidentes o extravíos; la creación de planes de respuesta ante emergencias; y la capacitación del personal involucrado para fortalecer la cultura de gestión de riesgos. Todo esto contribuye a garantizar que las operaciones se realicen de forma segura, ética y responsable.

Además, el sistema propuesto brinda mayor transparencia y facilita la rendición de cuentas frente a la comunidad, generando confianza y legitimidad hacia la institución policial. En definitiva, consideramos que este proyecto no solo cumplió con las metas trazadas, sino que deja un aporte sostenible para replicarse en otras unidades, adaptándose a diferentes realidades y necesidades operativas.

6.2.2. Contribución a la Gestión Empresarial.

La aplicación de la norma ISO 31000:2018, generara un eficiente manejo de los recursos, mejor planificación, mejor estructura organizacional y mejor capacidad de reacción ante eventos de control del orden público.

La identificación, valoración y gestión de riesgos es fundamental para el correcto manejo de la institución y esto ayuda a generar los procesos adecuados con visión al correcto uso de tecnologías menos letales por parte de los servidores policiales de la Unidad de Mantenimiento del Orden Z09.

Es vital que, para obtener el crecimiento de la institución, se generen procesos de cambio. Sobre los cuales se pueda trabajar en beneficio de la Unidad de Mantenimiento del Orden Z09. Estos procesos deben estar enfocados en la gestión y prevención de riesgos, la correcta administración del talento humano, el cual debe ser preparado y capacitado constantemente.

6.2.3. Contribución a Nivel Académico.

El proyecto de gestión de riesgos basado en la norma ISO 31000: 2018, busca generar un gran aporte académico para los estudiantes de la Maestría en Gestión de Riesgos. Nos ha enseñado a realizar de manera correcta el análisis, la gestión y valoración del riesgo. De igual formar nos ha enseñado a manejar de manera estratégica y operativa, las tecnologías menos letales usadas por los servidores policiales de la Unidad de Mantenimiento del Orden Z09.

Se reconoce el aprendizaje, pues nos ha enseñado a reconocer que es necesario la correcta administración del talento humano, para lograr los objetivos propuestos.

6.2.4. Contribución a Nivel Personal

El proyecto de gestión de riesgos basado en la norma ISO 31000:2018, nos ha ayudado a entender de cómo se debe realizar procesos en beneficio de una institución. La cual necesite mejorar su sistema de prevención y mitigación de riesgos. De igual forma nos ayuda a realizar acciones en beneficio de la institución, para estandarizar o mejorar el control de medios logísticos de uso institucional.

Aprendimos que la gestión de riesgos es cambiante con el tiempo. Es por eso que siempre se debe realizar diagnósticos y evaluaciones de riesgos, con la finalidad de que se pueda brindar una correcta gestión temprana ante la presencia de un nuevo riesgo.

6.3.Limitaciones a la Investigación.

Para el desarrollo del proyecto de gestión de riesgos basado en la norma ISO 31000:2018, han existido pequeñas limitaciones de poca importancia como seria: el tiempo necesario para trabajar con los compañeros en el desarrollo del proyecto.

Por parte de la Unidad de Mantenimiento del Orden Z09, se ha obtenido la predisposición y beneficio de obtener los documentos necesarios para realizar el proyecto. Se han presentado limitaciones necesarias pero la predisposición de los autores de este proyecto es grande, por lo cual de una manera eficiente y eficaz generaremos el proyecto en beneficio de la institución y los servidores policiales que laboran en esta.

7. BIBLIOGRAFÍA.

- Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador*. https://www.asambleanacional.gob.ec
- Asamblea Nacional del Ecuador. (2010). *Código Orgánico de Planificación y Finanzas Públicas*. https://www.finanzas.gob.ec
- Asamblea Nacional del Ecuador. (2017). *Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público*. https://www.asambleanacional.gob.ec
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. https://www.asambleanacional.gob.ec
- Ministerio del Interior. (2017). *Acuerdo Ministerial N.º 080 - Estatuto Orgánico por Procesos de la Policía Nacional del Ecuador*. https://www.ministeriodelinterior.gob.ec
- International Organization for Standardization. (2015). *ISO 9001:2015: Quality management systems – Requirements*. https://www.iso.org
- International Organization for Standardization. (2018). *ISO 31000:2018: Risk management – Guidelines*. https://www.iso.org
- International Organization for Standardization. (2018b). *ISO 45001:2018: Occupational health and safety management systems – Requirements with guidance for use*. https://www.iso.org
- International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements*. https://www.iso.org
- International Organization for Standardization. (2014). *ISO Guide 51:2014: Safety aspects – Guidelines for their inclusion in standards*. https://www.iso.org
- International Organization for Standardization & International Electrotechnical Commission. (2009). *ISO/IEC 31010:2009: Risk management – Risk assessment techniques*. https://www.iso.org
- International Organization for Standardization & International Electrotechnical Commission. (2013). *ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements*. https://www.iso.org ISO 31000:2018 – Directrices para la gestión del riesgo
- International Organization for Standardization. (2018). *ISO 31000:2018: Risk management – Guidelines*. https://www.iso.org
- Muñoz, J. (2016). *Gestión del riesgo: Conceptos básicos y aplicabilidad*. Revista Técnica de Seguridad, 8(2), 55–68.
- United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*. https://www.undrr.org

- A.Bernal, C. (2021). Metodologia de la investigacion. PEARSON.
- Hillson, D. (2009). Managing Risk in Projects (1st ed.). Routledge. https://doi.org/10.4324/9781315249865
- HOPKIN, P. (2018). FUNDAMENTOS DE LA GESTION DE RIESGOS-COMPRENSION,EVALUACIONE IMPLEMENTACION DE UNA GESTION DE RIEZGOS EFICAZ. Kogan Page.
- International Organization for Standardization. (2018). ISO 31000:2018 - Risk management: Guidelines. ISO.
- Muñoz, J. (2016). Gestión del riesgo: Conceptos básicos y aplicabilidad. Revista Técnica de Seguridad, 8(2), 55–68.
- United Nations Office for Disaster Risk Reduction. (2015). Sendai Framework for Disaster Risk Reduction 2015–2030. https://www.undrr.org
- Arce Labrada, S., & López Sierra, H. A. (2010). Valoración de la gestión de proyectos en empresas de Bogotá Nivel de madurez en gestión de proyectos. Revista EAN, 69, 60–87. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-81602010000200005&lng=en&nrm=iso&tlng=es.
- Fernanda, L., & Gómez, Q. (2015). Modelo basado en ITIL para la gestión de los servicios de TI en la cooperativa de caficultores de Manizales. Universidad Autónoma de Manizales. https://repositorio.autonoma.edu.co/handle/11182/631
- Noriega, E. (2019). Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000. SciELO.
- Cedeño-Ã• lava, K. J., De la Cruz Santillán, M. E., Zambrano-Zambrano, M. J., Cantos-Alcívar, G. J., Intriago-Miranda, S. A., & Soledispa-Canizares, R. G. (2018). Seguridad Laboral y Salud Ocupacional en los Hospitales del Ecuador. *Dominio De Las Ciencias*, *4*(4), 57–68. https://doi.org/10.23857/dc.v4i4.822
- Ley Orgánica de Protección de datos en Ecuador. (2021). Ley Orgánica de Protección de datos en Ecuador. Quinto Suplemento Del Registro, 459, 4–40.
- Sotelo, A. (2018). Diseño de propuesta para el tratamiento de riesgos basado en la norma ISO 31000 : 2018 para el proceso de elaboración de ofertas comerciales en empresa del sector eléctrico.
- NORMAS INTERNACIONALES PARA EL EJERCICIO PROFESIONAL DE LA AUDITORÍA INTERNA. (2017). www.globaliia.org
- ISO 31000. (2018). International Organization for Standardization. Obtenido de Gestión del riesgo-Directrices.: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ANEXOS.

1. Procedimiento Normal de Trabajo (PNT) de la UMO Z09.
2. Modelo de Auditoría Interna de la UMO Z09.
3. Modelo de No Conformidades y Acciones correctivas de la UMO Z09.

ANEXO 1:

Procedimiento Normal de Trabajo (PNT) de la UMO Z09.

RASTRILLO DE LA UNIDAD DE MANTENIMIENTO DEL ORDEN Z09	PROCEDIMIENTO GENERAL PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO.	PN/R/PG/001/01 **Página 1 de 12** **Rev.:** 0 **Fecha de Edición:** …..……
Procedimientos relacionados:		

1. Objetivo:

Establecer un sistema de gestión para el almacenamiento, manipulación, distribución y disposición final de las Tecnologías Menos Letales (TML) en la Unidad de Mantenimiento del Orden Z09 (UMO Z09), basado en los principios de la norma ISO 31000:2018, con el fin de:

a) Garantizar condiciones óptimas de almacenamiento

- Mantener parámetros ambientales controlados (temperatura, humedad, ventilación).
- Prevenir degradación, contaminación o activación accidental de los materiales.
- Minimizar riesgos de incendio, explosión o exposición química.
- Mejorar la conservación y preservación de las Tecnologías Menos Letales.

b) Optimizar la trazabilidad y control documental.

- Implementar registros digitales confiables (inventario en tiempo real con códigos QR de cada tecnología para un ágil control de inventario).
- Establecer protocolos claros de recepción, distribución y devolución.
- Garantizar la transparencia en la gestión de TML para auditorías internas y externas.

c) Reducir riesgos operativos y proteger al personal.

- Establecer medidas de seguridad física (control de acceso biométrico, señalización).
- Capacitar al personal en manipulación segura y respuesta a emergencias.
- Mitigar riesgos de robos, pérdidas o uso indebido.
- Concienciar al personal sobre el correcto uso, manipulación y traslado de las TML.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
	Página 2 de 12
Procedimientos relacionados:	

d) Cumplir con normativas nacionales e internacionales:

- Alinearse con la Ley Orgánica de Seguridad Pública y Orden Interno.
- Seguir estándares de derechos humanos en el uso de TML (Principios de Naciones Unidas sobre Uso de la Fuerza).
- Implementar buenas prácticas según ISO 31000 (gestión de riesgos).

e) Fomentar una cultura de mejora continua:

- Realizar revisiones periódicas del sistema.
- Actualizar protocolos según lecciones aprendidas en operativos.
- Promover la participación del personal en reporte de incidentes y sugerencias.

2. Responsabilidad de aplicación y alcance:

La responsabilidad de aplicación y alcance de este procedimiento recae sobre todo el personal técnico de la Unidad de Mantenimiento del Orden Quito (Z09) involucrado en la redacción, cumplimiento y aplicación de los procedimientos relacionados con la gestión de riesgos de las Tecnologías Menos Letales. El alcance abarca el diseño e implementación de un sistema de gestión de riesgos para el almacenamiento, custodia y uso de las TML dentro de la UMO Z09. Aplica a:

Talento Humano:

- ✓ Personal Policial de la UMO Z09 asignado al rastrillo (Rastrillero encargado, técnicos armeros).
- ✓ Personal Policial de la UMO Z09, con funciones operativas, quienes manipulan las tecnologías Menos Letales en intervenciones y acciones policiales.
- ✓ Supervisores y auditores de la UMO Z09.
- ✓ Proveedores y personal externo**.**

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	Código: PN/R/PG/001/01
	Página 3 de 12

Procedimientos relacionados:

Tecnologías Menos Letales:

- ✓ Agentes químicos lacrimógenos (CS, OC).
- ✓ Municiones menos letales (granadas aturdidoras, proyectiles de impacto controlado).
- ✓ Equipos de dispersión (lanzadores, pistolas de gas)

FUNCIÓN	RESPONSABILIDADES
Comandante de la UMO Z09	Aprobación final de protocolos y auditorías.
Jefe del Departamento de Soporte Operativo	Supervisión general, autorización de movimientos críticos.
Rastrillero Encargado	Control diario del inventario, cumplimiento del PNT.
Técnicos Armeros (2 designados)	Manipulación segura, mantenimiento preventivo.
Oficial de Semana y de Control	Verificación de accesos y respuesta a incidentes.
Personal Operativo	Uso responsable y devolución de TML después de operativos.

3. Definiciones:

- **Gestión de Riesgos:** Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las tareas de comunicar, consultar, establecer el contexto e identificar, analizar, evaluar, tratar, monitorear y revisar el riesgo.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	Código: PN/R/PG/001/01
	Página 4 de 12

Procedimientos relacionados:

- **Tecnologías Menos Letales (TML):** Herramientas diseñadas para reducir daños colaterales, riesgos legales y muertes innecesarias que afectan la legitimidad policial y la confianza ciudadana.
- **ISO 31000:2018:** Norma que establece los principios, el marco y el proceso para la gestión de riesgos.
- **Seguridad Operativa:** Medidas y procedimientos implementados para asegurar la protección en las operaciones diarias.
- **Procedimientos Estandarizados:** Conjunto de instrucciones detalladas y documentadas para realizar tareas de manera consistente y eficiente.
- **Capacitación de Emergencia:** Programas educativos orientados a la reducción del riesgo y la preparación para situaciones imprevistas.
- **Información Confidencial:** Todo dato, documento, material, plan, fotografía, coordenada, ubicación, distribución de recursos humanos y logísticos, inventario de armamento y equipo, así como cualquier otra información a la que se tenga acceso por razón de asignación.
- **Procedimiento**: Son los lineamientos metodológicos que se llevan a cabo para ejecutar una acción operativa de forma acertada y segura.
- **Procedimientos normalizados de trabajo (PNT)**: Son los procedimientos escritos y aprobados según las normas de correcta elaboración y control de calidad que describen, de forma específica, las actividades correspondientes que se deben ejecutar para la correcta administración de los recursos logísticos correspondiente a las Tecnologías Menos Letales.

4. Descripción:

Este Procedimiento Normalizado de Trabajo (PNL) detalla las actividades esenciales para el diseño, implementación y gestión de un sistema de riesgos robusto. Dicho sistema está enfocado en el almacenamiento y la seguridad de las Tecnologías Menos Letales (TML) dentro de la Unidad de Mantenimiento del Orden Quito (Z09), y se fundamenta en las directrices de la norma ISO 31000:2018, con la finalidad de establecer los lineamientos correspondientes para la seguridad del personal policial y de terceras personas.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
	Página 5 de 12

Procedimientos relacionados:

Tipos de Procedimientos:

Los procedimientos se organizan en las siguientes categorías, según su función principal:

a) **Procedimientos Generales (PG):** Describen las directrices y actividades fundamentales que enmarcan la elaboración y gestión del sistema de riesgos. Abarcan los aspectos organizativos y de control que garantizan la coherencia y el correcto funcionamiento del PNL.

- **Estructura del PNL:** Este documento se compone de secciones clave como el Objetivo, Responsabilidad y Alcance, Definiciones, la presente Descripción, Registros y el Control de Copias. Cada sección está diseñada para asegurar una comprensión y aplicación efectivas de los lineamientos.
- **Redacción:** Establece que todos los procedimientos derivados deben ser claros, concisos y unívocos. El objetivo es facilitar su comprensión y ejecución por parte de todo el personal, eliminando ambigüedades y asegurando la estandarización operativa.
- **Distribución:** Detalla el control de emisión y distribución de copias del PNL y sus procedimientos asociados. Se lleva un registro de cada copia distribuida, incluyendo la firma y fecha de lectura del personal, garantizando el conocimiento del contenido. Las versiones obsoletas se identifican, retiran y archivan adecuadamente.
- **Revisión y Control de Cambios:** Define la revisión periódica (mínimo anual o ante cambios relevantes) del PNL y sus procedimientos. Se documentan todas las modificaciones en un "Registro de Control de Cambios" (Anexo I), detallando la versión, descripción del cambio, motivo y fecha de aprobación. Las revisiones sistemáticas (inventarios, informes operativos, auditorías y simulacros) son cruciales para identificar brechas y actualizar protocolos.
- **Planteamiento del Problema e Importancia**: Argumenta la necesidad de este sistema para mitigar los riesgos inherentes al manejo de TML. Busca reducir incidentes, optimizar procesos operativos y fortalecer la confianza pública, utilizando ISO 31000:2018 como marco de referencia para abordar los desafíos de seguridad en un entorno complejo.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 6 de 12**

b) **Procedimientos de Seguridad y Gestión de Riesgos (PS):** Concentran las operaciones específicas para la implementación, operación y mantenimiento de las medidas de seguridad y el propio sistema de gestión de riesgos. Su propósito es asegurar la protección de los activos y la mitigación efectiva de las amenazas.

- Medidas de Seguridad: Implementa un conjunto robusto y diversificado de medidas de protección:

  - **Física:** Incluye control de condiciones ambientales (temperatura, humedad), prevención de incendios, sistemas de control de acceso rigurosos (biométricos, vigilancia 24/7), y la designación de áreas de almacenamiento restringidas con registro de acceso.
  - **Lógica (Informática):** Abarca protección avanzada contra ataques (DDoS, WAF), cifrado de datos, uso actualizado de antivirus y firewalls, realización de copias de seguridad periódicas, autenticación de doble factor (2FA) y configuración de seguridad avanzada para correos electrónicos (TLS 1.3, DANE/TLSA y HTTPS en sitios web).
  - **Personal:** Establece procesos rigurosos de selección de personal, capacitación continua en manejo de TML y protocolos de emergencia, y aplicación de códigos de conducta estrictos para información confidencial.
  - **Operacional:** Desarrolla procedimientos estandarizados para el uso, mantenimiento, transporte y almacenamiento de TML, complementados con simulacros periódicos para evaluar la efectividad de los protocolos.

c) **Procedimiento de Elaboración de Fichas Técnicas (PE):** Describe la información técnica correspondiente para la elaboración de cada una de las fichas técnicas para la adquisición de medios logísticos referente a: armas, municiones, y tecnologías menos letales.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 7 de 12**

d) **Procedimiento de Descargo TML (PD):** Mencionan los documentos de descargo y los pasos a seguir para realizar los informes o partes correspondientes necesarios para la justificación de la utilización de las armas, municiones y TML, con forme al uso legítimo de la fuerza, o por concepto de capacitación, para el registro correspondiente y dar de baja del inventario general.

e) **Procedimiento Operativo TML (PO)**: Describe cada uno de los lineamientos correspondientes y pasos a seguir para el correcto almacenamiento, traslado y uso de las diferentes armas, municiones y TML.

Todos estos procedimientos tendrán el mismo formato, con una primera página o portada y a continuación el número de páginas que sean necesarios.

Portada y encabezamiento:
Como encabezamiento de la primera página debe aparecer:

- Datos Informativos de la Unidad: UMO Z09
- Grupo al que pertenece el procedimiento normalizado.
- Título del PNT.
- Número de código, por ejemplo, en el Formulario Nacional se usa la siguiente codificación:
  Dos letras, "PN" de procedimiento normalizado / Una letra, "R" de Rastrillo /Dos letras que indican el tipo de procedimiento de que se trata / Tres números que identifican el procedimiento / Dos números para la versión. Así:
  - **PN/R/PG/000/00** -Procedimientos Generales.
  - **PN/R/PS/000/00** - Procedimientos de Seguridad y Gestión de Riesgos.
  - **PN/R/PE/000/00** - Procedimiento de Elaboración de Fichas Técnicas.
  - **PN/R/PD/000/00** - Procedimiento de Descargo TML
  - **PN/R/PO/000/00** - Procedimiento Operativo TML

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 8 de 12**

Ejemplo:
PN/R/PE/001/01 - Primera versión del primer procedimiento del grupo " Elaboración de Fichas Técnicas."

El número de código de los procedimientos de elaboración de fichas técnicas (Fichas técnicas de las TML) se obtendrá a partir del código del procedimiento de elaboración de la ficha técnica correspondiente de la TML, añadiéndole un subíndice:

Ejemplo:

- **PN/R/PE/001/01** - Primera versión del procedimiento de elaboración de Ficha Técnica de munición de propulsión Cal. 38
- **PN/R/PF/001.001/01 -** Primera versión del procedimiento de elaboración de Ficha Técnica de munición de propulsión Cal 38 de Agente Químico CS, Largo Alcance.
- Fecha de aprobación.
- Paginación individual respecto al total de páginas.
- Nombre del archivo.
- Versión y/o procedimiento al que sustituye.

Además, en esta primera página figurará:

- Índice.
- Persona que lo ha redactado, firma y fecha.
- Persona que lo ha revisado y aprobado, firma y fecha.

En el resto de las hojas sólo deberá indicarse el título, número de código y la paginación individual respecto al total.

También se incluye, si procede, referencia a los procedimientos relacionados con el que se está redactando o leyendo.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 9 de 12**

4.1 Apartados de los procedimientos normalizados de trabajo.
En todos los procedimientos siempre figurarán, como mínimo, los siguientes apartados:

a) **Objetivo:**
Explicar clara y brevemente el objetivo del procedimiento.
b) **Responsabilidad de aplicación y alcance:**
Establecer quién es el responsable de cumplir el procedimiento.
c) **Definiciones:**
Definir los términos que se consideren necesarios.
d) **Descripción**
Desarrollo del procedimiento
En este punto la estructura es distinta dependiendo del tipo de procedimiento de que se trate.
e) **Registros**
Se especifican, si procede, los registros que genere el procedimiento, así como su ubicación. En caso de no generar ningún registro, se indicará 'No aplica'.
f) **Control de copias y registro de lectura del procedimiento**: Se registrará el número de copias distribuidas y quién ha leído cada copia.

Anexos: En todos los procedimientos se incluirá aquellos que se consideren necesarios.

Todos los PNT llevarán adjunto un registro de control de revisiones o cambios como el que figura como Anexo I de este PNT.

4.2 Redacción de los procedimientos:

- Los procedimientos se redactarán de forma clara y concisa.
- Se han de evitar dudas en su interpretación.
- Cuando alguno de los apartados descritos no sea necesario, se indicará "no procede" o "no aplica".
- Los procedimientos son de lectura obligatoria y deben estar en todo momento a disposición del personal que los va a aplicar.

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 10 de 12**

4.3 Distribución:

Se emitirán tantas copias como sea necesario, el mínimo será dos (una para archivar y otra para el personal). Todas deben ir firmadas y fechadas y se dispondrá de un apartado en el que se registrará el número de copias distribuidas y el nombre y cargo de todo el personal que haya leído cada copia. Las versiones obsoletas deberán ser identificadas como tal y retiradas.

4.4 Revisión y control de cambios:

- Los procedimientos serán revisados periódicamente.
- Se recomienda la inclusión, como anexo, de un registro para documentar el control de cambios donde se indicarán las distintas versiones del procedimiento, una descripción general de los cambios realizados y la fecha de aprobación de cada versión. (Anexo I de este procedimiento)
- Cuando se actualice un PNT, este registro quedará siempre como anexo de la nueva versión realizada.

5. Registros:

Control de cambios del PNT (Anexo 1)

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 11 de 12**

6. Control de Copias y Registro de lectura del Procedimiento.

COPIA NUMERO…	NOMBRE	CARGO	FIRMA	FECHA

PROCEDIMIENTO DE ELABORACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)	**Código:** PN/R/PG/001/01
Procedimientos relacionados:	**Página 12 de 12**

ANEXO 1: Registro de Control de Cambios.

PNT		
VERSION Nº	**CAMBIOS REALIZADOS**	**FECHA**

Redactado por:	**Revisado por:**	**Aprobado por:**

ANEXO 2:

Modelo de Auditoría Interna de la UMO Z09.

POLICIA NACIONAL UMO	PLAN DE AUDITORIA INTERNA		USO INTERNO	
			PÁGINA 1 DE 5	
ELABORÓ:	APROBÓ:		FECHA APROBACIÓN:	27/07/2025

Fecha de Elaboración del Plan:	**Día:**	1	**Mes:**	Julio	**Año:**	2025
Fecha de Auditoría:	**Día (s):**	27	**Mes:**	Julio	**Año:**	2025
Unidad:	UMO (Unidad de Mantenimiento del Orden Z9)					
Auditoría Interna:	Proceso independiente y documentado para evaluar la conformidad del SGR con los requisitos establecidos.					
No conformidad:	Incumplimiento de un requisito del Sistema de gestión.					
Equipo Auditor:	**Auditor Líder:**					
	Licencia Auditor No.:					
	Auditor Acompañante:					
	Licencia Auditor No.:					
	Responsables del área:					

Planificación de la Auditoría:	**Áreas auditadas:** • Proceso de capacitación en uso de tecnologías menos letales. • Procedimientos operativos para su manipulación. • Sistema de control y mantenimiento de equipos (tasers, gas, proyectiles) **Objetivos específicos:** • Verificar la implementación del tratamiento de riesgos operativos asociados al uso de armas menos letales. • Evaluar la eficacia del sistema de capacitación del personal. • Identificar brechas frente a los principios de la ISO 31000

POLICIA NACIONAL UMO	PLAN DE AUDITORIA INTERNA		USO INTERNO	
			PÁGINA 2 DE 5	
ELABORÓ:	APROBÓ:		FECHA APROBACIÓN:	27/07/2025

Ejecución de la auditoria:	**Revisión Documental:**
	• **Documentos revisados:**
	  ○ Política de gestión de riesgos institucional.
	  ○ Manual de procedimientos para el uso de tecnologías menos letales.
	  ○ Registro de capacitaciones del personal.
	  ○ Informes de incidentes operativos en el último año.
	  ○ Matriz de riesgos vigente.
	Recolección de Evidencias:
	• Entrevistas realizadas:
	  ○ Responsable de logística de armamento.
	  ○ Jefe de formación operativa.
	  ○ 3 agentes de campo.
	• **Observaciones:**
	  ○ Se detectó incumplimiento parcial de los protocolos de uso en 2 simulacros.
	  ○ Falta de evaluación de riesgo previa a la entrega del equipamiento.
	• **Indicadores revisados:**

	○ Personal certificado: 65% ○ De incidentes por fallas humanas: 18% ○ De uso correcto según protocolo: 72%
Informe:	**Fortalezas:** • Existencia de protocolos y manuales actualizados. • Compromiso institucional con la gestión del riesgo. **No conformidad principal:** • 35% del personal operativo no cuenta con certificación vigente en el uso de tecnologías menos letales, incumpliendo los procedimientos establecidos y aumentando el riesgo de uso indebido." **Observación:** Realizar auditorías operativas por unidad táctica.

POLICIA NACIONAL UMO	PLAN DE AUDITORIA INTERNA		USO INTERNO	
			PÁGINA 3 DE 5	
ELABORÓ:	APROBÓ:		FECHA APROBACIÓN:	27/07/2025

Propósito de Auditoría:	Verificar y evidenciar el cumplimiento efectivo del sistema de Gestión de riesgo, según la Norma Internacional ISO 31000.
Alcance:	La unidad de mantenimiento y el orden, ubicada en la ciudad de quito, grupo encargado de la Gestión en el Almacenamiento y Seguridad de Tecnologías Menos Letales, aplicando el Estándar Internacional de la gestión de riesgo.
Referencia de Auditoría:	Norma Internacional ISO 31000
	Leyes aplicables
	Resultados de auditorías anteriores
	Documentos del SGCS de la organización
Planificación:	**Entrevistas:** • Se realizó una entrevista al responsable de logística de armamento y al jefe de capacitación para conocer el sistema de gestión de riesgos implementado. **Revisión documental:** • Se inspeccionaron registros de entrega de armamento, protocolos de seguridad, bitácoras de entrenamiento y certificados de capacitación del personal.

POLICIA NACIONAL UMO	PLAN DE AUDITORIA INTERNA		USO INTERNO	
			PÁGINA 4 DE 5	
ELABORÓ:	APROBÓ:		FECHA APROBACIÓN:	27/07/2025

	procedimientos establecidos para el uso seguro eran cumplidos
Informe de hallazgos:	**Hallazgo de no conformidad:** • Se identificó que el 35% del personal operativo no cuenta con la capacitación actualizada para el uso de tecnologías menos letales, lo que representa un riesgo elevado de uso indebido, lesiones y responsabilidad legal institucional." **Recomendación:** • Diseñar e implementar un sistema de control y alerta automática sobre vencimientos de certificaciones, y establecer un cronograma anual de

POLICIA NACIONAL UMO	PLAN DE AUDITORIA INTERNA		USO INTERNO	
			PÁGINA 4 DE 5	
ELABORÓ:	APROBÓ:		FECHA APROBACIÓN:	27/07/2025

Seguimiento:	**Fecha de seguimiento**: Semana 27 de junio, 2025 **Acciones verificadas:** • Se verificó la implementación de un sistema digital que notifica automáticamente sobre vencimientos de capacitaciones. Además, se observó la ejecución del primer ciclo de recertificación. **Resultados del seguimiento:** • El porcentaje de personal con capacitación vencida se redujo del 35% al 8%. Se espera que alcance el 0% para el tercer trimestre del año.
Conclusion:	La auditoría identificó una debilidad crítica en el tratamiento de riesgos asociados al factor humano en el uso de tecnologías menos letales. Sin embargo, la implementación de medidas correctivas ha sido efectiva y está alineada con los principios de mejora continua promovidos por la ISO 31000.
Idioma:	Español

Declaración de confidencialidad.

El Auditor se compromete a tratar de manera estrictamente confidencial todos los documentos y toda información evidenciada durante la ejecución de esta auditoría y no será divulgada a terceros sin una autorización.
El Auditor se compromete a guardar el secreto profesional con respecto a los resultados detallados de las Auditorías, de por vida.

…… ……

REPRESENTANTE ALTA DIRECCIÓN **AUDITOR LÍDER**

AGENDA AUDITORÍA					
Lugar:					
PROCESO	**REQUISITOS NORMA**	**REQUISITOS ESTÁNDAR**	**HORA INICIO**	**HORA FIN**	**POTENCIALES AUDITADOS**
Reunión de Apertura					
Reunión de Cierre					

ANEXO 3:

Modelo de No Conformidades y Acciones Correctivas de la UMO Z09

RASTRILLO DE LA UNIDAD DE MANTENIMIENTO DEL ORDEN Z09	**SOLICITUD DE NO CONFORMIDADES Y ACCIONES CORRECTIVAS.**	**Página 1 de 2** **Rev.:** 0 **Fecha de Edición:** …..……
Procedimientos relacionados: Aplicando la ISO 31000:2018 - Gestión del Riesgo		

Institución:	Policía Nacional	**Unidad:**	UMO Z09
Fecha Auditoría:	27/07/2025	**Auditor/Responsable:**	
Tipo de auditoria No.	Interna	**Numero:**	**1**
Referencia No conformidad:	3		
Proceso:	Gestión de riesgo aplicando la ISO 31000		

Criterios de referencia

- ISO 31000: Principios de gestión del riesgo (liderazgo, evaluación del contexto, tratamiento del riesgo, mejora continua).
- Normativa interna sobre uso de tecnologías menos letales.
- Buenas prácticas internacionales en seguridad y derechos humanos.
- Manual operativo de las fuerzas de seguridad.

Descripción de la no conformidad

Se detectó que parte del personal operativo no cuenta con una capacitación adecuada y actualizada sobre el uso seguro de tecnologías menos letales, como el taser y municiones de goma. Esto genera un riesgo significativo de uso indebido, afectando la integridad de civiles y vulnerando estándares de derechos humanos		
Causa		
• Falta de evaluación de riesgos previos a la asignación del equipamiento. • Carencia de un sistema de seguimiento de certificaciones y capacitaciones. • Ausencia de actualización periódica del protocolo de uso.		
RASTRILLO DE LA UNIDAD DE MANTENIMIENTO DEL ORDEN Z09	**SOLICITUD DE NO CONFORMIDADES Y ACCIONES CORRECTIVAS.**	**Página 2 de 2** **Rev.: 0** **Fecha de Edición:** **…..……**
Propuesta de acción correctiva y/o Preventiva		
Descripción de las actividades de desarrollar	**Responsable**	**Fecha**
Implementar un programa inmediato de recertificación obligatoria para el personal activo en el uso de tecnologías menos letales.	Jefe de Unidad	Inicio: 27/07/2025 Fin: 27/01/2025
Diseñar e integrar un sistema digital de gestión del riesgo que alerte sobre capacitaciones vencidas.	Auditor Interno	Inicio: 27/07/2025 Fin: 27/001/2025
Incluir simulacros anuales de uso con evaluación de desempeño basada en riesgos.	Encargado del área	Inicio: 27/07/2025 Fin: 27/07/2026
Evidencias y registros constatados		
1. Listado de personal sin certificación vigente (documentado). 2. Informes de incidentes donde se identificó mal uso (2 casos). 3. Registro de capacitaciones inexistente o incompleto en los últimos 3 meses.		
Observaciones		
	Responsable	**Fecha**

La aplicación del marco de la ISO 31000 demuestra que existe un riesgo sistemático mal gestionado, lo que puede afectar negativamente tanto a la misión institucional como a la percepción pública. Se recomienda priorizar esta no conformidad en el plan anual de mejora continua.		Inicio: 27/07/2025 Fin: 27/08/2025
Seguimiento a la Implementación		
Responsable del Seguimiento: Auditor Interno		