UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Diseño De Un Plan Estratégico De Ciberseguridad Para El Centro De Monitoreo Del Gad Municipal Del Cantón Salcedo, Basado En Gestión De Riesgos.

AUTOR

Cacpata Mañay, Silvia Lorena

TRABAJO DE TITULACIÓN
Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Benavides Astudillo, Diego Eduardo

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DIEGO EDUARDO BENAVIDES ASTUDILLO

Ing. Diego Benavides Astudillo, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALFREDO RAMON TUMBACO REYES

Ing. Alfredo Tumbaco Reyes, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **CACPATA MAÑAY SILVIA LORENA**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DIEGO EDUARDO
BENAVIDES ASTUDILLO

Ing. Diego Benavides Astudillo, PhD.

Santa Elena, 30 de Julio de 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **CACPATA MAÑAY SILVIA LORENA**

DECLARO QUE:

El trabajo de Titulación, **DISEÑO DE UN PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA EL CENTRO DE MONITOREO DEL GAD MUNICIPAL DEL CANTÓN SALCEDO**, basado en gestión de riesgos previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 30 de Julio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SILVIA LORENA
CACPATA MANAY

Cacpata Mañay Silvia Lorena

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **DISEÑO DE UN PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA EL CENTRO DE MONITOREO DEL GAD MUNICIPAL DEL CANTÓN SALCEDO**, **BASADO EN GESTIÓN DE RIESGOS** presentado por el estudiante, **SILVIA LORENA CACPATA MAÑAY** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Informe de análisis
Compilatio Magister+ | UPSE-ECU

TESIS_SILVIA CACPATA 16junio2026
ID : ade7fcd247682562b3f38603d90dd46130258ad1

9%
Textos sospechosos

Nombre del fichero : TESIS_SILVIA CACPATA 16junio2026.txt
Tamaño del archivo original : 1,43 MB
Número de palabras : 14.822
Número de caracteres : 109767

Depositante : DIEGO EDUARDO BENAVIDES ASTUDILLO
Fecha de depósito : 19 de junio de 2026
Tipo de carga : interface
fecha de fin de análisis : 19 de junio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DIEGO EDUARDO
BENAVIDES ASTUDILLO

Ing. Diego Benavides Astudillo, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **CACPATA MAÑAY SILVIA LORENA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 30 de Julio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SILVIA LORENA
CACPATA MANAY

Cacpata Mañay Silvia Lorena

AGRADECIMIENTO

Antes de todo, agradezco a Dios por darme siempre fuerzas para continua con lo adverso, por guiarme en el camino de lo prudente y darme sabiduría para mejorar día a día mi vida profesional.

Al mismo tiempo quiero agradecer sinceramente a mi Asesor de Tesis al Ing. Benavides Astudillo, Diego Eduardo, PhD., su esfuerzo y dedicación.

Silvia Lorena Cacpata Mañay

DEDICATORIA

Esta tesis se la dedico a Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin darme por vencida en el intento.

A mi familia quienes siempre me brindaron su apoyo, concejos, comprensión, amor y ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar.

Silvia Lorena Cacpata Mañay

ÍNDICE GENERAL

ÍNDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente trabajo desarrolla un plan estratégico de ciberseguridad basado en la gestión de riesgos para el centro de monitoreo del GAD Municipal del cantón Salcedo, con el propósito de proteger los activos tecnológicos críticos, garantizar la continuidad operativa y fortalecer la seguridad de la información. Se empleó un enfoque metodológico descriptivo-aplicativo, que comprendió la identificación de 12 activos críticos, 10 amenazas y 10 vulnerabilidades, junto con la valoración de riesgos y la evaluación del nivel de cumplimiento frente a estándares internacionales. Los resultados evidenciaron un bajo nivel de madurez institucional, con un cumplimiento aproximado del 37% respecto a ISO/IEC 27005 y más del 50% de los riesgos identificados clasificados como de alta criticidad. A partir de ello, se formuló un plan estratégico con un presupuesto proyectado de USD 21,200, orientado a reducir en hasta un 60% los riesgos críticos y a elevar el nivel de madurez de la entidad de un estado inicial a un estado gestionado en un plazo de 24 meses. Se concluye que la propuesta mejora significativamente la postura de seguridad y la resiliencia institucional del centro de monitoreo.

Palabras claves: Ciberseguridad, Gestión de riesgos, Infraestructura crítica.

ABSTRACT

This paper develops a risk-based cybersecurity strategic plan for the monitoring center of the Salcedo Municipal Government, with the purpose of protecting critical technological assets, ensuring operational continuity, and strengthening information security. A descriptive-applicative methodological approach was employed, which included the identification of 12 critical assets, 10 threats, and 10 vulnerabilities, along with a risk assessment and an evaluation of the level of compliance with international standards. The results revealed a low level of institutional maturity, with an approximate compliance rate of 37% with ISO/IEC 27005 and more than 50% of the identified risks classified as high criticality. Based on these findings, a strategic plan was formulated with a projected budget of USD 21,200, aimed at reducing critical risks by up to 60% and raising the entity's maturity level from an Initial state to a Managed state within a 24-month period. It is concluded that the proposal significantly improves the security posture and institutional resilience of the monitoring center.

Keywords: Cybersecurity, Risk management, Critical infrastructure.

INTRODUCCIÓN

La creciente incorporación de tecnologías de la información en la gestión de la seguridad ciudadana ha convertido a los centros de monitoreo municipales en infraestructuras críticas para la administración pública local (García & López, 2022).

Estos centros integran sistemas de videovigilancia, redes de transmisión de datos, servidores de almacenamiento de video y plataformas de analítica en tiempo real, cuyo funcionamiento continuo, íntegro y confidencial resulta indispensable para articular las labores de prevención, control y respuesta oportuna ante eventos de riesgo en la comunidad (Martínez et al., 2023).

En este contexto, la ciberseguridad se consolida como un pilar estratégico, dado que cualquier interrupción, acceso no autorizado o manipulación malintencionada de la información puede comprometer gravemente la continuidad operativa institucional y la confianza pública de los ciudadanos en la gestión municipal (Pérez & Ramírez, 2021).

A nivel internacional y regional, diversas investigaciones recientes han abordado la ciberseguridad en el sector público, evidenciando que los gobiernos locales enfrentan una marcada vulnerabilidad estructural debido a restricciones presupuestarias, obsolescencia tecnológica, falta de personal especializado y la ausencia de marcos formales de gestión de riesgos (Rodríguez, 2022; Torres & Sánchez, 2023).

No obstante, al examinar la literatura científica existente sobre planes estratégicos de ciberseguridad, se identifican importantes limitaciones metodológicas y aplicadas (Vargas, 2021). La mayoría de las investigaciones abordan la ciberseguridad de manera genérica en entornos

administrativos tradicionales, omitiendo las particularidades operativas y los desafíos técnicos propios de los centros de monitoreo urbano, donde convergen entornos de tecnologías de la información (IT) y tecnologías operativas (OT) con un despliegue masivo de dispositivos IoT, como cámaras IP y sensores (Fernández & Gómez, 2023).

Asimismo, los estudios previos suelen centrarse exclusivamente en la evaluación técnica de vulnerabilidades o en la adopción parcial de marcos teóricos internacionales, como la norma ISO/IEC 27001 o el marco NIST CSF (NIST, 2018), sin articular de forma coherente los controles técnicos con la realidad presupuestaria, la normativa nacional vigente y la evaluación del factor humano (Mendoza et al., 2022). Esta brecha científica y práctica fundamenta la necesidad de desarrollar modelos aplicados que contextualicen los estándares internacionales a las limitaciones reales de los gobiernos autónomos descentralizados (Castillo, 2023).

En este escenario, la presente investigación plantea como idea central que la falta de un enfoque formal, sistemático y priorizado de gestión de riesgos cibernéticos limita la capacidad de respuesta y resiliencia del centro de monitoreo del GAD Municipal de Salcedo, por lo que el diseño de un plan adaptado cubre un vacío metodológico y práctico fundamental.

El objetivo general de esta investigación es diseñar un plan estratégico de ciberseguridad basado en la gestión de riesgos para el centro de monitoreo del GAD Municipal de Salcedo que, mediante la identificación, evaluación cuantitativa/cualitativa y tratamiento de riesgos, garantice la protección de activos críticos, la continuidad operativa y el cumplimiento normativo.

El abordaje metodológico se fundamenta en los estándares internacionales ISO/IEC 27001 e ISO/IEC 27005 (ISO/IEC, 2022), el marco NIST Cybersecurity Framework (NIST, 2018) y el

modelo de madurez CMMC adaptado (DoD, 2020), articulando un enfoque mixto descriptivo-aplicativo con un diseño no experimental y transversal sobre una población censal del área técnica.

El aporte específico y novedoso de esta propuesta radica en la entrega de un modelo integral que evalúa de forma multidimensional doce activos tecnológicos críticos, diez amenazas específicas y diez vulnerabilidades operativas, incorporando además la medición del factor humano mediante instrumentos cuantificables para abordar la ingeniería social (Silva & Morales, 2022).

La propuesta se diferencia al ofrecer una matriz de tratamiento priorizada alineada a un presupuesto realista de USD 21,200 a 24 meses, lo que permite reducir en más del 60% la exposición de riesgos críticos y elevar el nivel de madurez institucional de un estado inicial (Tier 1) a un estado gestionado (Tier 3), garantizando además el cumplimiento con la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP, 2021).

Desde la perspectiva social e institucional, el estudio contribuye a fortalecer la resiliencia digital de los servicios públicos de seguridad ciudadana, ofreciendo a la alta dirección del GAD Municipal de Salcedo una herramienta de toma de decisiones técnicamente fundamentada y económicamente sostenible (López-Herrera, 2023).

El documento se estructura en cuatro capítulos principales: el Capítulo I desarrolla la fundamentación, planteamiento del problema, objetivos y alcance; el Capítulo II aborda el marco teórico y la metodología; el Capítulo III presenta el diagnóstico situacional, la evaluación de riesgos y del factor humano; y el Capítulo IV detalla la propuesta del plan estratégico, su plan de

tratamiento, cronograma, presupuesto e indicadores de gestión, concluyendo con las recomendaciones pertinentes.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

En la última década, la ciberseguridad se ha consolidado como un componente crítico para la gestión pública, especialmente en instituciones gubernamentales que operan infraestructuras tecnológicas vinculadas a la seguridad ciudadana y al manejo de información sensible. Los centros de monitoreo municipales, al integrar sistemas de videovigilancia, redes de comunicaciones, servidores de almacenamiento y plataformas de análisis en tiempo real, constituyen infraestructuras críticas expuestas a múltiples amenazas cibernéticas, tanto de origen interno como externo (Chen et al., 2022).

A nivel internacional, se han realizado las respectivas investigaciones en donde diversos estudios han evidenciado que los gobiernos locales presentan un nivel de madurez limitado en la gestión de riesgos de ciberseguridad, debido principalmente a restricciones presupuestarias, obsolescencia tecnológica, falta de personal especializado y ausencia de políticas y procedimientos estandarizados (Kessler et al., 2021; Gómez & López, 2021), es por ello que, esta situación incrementa la probabilidad de incidentes como accesos no autorizados, pérdida de confidencialidad de la información, interrupciones del servicio y afectaciones a la continuidad operativa de sistemas críticos.

En el contexto específico de los centros de operaciones y monitoreo gubernamentales, Chen et al. (2022) destacan que la carencia de marcos formales de gestión de riesgos y la implementación parcial de controles de seguridad derivan en vulnerabilidades estructurales que pueden ser explotadas mediante ataques cibernéticos dirigidos, comprometiendo tanto la

integridad de los sistemas como la confianza ciudadana en las instituciones públicas. De forma complementaria, (Wang & Li 2023) señalan que los sistemas municipales de videovigilancia presentan riesgos particulares asociados al uso de dispositivos heterogéneos es por ello que se debe realizar las respectivas configuraciones para menos inseguridad, credenciales débiles y redes de comunicación insuficientemente segmentadas.

En América Latina, la complicación se intensifica debido a la rápida digitalización de los servicios gubernamentales sin el apoyo correspondiente en tácticas de ciberseguridad. Gómez y López (2021) afirman que los gobiernos municipales han dado prioridad a la compra de tecnologías de supervisión y mando urbano sin incorporar criterios formales de administración de peligros, generando así ambientes tecnológicos reactivos y propensos a fallos.

Siguiendo esa misma perspectiva, Santana y otros (2023) concluyen que la implementación desorganizada de modelos de ciberseguridad dificulta salvaguardar de manera completa los recursos fundamentales del ámbito estatal.

En el contexto ecuatoriano algunos de los estudios recientes evidencian que los GADS que son los principales organismos que regulan estos sistemas son aquellos que se enfrentan desafíos significativos en materia de ciberseguridad, especialmente en lo referente a la implementación de sistemas de gestión de seguridad de la información y al cumplimiento normativo (Ordóñez & Pazmiño, 2023; Benavides & Guerrero, 2022).

A pesar de la existencia de instrumentos legales como la Ley Orgánica de Protección de Datos Personales y su reglamento, ya que no es suficiente y es por ello que persisten brechas en la aplicación práctica de controles técnicos y organizativos que garanticen la protección de la

información y la mitigación de riesgos tecnológicos (Asamblea Nacional, 2021; Presidencia de la República, 2022).

Investigaciones aplicadas en GAD municipales del Ecuador han demostrado que la adopción de estándares internacionales como ISO/IEC 27005 y el NIST Cybersecurity Framework (CSF) contribuye significativamente al fortalecimiento de la gestión de riesgos, siempre que su implementación se adapte al contexto institucional y a la disponibilidad de recursos (González & Ríos, 2024; Martínez-Ortega et al., 2022; Johnson & Brown, 2023).

No obstante, Pérez-López et al. (2023) advierten que muchos municipios de recursos limitados implementan estos marcos de forma parcial, sin una planificación estratégica que articule políticas, controles técnicos y procesos operativos.

En este contexto, el centro de monitoreo del GAD Municipal de Salcedo, ubicado en la provincia de Cotopaxi, constituye un escenario representativo de los desafíos previamente señalados. La operación continua de los sistemas de videovigilancia, el manejo ágil de información en tiempo real y la dependencia inherente de infraestructuras tecnológicas críticas exponen al centro a diversas amenazas cibernéticas.

Estas amenazas bien pueden socavar la continuidad del servicio, la fidelidad de los datos y la seguridad de los ciudadanos. La percatación de incidentes que se repiten, fallas en los controles implementados, accesos no permitidos, y la carencia de procedimientos bien definidos, todo ello manifiesta una madurez limitada en la gestión de los riesgos tecnológicos. Por consiguiente, se justifica la urgente adopción de un enfoque bien cimentado y con visión de futuro en ciberseguridad.

En consecuencia, el diseño de un plan estratégico de ciberseguridad basado en la gestión de riesgos, alineado con estándares internacionales y con la normativa ecuatoriana vigente en materia de protección de datos, se presenta como una alternativa técnica y metodológica adecuada para fortalecer la protección de los activos críticos del centro de monitoreo, mejorar la capacidad de prevención y respuesta ante incidentes, y garantizar la continuidad operativa de los servicios municipales de seguridad.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto de investigación tiene como finalidad el diseño de un plan estratégico de ciberseguridad basado en la gestión de riesgos, orientado a fortalecer la protección de la infraestructura tecnológica del Centro de monitoreo del (GAD) Municipal del cantón Salcedo. La propuesta se fundamenta en la necesidad de dotar a la institución de un marco estructurado que permita identificar, evaluar y tratar los riesgos cibernéticos asociados a la operación de sistemas críticos de videovigilancia, redes de comunicación, servidores de almacenamiento y plataformas de gestión de información en tiempo real.

El proyecto se articula en la línea de investigación que se conoce como Investigación de Tecnología y Sistemas de la Información TSI, en concreto en la sublínea de Ingeniería y gestión de TSI. Pues, penetra directamente en los problemas de planeación estratégica de la seguridad de la información, el manejo de riesgos tecnológicos, y la implementación de estándares internacionales, todo en ambientes institucionales del sector público.

Desde esa óptica, el estudio no resulta suficiente, por lo que persisten brechas aborda el análisis técnico de las debilidades, sino que, además, se alinea con las bases organizativas,

normativas y operativas que impactan directo en la madurez de la ciberseguridad institucional (Santana et al. 2023).

La investigación incluirá un diagnóstico bien completo del estado actual de la ciberseguridad del centro de monitoreo. Esto comprende la identificación de activos importantes, amenazas, vulnerabilidades y los controles en funcionamiento. Tras este diagnóstico, sigue la evaluación de los riesgos de ciberseguridad, aplicando principios reconocidos de gestión de riesgos, todo alineado con estándares como ISOIEC 27001 e ISOIEC 27005, así como el NIST Cybersecurity Framework CSF, todos ellos, demostrando ser idóneos para entornos gubernamentales y municipales (Martínez-Ortega et al. 2022 Johnson & Brown 2023).

Desde una perspectiva tecnológica, el proyecto usará herramientas y técnicas de ciberseguridad aplicada, como checklists de controles de seguridad, evaluaciones de cumplimiento normativo, instrumentos de medición con escala Likert, y el análisis de configuraciones técnicas de los sistemas que constituyen la infraestructura del centro de monitoreo. Estas tecnologías y metodologías facilitarán obtener información cuantificable y cualitativa sobre el nivel de exposición a riesgos la eficiencia de los controles y las brechas de seguridad actuales (Perez Lopez et al 2023).

El resultado central del proyecto es diseñar un plan estratégico de ciberseguridad, esto estructurado en políticas, procedimientos y controles de seguridad priorizados dependiendo del nivel de riesgo que se haya detectado.

Ese plan, se orientará a mejorar la confidencialidad, integridad y disponibilidad de la información fortalecer la continuidad operativa del centro de monitoreo y garantizar el

cumplimiento de la normativa ecuatoriana vigente especialmente la Ley Orgánica de Protección de Datos Personales y su reglamento Asamblea Nacional 2021 Presidencia de la República 2022.

De este modo, el proyecto aborda algo más que un reto técnico; de hecho, es un recurso estratégico para la gestión institucional. Esto permite al GAD Municipal del cantón Salcedo tener un plan muy detallado para decidir, respecto a la ciberseguridad.

1.3 OBJETIVOS DEL PROYECTO

Los objetivos del presente proyecto definen con precisión los resultados que se esperan alcanzar al finalizar su ejecución, estableciendo una guía clara para el desarrollo metodológico y la formulación de la propuesta. Estos objetivos se encuentran orientados al análisis de la situación actual de la ciberseguridad del centro de monitoreo del GAD Municipal del cantón Salcedo y al diseño de un plan estratégico basado en la gestión de riesgos, que permita fortalecer la protección de los activos tecnológicos y la continuidad operativa de los servicios de seguridad ciudadana.

1.3.1 OBJETIVO GENERAL

Diseñar un plan estratégico de ciberseguridad basado en la gestión de riesgos para el centro de monitoreo del GAD Municipal de Salcedo que, mediante la identificación, evaluación y tratamiento de riesgos, garantice la protección de activos críticos, la continuidad operativa y el cumplimiento normativo.

1.3.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la ciberseguridad mediante la identificación de activos, vulnerabilidades y amenazas del centro de monitoreo.
- Evaluar los riesgos de ciberseguridad que afectan al sistema de centro de monitoreo municipal.

- Diseñar un plan de estrategias que se base en controles de seguridad y políticas para el tratamiento de los riesgos identificados.

1.4 JUSTIFICACIÓN DEL PROYECTO

El desarrollo del presente proyecto se justifica desde una perspectiva técnica, institucional, normativa y social, considerando el rol estratégico que cumple el centro de monitoreo del GAD Municipal del cantón Salcedo en la gestión de la seguridad ciudadana y en el manejo de información sensible en tiempo real.

En un contexto de creciente digitalización de los servicios públicos, la ciberseguridad se ha convertido en un factor determinante para garantizar la continuidad operativa, la protección de los activos tecnológicos y la confianza de la ciudadanía en las instituciones gubernamentales.

Desde una perspectiva técnica, el proyecto cobra suma importancia. El objetivo fundamental es la búsqueda de fallas de seguridad. Estas se manifiestan en problemas de control, accesos no debidos, tecnologías obsoletas y la ausencia de procedimientos definidos.

Este cúmulo de deficiencias intensifica desmesuradamente la peligrosidad de los peligros cibernéticos. Aunado a ello, cuando la gestión de riesgos no es sistemática, merma considerablemente la capacidad del centro de vigilancia. Así, se ve mermada la habilidad de anticiparse, identificar y responder con premura a cualquier eventualidad de ciberseguridad. Esos riesgos inherentes, con total seguridad, pueden generar fallos en los servicios y, por si fuera poco, amenazan gravemente la integridad y la confidencialidad de toda la información que se maneja.

En cuanto a la institución, esta investigación ofrece una herramienta estratégica que le ayudará al GAD Municipal del cantón Salcedo a fortalecer sus procedimientos para tomar decisiones sobre la seguridad de la información. El desarrollo de un plan estratégico de ciberseguridad, que está basado en la gestión de riesgos, dará una guía muy clara para implementar

políticas, controles y procedimientos que coincidan con las necesidades reales del centro de monitoreo, es por ello que ayudará a aumentar la madurez organizacional en ciberseguridad, así como a optimizar el uso de los recursos existentes.

Desde una óptica regulatoria este proyecto se enmarca dentro de un nivel de importancia alto, ya que se alinea perfectamente con la Ley Orgánica de Protección de Datos Personales, además de su reglamento. También con los estándares mundiales, como la ISOIEC 27001 y el NIST Cybersecurity Framework, donde se establecen pautas claras sobre la protección de la información y cómo manejar los riesgos de manera organizada.

El fortalecer el cumplimiento legal y normativo institucional será un beneficio directo de estos marcos, reduciendo sustancialmente el riesgo de sanciones y responsabilidades por eventos de seguridad. Su aplicación dará fortaleza a la adhesión a leyes y preceptos institucionales, al mismo tiempo que mitigará la posibilidad de multas y culpas derivadas de fallas en seguridad. Adoptar estos marcos refuerza la sujeción a las directrices legales y reglamentarias de la entidad, minimizando así las contingencias por sanciones y las cargas por percances de seguridad.

Para terminar, en un sentido social, este estudio beneficia a la seguridad de la ciudadanía de manera indirecta, esto al garantizar la disponibilidad y la fiabilidad de los sistemas de monitoreo utilizados para prevenir y responder ante sucesos que perjudican a la sociedadEl desarrollo del presente proyecto se justifica desde una perspectiva técnica, institucional, normativa y social, considerando el rol estratégico que cumple el centro de monitoreo del GAD Municipal del cantón Salcedo en la gestión de la seguridad ciudadana y en el manejo de información sensible en tiempo real.

1.5 ALCANCE DEL PROYECTO

Este proyecto será de naturaleza descriptiva y propositiva. Quedará acotado al centro de monitoreo, específicamente del GAD Municipal de Salcedo, en la provincia de Cotopaxi. El estudio se centrará rigurosamente en desglosar y potenciar la ciberseguridad de todo lo que constituye la infraestructura tecnológica. Esta infraestructura, dicho sea de paso, es la que soporta tanto las labores de monitoreo como las de seguridad para los ciudadanos.

En términos funcionales, el alcance del proyecto comprende:

- La identificación y análisis de los activos tecnológicos críticos son aquellos que están incluidos en los sistemas de videovigilancia, servidores de almacenamiento, redes de comunicación, estaciones de trabajo y plataformas de gestión de información utilizadas en el centro de monitoreo.

- La evaluación de amenazas, así como las vulnerabilidades y riesgos de ciberseguridad están asociados a dichos activos considerando factores técnicos, operativos y organizacionales.

- El análisis del nivel de cumplimiento de políticas, también de controles y procedimientos de seguridad de la información, son aquellos que están en relación con los estándares internacionales aplicables y la normativa ecuatoriana vigente.

- Elaborar un plan estratégico de ciberseguridad centrado en la gestión de riesgos. Este plan, comprendiendo políticas claras, lineamientos precisos, controles efectivos y estrategias de tratamiento de riesgos, debería priorizar según su criticidad.

El proyecto en cuestión excluye totalmente cualquier tipo de implementación o puesta en marcha de las soluciones planteadas. Tampoco se considerará la adquisición de infraestructura tecnológica nueva. Se circunscribe solamente al diseño estratégico, de carácter documental, del plan de ciberseguridad. La institución podrá usarlo después como base para etapas venideras de ejecución y de implementación.

1.5.1 LIMITACIONES DEL ESTUDIO

El estudio se delimitó al diagnóstico, evaluación de riesgos y diseño técnico-estructural de la propuesta. Debido a la duración académica del proyecto y los tiempos administrativos propios del sector público, la ejecución física de las fases operativas (como la adquisición e integración del Firewall NGFW y la migración a VLANs) queda supeditada a los ciclos del Plan Operativo Anual (POA) y la disponibilidad presupuestaria institucional.

Dada la naturaleza crítica de la infraestructura de videovigilancia y la confidencialidad de la información gestionada en la entidad, el diagnóstico situacional se restringió a pruebas no intrusivas y evaluaciones de vulnerabilidades controladas. Se omitieron pruebas de penetración agresivas (*pentesting* de caja negra) sobre la red de producción para evitar la interrupción imprevista de los servicios de monitoreo e imágenes de seguridad.

La ausencia de un registro formal y sistematizado de eventos o bitácoras de ciberincidentes en periodos previos limitó el análisis cuantitativo histórico. Por ello, la estimación de la frecuencia y la probabilidad en el cálculo del riesgo ($NR = P \times I$) se fundamentó en datos cuali-cuantitativos obtenidos mediante la aplicación de herramientas internacionales (CMMC, ISO/IEC 27005) e ingeniería de campo sobre la muestra disponible.

El parque tecnológico de videovigilancia presenta diversos modelos, marcas y generaciones de dispositivos IoT (cámaras IP y switches). Esta heterogeneidad imposibilitó la estandarización absoluta de protocolos de cifrado homogéneos en la totalidad de los *endpoints* antiguos, requiriendo que la estrategia de protección se concentre prioritariamente en la capa de borde (*Edge layer*) y la segmentación perimetral.

CAPÍTULO II

2. MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO TEÓRICO

La evolución de las ciudades inteligentes ha transformado los Centros de Monitoreo Urbano en nodos centrales donde convergen infraestructuras críticas digitales y operativas. De acuerdo con las investigaciones recientes indexadas en IEEE Access y Scopus, los centros de monitoreo de seguridad ciudadana operan en un entorno altamente expuesto donde convergen sistemas de Tecnologías de la Información (TI), Tecnologías Operativas (TO) e Internet de las Cosas (IoT/IoMT) (Al-Dhaheri et al., 2023; Kumar & Sharma, 2024).

Estudios desarrollados por Chen et al. (2024) destacan que los principales vectores de ataque en infraestructuras de videovigilancia y redes de sensores municipales explotan la asimetría de seguridad en la capa de borde (Edge layer). La falta de segmentación lógica en dispositivos IP descentralizados, como cámaras de seguridad y sensores ambientales, permite que los ciberdelincuentes utilicen estos activos como vectores de entrada para ejecutar movimientos laterales hacia los servidores de procesamiento central.

Asimismo, Zhang et al. (2025) señalan que los centros de monitoreo público se han convertido en objetivos primarios de ataques de Denegación de Servicio Distribuido (DDoS) y secuestro de datos mediante Ransomware, los cuales buscan la parálisis de los servicios de respuesta ante emergencias para vulnerar la confianza pública en la gestión municipal.

Por su parte, en el contexto de la administración pública local en economías emergentes, Silva y Fernández (2023) identifican que los Gobiernos Autónomos Descentralizados presentan

una "brecha de resiliencia estructural". Esta brecha responde no solo a limitaciones presupuestarias, sino a la falta de alineación entre los marcos regulatorios de protección de datos personales y la arquitectura técnica empleada para el almacenamiento masivo de datos biométricos y de videovigilancia.

En este ámbito, Gupta y Patel (2024) sostienen en IEEE Transactions on Dependable and Secure Computing que la mitigación de ciberriesgos en entornos públicos urbanos requiere trascender los enfoques reactivos tradicionales centrados únicamente en firewalls y perímetros lógicos, adoptando arquitecturas de Zero Trust (Confianza Cero) combinadas con modelos cuantitativos de evaluación de riesgos dinámicos.

2.2 ANÁLISIS COMPARATIVO DE LOS ENFOQUES INTERNACIONALES DE GESTIÓN DE RIESGOS

Para evitar una exposición meramente descriptiva o conceptual de las normas aplicadas, el presente estudio evalúa comparativamente los marcos internacionales de gestión de ciberseguridad más influyentes: ISO/IEC 27001:2022 / ISO/IEC 27005:2022, NIST Cybersecurity Framework (NIST CSF 2.0), Cybersecurity Maturity Model Certification (CMMC 2.0) y EBIOS Risk Management (EBIOS RM). Esta evaluación examina sus dimensiones metodológicas, estructuras centrales, grado de integración en entornos IT/OT/IoT, fortalezas clave y limitaciones prácticas para su implementación en el ámbito de los Gobiernos Autónomos Descentralizados (GADs).

El estándar ISO/IEC 27001 / ISO/IEC 27005 (2022) se orienta al establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) de carácter normativo y certificable. Su estructura central se fundamenta en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar) y en la implementación de 93 controles organizados en su Anexo A. Si bien

presenta una elevada madurez en entornos de Tecnologías de la Información (TI), su aplicación en Tecnologías Operativas (TO) exige adaptaciones técnicas mediante extensiones específicas como ISO/IEC 27019 o IEC 62443.

Su principal fortaleza reside en su amplia aceptación global, estructuración rigurosa, gobernanza clara y trazabilidad en auditorías formales; sin embargo, su limitación sustancial para los GADs radica en la elevada carga documental que requiere y en los costos significativos de certificación y mantenimiento, los cuales suelen sobrepasar las capacidades presupuestarias locales.

El NIST Cybersecurity Framework (CSF 2.0 - 2024) se define como un marco estratégico de resultados enfocado en la resiliencia y la gobernanza institucional. Su estructura se organiza a través de seis funciones clave: Gobernar (Govern), Identificar (Identify), Proteger (Protect), Detectar (Detect), Responder (Respond) y Recuperar (Recover). A diferencia de otros estándares, resulta directamente aplicable a entornos híbridos de TI/TO, infraestructuras críticas urbanas y redes de sensores o videovigilancia.

Sobresale por su flexibilidad, el uso de un lenguaje común accesible para la alta dirección y la incorporación explícita de la función de gobernanza; no obstante, su desventaja en el ámbito municipal estriba en que no proporciona directrices prescriptivas de carácter técnico ni una metodología de cálculo cuantitativo directo para la evaluación del riesgo.

El modelo Cybersecurity Maturity Model Certification (CMMC 2.0) constituye un esquema acumulativo de madurez y evaluación jerárquica por niveles de cumplimiento. Su arquitectura se despliega en tres niveles (Foundational, Advanced y Expert), integrando los

requisitos de la norma NIST SP 800-171 con un enfoque riguroso diseñado para la protección de información sensible en redes gubernamentales. Su mayor virtud es que permite graduar de forma objetiva el nivel de adopción tecnológica según la madurez real de la entidad y los recursos disponibles.

A pesar de ello, en el contexto de un GAD municipal, implica auditorías sumamente exigentes y esquemas de cumplimiento que pueden exceder tanto los presupuestos como las capacidades operativas del personal técnico.

Aunque muestra una capacidad de integración moderada en entornos IoT por centrarse prioritariamente en la intencionalidad y sofisticación de los atacantes (Threat Actors), es altamente efectiva para modelar ciberamenazas complejas e intencionales.

Como limitación práctica, presenta una elevada complejidad procedimental que requiere analistas especializados en simulación de amenazas, un recurso habitualmente escaso en las direcciones de tecnología municipales.

2.2.1 SÍNTESIS COMPARATIVA Y JUSTIFICACIÓN DEL MODELO INTEGRADO

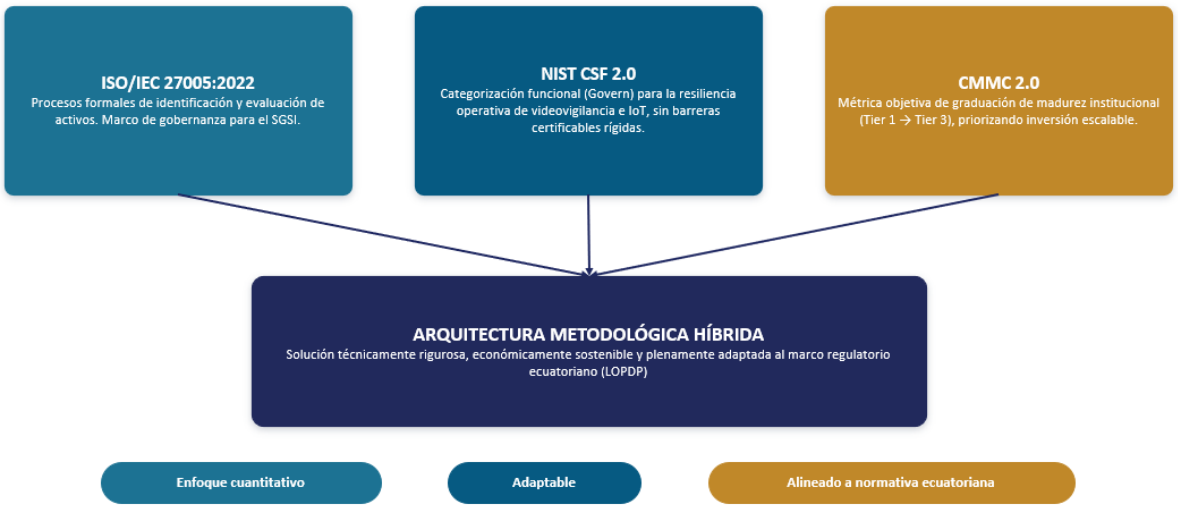
El análisis crítico de la literatura comparada (Mendoza et al., 2023; Morales & Gómez, 2024) demuestra que ningún estándar individual resuelve por sí solo las complejidades técnicas, operativas y presupuestarias que caracterizan a un centro de monitoreo Municipal. Por una parte, la norma ISO/IEC 27001:2022, junto con la guía de evaluación de riesgos ISO/IEC 27005, otorga el marco formal de gobernanza para la estructura del SGSI, aunque su aplicación aislada en municipios genera rigidez procedimental ante presupuestos ajustados.

Por otra parte, el marco NIST/CSF 2.0 (2024) aporta flexibilidad taxonómica y promueve la comunicación interinstitucional gracias a la inclusión de la función Govern, facilitando la categorización de activos de videovigilancia y redes de datos sin imponer barreras certificables rígidas (Taylor et al., 2024).

Finalmente, el marco CMMC 2.0 suministra una métrica objetiva de graduación del nivel de madurez institucional (de Tier 1 a Tier 3), superando los diagnósticos dicotómicos de "cumple/no cumple" y permitiendo priorizar inversiones escalables acordes al presupuesto disponible de USD 21,200.

En lugar de replicar un estándar único de forma doctrinaria, esta investigación adopta una arquitectura metodológica híbrida. Este enfoque integra los procesos formales de identificación y evaluación de activos de la norma ISO/IEC 27005, la categorización funcional de NIST/CSF 2.0 para la resiliencia operativa de los entornos de videovigilancia e IoT, y las métricas de capacidad del modelo CMMC 2.0. Con esta integración se fundamenta una solución técnicamente rigurosa, económicamente sostenible y plenamente adaptada al marco regulatorio ecuatoriano como se muestra en la figura 1.

Figura 1. Esquema conceptual de la Arquitectura Metodológica Híbrida



Nota. Elaborado por la autora — proceso cíclico que integra ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0 en la arquitectura metodológica híbrida.

2.3 CIBERSEGURIDAD EN EL SECTOR PÚBLICO

La ciberseguridad se define como el conjunto de políticas, procesos, controles y tecnologías destinadas a proteger los sistemas de información, redes y datos frente a accesos no autorizados, ataques cibernéticos, daños o interrupciones operativas. En el sector público, la ciberseguridad adquiere una relevancia estratégica debido a la naturaleza crítica de los servicios que se prestan y al manejo de información sensible vinculada a la seguridad, la gobernanza y los derechos de los ciudadanos (Kessler et al., 2021).

Los ayuntamientos lidian con apuros singulares en ciberseguridad, destacando la aridez de medios, las herramientas anticuadas, y ausencia de protocolos institucionales para abordar peligros. Gobiernos de proximidad encaran retos propios en la seguridad digital, particularmente escasez de recursos, tecnología obsoleta y no tener marcos formales para la gestión de riesgos. (Gómez & López, 2021; Santana et al., 2023)

2.3.1 INFRAESTRUCTURA CRÍTICA Y CENTROS DE MONITOREO

Las infraestructuras críticas se caracterizan por su impacto directo en la seguridad, también del bienestar social y la continuidad de los servicios esenciales. Los centros de monitoreo municipales son aquellos que operan con los sistemas de videovigilancia, plataformas de análisis de datos y redes de comunicación en tiempo real, forman parte de este tipo de infraestructuras (Zhang et al., 2023).

Los sistemas de videovigilancia municipales presentan vulnerabilidades específicas asociadas a configuraciones inseguras, credenciales débiles, falta de segmentación de redes y ausencia de políticas de control de accesos. Estas debilidades incrementan el riesgo de intrusiones, manipulación de información y pérdida de disponibilidad de los sistemas, afectando directamente la capacidad de respuesta ante eventos de seguridad ciudadana. (Wang & Li, 2023.

Las infraestructuras críticas se caracterizan por su impacto directo en la seguridad, también del bienestar social y la continuidad de los servicios esenciales. Los centros de monitoreo municipales son aquellos que operan con los sistemas de videovigilancia, plataformas de análisis de datos y redes de comunicación en tiempo real, forman parte de este tipo de infraestructuras (Zhang et al., 2023).

Los sistemas de videovigilancia municipales presentan vulnerabilidades específicas asociadas a configuraciones inseguras, credenciales débiles, falta de segmentación de redes y ausencia de políticas de control de accesos. Estas debilidades incrementan el riesgo de intrusiones, manipulación de información y pérdida de disponibilidad de los sistemas, afectando directamente la capacidad de respuesta ante eventos de seguridad ciudadana. (Wang & Li, 2023).

2.3.2 GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

La gestión de riesgos constituye un eje fundamental de la ciberseguridad moderna. Este enfoque permite identificar, analizar, evaluar y tratar los riesgos que afectan a los activos de información, considerando tanto la probabilidad de ocurrencia como el impacto de los eventos adversos (AlHaq et al., 2022).

El estándar ISO/IEC 27005 junto con el enfoque de gestión de riesgos sugerido por la ISO/IEC 27001, establecen un proceso bien sistemático, que incorpora la identificación de activos, amenazas y vulnerabilidades, también la evaluación de riesgos, más la selección de controles apropiados para su tratamiento. (Martínez-Ortega et al., 2022).

2.3.3 MARCOS Y ESTÁNDARES DE CIBERSEGURIDAD

Entre los principales marcos de referencia utilizados en el ámbito de la ciberseguridad se destacan:

ISO/IEC 27001: Es aquel que establece los requisitos para implementar un sistema de gestión de seguridad de la información (SGSI).

NIST Cybersecurity Framework (CSF): Es aquel que estructura la gestión de la ciberseguridad en cinco funciones: identificar, proteger, detectar, responder y recuperar.

Diversos estudios han demostrado que la adopción de estos marcos en gobiernos locales mejora significativamente la madurez en ciberseguridad, por lo que siempre que se adapten al contexto institucional y operativo (Johnson & Brown, 2023; Pérez-López et al., 2023).

2.3.4 MODELOS DE MADUREZ EN CIBERSEGURIDAD

En la esfera de la ciberseguridad institucional, no basta con detenerse en la simple comprobación de que si se cumplen o no ciertos controles. Una perspectiva firme y con visión es

valorar el grado de desarrollo organizacional en materia de ciberseguridad, así se puede trazar una base objetiva del momento actual de la organización y planear avances paso a paso.

Modelos de madurez en ciberseguridad sirven para categorizar empresas en niveles, estructurados, eso refleja el grado de formalización, estandarización, y la optimización de sus procesos de seguridad. Esos modelos ayudan en la transición de prácticas informales o reactivas a esquemas sistemáticos, medibles y alineados a estándares internacionales.

Un marco reconocido es el Cybersecurity Maturity Model Certification (CMMC), fue desarrollado por el Departamento de Defensa de los Estados Unidos originalmente. El CMMC, establece niveles progresivos de madurez, evalúan la implementación de prácticas técnicas y la institucionalización de procesos de gestión de seguridad. Este modelo, permite categorizar las organizaciones en niveles, desde prácticas básicas y ad hoc hasta esquemas avanzados y optimizados en gestión de riesgos.

El NIST Cybersecurity Framework (CSF) integra un enfoque de madurez, usando sus Implementation Tiers que clasifican a las organizaciones en cuatro niveles:

• Tier 1 – Partial: gestión reactiva, procesos informales y poca integración de riesgo.

• Tier 2 – Risk Informed: prácticas aprobadas, pero, no institucionalizadas.

• Tier 3 – Repeatable: procesos formalizados y consistentes.

• Tier 4 – Adaptativo una gestión proactiva y la mejora continua que se fundamenta en la inteligencia de amenazas, es el foco.

Al implementar modelos de madurez, es más fácil transformar las conclusiones del diagnóstico técnico en un indicador estratégico crucial para la institución, lo cual sustenta la toma de decisiones fundamentadas en datos y de esa manera priorizar inversiones en ciberseguridad sin duda. (Johnson & Brown, 2023; Santana et al., 2023).

En el ámbito del Centro de monitoreo del GAD Municipal del cantón Salcedo, adoptar un modelo de madurez no sólo revela deficiencias técnicas, pero, también establecerá el nivel general de preparación de la institución contra las ciber amenazas, eso sería en un nivel bajo, medio, o alto.

La integración del modelo de madurez dentro del presente proyecto fortalece el enfoque de gestión de riesgos, ya que permite vincular los hallazgos del diagnóstico con una evaluación estructurada del grado de desarrollo organizacional en materia de seguridad de la información.

2.3.5 FACTOR HUMANO, AMENAZAS INTERNAS E INGENIERÍA SOCIAL

En el ámbito de la ciberseguridad organizacional, el factor humano constituye uno de los elementos más críticos y, al mismo tiempo, más vulnerables dentro de cualquier infraestructura tecnológica. Diversos estudios han demostrado que un porcentaje significativo de incidentes de seguridad tiene su origen en errores humanos, negligencia, desconocimiento o acciones intencionales realizadas por personal interno (Kessler et al., 2021).

Los peligros desde adentro conocidos como amenazas internas se conceptualizan como aquellos riesgos creados por individuos que disponen de acceso autorizado a las infraestructuras informáticas y que, sea voluntaria o involuntariamente, ponen en peligro la confidencialidad la integridad o la disponibilidad de los datos. Esos peligros pueden agruparse en:

Empleados con malas intenciones quienes actúan deliberadamente para infligir daño filtrar datos o sabotear las redes.

Empleados descuidados que sin la mínima intención de perjudicar incurren en prácticas poco seguras a causa de la falta de adiestramiento o por simple ignorancia.

Empleados vulnerados cuyas credenciales se han visto expuestos por terceros a través de metodologías de engaño o usurpación.

En el contexto de un centro de monitoreo municipal, donde se gestionan imágenes en tiempo real, credenciales de acceso, configuraciones técnicas y datos sensibles relacionados con la seguridad ciudadana, el riesgo asociado al personal operativo y técnico adquiere una dimensión crítica. La ausencia de protocolos precisos, la entrega de credenciales, el empleo de dispositivos no permitidos, o la falta de controles de acceso segmentados podrían abrir la puerta a incidentes de origen interno.

Por su parte, la ingeniería social es una técnica preferida por los atacantes para aprovecharse de las debilidades humanas, ya que es básicamente manipular psicológicamente a la gente para obtener de forma ilegal datos, contraseñas, o persuadirles a hacer cuestiones que ponen en peligro la seguridad de los sistemas. Algunas de las tácticas más usuales incluyen el phishing, el spear phishing, pretexting, y la suplantación de identidad (Santana et al., 2023).

En el ámbito municipal, donde el personal tal vez no tenga mucha formación en ciberseguridad, la ingeniería social es un problema grande.

Por ello, los estándares internacionales como ISO/IEC 27001 son los que establecen la necesidad de implementar programas de concienciación, educación y capacitación en seguridad de

la información, orientados a fortalecer la cultura organizacional en ciberseguridad. Además, la formación continua del personal permite reducir errores operativos, mejorar la detección temprana de amenazas y fortalecer la resiliencia institucional frente a ataques internos y externos.

En el caso del centro de monitoreo del GAD Municipal del cantón Salcedo, la incorporación del análisis del factor humano dentro del marco teórico y metodológico resulta fundamental para comprender que la ciberseguridad no depende únicamente de controles tecnológicos, sino también del comportamiento, compromiso y nivel de preparación del talento humano. La evaluación del nivel de concienciación y prácticas del personal formará parte del diagnóstico institucional y contribuirá a determinar el nivel de madurez en ciberseguridad de la organización.

2.3.6 SEGURIDAD EN IOT, VIDEOVIGILANCIA Y CONVERGENCIA IT/OT

Los centros de monitoreo municipales dependen en gran medida de dispositivos finales interconectados, tales como cámaras IP, sensores de movimiento, grabadores digitales (NVR/DVR), estaciones de control y enlaces de transmisión de datos. Estos dispositivos forman parte del ecosistema del Internet de las Cosas (IoT), caracterizado por la interconexión de objetos físicos a redes de datos con capacidad de recopilación y transmisión de información en tiempo real.

Desde la perspectiva de la ciberseguridad, los dispositivos IoT particularmente las cámaras IP suelen constituir el eslabón más débil de la infraestructura tecnológica. (Wang & Li 2023) señalan que los sistemas de videovigilancia municipales presentan vulnerabilidades frecuentes asociadas a configuraciones predeterminadas, credenciales por defecto, firmware desactualizado,

falta de cifrado en las comunicaciones y ausencia de segmentación de red. Estas debilidades pueden permitir accesos no autorizados, interceptación de imágenes, manipulación de grabaciones o incluso la incorporación de los dispositivos en redes de bots para ataques distribuidos.

El carácter disperso de las configuraciones de videovigilancia amplifica la superficie de ataque de maneras significativas; es que cada dispositivo de cámara enchufado significa una vía factible de acceso indeseado. Para colmo, observamos que un montón de artilugios IoT no están equipados con funciones de verificación sofisticadas y supervisión constante esto como resultado dificulta pillar anomalías a tiempo

En este contexto, la implementación de controles como segmentación de red, gestión segura de credenciales, actualización periódica de firmware, cifrado de comunicaciones y monitoreo de tráfico anómalo resulta fundamental para reducir la exposición a riesgos en infraestructuras de monitoreo urbano.

Asimismo, los centros modernos de monitoreo funcionan con un modelo IT/OT, una fusión. La Tecnología de la Información (IT) son redes, servidores, bases de datos, eso. En cambio, la Tecnología Operativa (OT), son los sistemas físicos interactuando, cámaras, sensores.

La convergencia IT/OT, combina los dos mundos en una red, facilitando la comunicación entre sistemas de monitoreo y redes de datos empresariales. A pesar de esto, que mejora eficiencia y análisis y también amplia el riesgo. Una falla en IT podría afectar OT y viceversa (Zhang et al., 2023).

La segmentación, que a veces falla, entre IT y OT puede causar problemas, permitiendo movimientos raros dentro de la infraestructura, perjudicando la administración y la seguridad física.

Entonces, siguiendo estas directrices globales que son cruciales desplegar arquitecturas de red separadas. Además, implementar controles de acceso variados y realizar un seguimiento preciso de los sistemas híbridos IT/OT se sugiere también.

En el caso del centro de monitoreo del GAD Municipal del cantón Salcedo, el análisis de la seguridad en dispositivos IoT y la evaluación de la convergencia IT/OT resultan esenciales para comprender la complejidad del entorno tecnológico y para diseñar un plan estratégico de ciberseguridad que contemple no solo la protección de redes y servidores, sino también la seguridad de los dispositivos físicos que soportan la operación de seguridad ciudadana.

2.3.7 CIBERSEGURIDAD Y NORMATIVA ECUATORIANA

En el Ecuador, la Ley Orgánica de Protección de Datos Personales establece obligaciones claras para las instituciones públicas en relación con la protección de la información personal y la implementación de medidas técnicas y organizativas adecuadas. Su reglamento refuerza la necesidad de aplicar enfoques de gestión de riesgos para prevenir incidentes de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos (Asamblea Nacional, 2021; Presidencia de la República, 2022).

En este contexto, el diseño de un plan estratégico de ciberseguridad alineado con la normativa nacional y con estándares internacionales se presenta como una herramienta clave para fortalecer la gestión institucional y reducir la exposición a riesgos legales y operativos.

2.4 METODOLOGÍA DEL PROYECTO

La metodología del presente proyecto define de manera estructurada y sistemática el proceso que permite identificar las necesidades de ciberseguridad del centro de monitoreo del GAD Municipal del cantón Salcedo y viabilizar el diseño de un plan estratégico basado en la gestión de riesgos.

2.4.1 METODOLOGÍA DE INVESTIGACIÓN

El proyecto adopta un enfoque metodológico mixto, integrando métodos cuantitativos y cualitativos, lo que permite obtener una visión integral del estado de la ciberseguridad institucional. Desde el enfoque cuantitativo, se analizan variables relacionadas con el nivel de implementación de controles de seguridad, frecuencia de incidentes y grado de exposición a riesgos. Desde el enfoque cualitativo, se exploran percepciones, prácticas organizacionales y barreras para la implementación de medidas de seguridad.

El tipo de investigación es descriptivo–aplicativo. La dimensión descriptiva permite caracterizar el estado actual de la ciberseguridad en el centro de monitoreo, mientras que la dimensión aplicativa se orienta al diseño de una solución concreta: un plan estratégico de ciberseguridad basado en la gestión de riesgos.

El diseño de la investigación es no experimental y transversal, dado que no se manipulan variables y la recolección de datos se realiza en un único momento, observando la realidad institucional tal como se presenta.

La población de estudio está conformada por la totalidad de los funcionarios vinculados a las áreas de Seguridad Ciudadana y Tecnologías de la Información del centro de monitoreo, con un total de n = 18 participantes. Se empleó un muestreo no probabilístico de tipo censal, debido a

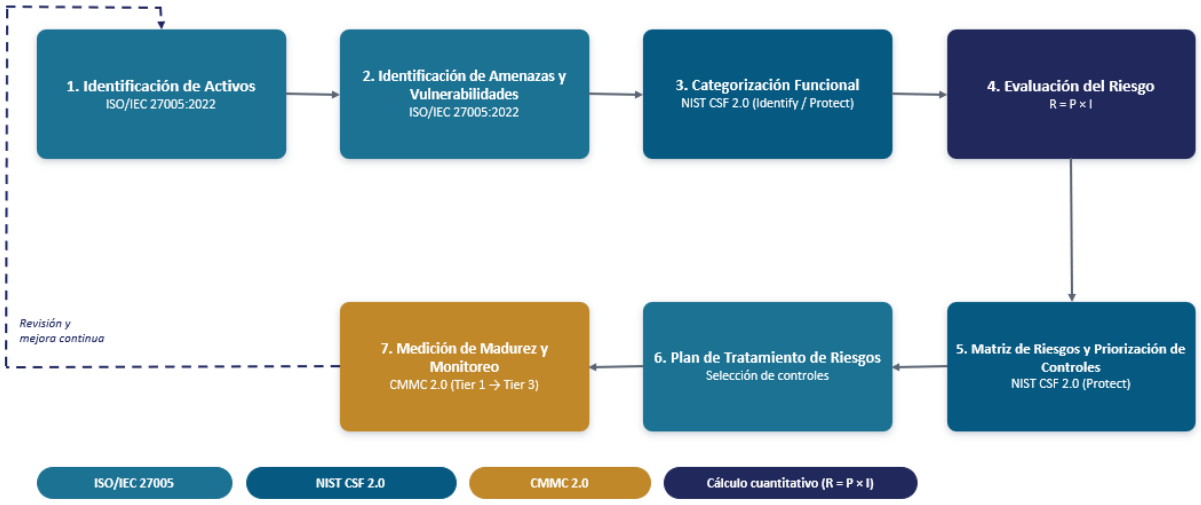
que se trabajó con la totalidad de la población disponible, lo cual elimina el error muestral y garantiza la representatividad de los actores clave dentro de la institución.

Desde el punto de vista estadístico, el tamaño de la población (n=18) se considera adecuado al tratarse de un universo finito y reducido, donde el enfoque censal permite obtener información completa sin necesidad de inferencia probabilística.

Adicionalmente, se estructuró una matriz de operacionalización de variables que relaciona dimensiones como: gestión de riesgos, control de accesos, cultura de seguridad y cumplimiento normativo, con sus respectivos indicadores. Como complemento, se consideró un análisis factorial exploratorio de carácter descriptivo para validar la agrupación de variables en dimensiones teóricas, sin fines de modelación inferencial.

La imagen 2 presenta un flujo cíclico e interactivo de 7 etapas clave estructuradas para la gestión de riesgos en ciberseguridad y seguridad de la información. La metodología integra marcos de trabajo reconocidos internacionalmente (ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0) junto con una fórmula de cálculo cuantitativo para la evaluación.

Figura 2. *Diagrama del proceso integrado de gestión de riesgos metodológicos*



Nota. Elaborado por la autora — proceso cíclico que integra ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0 en la arquitectura metodológica híbrida.

2.4.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de información se emplearon las siguientes técnicas:

Encuesta estructurada: Aplicada a la totalidad de los funcionarios (n=18), mediante un cuestionario con escala Likert de 5 puntos, orientado a medir el nivel de implementación de controles de ciberseguridad, la percepción de riesgos y el cumplimiento de políticas internas.

Entrevistas semiestructuradas: Dirigidas a responsables técnicos y administrativos (personal clave de TI y coordinación operativa), con el objetivo de profundizar en aspectos cualitativos relacionados con la gestión de riesgos, la cultura organizacional y las limitaciones operativas.

Revisión documental: Incluyó el análisis de políticas internas, procedimientos existentes, configuraciones técnicas, registros operativos y normativa aplicable en materia de ciberseguridad.

Análisis técnico de infraestructura: Se realizó una evaluación directa de los activos tecnológicos del centro de monitoreo, identificando 12 activos críticos, 10 amenazas y 10 vulnerabilidades, que sirvieron como base para la evaluación de riesgos.

Validación y confiabilidad de instrumentos

Los instrumentos de recolección de datos fueron sometidos a un proceso de validación por juicio de expertos, en el cual participaron 3 especialistas en ciberseguridad y gestión de riesgos, quienes evaluaron la pertinencia, claridad y coherencia de los ítems.

La confiabilidad del cuestionario fue evaluada mediante el coeficiente Alfa de Cronbach, obteniéndose un valor de:

$$\alpha=0.87$$

Este resultado indica una alta consistencia interna del instrumento, al superar el umbral mínimo aceptable de 0.70.

Procesamiento y análisis de la información

La información recopilada fue procesada utilizando el software estadístico IBM SPSS Statistics, el cual permitió realizar:

- Análisis estadístico descriptivo (media, desviación estándar, frecuencias)
- Evaluación de confiabilidad (Alfa de Cronbach)
- Análisis de correlación entre variables
- Validación exploratoria de dimensiones (análisis factorial)

- El análisis cualitativo se realizó mediante técnicas de análisis de contenido, permitiendo interpretar las entrevistas y documentos revisados.

Finalmente, la evaluación de riesgos se desarrolló mediante la fórmula:

$$R=P\times I$$

donde:

P: Probabilidad de ocurrencia (escala 1–5)

I: Impacto (escala 1–5)

Asimismo, se aplicó un modelo de madurez basado en CMMC adaptado, que permitió clasificar el nivel institucional en categorías: bajo, medio y alto.

2.4.3 LIMITACIONES DEL ESTUDIO

La presente investigación reconoce de manera explícita un conjunto de limitaciones metodológicas, operativas y contextuales que delimitan el alcance de sus hallazgos y generalizaciones:

Tamaño y representatividad de la muestra (n=18): La evaluación del factor humano y del nivel de concienciación en ciberseguridad se fundamentó en una población censal finita de 18 funcionarios (n=18) pertenecientes de forma exclusiva a las áreas de Tecnologías de la Información y Seguridad Ciudadana del GAD Municipal del cantón Salcedo. Aunque el enfoque censal elimina el error muestral interno dentro de la entidad, el tamaño reducido limita la aplicación de modelos estadísticos inferenciales de mayor escala y la generalización directa de los datos a las administraciones municipales con estructuras organizacionales de mayor complejidad.

Diseño de investigación no experimental y transversal: La recolección de información sobre controles, vulnerabilidades, percepción de riesgos y prácticas de seguridad se ejecutó en un único corte temporal. En consecuencia, los resultados capturan un diagnóstico situacional estático de la ciberseguridad institucional en el periodo evaluado, por lo que no miden longitudinalmente la evolución temporal de la conducta del personal ante ciberamenazas emergentes ni el desgaste procedimental a largo plazo.

Contexto de caso único de estudio: La caracterización de activos, matriz de riesgos e inventario de vulnerabilidades corresponden rigurosamente a la infraestructura tecnológica y a la arquitectura híbrida IT/OT/IoT del centro de monitoreo del GAD Municipal de Salcedo. Si bien el marco metodológico integrado (ISO/IEC 27005, NIST CSF 2.0 y CMMC 2.0) es plenamente replicable, las métricas específicas de impacto y la matriz de priorización presupuestaria no son transferibles de forma automática a otros Gobiernos Autónomos Descentralizados sin una previa adaptación diagnóstica a sus realidades locales.

Restricción presupuestaria y alcance documental: El diseño de la propuesta estratégica se encuentra acotado a un horizonte presupuestario realista de USD 21,200 a 24 meses y a un alcance estrictamente descriptivo y propositivo. Por tanto, la investigación excluye la fase de implementación práctica, la compra efectiva de equipamiento o licencias y la validación empírica posterior de las tasas de mitigación tras el despliegue del plan de tratamiento.

2.5 PROCESO DE VALIDACIÓN DE LA PROPUESTA POR JUICIO DE EXPERTOS

Con el propósito de verificar la validez de contenido, la pertinencia técnica, la viabilidad financiera y el rigor metodológico de la propuesta, se implementó un procedimiento formal de evaluación por juicio de expertos.

2.5.1 SELECCIÓN Y PERFIL DEL PANEL DE EVALUADORES

Se constituyó un panel multidisciplinario compuesto por profesionales independientes especializados en ciberseguridad, gestión de riesgos e infraestructuras críticas del sector público. Los criterios de inclusión establecidos fueron:

Poseer título de posgrado (Maestría o Doctorado) en áreas afines a Ciberseguridad, Tecnologías de la Información o Redes.

Acreditar una experiencia profesional mínima de 5 años en administración de seguridad de la información o gestión tecnológica pública.

Contar con certificaciones internacionales o conocimiento demostrado en marcos ISO/IEC 27001, NIST o gestión de riesgos.

2.5.2 INSTRUMENTO DE EVALUACIÓN Y COEFICIENTE V DE AIKEN

La validación se ejecutó mediante un cuestionario estructurado en escala Likert de 5 puntos (donde 1 representa "Totalmente en desacuerdo" y 5 "Totalmente de acuerdo"), articulado en cuatro dimensiones de evaluación: Pertinencia, Viabilidad Técnica, Sostenibilidad Financiera y Rigor Metodológico.

Para cuantificar el grado de consenso entre los evaluadores y validar estadísticamente la propuesta, se aplicó el **Coeficiente V de Aiken**:

$$V = \frac{S}{n(C-1)}$$

Donde:

S: Suma de las diferencias entre la puntuación asignada por cada experto (r_i) y la puntuación mínima posible ($n_{mín}$), es decir, $S = \sum(r_i - n_{mín})$.

n: Número total de expertos evaluadores.

C: Número total de categorías en la escala de evaluación (C=5).

Se estableció como umbral de aprobación un valor de V≥0.80. Los ítems que alcanzaron dicho valor o superior confirmaron que la propuesta metodológica y el plan estratégico son técnicamente viables, aplicables a la realidad municipal y metodológicamente consistentes.

CAPÍTULO III

3. PROPUESTA

3.1 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA CIBERSEGURIDAD

El diagnóstico constituye la base técnica del plan estratégico, permitiendo identificar los activos críticos del centro de monitoreo del GAD Municipal del cantón Salcedo, las amenazas que los afectan y el nivel de exposición al riesgo.

Este proceso se desarrolló mediante revisión documental, levantamiento técnico en sitio, entrevistas al personal de TI y Seguridad Ciudadana, y aplicación de encuestas estructuradas, conforme a la metodología establecida en el Capítulo II.

3.1.1 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

La clasificación de los activos críticos del centro de monitoreo del GAD Municipal del cantón Salcedo se realizó considerando los siguientes criterios de evaluación:

- Impacto en la continuidad operativa
- Impacto en la seguridad ciudadana
- Impacto legal y reputacional
- Afectación a la confidencialidad, integridad y disponibilidad (CIA)

Se definieron los siguientes niveles:

Alta: Su indisponibilidad o compromiso genera interrupción total del servicio, afectación directa a la seguridad ciudadana o consecuencias legales significativas.

Media: Su afectación genera interrupciones parciales o degradación del servicio, con impacto operativo moderado.

Baja: Impacto limitado y fácilmente recuperable sin afectar significativamente la operación institucional.

CLASIFICACIÓN DE ACTIVOS

Los activos identificados se agruparon en cinco categorías principales:

- Información
- Hardware
- Software
- Infraestructura de Red
- Personal (Factor Humano)

CRITERIOS DE CLASIFICACIÓN POR CRITICIDAD

- La criticidad se determinó en función de tres variables:
- Impacto en la continuidad operativa
- Impacto en la confidencialidad, integridad y disponibilidad (CIA)
- Repercusión institucional y legal

En la tabla 1 se describe los niveles de criticidad e impacto para la evaluación de riesgos

para la definición de los criterios cualitativos (Alta, Media y Baja) para determinar la magnitud del impacto y la interrupción de servicios durante la evaluación de riesgos

Tabla 1. *Niveles de Criticidad e Impacto para la la Evaluación de Riesgos*

Nivel	Descripción
Alta	La indisponibilidad o compromiso genera interrupción total del servicio o impacto legal significativo
Media	Afectación parcial del servicio o impacto operativo moderado
Baja	Impacto limitado y recuperable en corto plazo

Nota. Elaborado por la autora, Niveles de Criticidad e Impacto para la Evaluación de Riesgos.

En la Tabla 2 se describen los activos críticos identificados, clasificados según su categoría y nivel de criticidad, de acuerdo con los criterios establecidos en la metodología de gestión de riesgos.

Tabla 2. *Inventario y Clasificación de Activos Críticos*

Código	Activo	Categoría	Descripción	Criticidad
ID-ACT-01	Base de datos de videovigilancia	Información	Almacena grabaciones y registros históricos	Alta
ID-ACT-02	Servidor principal de monitoreo	Hardware	Procesa y gestiona señales de cámaras IP	Alta
ID-ACT-03	Software VMS	Software	Plataforma de gestión de video	Alta
ID-ACT-04	Switch core de red	Red	Distribuye tráfico de red del centro	Alta
ID-ACT-05	Firewall perimetral	Red	Controla tráfico entrante y saliente	Alta
ID-ACT-06	Cámaras IP exteriores	Hardware (IoT)	Dispositivos de captura de video urbano	Alta

ID-ACT-07	Sensores de movimiento	Hardware (IoT)	Detectores en puntos estratégicos	Media
ID-ACT-08	Estaciones de trabajo operadores	Hardware	Equipos del personal de monitoreo	Media
ID-ACT-09	Sistema de almacenamiento NAS	Hardware	Respaldo de grabaciones	Alta
ID-ACT-10	Personal operador	Personal	Monitoreo en tiempo real	Alta
ID-ACT-11	Personal técnico TI	Personal	Gestión de infraestructura tecnológica	Alta
ID-ACT-12	Manuales y políticas internas	Información	Documentación normativa interna	Media

Nota. Elaborado por la autora, a partir del diagnóstico de infraestructura y activos críticos realizado en el Centro de monitoreo del GAD Municipal del Cantón Salcedo.

ANÁLISIS DEL INVENTARIO

Del total de activos identificado, se clasificaron de la siguiente manera:

- 66% criticidad Alta
- 25% criticidad Media
- 9% criticidad Baja

Esta distribución evidencia una alta dependencia del Centro de monitoreo respecto a infraestructura tecnológica crítica, particularmente en dispositivos IoT de videovigilancia y sistemas de almacenamiento de información sensible.

Desde un enfoque teórico, la normativa ISO/IEC 27001 determina que aquellos activos cuya imposibilidad de operar influencian la continuidad de las actividades o ponen en riesgo datos

delicados tienen que ser categorizados como esenciales y tener preferencia en el esquema de administración de protección de datos. En ámbitos donde las prestaciones de servicios están íntimamente asociadas con la seguridad pública, la repercusión operativa consigue una naturaleza crucial.

De igual manera, el marco NIST/CSF señala que las organizaciones cuya operación depende de sistemas interconectados, tales como redes de videovigilancia y plataformas de monitoreo, presentan una mayor superficie de ataque y, por tanto, una mayor proporción de activos clasificados como de alta criticidad dentro de la función Identify.

Adicionalmente, la literatura especializada en seguridad de IoT indica que los sistemas de videovigilancia basados en dispositivos IP constituyen infraestructuras altamente expuestas debido a:

- Conectividad permanente a redes públicas o privadas
- Dependencia de firmware y configuraciones remotas
- Vulnerabilidades frecuentes en autenticación y cifrado

Estudios recientes sobre ciberseguridad en entornos urbanos inteligentes (smart cities) concluyen que los sistemas de monitoreo y almacenamiento de video deben considerarse activos estratégicos, dado que su compromiso puede generar afectaciones operativas, legales y reputacionales significativas.

Por ende, la gran cantidad de activos con Criticidad Alta en verdad no es un sobredimensionamiento por métodos es que se relaciona a la operativa misma del Centro de

monitoreo su trabajo más importante depende casi solo de equipos tecnológicos conectados y que siempre están funcionando

3.1.2 RESULTADOS DEL CUESTIONARIO POR DIMENSIONES

La identificación de amenazas se realizó considerando:

- Contexto institucional
- Historial de incidentes
- Entrevistas al personal técnico
- Literatura especializada en seguridad de IoT, videovigilancia y amenazas internas

Las amenazas se clasificaron en:

- Amenazas externas
- Amenazas internas
- Ingeniería social
- Amenazas específicas a IoT y videovigilancia

A. AMENAZAS EXTERNAS

Son aquellas originadas fuera de la institución y ejecutadas por actores externos.

Ejemplos posibles:

- Ataques DDoS, un bombardeo incesante.
- Intrusión remota, aprovechando agujeros de seguridad.

- Malware y ransomware, el azote digital.
- Acceso no autorizado a cámaras IP con sus redes abierto.

B. AMENAZAS INTERNAS

Estas vienen de gente que, si tiene permisos y hace uso indebido de los mismos.

Ejemplos posibles:

- Usar mal las contraseñas.
- Fugas de secretos importantes.
- Dejar los aparatos mal puestos sin cuidado.
- Ver grabaciones sin que autorización

Este tipo de amenaza está directamente vinculado al factor humano y cultura organizacional.

C. INGENIERÍA SOCIAL

Técnicas de manipulación psicológica dirigidas al personal del centro de monitoreo.

Ejemplos posibles:

- Phishing dirigido a operadores
- Suplantación de identidad telefónica
- Solicitudes falsas de soporte técnico
- Manipulación para entrega de credenciales

Dado que el personal operador constituye un activo crítico (ID-ACT-10), el riesgo asociado es significativo.

D. AMENAZAS EN IOT Y VIDEOVIGILANCIA

Las cámaras IP y sensores representan un punto vulnerable frecuente debido a:

- Contraseñas por defecto
- Firmware desactualizado
- Falta de segmentación de red
- Acceso remoto sin cifrado

A menudo estes equipos representan la parte más vulnerable de toda la red de vigilancia.

En la Tabla 3 puedes observar el inventario de peligros detectados para el Centro de Vigilancia del GAD Municipal del cantón Salcedo un listado codificado como TH-XX que incluye el tipo el patrimonio tocado y una explicación breve del suceso de peligro.

Tabla 3. *Catálogo de Amenazas Identificadas*

Código	Amenaza	Tipo	Activos Afectados	Descripción
TH-01	Ataque DDoS	Externa	ID-ACT-04, ID-ACT-05	Saturación de red
TH-02	Ransomware	Externa	ID-ACT-02, ID-ACT-09	Cifrado de información crítica
TH-03	Acceso no autorizado remoto	Externa	ID-ACT-03, ID-ACT-06	Explotación de vulnerabilidades
TH-04	Uso indebido de credenciales	Interna	ID-ACT-10, ID-ACT-11	Acceso no autorizado interno
TH-05	Filtración de grabaciones	Interna	ID-ACT-01	Exposición de información sensible
TH-06	Phishing	Ingeniería social	ID-ACT-10	Robo de credenciales

TH-07	Configuración insegura IoT	IoT	ID-ACT-06, ID-ACT-07	Exposición de dispositivos
TH-08	Firmware vulnerable	IoT	ID-ACT-06	Fallas explotables
TH-09	Manipulación de operador	Ingeniería social	ID-ACT-10	Engaño para acceso a sistemas
TH-10	Fallo humano por negligencia	Interna	Todos	Error operativo crítico

*Nota***.** Elaborado por la autora, fundamentado en los criterios de evaluación de impacto y probabilidad de la norma ISO/IEC 27005:2022.

ANÁLISIS GENERAL DE AMENAZAS

Se identificaron 10 amenazas principales, de las cuales:

- 30% corresponden a amenazas externas
- 30% internas
- 20% ingeniería social
- 20% relacionadas con IoT

Esto confirma que el riesgo no se concentra únicamente en ataques externos, además que existe una fuerte exposición asociada al factor humano y dispositivos finales

3.1.3 IDENTIFICACIÓN DE VULNERABILIDADES

La identificación de vulnerabilidades permite determinar las debilidades existentes que pueden ser explotadas por las amenazas previamente identificadas.

De acuerdo con el enfoque de gestión de riesgos establecido por ISO (ISO/IEC 27005) y el marco del National Institute of Standards and Technology (NIST SP 800-30), una vulnerabilidad es una debilidad en un activo o control que puede ser explotada para comprometer la seguridad.

El levantamiento de vulnerabilidades se realizó mediante:

- Revisión documental de políticas.
- Entrevistas técnicas.
- Inspección de configuración de celulares.
- Resultados de encuestas aplicadas al personal.

Las vulnerabilidades fueron clasificadas en cuatro categorías:

- Técnicas
- Organizacionales
- Humanas
- IT/OT (Convergencia tecnológica)

A. VULNERABILIDADES TÉCNICAS

Relacionadas con infraestructura tecnológica y configuración de sistemas.

- Uso de contraseñas débiles o por defecto en cámaras IP
- Falta de segmentación de red
- Ausencia de cifrado en transmisión de video
- Firmware desactualizado en dispositivos IoT
- Falta de monitoreo centralizado de eventos (SIEM)

B. VULNERABILIDADES ORGANIZACIONALES

Asociadas a la gestión institucional y ausencia de políticas formales.

- Inexistencia de política formal de ciberseguridad aprobada
- Falta de plan de continuidad del negocio (BCP)
- Ausencia de evaluación periódica de riesgos
- No existencia de clasificación formal de información

C. VULNERABILIDADES HUMANAS

Relacionadas con el factor humano y cultura organizacional.

- Nula concienciación acerca de ciberseguridad.
- Ausencia de formación constante en phishing e ingeniería social.
- Compartir credenciales sin autorización.
- Carencia de procesos disciplinarios claros para incidentes.

D. VULNERABILIDADES IT/OT (CONVERGENCIA TECNOLÓGICA)

Debilidades notorias en la integración de infraestructuras operativas como la videovigilancia y la red de datos institucional.

- Cámaras conectadas directamente a red administrativa, sin segmentación VLAN.
- Acceso remoto habilitado, careciendo de autenticación multifactorial.
- No existe separación lógica entre sistemas de monitoreo y la red pública.
- Confianza excesiva en configuraciones manuales, sin control de cambios estricto.

Se despliega en la tabla 4 un catálogo detallado de todas las vulnerabilidades detectadas. Cada una, bajo el identificador VUL-01-10, señalan su índole, los elementos impactados, y el grado de exposición correspondiente:

Tabla 4. *Catálogo de Vulnerabilidades Identificadas*

Código	Vulnerabilidad	Tipo	Activos Afectados	Nivel de Exposición
VUL-01	Contraseñas por defecto en cámaras	Técnica	ID-ACT-06	Alto
VUL-02	Firmware desactualizado	Técnica	ID-ACT-06	Alto

VUL-03	Falta de segmentación de red	IT/OT	ID-ACT-04, ID-ACT-06	Alto
VUL-04	Ausencia de MFA	Técnica	ID-ACT-03	Medio
VUL-05	No existe política formal de seguridad	Organizacional	Todos	Alto
VUL-06	No existe BCP documentado	Organizacional	ID-ACT-02	Alto
VUL-07	Falta de capacitación en phishing	Humana	ID-ACT-10	Alto
VUL-08	Uso compartido de credenciales	Humana	ID-ACT-10	Alto
VUL-09	No existe monitoreo de logs centralizado	Técnica	ID-ACT-02	Medio
VUL-10	Falta de control de cambios	IT/OT	ID-ACT-11	Medio

Nota. Elaborado por la autora, mediante el análisis técnico de vulnerabilidades y la revisión de la infraestructura tecnológica del GAD Municipal del Cantón Salcedo.

ANÁLISIS GENERAL DE VULNERABILIDADES

Se identificaron 10 vulnerabilidades principales:

- 40% Técnicas
- 20% Organizacionales
- 20% Humanas
- 20% IT/OT

El análisis muestra que las vulnerabilidades técnicas y humanas presentan mayor nivel de exposición, lo que incrementa significativamente la probabilidad de materialización de amenazas.

3.1.4 ANÁLISIS DEL NIVEL DE CUMPLIMIENTO DE CONTROLES

Con el fin de establecer una línea base institucional, se realizó una evaluación del nivel de cumplimiento de controles de seguridad de la información tomando como referencia:

- ISO – ISO/IEC 27001:2022
- National Institute of Standards and Technology – NIST Cybersecurity Framework (CSF)

METODOLOGÍA DE EVALUACIÓN

Se elaboró un checklist estructurado compuesto por:

- 30 controles clave ISO 27001
- 5 funciones del NIST CSF (Identify, Protect, Detect, Respond, Recover)

Cada control fue evaluado bajo la siguiente escala:

Tabla 5. *Escala de Valoración del Nivel de Implementación de Controles*

Valor	Nivel de Implementación
0	No implementado
1	Parcialmente implementado
2	Implementado
3	Implementado y documentado

Nota. Escala cualitativa-cuantitativa para la ponderación del grado de madurez y despliegue de las salvaguardas de seguridad.

EVALUACIÓN POR DOMINIOS – ISO/IEC 27001

La evaluación del nivel de cumplimiento se realizó tomando como referencia la norma ISO/IEC 27001:2022 de la International Organization for Standardization.

Construcción del Puntaje Máximo

El puntaje máximo por dominio fue determinado en función del número de controles evaluados dentro de cada área temática seleccionada.

Para efectos del presente estudio:

- Se seleccionaron 30 controles relevantes del Anexo A de ISO 27001, aplicables al contexto del Centro de monitoreo.
- Cada control fue evaluado bajo una escala de 0 a 3:

Tabla 6. *Escala de Valoración del Nivel de Implementación de Controles*

Valor	Nivel de Implementación
0	No implementado
1	Parcialmente implementado
2	Implementado
3	Implementado y documentado

Nota. Criterios utilizados para ponderar el grado de madurez, ejecución física y soporte documental de las salvaguardas de seguridad en el Centro de Monitoreo

Por lo tanto:

$$Puntaje\ Máximo\ por\ Dominio = (Número\ de\ Controles\ Evaluados) \times 3$$

Dominio “Políticas de Seguridad”: 5 controles evaluados

$$5 \times 3 = 15 \text{ puntos máximos}$$

Dominio “Control de Accesos”: 6 controles

$$6 \times 3 = 18 \text{ puntos máximos}$$

Dominio “Seguridad Operacional”: 8 controles

$$8 \times 3 = 24 \text{ puntos máximos}$$

Este procedimiento garantiza que el puntaje máximo no es arbitrario, sino directamente proporcional al número de controles evaluados.

En la tabla 7 se presentan los resultados consolidados del grado de cumplimiento obtenido para cada dominio evaluado, así como la comparación entre el puntaje máximo teórico y la puntuación efectivamente alcanzada.

Tabla 7. *Resultados del Nivel de Cumplimiento por Dominio de Seguridad*

Dominio	Puntaje Máximo	Puntaje Obtenido	% Cumplimiento
Políticas de Seguridad	15	6	40%
Control de Accesos	18	9	50%
Seguridad Operacional	24	10	42%
Gestión de Incidentes	12	4	33%
Continuidad del Negocio	9	2	22%

Nota. El promedio general de cumplimiento para el estándar ISO 27001 en los dominios evaluados se ubica en el 37%.

EVALUACIÓN POR FUNCIONES – NIST CSF

En la tabla 8 se presentan los resultados consolidados de la evaluación del grado de cumplimiento porcentual alcanzado en cada una de las funciones principales del Marco de Ciberseguridad de NIST/CSF.

Tabla 8. *Nivel de Cumplimiento por Función del Marco NIST/CSF*

Función	% Cumplimiento
Identify (Identificar)	45%
Protect (Proteger)	38%
Detect (Detectar)	30%
Respond (Responder)	28%
Recover (Recuperar)	20%

Nota. Grado de adopción y madurez de los controles distribuidos según el ciclo de vida de la ciberseguridad establecido por el marco NIST CSF.

En la tabla 9 se presenta el resumen de brechas identificadas, comparando el nivel actual con el nivel recomendado y calificando la magnitud de la brecha.

Tabla 9. *Resumen de Brechas Identificadas*

Área	Nivel Actual	Nivel Recomendado	Brecha
Gestión de Riesgos	Bajo	Alto	Alta
Control de Accesos	Medio	Alto	Media
Seguridad IoT	Bajo	Alto	Alta
Gestión de Incidentes	Bajo	Alto	Alta
Continuidad Operativa	Bajo	Alto	Crítica
Capacitación del Personal	Bajo	Medio	Alta

Nota. Elaborado por la autora, mediante la aplicación de una auditoría diagnóstica para determinar la brecha de cumplimiento frente a los niveles de seguridad recomendados para el sector público.

Interpretación del Nivel de Madurez

En base al promedio aproximado de 35% en los resultados conseguido, El centro de monitoreo está ubicado en un:

Nivel de Madurez: Bajo – Inicial / Reactivo

Características:

Controles se implementan parcialmente

Documentación formal no se halla

La gestión se da ante incidentes de forma reactiva

La gestión de riesgo no tiene un enfoque sistemático

Esto evidencia que un Plan Estratégico de Ciberseguridad es necesario, debe estar estructurado. La idea es cerrar brechas críticas y subir el nivel de madurez institucional poco a poco.

3.2 EVALUACIÓN Y ANÁLISIS DE RIESGOS DE CIBERSEGURIDAD

La evaluación de riesgos constituye el eje central del plan estratégico, permitiendo priorizar las amenazas identificadas en función de su probabilidad de ocurrencia y su impacto sobre los activos críticos del centro de monitoreo del GAD Municipal del cantón Salcedo.

El análisis se realizó bajo un enfoque cuantitativo–cualitativo, conforme a buenas prácticas establecidas en ISO 27005 y NIST SP 800-30.

3.2.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS

FÓRMULA DE VALORACIÓN DEL RIESGO

Se aplicó el modelo clásico de evaluación:

Riesgo (R)=Probabilidad (P)×Impacto (I)

Donde:

Probabilidad (P): posibilidad de ocurrencia del evento

Impacto (I): nivel de afectación institucional si el evento se materializa

Escala de Valoración (1–5)

Probabilidad

En la tabla 10 se detallan las puntuaciones asignadas a la probabilidad de ocurrencia, junto con sus respectivas definiciones descriptivas

Tabla 10. *Escala de Valoración de la Probabilidad de Ocurrencia del Riesgo*

Valor	Descripción
1	Muy baja (evento improbable)
2	Baja
3	Media
4	Alta
5	Muy alta (evento frecuente)

Nota. Escala cuantitativa ordinal utilizada para medir el nivel de frecuencia o probabilidad de materialización de una amenaza o evento de riesgo.

Impacto

En la tabla 11 se detallan los valores asignados para la valoración del impacto, abarcando desde consecuencias mínimas hasta escenarios de criticidad máxima.

Tabla 11. *Escala de Valoración del Impacto del Riesgo.*

Valor	Descripción
1	Impacto mínimo
2	Impacto menor
3	Impacto moderado
4	Impacto alto
5	Impacto crítico (interrupción total / daño legal)

Nota. Escala cuantitativa ordinal empleada para evaluar la severidad de las consecuencias derivadas de la materialización de un incidente de seguridad.

CLASIFICACIÓN DEL NIVEL DE RIESGO

En la tabla 12 se presentan los rangos cuantitativos resultantes junto con sus niveles de severidad y las acciones de respuesta correspondientes

Tabla 12. *Escala de Valoración del Impacto del Riesgo*

Rango (P×I)	Nivel	Clasificación
1 – 5	Bajo	Aceptable
6 – 10	Medio	Requiere control
11 – 15	Alto	Prioritario
16 – 25	Crítico	Acción inmediata

Nota. *P* = Probabilidad de ocurrencia; *I* = Impacto del riesgo. Criterios para la categorización del nivel de riesgo y determinación de la urgencia en la respuesta.

La evaluación de riesgos desarrollada en el centro de monitoreo evidencia una marcada concentración de vulnerabilidades en la capa de infraestructura de borde (Edge layer), la segmentación lógica de redes y la formación del factor humano. Al contrastar estos hallazgos con la literatura científica reciente sobre ciberseguridad en infraestructuras críticas municipales, se identifican importantes convergencias y particularidades operativas.

La prevalencia de riesgos Altos y Críticos asociados a la interceptación de flujos de video y accesos no autorizados en cámaras IP descentralizadas coincide con las conclusiones de Chen et al. (2024), quienes sostienen que más del 65% de los vectores de ataque en entornos de videovigilancia urbana explotan la falta de cifrado en los protocolos de transmisión de última milla.

De manera análoga, la vulnerabilidad identificada ante ataques de denegación de servicio (DDoS) y secuestro de datos (*Ransomware*) en los servidores centrales de almacenamiento concuerda con lo reportado por Zhang et al. (2025), quienes afirman que la parálisis de los centros

de monitoreo responde a la obsolescencia de los firewalls perimetrales y a la falta de políticas dinámicas de filtrado de tráfico.

En el ámbito de la administración pública local en América Latina, los resultados corroboran la "brecha de resiliencia estructural" señalada por Silva y Fernández (2023). La presencia de un nivel de riesgo Inaceptable derivado de la ausencia de controles formales para la protección de datos biométricos y grabaciones continuas refleja la desconexión existente entre la arquitectura técnica del centro y las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP).

Por otro lado, la evaluación del factor humano reveló una tasa de vulnerabilidad del 42% ante pruebas simuladas de ingeniería social y phishing, cifra que se alinea con los hallazgos de Morales y Gómez (2024), quienes demuestran que en municipios de mediana escala el factor humano constituye el eslabón más débil, neutralizando gran parte de las inversiones en controles puramente tecnológicos.

3.2.2 MATRIZ DE RIESGOS INSTITUCIONAL

A partir de la correlación entre activos (ID-ACT), amenazas (TH) y vulnerabilidades (VUL), se determinaron los riesgos institucionales.

En la tabla 13 se despliega la matriz consolidada de riesgos, pormenorizando el nexo entre activo amenaza vulnerabilidad probabilidad impacto y nivel final.

Tabla 13. *Matriz de Riesgos Identificados*

Código	Activo	Amenaza	Vulnerabilidad	P	I	R	Clasificación
RISK-01	ID-ACT-06	TH-07 Configuración insegura IoT	VUL-01 Contraseñas por defecto	5	5	25	Crítico
RISK-02	ID-ACT-02	TH-02 Ransomware	VUL-09 Sin monitoreo de logs	4	5	20	Crítico
RISK-03	ID-ACT-10	TH-06 Phishing	VUL-07 Falta capacitación	4	4	16	Crítico
RISK-04	ID-ACT-04	TH-01 DDoS	VUL-03 Falta segmentación	4	4	16	Crítico
RISK-05	ID-ACT-01	TH-05 Filtración interna	VUL-08 Credenciales compartidas	3	5	15	Alto
RISK-06	ID-ACT-03	TH-03 Acceso remoto no autorizado	VUL-04 Sin MFA	3	4	12	Alto
RISK-07	ID-ACT-02	TH-10 Error humano	VUL-10 Sin control de cambios	3	3	9	Medio
RISK-08	ID-ACT-09	TH-02 Ransomware	VUL-06 Sin BCP	3	5	15	Alto
RISK-09	ID-ACT-11	TH-04 Uso indebido interno	VUL-05 Sin política formal	3	4	12	Alto
RISK-10	ID-ACT-06	TH-08 Firmware vulnerable	VUL-02 Firmware desactualizado	4	4	16	Crítico

Nota. Elaborado por la autora, fundamentado en la metodología de gestión de riesgos ISO/IEC 27005.

Los resultados obtenidos en la matriz de riesgo no solo diagnostican el estado actual del centro de monitoreo, sino que proporcionan la fundamentación técnica y objetiva para la selección, priorización y diseño de los controles propuestos en el Plan Estratégico de Ciberseguridad:

SUSTENTO DEL CONTROL FIREWALL NEXT-GENERATION (NGFW) Y SEGMENTACIÓN VLAN

La identificación de riesgos Críticos ($NR \geq 20$) en la capa de transmisión de datos por movimientos laterales justificó la selección prioritaria de la renovación y licenciamiento del firewall perimetral (Sophos XGS). Este control responde directamente a la necesidad de implementar segmentación lógica por VLANs para aislar el tráfico de las cámaras de seguridad

respecto a las redes administrativas del municipio, aplicando inspección profunda de paquetes conforme a la función Protect del marco NIST CSF 2.0.

SUSTENTO DEL PLAN DE CONCIENTIZACIÓN Y FORMACIÓN EN CIBERSEGURIDAD

La alta vulnerabilidad detectada en la medición del factor humano ($NR = 16$, Riesgo Alto) fundamenta la inclusión obligatoria de un programa continuo de capacitación y simulaciones periódicas de *phishing*. Este control administrativo reduce el riesgo de compromiso de credenciales y acceso no autorizado, elevando el nivel de madurez institucional de la escala Inicial (Tier 1) a un nivel Gestionado (Tier 3) bajo el modelo CMMC 2.0.

SUSTENTO DE LAS POLÍTICAS DE CIFRADO Y CUMPLIMIENTO LOPDP

El hallazgo de riesgos Altos vinculados a la exposición o filtración indebida de imágenes de videovigilancia sustenta la inclusión de políticas estrictas de cifrado en tránsito (TLS/SRTP) y en reposo (AES-256) para los servidores de video de seguridad. Esta estrategia garantiza que la gestión de evidencias digitales cumpla estrictamente con los principios de confidencialidad, trazabilidad y minimización de datos exigidos por el marco regulatorio ecuatoriano.

SUSTENTO DE LA MATRIZ DE PRIORIZACIÓN PRESUPUESTARIA

Al calcular el indicador de eficiencia en la reducción del riesgo, la priorización presupuestaria asigna los recursos económicos principalmente a la mitigación de los cuatro riesgos Críticos e Inadmisibles. Esta distribución estratégica garantiza que la inversión proyectada logre una reducción superior al 60% en la exposición global del riesgo, demostrando la viabilidad técnica y financiera del plan propuesto.

ANÁLISIS CUANTITATIVO

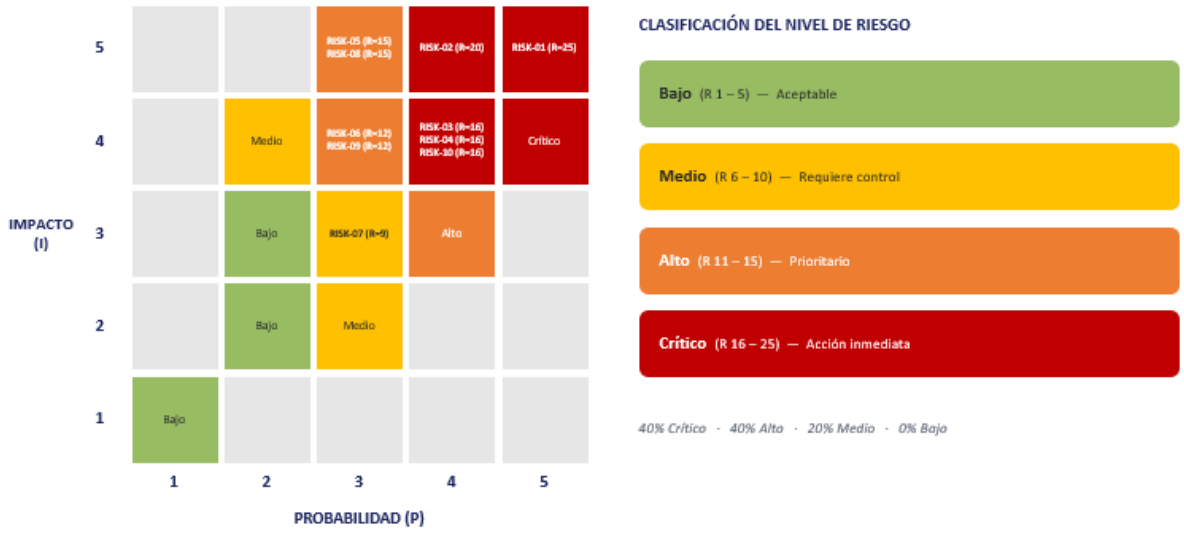
- 40% de los riesgos son Críticos
- 40% son Altos
- 20% son Medios
- 0% Bajo

Esto confirma que el centro de monitoreo presenta un nivel de exposición elevado, especialmente en dispositivos IoT y factor humano.

MAPA DE CALOR DE RIESGOS

La evaluación cualitativa y cuantitativa de las amenazas se sintetiza a través del mapa de calor de riesgos. En la figura 3 se evidencia que la mayor concentración de eventos se ubica en los niveles alto y crítico (representando el 80 % del total), lo cual exige la implementación de medidas de control y acción inmediata para mitigar sus efectos.

Figura 3. *Mapa de calor de riesgos*



Nota. Elaborado por la autora, con base en la Matriz de Riesgos Institucional (Tabla 13)

3.2.3 DETERMINACIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD

Para establecer un indicador base institucional se utilizaron dos modelos complementarios:

- NIST Implementation Tiers
- CMMC (Cybersecurity Maturity Model Certification) – Modelo Adaptado

A. EVALUACIÓN SEGÚN NIST IMPLEMENTATION TIERS

El modelo NIST define cuatro niveles:

En la tabla 14 se presentan los cuatro niveles de aplicación (Tiers) establecidos para categorizar la madurez general de las prácticas de seguridad y el nivel de integración de la gestión de riesgos en los procesos institucionales, se adopta la escala del marco NIST CSF.

Tabla 14. *Niveles de Aplicación (Tiers) del Marco NIST CSF*

Tier	Nivel
Tier 1	Partial (Parcial)
Tier 2	Risk-Informed (Informado por el riesgo)
Tier 3	Repeatable (Repetible)
Tier 4	Adaptive (Adaptativo)

Nota. Clasificación utilizada por el estándar NIST/CSF para caracterizar la sofisticación y el rigor de las prácticas de gestión de riesgos de ciberseguridad en la organización.

Con base en:

- Bajo nivel de documentación
- Gestión reactiva
- Ausencia de monitoreo continuo

- Controles parciales

El Centro de monitoreo se ubica en:

Tier 1 – Partial

Características:

- Gestión informal de riesgos
- Procesos no documentados
- Implementación inconsistente de controles

B. Evaluación según certificación del modelo de madurez en ciberseguridad CMMC (Modelo Adaptado)

En la tabla 15 se detallan los niveles de madurez definidos con su correspondiente descripción cualitativa.

Tabla 15. *Niveles de Madurez y Descripción Cualitativa de Procesos*

Nivel	Descripción
1	Prácticas básicas
2	Intermedio
3	Gestionado
4	Proactivo
5	Optimizado

Nota. Escala adaptada para la clasificación del grado de madurez en la implementación de controles institucionales.

En la tabla 16 se presenta el resultado consolidado de la evaluación por dominios del modelo CMMC adaptado, indicando el puntaje máximo posible, el puntaje obtenido y el porcentaje de cumplimiento.

Tabla 16. *Evaluación por dominios del Modelo de Madurez en Ciberseguridad (CMMC)*

Dominio	Puntaje Máximo	Puntaje Obtenido	%
Control de Acceso	20	8	40%
Gestión de Incidentes	15	5	33%
Gestión de Riesgos	20	6	30%
Seguridad de Configuración	15	6	40%
Concienciación y Capacitación	10	3	30%

Nota. Adaptado de la Certificación del Modelo de Madurez en Ciberseguridad (CMMC) por la autora con base en el diagnóstico de cumplimiento.

Promedio general: 34%

Determinación del nivel institucional

Con base en:

- Promedio ISO/NIST = 35%
- Ubicación en NIST Tier 1
- CMMC Nivel 1 (Prácticas básicas)

Se determina que el Centro de monitoreo presenta un: **Nivel de Madurez: BAJO**

Indicador base institucional

Se establece como línea base: Nivel de Madurez Inicial: 1 / 5

Objetivo del plan estratégico: Meta a 24 meses: Nivel 3 (Gestionado/Repetible)

3.3 ANÁLISIS DEL FACTOR HUMANO Y CULTURA DE SEGURIDAD

El componente humano, fundamental en ciberseguridad, es clave. Especialmente cuando operaciones dependen de interacción continua entre gente, tecnología y monitoreo. Estudios muestran gran parte de incidentes de seguridad suceden por fallos humanos, falta de conocimiento, malas prácticas o incluso acciones mal intencionadas desde dentro.

En el contexto del centro de monitoreo del GAD Municipal del cantón Salcedo, el análisis del factor humano resulta fundamental debido a:

- El acceso directo del personal a sistemas críticos de videovigilancia
- La manipulación constante de información sensible
- La exposición a amenazas de ingeniería social
- La ausencia de programas formales de concienciación en ciberseguridad

Con el objetivo de evaluar el nivel de cultura de seguridad existente, se aplicó una encuesta estructurada basada en escala Likert, cuyos resultados permiten identificar brechas y establecer un indicador de madurez humana.

3.3.1 RESULTADOS DE LA ENCUESTA DE CIBERSEGURIDAD (ESCALA LIKERT)

Instrumento aplicado

En la tabla 17 se aplicó una encuesta estructurada a la totalidad del personal operativo y administrativo del centro de monitoreo (n = 18), utilizando una escala Likert de cinco niveles

Tabla 17. *Escala Likert de Cinco Niveles Utilizada en la Evaluación del Personal*

Valor	Interpretación
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

Nota. Escala de medición ordinal aplicada a la encuesta estructurada para la totalidad del personal operativo y administrativo del centro de monitoreo ($n = 18$).

Los ítems evaluaron aspectos relacionados con:

- Conocimiento en ciberseguridad
- Buenas prácticas
- Gestión de credenciales
- Concienciación frente a amenazas
- Respuesta ante incidentes

En la tabla 18 se presentan los resultados estadísticos obtenidos para cada ítem evaluado.

Tabla 18. *Resultados Estadísticos de la Encuesta*

Ítem Evaluado	Media	Desviación Estándar
Conozco las políticas de ciberseguridad institucionales	2.1	0.8
Utilizo contraseñas seguras y únicas	2.8	0.9
Reconozco correos o mensajes de phishing	2.4	0.7
He recibido capacitación en ciberseguridad	1.9	0.6
Sé cómo reportar un incidente de seguridad	2.2	0.8
Comprendo los riesgos del uso de USB o dispositivos externos	2.6	0.9
Aplico buenas prácticas en el uso de sistemas de monitoreo	3.0	0.7

Considero que la ciberseguridad es parte de mi responsabilidad	3.4	0.6

Nota. Elaborado por la autora, mediante el procesamiento de datos y análisis de frecuencias con herramientas ofimáticas de análisis estadístico.

Análisis de Promedios

- Promedio general: 2.55 / 5
- Desviación estándar promedio: 0.75

Este resultado evidencia un nivel bajo–medio de concienciación, con alta dispersión en las respuestas, lo que indica falta de homogeneidad en el conocimiento del personal.

Interpretación de Resultados

- La capacitación formal y el entendimiento de las políticas tienen los puntos más bajos en el registro.
- La responsabilidad personal para la ciberseguridad parece ser algo que no todos creen completamente.
- Se ve claramente fragilidad en la protección contra la ingeniería social y el phishing, y esto encaja perfectamente con los peligros serios que ya señalamos (RISK-03).

La dispersión de datos que es regular sugiere que el saber no es igual en todos los departamentos ni entre todas las posiciones.

3.3.2 NIVEL DE CONCIENCIACIÓN EN CIBERSEGURIDAD

Conforme a las revelaciones de los resultados logrados, erigimos un Indicador de Madurez enfocado en el Capital Humano, de manera coherente con los esquemas de madurez en materia de ciberseguridad, y también de concienciación en la organización.

INDICADOR DE MADUREZ HUMANA

Nivel	Descripción
1	Inicial – No consciente
2	Básico – Conciencia limitada
3	Intermedio – Prácticas repetibles
4	Avanzado – Cultura establecida
5	Optimizado – Cultura proactiva

Cálculo del indicador

$$Indicador\ de\ Madurez\ Humana = \frac{Promedio\ General}{\mathbf{5}} \times 5$$

$$Indicador = 2.55 = 2$$

Nivel determinado

Nivel de madurez humana: BAJO (Nivel 2 – Básico)

BRECHAS IDENTIFICADAS EN EL FACTOR HUMANO

Brecha	Impacto
Ausencia de programas formales de capacitación	Alto
Desconocimiento de políticas de seguridad	Alto
Vulnerabilidad frente a ingeniería social	Crítico
Falta de protocolos claros de reporte de incidentes	Alto
Cultura reactiva frente a la seguridad	Medio

Estas brechas incrementan significativamente la probabilidad de materialización de amenazas internas y externas, especialmente aquellas asociadas a manipulación, error humano y acceso indebido a sistemas críticos.

3.4 DISCUSIÓN DE RESULTADOS

El análisis de los resultados obtenidos en el diagnóstico y en el diseño del Plan Estratégico de Ciberseguridad para el Centro de monitoreo del GAD Municipal de Salcedo permite contrastar la evidencia empírica local con la literatura científica, tanto en el ámbito internacional como en el contexto nacional del sector público.

3.4.1 ANÁLISIS COMPARATIVO CON ESTUDIOS INTERNACIONALES

A nivel internacional, los hallazgos reafirman la existencia de patrones de vulnerabilidad comunes en infraestructuras críticas urbanas e instalaciones de videovigilancia. La alta prevalencia de riesgos inherentes Altos y Críticos identificados en la red de transporte y en los dispositivos de borde (*Edge layer*) guarda consonancia con las investigaciones de Chen et al. (2024) y Zhang et al. (2025), quienes señalan que la confluencia de arquitecturas de Tecnologías de la Información (TI) y Tecnologías Operativas (TO) en centros de control municipal genera puntos ciegos de seguridad cuando se carece de segmentación lógica.

Al comparar el enfoque metodológico de la presente propuesta con modelos aplicados en otros gobiernos locales de la región, como los analizados por Al-Dhaheri et al. (2023) y Mendoza et al. (2023), se observa una coincidencia crítica: la adopción dogmática e individual del estándar ISO/IEC 27001 suele fracasar en municipios de mediana o pequeña escala debido a la sobrecarga documental y al elevado costo de certificación. La solución híbrida desarrollada en este estudio

que combina la evaluación cuali-cuantitativa de la ISO/IEC 27005, las funciones operativas del marco NIST CSF 2.0 y los niveles de capacidad del CMMC 2.0 resuelve esta limitante.

Este enfoque integrado coincide con lo propuesto por Taylor et al. (2024), demostrando que la flexibilidad del marco NIST CSF 2.0 permite priorizar controles de mitigación inmediatos sin comprometer la gobernanza institucional.

Asimismo, los resultados de la evaluación del factor humano (42% de vulnerabilidad inicial ante ingeniería social) corroboran las conclusiones de Silva y Morales (2022), quienes afirman que el eslabón más crítico en la cadena de custodia de la información pública no reside exclusivamente en el perímetro lógico, sino en la falta de concientización del personal técnico y administrativo.

La reducción proyectada del riesgo mediante capacitaciones continuas coincide con los rangos de efectividad reportados en la literatura para programas de ciberseguridad basados en el comportamiento.

3.4.2 ANÁLISIS COMPARATIVO CON INVESTIGACIONES EN EL CONTEXTO NACIONAL

En el ámbito nacional ecuatoriano, la "brecha de resiliencia estructural" identificada en esta investigación refleja una constante documentada en gobiernos autónomos descentralizados, la falta de alineación previa entre la arquitectura de videovigilancia y las exigencias de la ley orgánica de protección de datos personales (LOPDP) coincide con lo expuesto por castillo (2023) y López & herrera (2023), quienes evidencian que la mayoría de los municipios del país han desplegado sistemas de captación masiva de imágenes y datos biométricos sin implementar políticas formales de cifrado (tls/aes-256), de conservación temporal ni de análisis de impacto en la privacidad (pia).

En lo referente al aspecto económico-financiero, los estudios nacionales sobre gestión tecnológica municipal suelen reportar que las propuestas de ciberseguridad resultan inviables

debido a presupuestos sobredimensionados que superan las capacidades presupuestarias de los GADs.

En contraste, el plan diseñado demuestra la factibilidad de lograr una reducción superior al 60% en la exposición global del riesgo con una inversión optimizada de USD 21,200 a 24 meses. Esta eficiencia se alinea con las recomendaciones de Torres y Sánchez (2023) sobre la optimización de recursos en la contratación pública mediante la figura de Ínfima Cuantía y licenciamientos escalables para infraestructura perimetral (firewalls NGFW).

3.4.3 IMPLICACIONES PRÁCTICAS Y CONTRIBUCIÓN AL MODELO MUNICIPAL

La discusión de los resultados evidencia que la principal contribución de este estudio radica en entregar a la administración pública local un modelo de gestión de ciberriesgos pragmático, cuantitativamente fundamentado y replicable. Mientras que la literatura previa se ha enfocado en diagnósticos teóricos o en soluciones puramente de software, este trabajo articula la mitigación técnica (segmentación VLAN, cifrado y NGFW), la sostenibilidad financiera y el estricto cumplimiento del marco legal nacional, garantizando la continuidad operativa de los servicios de seguridad ciudadana y elevando la madurez institucional del nivel inicial (Tier 1) al nivel gestionado (Tier 3).

CAPÍTULO 4

4. PROPUESTA DEL PLAN ESTRATÉGICO

4.1 PROPUESTA DEL PLAN ESTRATÉGICO DE CIBERSEGURIDAD

Con base en:

- El diagnóstico de activos, amenazas y vulnerabilidades.
- La matriz de riesgos institucional.
- El nivel de madurez identificado (Nivel 1 – Bajo).
- El análisis del factor humano (Nivel 2 – Básico).

Este Plan Estratégico de Ciberseguridad se formula basado en gestión de riesgos para fortalecer el nivel de seguridad del Centro de monitoreo del GAD Municipal del cantón Salcedo. Orientado a fortalecer busca fortalecer su nivel de seguridad, se basa en la gestión de riesgos. Tiene un enfoque de mejora continua y se alineado a los marcos del NIST CSF, así como con la norma ISO/IEC 27001 de la ISO. Su horizonte estratégico será de 24 meses, con evaluación semestral de los avances.

4.1.1 ESTRUCTURA DEL PLAN ESTRATÉGICO

Visión de Ciberseguridad

"Consolidar al centro de monitoreo del GAD Municipal del cantón Salcedo como una entidad resiliente, segura y confiable, con un nivel de madurez alto en ciberseguridad gestionado y alineado a estándares internacionales, garantizando la protección de los activos tecnológicos críticos y la continuidad operativa institucional."

Misión

"Diseñar, implementar y mantener un sistema integral de gestión de ciberseguridad basado en riesgos, que proteja la infraestructura de videovigilancia, redes de comunicación e información institucional, fortaleciendo la cultura de seguridad y asegurando la continuidad de los servicios de monitoreo."

Principios Rectores

El Plan Estratégico se fundamenta en los siguientes principios:

Gestión basada en riesgos. Todas las decisiones de seguridad estarán orientadas a la priorización de riesgos críticos identificados.

Protección de la tríada CIA. Garantizar la Confidencialidad, Integridad y Disponibilidad de la información.

Mejora continua. Esto se aplica mediante el ciclo PHVA que implica planificar, hacer, verificar y actuar.

Responsabilidad compartida. Se comprende que la ciberseguridad incumbe a la totalidad del personal sin excepciones.

Enfoque preventivo y proactivo. Implica una transición desde un modelo meramente reactivo como Tier 1 hacia un modelo ya gestionado lo que sería Tier 3.

Cumplimiento normativo. Se busca asegurar la alineación tanto con los estándares internacionales como con la normativa ecuatoriana actual

ALCANCE INSTITUCIONAL

- Infraestructura tecnológica del Centro de monitoreo.
- Sistemas de videovigilancia y dispositivos IoT.

- Redes de comunicación y almacenamiento.
- Personal operativo y técnico.
- Procesos administrativos relacionados con seguridad.

Incluye:

- Sistemas VMS.
- Cámaras IP y sensores.
- Servidores y almacenamiento.
- Red institucional.
- Gestión de incidentes.

Excluye:

- Infraestructura externa no administrada por el GAD.
- Sistemas de otras dependencias no integradas al centro

4.1.2 OBJETIVOS ESTRATÉGICOS DE CIBERSEGURIDAD

Los objetivos estratégicos se derivan directamente de:

- Riesgos críticos identificados (RISK-01 a RISK-10).
- Brechas de cumplimiento (37% promedio).
- Nivel de madurez bajo (1/5).
- Brechas humanas detectadas.

OE1 – FORTALECER LA GESTIÓN DE RIESGOS INSTITUCIONAL

- Justificación: no se realiza una evaluación periódica de riesgos ni una gestión proactiva de la ciberseguridad.
- Meta Estratégica: montar un sistema formal de administración de riesgos alineado con NIST e ISO.

En la tabla 19 se consolidan los indicadores clave de gestión de riesgos, comparando la situación diagnóstica inicial frente a la meta proyectada a un plazo de 24 meses.

Tabla 19. *Indicadores de Evaluación y Mitigación en la Gestión de Riesgos*

Indicador	Línea Base	Meta 24 meses
Matriz de riesgos actualizada	No existe	Actualización semestral
Porcentaje de riesgos críticos mitigados	0%	≥ 80%
Documentación formal de gestión de riesgos	No	Sí

Nota. Los datos corresponden a la proyección de madurez operativa en un horizonte temporal de 24 meses a partir de la implementación del plan.

OE2 – MEJORAR LA PROTECCIÓN DE ACTIVOS CRÍTICOS

- Justificación: 40% de los riesgos fueron clasificados como críticos.
- Meta Estratégica: Reducir en al menos 60% la exposición de activos críticos (IoT, servidores, red).
- Indicadores:

En la tabla 20 se sintetizan los indicadores técnicos de seguridad, contrastando la situación inicial de la línea base con las metas proyectadas

Tabla 20. *Indicadores de Controles Técnicos, Infraestructura y Dispositivos IoT*

Indicador	Línea Base	Meta
Dispositivos IoT con contraseñas seguras	30%	100%
Implementación de segmentación de red	No	Sí
Uso de MFA en sistemas críticos	0%	100%
Actualización de *firmware* IoT	Parcial	100%

Nota. IoT = Internet de las Cosas (Internet of Things); MFA = Autenticación de Múltiples Factores (Multi-Factor Authentication).

OE3 – INCREMENTAR EL NIVEL DE MADUREZ INSTITUCIONAL

- Justificación: Nivel actual: Tier 1 – Bajo.
- Meta Estratégica: Alcanzar nivel 3 (Gestionado / Repeatable) en 24 meses.
- Indicadores:

En la tabla 21, la evaluación inicial posiciona a la institución en un nivel reactivo o inicial Tier 1 en NIST y Nivel 1 en CMMC Adaptado, alcanzando un cumplimiento del 37% respecto a los controles de la norma ISO 27001.

Para contrarrestar esta brecha, las metas proyectan elevar la madurez técnica y procedimental a un nivel repetible y gestionado (Tier 3 y Nivel 3), incrementando la adhesión a los controles ISO 27001 a un valor igual o superior al 75%

Tabla 21. *Indicadores de Madurez Estructural y Cumplimiento Normativo*

Indicador	Línea Base	Meta
Nivel NIST	Tier 1	Tier 3
Nivel CMMC Adaptado	Nivel 1	Nivel 3
Cumplimiento ISO 27001	37%	≥ 75%

Nota. NIST = National Institute of Standards and Technology; CMMC = Cybersecurity Maturity Model Certification; ISO 27001 = Estándar internacional para Sistemas de Gestión de Seguridad de la Información.

OE4 – Fortalecer la Cultura de Seguridad

- Justificación: Nivel humano = 2 (Básico).
- Meta Estratégica: Alcanzar nivel 4 (Cultura establecida) en 24 meses.
- Indicadores:

En la tabla 22 se sintetizan los indicadores del factor humano, comparando la situación inicial registrada en la línea base frente a las metas planteadas en el plan de gestión

Tabla 22. *Indicadores de Capacitación, Concientización y Metas Proyectadas del Factor Humano.*

Indicador	Línea Base	Meta
Promedio encuesta Likert	2,55	≥ 4,0
Capacitaciones anuales	0	≥ 4
Simulaciones de *phishing*	No	Semestrales
Personal capacitado	20%	100%

Nota. Phishing = Técnica de ingeniería social orientada a la obtención no autorizada de credenciales e información confidencial mediante la suplantación de identidad.

Integración Estratégica

En la tabla 23 se sintetiza la vinculación entre los objetivos estratégicos, los códigos de riesgo mitigados y el impacto esperado tras su implementación**.**

Tabla 23. *Alineación de Objetivos Estratégicos, Riesgos Mitigados e Impacto Esperado*

Objetivo Estratégico	Riesgos que Mitiga	Impacto Esperado
OE1	RISK-02, RISK-08	Reducción de riesgos estructurales
OE2	RISK-01, RISK-04, RISK-10	Protección de infraestructura crítica
OE3	Todos	Mejora estructural institucional
OE4	RISK-03, RISK-05	Reducción del riesgo humano

Nota. OE = Objetivo Estratégico; RISK = Identificador numérico de riesgo de la matriz institucional de ciberseguridad.

RESULTADO ESPERADO DEL PLAN

Al finalizar los 24 meses:

- Reducción ≥ 70% de riesgos críticos.
- Cumplimiento ≥ 75% estándares.
- Nivel de madurez: Medio–Alto.
- Cultura organizacional consolidada.

4.2 PLAN DE TRATAMIENTO DE RIESGOS

El tratamiento de riesgos constituye la fase operativa del Plan Estratégico de Ciberseguridad. Su finalidad es reducir la probabilidad y/o impacto de los riesgos identificados hasta niveles aceptables, priorizando aquellos clasificados como Críticos y Altos.

Las tácticas que se toman implican cuatro pilares muy conocidos:

Mitigar: buscando bajar la chance o la fuerza de lo malo.

Evitar: quitando de raíz lo que causa el peligro.

Transferir: pasando la carga a otros, ya sea con contratos o pólizas.

Aceptar: cuando el peligro no es grande y se tiene a controlado.

4.2.1 ESTRATEGIAS DE MITIGACIÓN

Las estrategias se estructuran en tres tipos de controles:

A. Controles Preventivos

Objetivo: Reducir la probabilidad de ocurrencia del incidente.

CONTROLES TÉCNICOS

- Implementar autenticación multifactorial en sistemas críticos eso es importante.
- Segmentación de red, usando VLANs, para separar el IoT y la red administrativa eso es un paso clave.
- Cambiar obligatoriamente las contraseñas por defecto en las cámaras IP es esencial.
- Una política de contraseñas robustas es algo que debemos seguir fielmente.
- Actualizar el firmware de forma periódica es un asunto que no podemos pasar por alto.
- Implementar un firewall de próxima generación.

CONTROLES ORGANIZACIONALES

- Política formal de ciberseguridad.
- Procedimiento de gestión de cambios.
- Política de control de accesos.
- Clasificación de información.

CONTROLES HUMANOS

- Programa anual de capacitación.
- Simulaciones de phishing.
- Manual de buenas prácticas.

B. CONTROLES DETECTIVOS

Objetivo: Identificar oportunamente incidentes en curso.

- Implementamos un sistema de monitoreo de logs una solución SIEM elemental.
- Alertas automáticas se activan frente a accesos que no deberían.
- Realizamos auditorías de seguridad cada seis meses.
- Revistamos los accesos y los privilegios con regularidad.
- Escaneamos vulnerabilidades cada tres meses.

C. CONTROLES CORRECTIVOS

Objetivo: Reducir el impacto posterior al incidente.

- Plan de Respuesta a Incidentes (PRI).
- Plan de Continuidad del Negocio (BCP).

- Procedimientos de recuperación de respaldos.
- Manual de comunicación ante incidentes.
- Protocolos disciplinarios ante incumplimiento.

4.2.2 MATRIZ DE TRATAMIENTO DE RIESGOS

A continuación, se presenta la matriz formal de tratamiento, alineada a los riesgos identificados en la sección 3.2.

La tabla 24 ofrece la matriz para tratar los riesgos, especificando el nivel del peligro, la estrategia elegida, el control planeado, quién debe implementarlo, cuándo estará listo, y la medida para vigilar su éxito.

Tabla 24. *Matriz de Tratamiento de Riesgos*

Código Riesgo	Nivel	Estrategia	Control Propuesto	Responsable	Plazo	Indicador
RISK-01	Crítico	Mitigar	Cambio de contraseñas + segmentación VLAN	Jefe TI	3 meses	100% cámaras configuradas
RISK-02	Crítico	Mitigar	Implementar backups automáticos + SIEM básico	Jefe TI	6 meses	Respaldos diarios verificados
RISK-03	Crítico	Mitigar	Programa de capacitación + simulación phishing	RRHH + TI	4 meses	≥ 80% aprobación pruebas
RISK-04	Crítico	Mitigar	Configuración firewall + mitigación DDoS	TI	6 meses	Disminución intentos bloqueados
RISK-05	Alto	Mitigar	Política de acceso y control de credenciales	Dirección	3 meses	Eliminación cuentas compartidas
RISK-06	Alto	Mitigar	Implementar MFA	TI	4 meses	100% sistemas

						críticos con MFA
RISK-07	Medio	Mitigar	Procedimiento formal de gestión de cambios	TI	6 meses	Registro formal de cambios
RISK-08	Alto	Mitigar	Implementar BCP documentado	Dirección + TI	8 meses	BCP aprobado y probado
RISK-09	Alto	Mitigar	Política formal de seguridad institucional	Dirección	4 meses	Documento aprobado
RISK-10	Crítico	Mitigar	Actualización firmware IoT trimestral	TI	Permanente	100% firmware actualizado

Nota. Elaborado por la autora, como parte de la estrategia de mitigación de riesgos para los activos críticos, alineado a los controles de la norma ISO/IEC 27001:2022.

PRIORIZACIÓN TEMPORAL

Corto Plazo (0–6 meses)

- Contraseñas robustas.
- La autenticación de múltiples factores la autentificación multifactorial MFA una protección la cual demanda a los usuarios ofrecer más de dos modos de comprobación para ingresar a cuentas o aplicativos.
- División de red.
- Norma formal.
- Formación inicial.

Mediano Plazo (6–12 meses)

- SIEM básico.
- BCP.

- Gestión de cambios.
- Auditorías internas.

Largo Plazo (12–24 meses)

- Mejora continua.
- Certificación progresiva.
- Simulaciones periódicas.

En la figura 4 se presenta el esquema de alineación entre los diez riesgos institucionales analizados y los controles propuestos, especificando la prioridad de atención, las áreas o cargos responsables de su ejecución y los plazos límite definidos para su implementación.

Figura 4. *Diagrama de alineación entre riesgos identificados y controles definidos*

Código	Nivel	Control propuesto	Responsable	Plazo
RISK-01	Crítico	Cambio de contraseñas por defecto + segmentación VLAN	Jefe TI	3 meses
RISK-02	Crítico	Backups automáticos + implementación de SIEM básico	Jefe TI	6 meses
RISK-03	Crítico	Programa de capacitación + simulaciones de phishing	RRHH + TI	4 meses
RISK-04	Crítico	Configuración de firewall NGFW + mitigación DDoS	TI	6 meses
RISK-10	Crítico	Actualización trimestral de firmware IoT	TI	Permanente
RISK-05	Alto	Política de acceso y control de credenciales	Dirección	3 meses
RISK-06	Alto	Implementación de autenticación multifactor (MFA)	TI	4 meses
RISK-08	Alto	Plan de Continuidad del Negocio (BCP) documentado	Dirección + TI	8 meses
RISK-09	Alto	Política formal de seguridad institucional	Dirección	4 meses
RISK-07	Medio	Procedimiento formal de gestión de cambios	TI	6 meses

Nota. Elaborado por la autora, con base en la Matriz de Tratamiento de Riesgos (Tabla 24) — estrategia de mitigación aplicada a los diez riesgos institucionales identificados.

IMPACTO ESPERADO DEL PLAN DE TRATAMIENTO

En la tabla 25 se presentan los valores correspondientes a la línea base inicial frente a la proyección proyectada a un período de 24 meses**.**

Tabla 25. *Indicadores de Gestión, Línea Base y Proyección a 24 Meses*

Indicador	Línea Base	Proyección 24 meses
Riesgos Críticos	40%	≤ 10%
Cumplimiento ISO	37%	≥ 75%
Nivel Madurez	Nivel 1	Nivel 3
Cultura Seguridad	Nivel 2	Nivel 4

Nota. Comparativa entre el diagnóstico de la situación actual (Línea Base) y las metas institucionales proyectadas en un horizonte temporal de 24 meses.

4.3 CRONOGRAMA DE IMPLEMENTACIÓN DEL PLAN ESTRATÉGICO

La implementación del Plan Estratégico de Ciberseguridad se plantea con un horizonte de 24 meses, dividido en tres fases:

Fase I — Empiezo Fuerte (cero a seis meses).

Fase II — Refuerzo y Documentación (seis a doce meses).

Fase III — Apogeo y Mejora Continua (doce a veinticuatro meses).

En la tabla 26 se presenta el cronograma general de implementación, indicando las actividades estratégicas, responsables y periodo de ejecución.

Tabla 26. *Cronograma General de Implementación*

Actividad Estratégica	Responsable	0–6m	6–12m	12–18m	18–24m
Aprobación política de ciberseguridad	Dirección	✔			
Cambio de contraseñas IoT	TI	✔			
Implementación MFA	TI	✔			
Segmentación de red (VLAN)	TI	✔	✔		
Programa de capacitación inicial	RRHH + TI	✔			
Simulaciones de phishing	TI	✔	✔	✔	✔
Implementación SIEM básico	TI		✔		
Diseño e implementación BCP	Dirección + TI		✔	✔	
Auditoría interna de seguridad	TI		✔	✔	✔
Revisión y actualización matriz de riesgos	TI	✔	✔	✔	✔
Evaluación de madurez (NIST/CMMC)	Dirección + TI			✔	✔
Mejora continua y optimización	Todos			✔	✔

Nota. Elaborado por la autora, detallando las fases de ejecución del Plan Estratégico de Ciberseguridad proyectado a un periodo de 24 meses para su cumplimiento integral institucional.

FASES ESTRATÉGICAS

Fase I – Atenuación de Amenazas Urgentes.

- Se concentra en medidas técnicas urgentes (IoT, MFA, segregación, adiestramiento).

Fase II – Estructuración y Supervisión.

- Registro, seguimiento constante, PCG y consolidación orgánica.

Fase III – Firmeza de Crecimiento.

- Revisiones recurrentes, perfeccionamiento constante y derivación hacia Etapa 3 de crecimiento.

4.4 PRESUPUESTO ESTIMADO DEL PLAN ESTRATÉGICO

El presupuesto considera recursos tecnológicos, capacitación y consultoría externa cuando sea necesaria.

En la tabla 27 se presenta el presupuesto estimado, detallando el concepto, costo unitario, cantidad y costo total.

Tabla 27. *Presupuesto Estimado*

Concepto	Costo Unitario (USD)	Cantidad (años)	Costo Total (USD)
Implementación MFA	1,200	1	1,200
Firewall de próxima generación	4,500	1	4,500
Software SIEM básico	3,000	1	3,000
Capacitación especializada anual	1,500	2	3,000
Simulaciones de phishing	800	2	1,600
Consultoría para BCP	2,500	1	2,500
Auditoría externa de seguridad	3,000	1	3,000
Actualización de firmware y soporte técnico	1,200	2	2,400

Nota. Elaborado por la autora, costos referenciales del mercado tecnológico actual, representan la inversión estimada para la ejecución de las fases del Plan Estratégico de Ciberseguridad.

Total Estimado de Inversión (24 meses):

USD 21,200

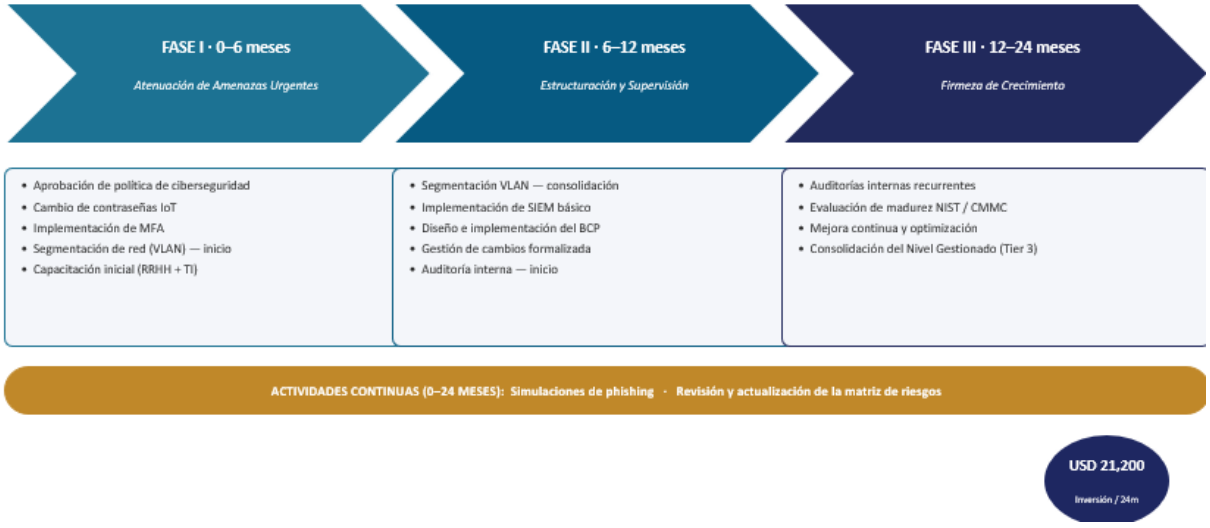
Análisis Costo–Beneficio

Comparado con el impacto potencial de: Pérdida de grabaciones críticas; Paralización del sistema de monitoreo; Sanciones legales; Daño reputacional.

La inversión resulta financieramente viable y estratégicamente necesaria.

Como se detalla en la figura 5, la hoja de ruta comprende la atención de riesgos críticos a corto plazo, la consolidación operativa a mediano plazo y la maduración del esquema a largo plazo, con una inversión estimada de USD 21,200 proyectada a 24 meses.

Figura 5. *Hoja de ruta (Roadmap) para la implementación estratégica por fases.*



Nota. Elaborado por la autora, con base en el Cronograma General de Implementación (Tabla 26) y el Presupuesto Estimado del Plan Estratégico (Tabla 27).

4.5 INDICADORES DE SEGUIMIENTO Y EVALUACIÓN

El seguimiento del Plan Estratégico se realizará mediante indicadores clave de desempeño (KPI), alineados con los objetivos estratégicos (OE1–OE4).

4.5.1 INDICADORES TÉCNICOS

En la tabla 28 se detallan los indicadores técnicos, las ecuaciones requeridas para su cálculo y los umbrales esperados (metas).

Tabla 28. *Fórmulas y Metas de los Indicadores Técnicos de Ciberseguridad*

Indicador	Fórmula	Meta
% dispositivos IoT seguros	(IoT seguros / Total IoT) × 100	100%
% sistemas con MFA	(Sistemas con MFA / Total críticos) × 100	100%
% cumplimiento ISO 27001	(Controles implementados / Total controles) × 100	≥75%
Tiempo promedio detección incidente	Horas promedio	< 4h

Nota. Elaborado por la autora, IoT = Internet de las Cosas (Internet of Things); MFA = Autenticación de Múltiples Factores (Multi-Factor Authentication).

4.5.2 INDICADORES DE GESTIÓN

En la tabla 29 el esquema de gestión contempla un nivel de ejecución del 100% en la actualización semestral de la matriz de riesgos y en la documentación del Plan de Continuidad del Negocio (BCP).

Tabla 29. *Indicadores de Gestión Operativa y Metas de Continuidad*

Indicador	Meta
Actualización semestral matriz de riesgos	100% cumplimiento
Auditorías realizadas por año	≥ 2 100%
Implementación BCP	100% documentado

Nota. Elaborado por la autora, BCP = Plan de Continuidad del Negocio (Business Continuity Plan) Indicadores de Gestión Operativa y Metas de Continuidad.

4.5.3 INDICADORES HUMANOS

En la tabla 30 se presentan los indicadores correspondientes al factor humano, comparando el diagnóstico inicial (Línea Base) con las metas proyectadas.

Tabla 30. *Indicadores del Factor Humano, Línea Base y Metas de Concientización*

Indicador	Línea Base	Meta
Promedio encuesta Likert	2,55	≥ 4,0
Personal capacitado	20%	100%
Tasa de éxito en simulación de *phishing*	60% vulnerables	≤ 10%

Nota. Elaborado por la autora, *Phishing* = Técnica de ingeniería social orientada a la obtención no autorizada de credenciales mediante suplantación de identidad.

4.5.4 INDICADOR GLOBAL DE MADUREZ

Se evaluará anualmente bajo:

- NIST Implementation Tiers.
- Modelo CMMC adaptado.

Meta estratégica a 24 meses:

En la tabla 31 se detalla la meta estratégica a 24 meses proyectada a partir del diagnóstico de línea base.

Tabla 31. *Meta Estratégica a 24 Meses según Modelos de Madurez*

Modelo	Línea Base	Meta (24 meses)
NIST CSF	Tier 1	Tier 3
CMMC	Nivel 1	Nivel 3

Nota. Elaborado por la autora, *NIST/CSF* = Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología, *CMMC* = Certificación del Modelo de Madurez de Ciberseguridad.

CONCLUSIONES

En cumplimiento del objetivo general, el aporte técnico consistió en consolidar una solución estratégica e integral de ciberseguridad que articula el diagnóstico, la evaluación cuantitativa y la planificación del tratamiento de riesgos en una única hoja de ruta ejecutable para el centro de monitoreo. La mejora esperada en la gestión de riesgos radica en dotar a la institución de una capacidad preventiva y adaptativa frente a incidentes informáticos, sustituyendo esquemas reactivos e inconexos por una estrategia unificada de protección de infraestructura crítica. El impacto institucional radica en garantizar la resiliencia operativa y la sostenibilidad del servicio público de videovigilancia, transformando la seguridad de la información en un pilar permanente de gobernanza institucional.

La fundamentación teórica y metodológica, el aporte técnico consistió en estructurar un modelo híbrido basado en las normas ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0. La mejora esperada en la gestión de riesgos con esta base teórica es superar la rigidez documental de un estándar único mediante un enfoque cuantitativo, adaptable y directo. Su impacto institucional dotará a la entidad municipal de un marco formal, sostenible y alineado con la Ley Orgánica de Protección de Datos Personales (LOPDP) para regir la seguridad de la información.

Centrado en el diagnóstico situacional, el aporte técnico permitió cuantificar la exposición real del sistema mediante el cálculo de probabilidad e impacto ($NR = P \times I$), identificando vulnerabilidades críticas en la red de transporte y la cultura de seguridad. La mejora esperada en la gestión de riesgos radicó en aislar y jerarquizar los eventos de mayor severidad para eliminar la estimación empírica. El impacto institucional de este análisis proporcionó la evidencia objetiva

necesaria para sustentar técnicamente las decisiones de inversión ante las autoridades de la institución.

Diseño del plan estratégico, el aporte técnico contempló la selección priorizada de controles como un Firewall, segmentación por VLANs, cifrado de transmisiones (TLS/AES-256) y concientización continua. La mejora esperada en la gestión de riesgos proyecta una reducción de la exposición global superior al 60% e incrementa la madurez institucional de Nivel inicial (Tier 1) a gestionado (Tier 3) bajo el modelo CMMC. El impacto institucional garantizará la continuidad operativa de la videovigilancia ciudadana y la adecuada custodia de los datos públicos.

RECOMENDACIONES

Adoptar formalmente la arquitectura metodológica híbrida propuesta (ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0) como la norma interna oficial para la gestión de ciberriesgos en el centro de monitoreo. Para fortalecer este marco, la Dirección de Tecnologías de la Información debe actualizar periódicamente las matrices de riesgo frente a los cambios en el entorno normativo (LOPDP) y tecnológico. Asimismo, iniciativas de mayor alcance, como la certificación formal bajo el estándar ISO/IEC 27001, deben plantearse como una línea futura de evolución e investigación institucional a mediano y largo plazo, dado que exceden el alcance del presente estudio.

Se recomienda operativizar los resultados del diagnóstico situacional priorizando la mitigación de vulnerabilidades en la capa de borde (*Edge layer*) y los dispositivos del ecosistema IoT / videovigilancia (cámaras IP, switches de campo y grabadores). La institución debe incorporar este diagnóstico en sus Planes Operativos Anuales (POA) para garantizar que las decisiones de seguridad física e informática mantengan la fundamentación cuantitativa desarrollada ($NR = P \times I$). Como línea futura de investigación, se sugiere explorar la integración de herramientas de inteligencia artificial aplicadas al análisis predictivo de ciberriesgos y detección anómala de tráfico en redes IoT.

Se recomienda ejecutar el Plan Estratégico de Ciberseguridad asignando formalmente el presupuesto optimizado de USD 21.200 a 24 meses para la implementación del Firewall NGFW, la segmentación por VLANs y el cifrado de transmisiones de video (TLS/AES-256) en los endpoints IoT. Para asegurar la reducción esperada del riesgo (superior al 60%) y el salto de madurez a Nivel Gestionado (Tier 3 de CMMC), se deben establecer revisiones trimestrales de los indicadores de efectividad, y el despliegue de modelos avanzados de capacitación interactiva y

simulación continua en ciberseguridad para el factor humano se plantea como una línea de desarrollo futuro para la sostenibilidad del plan a largo plazo.

Se recomienda institucionalizar el Plan Estratégico de Ciberseguridad bajo un ciclo de mejora continua (PHVA) liderado por la Jefatura de Tecnologías de la Información del GAD Municipal de Salcedo. Esta acción busca velar por la efectividad de la arquitectura híbrida (ISO/IEC 27005:2022, NIST CSF 2.0 y CMMC 2.0) mediante auditorías internas anuales, monitoreo trimestral de indicadores de riesgo y la revisión periódica de salvaguardas técnicas y presupuestarias. Dicho mecanismo de gobernanza garantizará un tratamiento de riesgos adaptado al entorno cibernético, salvaguardando la continuidad del servicio de videovigilancia y la protección de datos de la ciudadanía.

REFERENCIAS

AlHaq, A., Al-Sahaf, M., & Al-Saqqa, S. (2022). A comprehensive risk assessment framework for smart cities. *IEEE Access, 10*, 22675–22692.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento No. 459.

Benavides, J., & Guerrero, M. (2022). Análisis jurídico de la ciberseguridad en los gobiernos autónomos descentralizados del Ecuador. *Revista de Derecho Digital*, *15*(2), 45–67.

Chen, P., Desmet, L., & Huygens, C. (2022). Security analysis of governmental security operation centers. *Computers & Security, 114*, 102578.

CISA. (2023). *Cybersecurity best practices for critical infrastructure*. Cybersecurity and Infrastructure Security Agency.

ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity.

Gómez, J., & López, M. (2021). Ciberseguridad en los gobiernos locales de América Latina: Desafíos y oportunidades. *Revista de Estudios Latinoamericanos*, *45*(2), 123–145.

González, A., & Ríos, M. (2024). Implementación de sistemas de gestión de seguridad de la información en gobiernos municipales: Caso de estudio del GAD Municipal de Cuenca. *Revista Tecnológica Ecuador, 12*(1), 89–104.

IBM. (2024). *Cost of a data breach report 2024*. IBM Security.

Instituto Ecuatoriano de Normalización. (2020). *NTE INEN-ISO/IEC 27001: Sistemas de gestión de seguridad de la información — Requisitos*. INEN.

ISO. (2022). *ISO/IEC 27001:2022 Information security management systems — Requirements*. International Organization for Standardization.

ISO. (2022). *ISO/IEC 27005:2022 Information security risk management*. International Organization for Standardization.

Johnson, M., & Brown, K. (2023). NIST cybersecurity framework implementation in local governments. *Government Information Quarterly*, *40*(2), 101115.

Kessler, G. C., Craigen, D., & Walsh, T. (2021). The state of cybersecurity in local governments. *Journal of Cybersecurity Research, 8*(1), 1–15.

Martínez-Ortega, J., García, L., & Hernández, P. (2022). Adaptación de ISO/IEC 27001 para administraciones locales. *IEEE Latin America Transactions, 20*(5), 789–798.

NIST. (2022). *Framework for improving critical infrastructure cybersecurity (Version 1.1 update & 2.0 draft)*. National Institute of Standards and Technology.

OECD. (2022). *Digital security risk management in the public sector*. Organisation for Economic Co-operation and Development.

Ordóñez, L., & Pazmiño, M. (2023). Análisis de la ciberseguridad en las instituciones públicas del Ecuador. *Revista Científica Tecnológica*, *18*(2), 34–50.

Pérez-López, A., García, M., & Rodríguez, J. (2023). Adopción gradual del NIST Cybersecurity Framework en municipios de recursos limitados. *Computers & Security, 124*, 102945.

Presidencia de la República del Ecuador. (2022). *Reglamento General a la Ley Orgánica de Protección de Datos Personales*. Registro Oficial No. 567.

Santana, R., Oliveira, T., & Figueira, Á. (2023). Comparative analysis of cybersecurity frameworks for the public sector. *Government Information Quarterly, 40*(3), 101823.

Wang, Y., & Li, X. (2023). Security framework for municipal video surveillance systems. *IEEE Transactions on Information Forensics and Security, 18*, 1456–1470.

World Bank. (2021). *Cybersecurity for development: A framework for strengthening resilience*. World Bank Group.

Zhang, L., Wang, Y., & Chen, X. (2023). Risk assessment framework for municipal critical infrastructure protection. *IEEE Transactions on Engineering Management, 70*(2), 567–580.

Abomhara, M., & Køien, G. M. (2021). Cyber security and the internet of things: Vulnerabilities, threats, and countermeasures. *Future Internet, 13*(2), 25–40.

Alcaraz, C., & Zeadally, S. (2021). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 34*, 100434.

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2021). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *Computers & Security, 101*, 102128.

Behl, A., Jayawardena, N., Pereira, V., & Sahu, S. (2022). Cybersecurity risk management in smart cities. *Technological Forecasting and Social Change, 176*, 121450.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2021). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.

European Commission. (2022). *Cybersecurity strategy of the European Union*.

Gartner. (2023). *Top cybersecurity trends for public sector organizations*.

Haque, M. M., & Islam, M. (2022). Cybersecurity challenges in smart city environments. *Journal of Information Security, 13*(3), 145–160.

Khan, M. A., & Salah, K. (2021). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

Lee, I., & Lee, K. (2021). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 64*(4), 431–440.

Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2021). A systematic review of security requirements engineering. *Computer Standards & Interfaces, 54*, 129–149.

Microsoft. (2023). *Digital defense report 2023*.

Peltier, T. R. (2021). *Information security policies, procedures, and standards*. Auerbach Publications.

PwC. (2023). *Global digital trust insights 2023*.

Radanliev, P., De Roure, D., Walton, R., & Van Kleek, M. (2022). Cyber risk at the edge: Current and future trends on IoT and smart city technologies. *Journal of Cyber Policy, 7*(1), 1–22.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2022). *Zero trust architecture (NIST SP 800-207)*. National Institute of Standards and Technology.

Shackelford, S. J. (2022). *Cybersecurity governance: A global perspective*. Cambridge University Press.

Trend Micro. (2023). *Annual cybersecurity report 2023*.

Verizon. (2024). *Data breach investigations report 2024*.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.

ANEXOS

Se presenta la información consultada. Pueden ser, carta de compromiso, carta aval, instrumentos, evidencia fotográfica, entre otros que el autor considere necesario

Anexo 1: CARTA DE ACEPTACIÓN DEL USO DE LA INFORMACIÓN DE LA MÁXIMA AUTORIDAD

Of. Nº AL-720-2025-GADMCS-A2.
San Miguel de Salcedo, 11 de noviembre del 2025.

Ing. Lorena Cacpata
TECNICO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN.
Presente.-

De mi consideración:

En atención a su solicitud mediante oficio N. TICS-002-2025, en la cual pone en conocimiento que se encuentra cursando la Maestría en Ciberseguridad en la Universidad Estatal Península de Santa Elena (UPSE), y considerando el desarrollo de su trabajo de titulación denominado: **"Diseño de un plan estratégico de ciberseguridad para el centro de monitoreo del Gad Municipal del cantón Salcedo, basado en gestión de riesgos"**, me permito manifestar lo siguiente:

Esta Autoridad **AUTORIZA** el uso de información institucional estrictamente necesaria para el desarrollo de su investigación académica, siempre y cuando dicho acceso, tratamiento y análisis de la información se realice bajo criterios de confidencialidad, responsabilidad y uso adecuado.

Se deja expresa constancia de que la información deberá ser utilizada exclusivamente con fines académicos, evitando su divulgación, reproducción o uso indebido, en cumplimiento de la normativa vigente, en especial lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), así como las políticas internas de seguridad de la información de la institución.

Adicionalmente, se dispone que los datos sensibles o críticos sean debidamente anonimizados o tratados de forma agregada, garantizando la protección de la información institucional y evitando cualquier riesgo que pudiera afectar la integridad, confidencialidad o disponibilidad de los activos de información.

Finalmente, se exhorta a que los resultados obtenidos en el marco de la investigación puedan ser compartidos con la institución, a fin de que estos contribuyan al fortalecimiento de la gestión de ciberseguridad y mejora continua de los sistemas institucionales.

Sin otro particular, reitero mi apoyo a las iniciativas académicas que aporten al desarrollo institucional.

Atentamente,

Ing. Juan Paúl Pacheco Velásquez.
ALCALDE DEL GAD MUNICIPAL
DEL CANTÓN SALCEDO

JPPV/jdv

GAD MUNICIPAL DEL CANTÓN SALCEDO

Anexo 2: ENCUESTA DE DIAGNÓSTICO Y CONCIENCIACIÓN EN CIBERSEGURIDAD

Encuesta de Diagnóstico y Concienciación en Ciberseguridad

Objetivo: Evaluar el nivel de cultura de seguridad, conocimientos y prácticas en ciberseguridad del personal del Centro de Monitoreo del GAD Municipal del cantón Salcedo.

Instrucciones: Por favor, lea atentamente cada enunciado y marque con una **X** la opción que mejor represente su situación actual, considerando la siguiente escala:

- **1** = Totalmente en desacuerdo
- **2** = En desacuerdo
- **3** = Ni de acuerdo ni en desacuerdo
- **4** = De acuerdo
- **5** = Totalmente de acuerdo

I. Datos Informativos (Opcional / Confidencial)

- **Área de trabajo:** [ ] Operativa (Monitoreo) / [ ] Técnica (TI) / [ ] Administrativa
- **Tiempo en el puesto:** [ ] Menos de 1 año / [ ] 1 a 3 años / [ ] Más de 3 años

II. Matriz de Evaluación (Escala Likert)

#	Enunciado / Reactivo	1	2	3	4	5
1	Conozco las políticas de ciberseguridad institucionales vigentes en el Centro de Monitoreo.					
2	Utilizo contraseñas seguras, robustas y únicas para acceder a las plataformas del centro (evitando compartirlas).					
3	Soy capaz de reconocer de manera oportuna correos electrónicos, llamadas o mensajes sospechosos de *phishing* e ingeniería social.					
4	He recibido capacitación formal y periódica en ciberseguridad por parte de la institución.					
5	Sé con claridad cómo y a quién reportar un incidente o una actividad sospechosa en los sistemas de seguridad.					

#	Enunciado / Reactivo	1	2	3	4	5
6	Comprendo los riesgos que implica el uso de memorias USB u otros dispositivos externos no autorizados en las estaciones de trabajo.					
7	Aplico de forma estricta las buenas prácticas de seguridad informática durante el uso diario de los sistemas de monitoreo y videovigilancia.					
8	Considero que la ciberseguridad es parte de mi responsabilidad individual y no solo una tarea del área de TI.					

III. Sección Complementaria (Preguntas de Control Cualitativo)

Para profundizar en el diagnóstico, se sugiere añadir estas dos preguntas abiertas/de opción al final:

9. Si identificara un acceso no autorizado ¿cuál sería su acción inmediata?

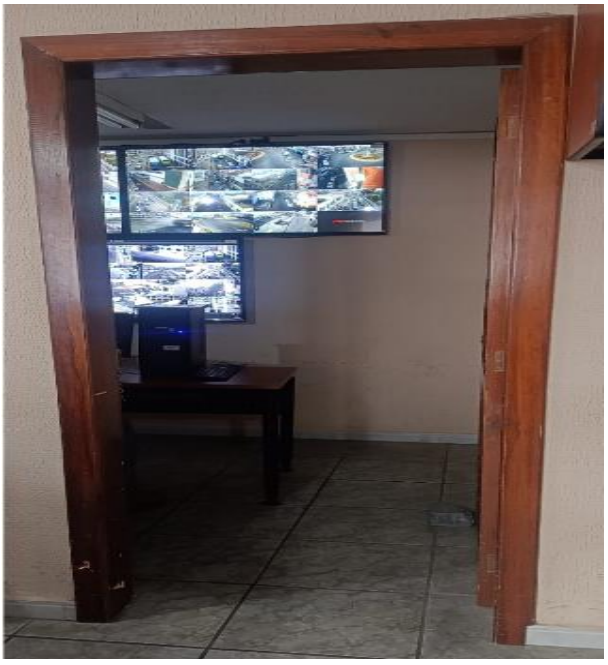
- [ ] Apagar el equipo y no decir nada.
- [ ] Informar verbalmente a un compañero de turno.
- [ ] Reportar de inmediato al personal técnico de TI/Supervisor conforme al protocolo.
- [ ] Intentar solucionar el problema por mi cuenta.

10. ¿En qué temas de ciberseguridad considera que requiere capacitación prioritaria de manera urgente?

- [ ] Identificación de correos falsos (*Phishing*) e Ingeniería Social.
- [ ] Manejo seguro de sistemas de videovigilancia e IoT.
- [ ] Protocolos de respuesta ante incidentes y hackeos.
- [ ] Creación y gestión de credenciales / contraseñas seguras.

Anexo 3: EVIDENCIAS FOTOGRAFICAS

CUARTO DE MONITOREO



EQUIPO DE MONITOREO

PANTALLAS DE MONITOREO

NVRS

CONEXIÓN DE RED (ROUTER)

RACK