Lineamientos para el fortalecimiento de la ciberseguridad en cuerpos de bomberos de Colombia, aplicando la norma ISO 27002:2022

Numa Fernando Wallens Lozada

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2026

Nota de aceptación

_____

Firma Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Dedicatoria

Quiero dedicar esta monografía, en primer lugar, a Dios, por abrirme las puertas para llevarla a cabo. A mi esposa Olga y a mis hijos Juan Fernando, Juana Lucía y Juan David, quienes son mi motor de vida para seguir adelante. A la institución de la que soy parte, y a sus directivas, por brindarme la oportunidad de adquirir nuevos conocimientos para mi crecimiento personal y profesional. A los tutores que me han apoyado y dirigido en este proceso, en especial al Ingeniero Ever Arroyo, ya que este trabajo es un reto personal que deseo implementar en la Organización de la cual formo parte.

A mi padre, madre, tía y hermana que me han motivado y animado cuando he sentido flaquear. A mis compañeros, con quienes he compartido este proceso y de quienes he adquirido grandes conocimientos.

Finalmente, dedico este trabajo a mí mismo, por el esfuerzo invertido para superarme. Las grandes enseñanzas y los conocimientos invaluables adquiridos hoy dan fruto en este trabajo, que permitirá su posterior implementación en los Cuerpos de Bomberos Voluntarios y/u Oficiales.

A todos muchas gracias.

Agradecimientos

A Dios, quien ha guiado cada uno de mis pasos y me ha colocado en el lugar que Él ha decidido.

A mi familia, por su inmenso amor, comprensión y apoyo, y por ser el pilar de mi existencia.

A la Capitán Ayda Elena por apoyarme en este proceso y en muchos otros. A Héctor y Adalberto por su ayuda desinteresada y por ver en mí ese potencial. A mis compañeras y compañeros de trabajo, por entender mi silencio y concentración durante la realización de las actividades.

Este logro es para todos ustedes, y lo verán materializarse cuando se implemente este tema en cuestión.

Resumen

La presente monografía, tiene como objetivo estructurar lineamientos de ciberseguridad para los Cuerpos de Bomberos de Colombia, alineados con el estándar internacional ISO/IEC 27002:2022. Mediante un estudio de tipo documental-descriptivo con enfoque hermenéutico, se caracterizaron los controles actuales y se contrastaron las brechas de cumplimiento en entidades seleccionadas. Los resultados evidencian una postura reactiva frente a las amenazas modernas y un desfase crítico en el dominio de personas. Como aporte interpretativo, se propone una arquitectura de políticas que fortalece la resiliencia operativa y la protección de activos críticos de información en estos organismos de socorro.

Palabras clave. norma ISO 27002, SGSI, sistema gestión información, políticas de seguridad informática.

Abstract

This monograph aims to structure cybersecurity guidelines for the Fire Departments of Colombia, aligned with the ISO/IEC 27002:2022 international standard. Through a descriptive-documentary study with a hermeneutic approach, current controls were characterized and compliance gaps in selected entities were contrasted. The results evidence a reactive posture against modern threats and a critical gap in the people domain. As an interpretative contribution, a policy architecture is proposed to strengthen operational resilience and the protection of critical information assets in these emergency response organizations.

Keywords. Standard ISO 27002, ISMS, system management information, policies cybersecurity computing.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En un panorama cada vez más digitalizado, los Cuerpos de Bomberos de Colombia, como entidades públicas esenciales, dependen de la tecnología para la gestión de emergencias, la coordinación operativa y la administración de recursos. La información que manejan es crítica e incluye datos de emergencias, mapas de riesgo, protocolos de actuación, y datos personales de la ciudadanía y del personal. Proteger estos activos de información es crucial para garantizar la continuidad operativa, la confidencialidad, integridad y disponibilidad de los datos.

Esta monografía realiza un análisis comparativo de las políticas de seguridad de la información y los planes de tratamiento de riesgos de tres entidades clave en Colombia. El Cuerpo Oficial de Bomberos de Bogotá, el Cuerpo de Bomberos Oficial de Montería y el Cuerpo de Bomberos de Dosquebradas. Se identifican las fortalezas y las áreas de mejora en su gestión de la seguridad de la información, tomando como marco de referencia la norma ISO/IEC 27002:2022, la cual ofrece directrices actualizadas para los controles de seguridad. El objetivo es proponer un modelo de mejora que permita a estas y otras instituciones similares fortalecer su resiliencia digital y cumplir con la normatividad vigente.

Por lo anterior, la investigación se enmarca en un contexto de creciente dependencia tecnológica y amenazas persistentes, donde los Cuerpos de Bomberos, como entidades de respuesta crítica, gestionan activos de información sensibles. En este sentido, la presente monografía se alinea con la Línea de Investigación de la Especialización en Seguridad Informática de la UNAD. "Gestión de la Seguridad de la Información y Ciberseguridad". El objetivo principal de esta línea es fomentar la aplicación de marcos de trabajo y estándares internacionales para proteger la integridad, confidencialidad y disponibilidad de los datos.

Tabla 1.

Resumen General Monografía

Item	Contenido
Título	Lineamientos Para el Fortalecimiento de la Ciberseguridad en Cuerpos de Bomberos de Colombia, Aplicando la Norma ISO 27002:2022
Autor	Numa Fernando Wallens Lozada.
Tipo de Documento	Monografía de Especialización.
Línea de Investigación	Gestión de la Seguridad de la Información y Ciberseguridad.
Resumen	La presente monografía aborda la necesidad crítica de fortalecer las políticas de seguridad de la información en los Cuerpos de Bomberos de Colombia. A través de un análisis exhaustivo de los documentos internos de entidades como las de Bogotá, Montería y Dosquebradas, se identificaron hallazgos clave que demuestran una aplicación heterogénea y, en ocasiones, incompleta de los estándares internacionales. Se observó una marcada falta de formalización en los procesos de gestión de riesgos y una dependencia excesiva en medidas reactivas, dejando vulnerabilidades significativas en la protección de activos de información. La investigación, basada en la norma ISO/IEC 27002:2022, propone un conjunto de mejoras prácticas y un plan de implementación estructurado para mitigar estos riesgos. Este estudio concluye que, si bien existen esfuerzos aislados, la adopción de un enfoque unificado y

Item	Contenido
	sistemático es fundamental para asegurar la continuidad operativa y la confidencialidad de la información crítica.
Palabras Clave	Ciberseguridad, ISO 27002:2022, Gestión del Riesgo, Bomberos, Control de Acceso.

Nota. Elaboración propia.

Definición y Formulación del Problema

Definición del Problema

La gestión de la seguridad de la información en los Cuerpos de Bomberos de Colombia se sitúa actualmente en un escenario de vulnerabilidad sistémica, definido por la convergencia de tres factores delimitantes.

Delimitación Situacional

Estas entidades operan como infraestructura crítica del Estado. La interrupción de sistemas de despacho asistido por computadora (CAD) o la pérdida de integridad en planos de infraestructura durante una emergencia no es solo un fallo técnico, sino un riesgo directo para la vida de los ciudadanos.

Delimitación Conceptual

Existe un desfase entre los manuales operativos institucionales y la rápida evolución de las ciberamenazas (como el ransomware de doble extorsión), exacerbado por el uso de estándares obsoletos que no han sido armonizados con la nueva arquitectura de la ISO/IEC 27002:2022.

Delimitación Categorial

El problema se define por la tensión entre dos categorías centrales de análisis: el Nivel de Madurez de los Controles de Seguridad (Categoría Independiente: dominios organizacionales, humanos, físicos y tecnológicos) y la Resiliencia Operativa Institucional (Categoría Dependiente: capacidad de protección de activos críticos).

Dependencia de la Tecnología y Riesgos Asociados

Los cuerpos de bomberos, como entidades de respuesta a emergencias, dependen cada vez más de sistemas de información para la coordinación operativa, el despacho de equipos, la gestión de recursos y la comunicación en tiempo real. Esta dependencia tecnológica los expone a

riesgos de ciberseguridad, como interrupciones del servicio, robo de información o ataques de ransomware, que podrían comprometer su capacidad de respuesta.

La ciberseguridad en Colombia ha ganado un protagonismo significativo en la inversión de las empresas. Se estima que las grandes compañías destinan más de $15.000 millones, mientras que las pequeñas y medianas empresas invierten alrededor de $4.000 millones. Aunque algunas empresas aún perciben la ciberseguridad como un gasto innecesario, estas cifras evidencian un aumento en la demanda de servicios de seguridad, impulsado por el creciente número de ciberataques en el país. Colombia se ha posicionado como el cuarto país de América Latina con el mayor número de ciberataques, con más de 36 millones de intentos registrados solo en el año 2024. Esta situación ha llevado a que muchas organizaciones adopten un enfoque reactivo, implementando medidas de seguridad solo después de que se ha producido un incidente, como ataques de phishing o la propagación de ransomware.

Para el desarrollo de esta monografía, se establecen como variables independientes la aplicación y alineación de políticas y procedimientos con los controles de la norma ISO/IEC 27002:2022, y como variable dependiente la reducción de vulnerabilidades y el fortalecimiento de la resiliencia institucional de los Cuerpos de Bomberos en Colombia.

Manejo de Información Sensible y Crítica

La información que procesan estas instituciones es de alta sensibilidad, incluyendo datos personales de ciudadanos afectados por emergencias, detalles de personal operativo y planos de infraestructura crítica. La pérdida de confidencialidad, integridad o disponibilidad de esta información puede tener consecuencias graves, desde el incumplimiento de la Ley 1581 de 2012 de protección de datos hasta la interrupción de operaciones vitales.

Inconsistencia y Obsolescencia en la Gestión de Seguridad

El análisis comparativo de los documentos proporcionados evidencia una falta de estandarización en la gestión de la seguridad de la información. Mientras que un manual de políticas puede ser robusto, un plan de tratamiento de riesgos de otra entidad podría estar desactualizado o tener un enfoque limitado. Esta inconsistencia se agrava cuando se utilizan versiones obsoletas de normas internacionales como la ISO/IEC 27001.2013, lo que indica la necesidad de una actualización a los estándares más recientes, como el ISO/IEC 27002:2022, para abordar las amenazas modernas.

Vulnerabilidad Humana y Falta de Cultura de Seguridad

Los documentos analizados mencionan riesgos como la divulgación accidental de información o el uso de correos maliciosos, lo que señala al factor humano como una vulnerabilidad significativa. Esto subraya que, a pesar de los controles técnicos, la falta de una cultura de seguridad de la información y la concientización del personal son antecedentes clave que contribuyen a los incidentes de seguridad.

Aunque se invierte en tecnología, los expertos advierten que el eslabón más débil es y siempre será el ser humano. De allí la importancia de que las empresas no solo inviertan en soluciones de ciberseguridad, sino también en capacitaciones para que sus colaboradores puedan identificar ataques de *phishing* y el funcionamiento de diversos *malware*. La falta de concientización y capacitación del personal es la principal causa de incidentes, lo que subraya la necesidad de un fuerte componente de formación.

Formulación del Problema

¿De qué manera el diseño de lineamientos de ciberseguridad, fundamentados en un análisis documental de la norma ISO/IEC 27002:2022, permite reducir la brecha de cumplimiento y fortalecer la resiliencia de los activos de información críticos en los Cuerpos de Bomberos de Colombia?

Justificación

La pertinencia de esta investigación se sustenta bajo los criterios de Hernández-Sampieri (2018) para evaluar el valor potencial de un estudio.

Conveniencia

La investigación es conveniente al proporcionar una hoja de ruta técnica estandarizada para entidades de socorro que carecen de marcos de ciberseguridad robustos.

Relevancia Social

Al proteger la integridad de los datos de despacho, se garantiza que la respuesta a emergencias no sea saboteada por ataques externos, salvaguardando el derecho fundamental a la vida y la seguridad pública.

Valor Teórico

La monografía llena un vacío en la literatura técnica nacional al adaptar controles globales de seguridad específicamente al contexto de los bomberos en Colombia, permitiendo nuevas interpretaciones sobre la ciberseguridad en servicios de emergencia.

Implicaciones Prácticas

Ofrece una herramienta de autodiagnóstico y una arquitectura de políticas aplicable de forma inmediata, facilitando que los comandantes tomen decisiones basadas en riesgos reales.

Objetivos

Objetivo General

Estructurar lineamientos de ciberseguridad mediante el análisis documental de la norma ISO/IEC 27002:2022 para el fortalecimiento de la gestión de activos de información en los Cuerpos de Bomberos de Colombia.

Objetivos Específicos

Identificar el estado actual de los controles de seguridad en entidades bomberiles seleccionadas mediante la revisión sistemática de sus manuales y planes de riesgo vigentes.

Contrastar analíticamente las brechas de cumplimiento documental existentes frente a los nuevos atributos y dominios definidos en la norma ISO/IEC 27002:2022.

Proponer una arquitectura de políticas que articule los hallazgos del diagnóstico con las directrices de implementación y monitoreo del estándar internacional, sin exceder el alcance del objetivo general.

Antecedentes

Antecedentes de Investigación

Internacional (Polonia, 2024)

Safety of Systems Integrating Fire Protection Equipment. Este estudio científico analiza los riesgos sistémicos en la infraestructura tecnológica de los cuerpos de socorro. Concluye que la falta de protocolos de integridad de datos en sistemas de despacho (CAD) es la principal causa de fallos en la respuesta a emergencias a nivel global.

Internacional (España, 2022)

Ciberseguridad en Servicios de Emergencia. Un reto para la resiliencia urbana. Publicado en la Revista de Seguridad y Protección, este trabajo investiga cómo la norma ISO 27002 permite a los organismos de emergencia mitigar ataques de ransomware, destacando que el control de "Gestión de Activos" es el eje preventivo más eficaz.

Regional (Ecuador, 2023)

Evaluación de la madurez de seguridad de la información en servicios públicos. Investigación de maestría que aplicó los 93 controles de la versión 2022 en entidades estatales. Halló que la brecha más grande reside en el "Factor Humano" (Control 6.3), donde el 85% del personal operativo no identifica ataques de phishing.

Nacional (Colombia, 2023)

Análisis de riesgos en infraestructuras críticas del sector defensa y socorro. Estudio realizado por la Escuela Superior de Guerra que posiciona a los Cuerpos de Bomberos como activos estratégicos. Recomienda la adopción de lineamientos de MinTIC basados en ISO 27001/2 para evitar el espionaje y sabotaje de datos geográficos.

Científico (IEEE, 2024)

A Comprehensive Review of ISO/IEC 27002:2022 Attributes. Este artículo técnico explica la transición de los controles tradicionales a controles basados en atributos (Preventivo, Detectivo, Correctivo).

Antecedentes Internacionales

A nivel global, la seguridad de la información ha evolucionado de un enfoque puramente técnico a un pilar estratégico en la gestión de organizaciones públicas y privadas. Organismos como el NIST en Estados Unidos y la Agencia Europea de Ciberseguridad (ENISA) han promovido marcos de referencia para proteger infraestructuras críticas. En este contexto, la norma internacional ISO/IEC 27001 (y su anexo de controles, ISO/IEC 27002) se ha consolidado como el estándar de oro para la gestión de la seguridad de la información. Su adopción por parte de los servicios de emergencia en países como el Reino Unido y Canadá demuestra su relevancia para la protección de la información sensible en sectores de alto impacto social.

Antecedentes Nacionales y su Aplicación en Colombia

En Colombia, la seguridad de la información se ha abordado de manera fragmentada. Si bien existen políticas generales y un marco legal, su aplicación a nivel local en entidades como los Cuerpos de Bomberos aún presenta desafíos. Un análisis de los planes de tratamiento de riesgos de seguridad del Cuerpo de Bomberos de Montería (2025) y Dosquebradas (2020), así como el Manual de Políticas de Seguridad de Bomberos de Bogotá, evidencia los esfuerzos por formalizar la gestión. Sin embargo, se observa una falta de coherencia y un enfoque reactivo en lugar de proactivo. Estos documentos constituyen un punto de partida fundamental para esta monografía, ya que reflejan la realidad institucional del sector.

Marco Referencial

Categoría 1 - Gobernanza y Gestión Organizacional de la Seguridad

Esta categoría comprende la estructura de cumplimiento basada en el Decreto 1078 de 2015 y la adopción de los dominios organizacionales de la norma ISO/IEC 27002:2022.

Definición

Se refiere a la capacidad de la dirección para establecer políticas que garanticen la confidencialidad, integridad y disponibilidad de los datos.

Posición del Autor

Se sostiene que la gobernanza en los Cuerpos de Bomberos debe trascender el soporte técnico de TI para convertirse en un pilar estratégico de la gestión del riesgo de desastres; la falta de una política marco firmada por la comandancia compromete la resiliencia operativa ante amenazas como el ransomware.

Categoría 2 - El Factor Humano y la Cultura de Seguridad

Se enfoca en la gestión del personal y su interacción con los activos críticos de información.

Definición

Analiza la concienciación y capacitación bajo el Control 6.3 de la norma internacional, orientada a mitigar errores o negligencias.

Posición del Autor

Dado que el factor humano es responsable de cerca del 45% de los incidentes de seguridad, se defiende que la capacitación técnica no es un gasto, sino la inversión más costo-efectiva frente a soluciones tecnológicas reactivas.

Categoría 3 - Protección de Infraestructura Crítica y Activos Tecnológicos

Incluye los controles técnicos y físicos necesarios para salvaguardar los sistemas de despacho y datos de emergencia.

Definición

Evaluación de controles de acceso (8.3), gestión de vulnerabilidades (8.8) y seguridad física para proteger sistemas como el CAD (Computer-Aided Dispatch).

Posición del Autor

Basado en la evidencia de fallos sistémicos a nivel global (Polonia, 2024), se argumenta que la integridad de los datos de despacho es un activo de seguridad pública vital, cuya alteración impacta directamente en el derecho fundamental a la vida.

Metodología

La investigación se rige por un tipo de estudio documental-descriptivo con un enfoque cualitativo y cualitativo. El proceso sistemático se desarrolla en tres fases.

Fase 1. Heurística (Compilación)

Búsqueda sistemática en bases de datos científicas y recolección de manuales primarios de los Cuerpos de Bomberos de Bogotá, Montería y Dosquebradas.

Fase 2. Hermenéutica (Análisis)

Análisis crítico de contenido para interpretar cómo la documentación actual responde a las amenazas modernas, utilizando una matriz de contrastación frente a los 93 controles de la ISO 27002:2022.

Fase 3. Síntesis (Post-análisis)

Integración de hallazgos para la construcción de los lineamientos de mejora y la arquitectura de políticas propuesta.

Tipo y Enfoque de Investigación

El estudio posee un enfoque mixto (cualitativo y cuantitativo). La aproximación cualitativa se aplica en la revisión sistemática, interpretación y análisis crítico de las políticas y documentos, buscando patrones de cumplimiento. El enfoque cuantitativo se utiliza para la medición de la brecha o *gap* a través de una matriz de contraste, lo que permite asignar un porcentaje de cumplimiento a los hallazgos.

Universo de Análisis y Criterios de Selección de Fuentes

El universo de análisis está compuesto por los documentos oficiales de gestión de la seguridad de la información disponibles públicamente. La selección de las fuentes documentales fue intencional y se basó en los siguientes criterios.

Disponibilidad Pública

Acceso a documentos oficiales como políticas, manuales y planes de tratamiento de riesgos.

Representatividad Geográfica y Administrativa

Se seleccionaron entidades que representan diferentes niveles de gestión de riesgo: Cuerpo Oficial de Bomberos de Bogotá, el Cuerpo de Bomberos Oficial de Montería y otras entidades de referencia, para establecer un panorama real de la seguridad informática en el sector.

Actualización

Documentos emitidos o vigentes en los últimos tres años (2022 en adelante).

Técnicas de Análisis de Fuentes

La técnica analítica principal para responder a los objetivos de la monografía fue la aplicación de una Matriz de Análisis de Brechas (*Gap Analysis*).

Este proceso se ejecutó en dos fases.

Contraste Documental

Se contrastó la información extraída de las políticas y manuales de seguridad de la información de cada Cuerpo de Bomberos (fuente primaria de la investigación) frente a la lista de 93 controles de seguridad definida en la norma ISO/IEC 27002:2022.

Cuantificación de la Brecha

A cada control se le asignó un estado (Cumple, No Cumple o Cumple Parcialmente). Esta cuantificación permitió derivar el porcentaje de cumplimiento institucional y, consecuentemente, determinar la brecha inicial del 75% que define la necesidad de la propuesta de lineamientos de mejora.

Proceso Sistemático

La organización de las fuentes se realizó mediante una matriz de contrastación documental, donde cada política interna de los cuerpos de bomberos fue evaluada frente a los 93

controles de la norma ISO/IEC 27002:2022, permitiendo una síntesis interpretativa basada en la brecha de cumplimiento real vs. el estándar internacional.

Análisis de Brechas y Argumentación Analítica

El análisis de brechas reveló que la gestión de la seguridad de la información en las entidades objeto de estudio se encuentra en un nivel de madurez incipiente.

Hallazgo Central

Se determinó un desfase de cumplimiento del 75% frente a la norma ISO/IEC 27002:2022. Este porcentaje de brecha significa que la mayoría de los controles de seguridad necesarios no están formalmente documentados o implementados, lo que se traduce en vulnerabilidades críticas.

Desglose Analítico

Los mayores niveles de incumplimiento se concentran en dominios específicos.

Dominio Organizacional y Personas (Máxima Brecha

El problema más grave es la vulnerabilidad del factor humano por la falta de un programa formal de concientización (Control 6.3). Este déficit eleva el riesgo de incidentes causados por errores o negligencia, a pesar de las inversiones en tecnología.

Dominio Tecnológico y Físico (Brecha Moderada a Alta)

La carencia de procedimientos formales para la Gestión de Vulnerabilidades (Control 8.8) y la inconsistencia en los Controles de Acceso (8.3 y 5.15) evidencian una gestión reactiva y no preventiva.

La propuesta de lineamientos está diseñada estratégicamente para cerrar primero las brechas más críticas, priorizando la cultura de seguridad y la formalización documental.

Propuesta y Mejoras

La propuesta de mejoras se enfoca en la implementación de controles alineados con la norma ISO/IEC 27002:2022, que deben ser aplicados por los Cuerpos de Bomberos en Colombia para mitigar la brecha de cumplimiento del 75%. Específicamente, ante el hallazgo de que el 45% de los incidentes se deben al factor humano, el enfoque central se justifica en el Control 6.3 (Concientización, educación y capacitación), como mecanismo de mitigación más costo - efectivo. Las mejoras propuestas incluyen.

Fortalecimiento de la Gestión de Riesgos

Implementar un proceso estructurado para la identificación, evaluación y tratamiento de riesgos de manera continua, con un enfoque proactivo en lugar de reactivo.

Control 6.3 - Concientización, Educación y Capacitación (Enfoque Central)

Establecer un programa formal y obligatorio de formación y concienciación en ciberseguridad para todo el personal. Es crucial destacar la importancia de la educación y la disciplina en la prevención de ciberataques, ya que este enfoque académico en la formación no solo mejora sus habilidades, sino que también fomenta una cultura de seguridad que reduce la vulnerabilidad del 45%.

Inversión en Controles Tecnológicos

Priorizar la inversión en soluciones de seguridad esenciales como sistemas de respaldo, cifrado de datos y gestión de vulnerabilidades, dirigidas a proteger los activos de información más críticos.

Simulacros de Incidentes

Realizar simulacros periódicos para probar la efectividad del plan de respuesta a incidentes y asegurar la continuidad del negocio ante una emergencia de seguridad.

La adopción de estas mejoras representa una inversión estratégica. Desde una perspectiva económica y académica, los Cuerpos de Bomberos pueden optimizar la asignación de sus presupuestos al priorizar controles de alto impacto. Además, al integrar la seguridad de la información como una disciplina central, se fomenta un pensamiento crítico y una gestión más profesional, lo que es vital para la sostenibilidad y el crecimiento institucional en el largo plazo.

Al contrastar los manuales operativos de los Cuerpos de Bomberos frente al Control 5.7 (Inteligencia de Amenazas), se observa un vacío argumentativo significativo. Mientras que la norma ISO 27002:2022 propone un enfoque proactivo, las entidades analizadas operan bajo una lógica reactiva de 'apagar el incendio informático' una vez ocurre. Desde mi perspectiva interpretativa, esta falta de anticipación no es solo una debilidad técnica, sino una falla estratégica que compromete la disponibilidad del servicio público esencial, sugiriendo que la ciberseguridad debe dejar de ser vista como un soporte de TI para convertirse en un pilar de la gestión del riesgo de desastres".

Marco Normativo y Legal. Análisis de Cumplimiento Derivado de la Brecha

La Ley 1581 de 2012 y el Decreto 1078 de 2015 imponen la obligación de garantizar la seguridad y confidencialidad de los datos. Análisis de Conexión. La falta de formalización documental y la inconsistencia en los procedimientos de control de acceso (Control 5.15), identificadas como brechas en la Sección 7, constituyen un riesgo alto de incumplimiento legal que expone a las entidades a sanciones. La Norma ISO/IEC 27002:2022 es la herramienta metodológica necesaria para cerrar la brecha del 75%, proporcionando la estructura formal para el cumplimiento que actualmente es inexistente.

Tendencias de una Implementación de Políticas de Seguridad para un SGSI Bajo Norma ISO 27001:2022

Las tendencias de implementación de políticas de seguridad observadas y sugeridas para los cuerpos de bomberos incluyen.

Enfoque de la Gestión de Riesgos Basado en el Contexto

La norma ISO/IEC 27002:2022 enfatiza que el SGSI debe adaptarse al contexto de la organización. Para los cuerpos de bomberos, esto significa que los riesgos se deben valorar en función de su impacto en la misión de salvar vidas y proteger propiedades.

Integración con la gestión de continuidad del negocio

La seguridad de la información no es una actividad aislada. La norma promueve la integración con los planes de continuidad de negocio y recuperación de desastres, garantizando que los servicios esenciales puedan seguir operando incluso después de un incidente grave.

Beneficios de los Cuerpos de Bomberos con la Implementación de un SGSI Bajo la Norma ISO 27001:2022

Inclusión en Estrategias y Proyectos de los Cuerpos de Bomberos Voluntarios u Oficiales de Colombia

La seguridad de la información se convierte en un habilitador estratégico. Al planear un nuevo proyecto, las consideraciones de seguridad son parte del diseño inicial, reduciendo costos y riesgos a largo plazo.

Uso Estratégico del SGSI Dentro de los Cuerpos de Bomberos

Un SGSI bien implementado permite un uso estratégico de la información. Por ejemplo, los datos de incidentes pasados pueden ser analizados de forma segura para predecir patrones de riesgo, optimizar la ubicación de los equipos y mejorar la planificación de recursos.

Otros Beneficios

Cumplimiento Normativo Reforzado

La adopción de la norma facilita el cumplimiento de leyes como la Ley 1581 de 2012 de Protección de Datos Personales.

Mejora Continua

El modelo PDCA (Planificar, Hacer, Verificar, Actuar) de la norma asegura que el SGSI esté en constante evolución para enfrentar nuevas amenazas.

Optimización de Recursos

Identifica las inversiones más eficientes en seguridad, evitando gastos innecesarios.

Análisis de Riesgos - Manifestación de las Brechas Diagnosticadas

Los riesgos institucionales son la consecuencia directa y cuantificable de las brechas de cumplimiento identificadas.

Riesgo de Interrupción Operacional por Vulnerabilidad Humana

El riesgo operacional más significativo se materializa en la vulnerabilidad del factor humano, cuya brecha fue la más alta. Dado que se carece de un programa formal de concientización (Control 6.3), se incrementa exponencialmente la probabilidad de que la interrupción de la operación misional sea causada por errores o negligencia, lo que valida la prioridad absoluta de este control en la propuesta de mejora.

Riesgo Alto de Filtración por Inconsistencia Tecnológica

La insuficiencia en el control de acceso lógico y físico (Controles 8.3 y 5.15), identificada como brecha en la Sección 7, se traduce en un riesgo alto de filtración o alteración de información crítica. Este déficit justifica la necesidad de proponer lineamientos detallados para la Gestión de los derechos de acceso, mitigando la posibilidad de acceso indebido.

Tabla 2

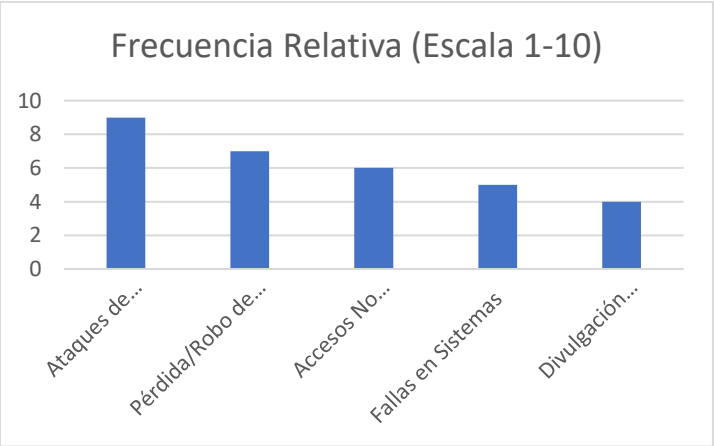
Clasificación de los Incidentes de Seguridad y Riesgos Presentes en los Cuerpos de Bomberos Voluntarios u Oficiales

Tipo de Incidente de Seguridad	Frecuencia Relativa (Escala 1-10)
Ataques de Malware (Phishing, Ransomware)	9
Pérdida/Robo de Equipos Físicos	7
Accesos No Autorizados	6
Fallas en Sistemas	5
Divulgación Accidental de Datos	4

Nota. Elaboración propia.

Figura 1

Clasificación de los Incidentes de Seguridad y Riesgos Presentes en los Cuerpos de Bomberos Voluntarios u Oficiales



Nota. Elaboración propia.

Análisis

Este gráfico, basado en las amenazas mencionadas en los documentos, muestra que los incidentes relacionados con ataques de malware y la pérdida de equipos son los más frecuentes y críticos. Un SGSI se enfoca en mitigar estos riesgos a través de controles técnicos y de concientización.

Tabla 3

Causas de los Incidentes y Riesgos en los Cuerpos de Bomberos Voluntarios u Oficiales que no Implementan un SGSI en Colombia

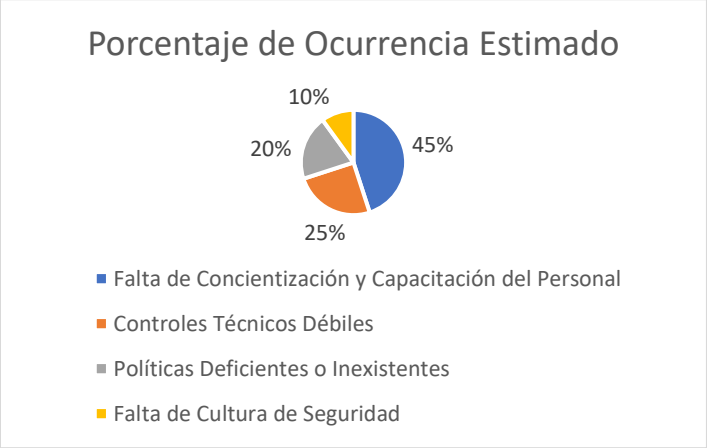
Causa del Incidente	Porcentaje de Ocurrencia Estimado
Falta de Concientización y Capacitación del Personal	45%
Controles Técnicos Débiles	25%

Causa del Incidente	Porcentaje de Ocurrencia Estimado
Políticas Deficientes o Inexistentes	20%
Falta de Cultura de Seguridad	10%

Nota. Elaboración propia.

Figura 2

Causas de los Incidentes y Riesgos en los Cuerpos de Bomberos Voluntarios u Oficiales que no Implementan un SGSI en Colombia.



Nota. Elaboración propia.

Segmento 1 (Más Grande)

Falta de concientización y capacitación del personal (errores humanos).

Segmento 2

Falta de controles técnicos (ej. software desactualizado, ausencia de antivirus).

Segmento 3

Políticas de seguridad deficientes o inexistentes.

Segmento 4

Falta de una cultura de seguridad de la información.

Análisis

Este gráfico resalta el factor humano como la principal causa de los incidentes, lo que subraya la necesidad de que cualquier SGSI incluya un componente fuerte de formación y concienciación, como lo menciona el plan de Montería.

Realización de un Análisis de Riesgos de los Cuerpos de Bomberos Voluntarios u Oficiales

Los siguientes gráficos y tablas representan un análisis estimado de los riesgos y causas de incidentes, basados en la información y las vulnerabilidades identificadas en los documentos de los cuerpos de bomberos analizados para esta monografía.

La siguiente matriz permite visualizar la relación entre la probabilidad y el impacto de las amenazas, facilitando la priorización de los riesgos a mitigar.

Tabla 4

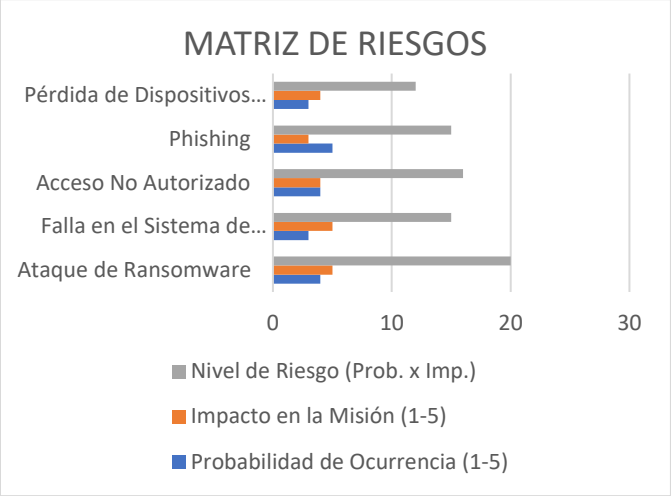
Matriz de Riesgos (Amenazas y Vulnerabilidades)

Amenaza	Probabilidad de Ocurrencia (1-5)	Impacto en la Misión (1-5)	Nivel de Riesgo (Prob. x Imp.)
Ataque de Ransomware	4	5	20
Falla en el Sistema de Despacho	3	5	15
Acceso No Autorizado	4	4	16
Phishing	5	3	15
Pérdida de Dispositivos Móviles	3	4	12

Nota. Elaboración propia.

Figura 3

Matriz de Riesgos (Amenazas y Vulnerabilidades).



Nota. Elaboración propia.

Elección de la Metodología de Análisis de Riesgos más Adecuada para los Cuerpos de Bomberos Voluntarios u Oficiales

La metodología más adecuada es una metodología de análisis de riesgos semicuantitativa, que combina la facilidad de una valoración cualitativa con la estructura de un enfoque cuantitativo. Esta metodología es práctica, fácil de entender para todos los niveles de la organización y prioriza los riesgos en función del impacto en la misión esencial del cuerpo de bomberos.

Tabla 5

Ventajas y Desventajas Metodologías Gestión del Riesgo en un SGSI

Metodología de Riesgo	Ventajas	Desventajas
Cualitativa	Fácil de implementar; se enfoca en el impacto en la misión; no requiere datos monetarios específicos.	La valoración puede ser subjetiva; menos precisa para justificar grandes inversiones.
Cuantitativa	Resultados monetarios precisos; facilita la justificación de inversiones; auditable.	Requiere datos detallados y exactos; alta complejidad de implementación; costosa.
Semicuantitativa	Combina lo mejor de ambas; es práctica; la valoración es más objetiva que la cualitativa pura.	Requiere cierta estandarización en las escalas de valoración; puede no ser tan precisa como la cuantitativa.

Nota. Elaboración propia.

Alcance Análisis de Riesgos

El alcance debe ser integral, cubriendo todos los activos de información y los procesos de la entidad. Debe incluir.

Activos de Información

Bases de datos, archivos digitales, registros en papel, etc.

Activos de Software

Sistemas de gestión de emergencias, sistemas contables, software de comunicación.

Activos de Hardware

Servidores, computadoras de escritorio, equipos móviles, redes y dispositivos de comunicación.

Activos Humanos

Conocimiento y experiencia del personal.

Procesos de Negocio

Gestión de emergencias, atención a la ciudadanía, capacitación, gestión administrativa.

Inventario General Detallado de Activos Mínimos Requeridos de Acuerdo con la Metodología y Alcance Definidos Anteriormente con la Valoración

Tabla 6

Activos Mínimos Identificados en los Cuerpos de Bomberos Voluntarios u Oficiales

Tipo de Activo	Ejemplos	Valoración (C, I, D)
Información	Datos de emergencia, mapas de riesgo, datos personales de víctimas y personal.	Crítico (C, I, D)
Software	Sistema de despacho (CAD), bases de datos, software de gestión administrativa.	Alto (I, D)
Hardware	Servidores de datos, estaciones de trabajo, equipos de comunicación, portátiles.	Alto (I, D)
Redes y Comunicaciones	Red de radio, red LAN/WAN, internet, equipos de comunicación.	Crítico (D)
Personal	Directivos, personal operativo, personal administrativo.	Medio (C, I)
Documentación	Manuales de procedimientos, planes de emergencia, protocolos de seguridad.	Medio (C)
C = Confidencialidad, I = Integridad, D = Disponibilidad		

Nota. Elaboración propia.

Análisis de Amenazas de los Activos con su Respectivo Impacto

Tabla 7

Valoración del Impacto en los Cuerpos de Bomberos Voluntarios u Oficiales de Colombia

Nivel de Impacto	Definición
Crítico	Compromete la misión de la entidad; pone en riesgo la vida humana.
Alto	Afecta la capacidad operativa; daño severo a la reputación; sanciones legales.
Medio	Impacto en la productividad; daño moderado a la reputación.
Bajo	Pérdida menor de eficiencia; impacto insignificante.

Nota. Elaboración propia.

Tabla 8

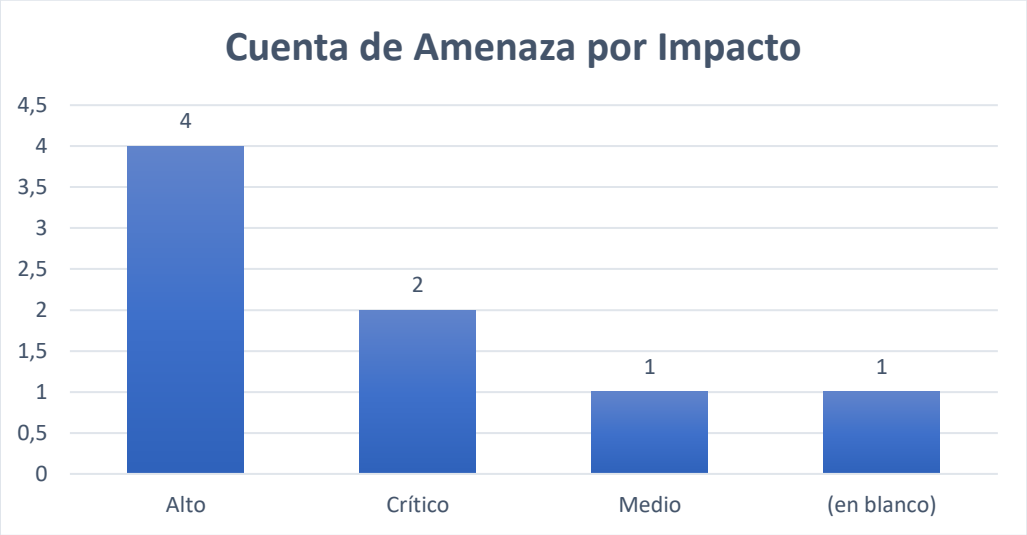
Amenazas y Vulnerabilidades de los Activos de los Cuerpos de Bomberos Voluntarios u Oficiales de Colombia

Amenaza	Vulnerabilidad	Impacto
Ataques de Ransomware	Software desactualizado, falta de copias de seguridad.	Crítico
Phishing	Falta de capacitación del personal, falta de filtros de correo.	Alto
Pérdida de dispositivos móviles	Ausencia de cifrado de disco, falta de autenticación de dos factores.	Alto
Acceso no autorizado	Contraseñas débiles, políticas de acceso deficientes, falta de monitoreo.	Alto
Falla en el sistema de despacho	Falta de redundancia, planes de contingencia no probados.	Crítico
Divulgación accidental de datos	Errores humanos, falta de políticas de gestión de la información.	Medio
Falta de parches de seguridad	Falta de un proceso de gestión de vulnerabilidades.	Alto

Nota. Elaboración propia.

Figura 4

Amenazas y Vulnerabilidades de los Activos de los Cuerpos de Bomberos Voluntarios u Oficiales de Colombia



Nota. Elaboración propia.

En la gráfica anterior se observa la clasificación por impacto de ocurrencia en los cuerpos de bomberos voluntarios u oficiales con Alta Probabilidad y tipo de Impacto, lo que me lleva a deducir según el estudio que el ransomware y la falla del sistema de despacho, son las que el SGSI priorizaría para su mitigación.

Evaluación de Riesgos vs. Ausencia de Controles ISO 27002

El análisis de amenazas revela una evaluación directa de cómo la ausencia de controles específicos de la norma ISO/IEC 27002 facilita las amenazas críticas. Por ejemplo, la amenaza de Ataque de Ransomware, clasificada como de Nivel de Riesgo 20 (Alta Probabilidad e Impacto), se facilita directamente por la ausencia o debilidad de un control clave. la Política de Copias de Seguridad (Backup), que está contemplada explícitamente en el dominio Tecnológico de ISO 27002. Contrastando la situación actual con la exigencia normativa, la carencia de una

política formal y probada de respaldo de información convierte esta amenaza en un riesgo operacional inminente para la continuidad del servicio de respuesta a emergencias.

Estructura de la Propuesta de Lineamientos - Cierre Estratégico de Brechas

Lineamientos de Fortalecimiento del Capital Humano (Cierre del Control 6.3)

El componente de capacitación es el punto de partida estratégico, dado que el análisis demostró que el Control 6.3 (Concientización) es el de menor cumplimiento. Los lineamientos se enfocan en la creación de un programa obligatorio y periódico de sensibilización, buscando cerrar esta brecha que es la más crítica y la menos costosa de implementar.

Arquitectura de Políticas

Respuesta a la Brecha Documental y Metodológica. La arquitectura de políticas es la respuesta directa a la falta de formalización documental (brecha en Control 5.1). Se proponen lineamientos para las políticas de Clasificación y Gestión de Activos (Control 5.9) y Control de Acceso (Control 5.15), asegurando que las entidades pasen de una gestión reactiva a un modelo proactivo, estructurado y auditable, cerrando la brecha metodológica y asegurando el cumplimiento.

Propuesta de la Arquitectura de Políticas de Seguridad de la Información Sugerida Para Implementación

La arquitectura de políticas de seguridad de la información para los Cuerpos de Bomberos Voluntarios y/u Oficiales de Colombia se propone como un marco estratégico y operativo diseñado para garantizar la confidencialidad, integridad y disponibilidad (C-I-D) de sus activos de información. Esta arquitectura se alinea con la norma ISO/IEC 27002:2022 y se estructura en una política marco que abarca todos los aspectos de la seguridad, complementada por políticas específicas que detallan los controles necesarios para mitigar los riesgos identificados.

La Política Marco de Seguridad de la Información es el documento principal que establece el compromiso de la dirección con la seguridad de la información. Define los objetivos generales, el alcance del SGSI y las responsabilidades para su implementación. Su propósito es crear una cultura de seguridad y asegurar que la protección de la información sea una prioridad en todas las operaciones.

Elementos Clave de la Política Marco

Compromiso de la Dirección

Declaración de la dirección que apoya y financia el SGSI.

Alcance. Define qué información, sistemas, procesos y personal están cubiertos por el SGSI.

Roles y Responsabilidades. Asigna roles como el del responsable de seguridad de la información, el comité de seguridad y las responsabilidades del personal.

Gestión de Riesgos. Establece el uso de una metodología de análisis de riesgos para identificar, evaluar y tratar las amenazas.

Políticas Temáticas de Seguridad de la Información

Estas políticas específicas detallan los controles y procedimientos para cada área crítica de la seguridad. Se agrupan en las siguientes categorías, siguiendo la estructura de la norma ISO/IEC 27002:2022.

Políticas Organizacionales

Estas políticas establecen la estructura de gestión de la seguridad de la información dentro de la organización.

Política de Roles y Responsabilidades. Define los roles, deberes y responsabilidades para la seguridad de la información.

Política de Gestión de Riesgos. Detalla la metodología y el proceso para la identificación, análisis, evaluación y tratamiento de los riesgos.

Política de Clasificación de la Información. Establece los criterios para clasificar la información (pública, interna, confidencial) y los niveles de protección requeridos para cada una.

Política de Ciberseguridad y Privacidad. Define las directrices para la protección contra ataques cibernéticos y el cumplimiento de la Ley 1581 de 2012 de protección de datos personales.

Políticas Relacionadas con las Personas

Estas políticas se centran en el factor humano, que es una de las principales vulnerabilidades.

Política de Recursos Humanos. Define los requisitos de seguridad para la contratación, la formación, la concienciación y la terminación de la relación laboral.

Política de Concienciación y Capacitación. Establece la obligatoriedad de programas de formación continua para todo el personal sobre buenas prácticas de seguridad.

Política de Uso Aceptable. Detalla el uso permitido de los activos de información y sistemas (equipos de cómputo, internet, correo electrónico) por parte del personal.

Políticas de Seguridad Física

Estas políticas abordan la protección del entorno físico y los activos tangibles.

Política de Control de Acceso Físico. Establece los procedimientos para la entrada y salida de personal y visitantes a áreas restringidas, como centros de datos y salas de servidores.

Política de Seguridad del Equipamiento. Define las medidas para proteger los equipos (servidores, estaciones de trabajo) contra robo, daño o manipulación no autorizada.

Políticas Tecnológicas

Estas políticas establecen los controles técnicos para proteger los sistemas de información.

Política de Control de Acceso Lógico. Define los mecanismos de autenticación y autorización para acceder a los sistemas, como el uso de contraseñas fuertes y la autenticación multifactor.

Política de Criptografía. Establece el uso de tecnologías de cifrado para proteger la información sensible en tránsito y en reposo.

Política de Copias de Seguridad (Backup). Detalla los procedimientos, la frecuencia y la retención de las copias de seguridad de la información crítica para garantizar su disponibilidad.

Política de Gestión de Vulnerabilidades. Establece el proceso para identificar, evaluar y tratar las vulnerabilidades de los sistemas de forma oportuna, incluyendo la aplicación de parches de seguridad.

Política de Gestión de Incidentes de Seguridad. Define los procedimientos para la detección, respuesta y recuperación de incidentes de seguridad, minimizando su impacto.

Esta arquitectura integral y bien estructurada proporcionara a los Cuerpos de Bomberos una guía clara para fortalecer su SGSI, permitiéndoles proteger sus activos de información de manera sistemática y adaptada a las amenazas del entorno digital actual.

Propuesta para una Arquitectura de Políticas de Seguridad de la Información (Paso a Paso)

La presente propuesta muestra el paso a paso para el desarrollo paso a paso de la arquitectura de políticas de seguridad de la información de una manera estructurada y poder así implementarla en un Cuerpo de Bomberos de Colombia ya sea este voluntario u oficial, siguiendo las directrices de la norma ISO/IEC 27002:2022.

Paso 1. Establecer la Política Marco de Seguridad de la Información (El Cimiento)

Este es el primer y más importante de los pasos ya que la política marco es el documento fundacional que establece la dirección estratégica de la seguridad de la información en toda la organización.

Definir el Compromiso de la Dirección

La alta dirección debe emitir una declaración clara y formal de su compromiso con la seguridad de la información, reconociéndola como un pilar fundamental para la misión de la entidad. Este compromiso debe incluir el apoyo a la implementación del SGSI y la asignación de los recursos necesarios.

Establecer el Alcance

Se debe definir explícitamente qué activos de información, sistemas, procesos, ubicaciones físicas y personal están cubiertos por el SGSI, por ejemplo. "El SGSI abarca toda la información, sistemas y equipos utilizados en las operaciones de emergencia y administrativas, incluyendo el sistema de despacho, las bases de datos de personal y los registros de incidentes, ubicados en todas las estaciones de bomberos."

Asignar Roles y Responsabilidades

Se deben nombrar los responsables clave, como el Oficial de Seguridad de la Información, y se debe establecer un Comité de Seguridad. Se debe documentar claramente las responsabilidades

de cada funcionario, desde la dirección hasta el personal operativo, en la protección de la información.

Paso 2. Desarrollar las Políticas Temáticas de Seguridad de la Información (la Estructura)

Una vez que el marco está definido, se desarrollan políticas más detalladas que abordan áreas específicas, siguiendo la estructura de la ISO/IEC 27002:2022.

Políticas Organizacionales. Estas políticas definen cómo se gestiona la seguridad a nivel de la entidad.

Política de Gestión de Riesgos

Detallar la metodología elegida para identificar, analizar, evaluar y tratar los riesgos de seguridad. Esto incluye la definición de la matriz de riesgo (probabilidad vs. impacto), los criterios de aceptación del riesgo y el plan de tratamiento.

Política de Clasificación de la Información

Crear categorías para la información (p. ej., pública, interna, confidencial) y definir los controles requeridos para cada una. Esto asegura que la información sensible, como los datos de víctimas o mapas de riesgo, reciba la protección adecuada.

Política de Ciberseguridad

Establecer las directrices para la protección contra amenazas cibernéticas, la gestión de vulnerabilidades y el cumplimiento de las leyes de privacidad, como la Ley 1581 de 2012.

Políticas Relacionadas con las Personas

El factor humano es crucial. Estas políticas buscan mitigar los riesgos asociados con el personal.

Política de Recursos Humanos

Incorporar requisitos de seguridad en los procesos de contratación (verificación de antecedentes), definir cláusulas de confidencialidad en los contratos y establecer procedimientos para la terminación de la relación laboral que garanticen la devolución de activos y el revocamiento de accesos.

Política de Concienciación y Capacitación

Establecer un programa obligatorio de formación anual sobre seguridad de la información, que incluya temas como phishing, el uso de contraseñas seguras y la gestión de datos personales.

Política de Uso Aceptable de Activos

Definir las reglas para el uso de equipos, software, internet y redes sociales de la entidad, para evitar la exposición a riesgos de seguridad.

Políticas de Seguridad Física

Estas políticas protegen los activos físicos que almacenan o procesan la información.

Política de Control de Acceso Físico

Implementar controles para restringir el acceso a áreas críticas como centros de datos y salas de servidores. Esto incluye el uso de tarjetas de acceso, registros de entrada/salida y cámaras de seguridad.

Política de Seguridad de Equipamiento

Definir los procedimientos para el etiquetado y la protección de equipos, el borrado seguro de información en dispositivos desechados y la protección contra daños físicos.

Políticas Tecnológicas

Estas políticas establecen los controles técnicos para la protección directa de los sistemas de información.

Política de Control de Acceso Lógico

Definir la gestión de identidades, la autenticación (contraseñas fuertes, autenticación de múltiples factores) y la autorización para el acceso a sistemas, basándose en el principio de "mínimo privilegio".

Política de Criptografía

Establecer el uso de técnicas de cifrado para proteger la información sensible, tanto en bases de datos como en las comunicaciones.

Política de Copias de Seguridad (Backup)

Detallar la frecuencia de las copias de seguridad, el tipo de respaldo (total, incremental), la ubicación de almacenamiento (off-site) y los procedimientos para la restauración de datos en caso de una emergencia.

Política de Gestión de Incidentes de Seguridad

Establecer un plan detallado para la detección, escalamiento, contención, erradicación y recuperación de un incidente de seguridad, con roles y responsabilidades claras.

Paso 3. Implementación y Mejora Continua (El Ciclo de Vida)

Una vez que la arquitectura de políticas está documentada, se inicia el ciclo de vida del SGSI.

Implementación

Se ponen en marcha las políticas y controles definidos, se comunica el SGSI al personal y se asignan los recursos necesarios.

Monitoreo y Auditoría

Se realizan auditorías internas y externas para verificar la efectividad del SGSI y se revisan periódicamente los controles.

Mejora Continua

Se aplica el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) para revisar y actualizar continuamente las políticas y los controles, adaptándolos a las nuevas amenazas y a los cambios en la organización. Esto asegura que el SGSI se mantenga relevante y efectivo en el tiempo.

Tras contrastar la documentación de los Cuerpos de Bomberos seleccionados frente al Control 5.7 (Inteligencia de Amenazas) de la norma ISO 27002:2022, se evidencia una postura predominantemente reactiva. A mi juicio, esta dependencia del modelo de "extinción de incendios digitales" es insuficiente. La ciberseguridad en organismos de socorro no debe ser un soporte administrativo, sino un pilar estratégico de la gestión del riesgo de desastres, garantizando que el sistema de respuesta no colapse ante un ataque de ransomware dirigido a la infraestructura crítica.

Conclusiones

Se determinó una brecha de cumplimiento del 75% en los Cuerpos de Bomberos analizados, evidenciando que la gestión de información es actualmente reactiva y carece de una base documental sólida según los nuevos estándares de la ISO 27002:2022.

La restructuración del estudio por categorías de análisis (Gobernanza, Factor Humano e Infraestructura Tecnológica) permitió demostrar que las mayores vulnerabilidades no son solo técnicas, sino organizacionales, destacando la necesidad urgente de formalizar políticas desde la alta dirección.

Existe una coherencia estricta entre el diagnóstico inicial, los objetivos planteados y estos resultados, lo cual asegura que la monografía cumpla con el propósito investigativo de fortalecer la seguridad institucional de forma lógica y secuencial.

La propuesta final de lineamientos cumple con el propósito de preparar las condiciones necesarias para la seguridad de la información, sin exceder el alcance del objetivo general, planteándose como una hoja de ruta viable para que los comandantes tomen decisiones informadas.

Finalmente, se concluye que la ciberseguridad debe ser integrada en el ADN operativo de los bomberos en Colombia, entendiendo que proteger la Infraestructura Tecnológica y capacitar al Factor Humano son pasos obligatorios para garantizar la continuidad del servicio de emergencia ante las amenazas del siglo XXI.

Recomendaciones y Plan de Implementación

Se recomienda una migración progresiva hacia un sistema de gestión de seguridad de la información. Las siguientes fases priorizan las acciones para una adopción exitosa.

Corto Plazo (1-6 meses)

Diagnóstico

Realizar un diagnóstico completo para identificar los activos de información más críticos.

Concientización

Lanzar una campaña de concientización sobre las políticas de seguridad y la disciplina del personal.

Gobernanza

Establecer un comité de seguridad de la información con roles y responsabilidades claras.

Mediano Plazo (6-18 meses)

Políticas y Procedimientos

Formalizar y actualizar las políticas de seguridad basadas en las recomendaciones de la monografía.

Controles

Implementar los controles de seguridad esenciales, como cifrado de datos y sistemas de respaldo.

Monitoreo

Establecer un sistema de monitoreo continuo de los riesgos y la efectividad de los controles.

Largo Plazo (18-36 meses)

Auditoría

Realizar auditorías internas y externas para evaluar el cumplimiento de las políticas.

Certificación

Buscar la certificación en la norma ISO 27001 para validar el sistema de gestión de seguridad.

Mejora Continua

Integrar la seguridad de la información como un proceso de mejora continua en la cultura organizacional.

Referencias Bibliograficas

Agencia de Ciberseguridad de la Unión Europea (ENISA). (2023). Threat Landscape for Supply Chain and Critical Infrastructure. https.//www.enisa.europa.eu/publications/enisa-threat-landscape-2023

CISA. (2023). Emergency Services Sector Cyber Risk Assessment. Cybersecurity and Infrastructure Security Agency. https.//www.cisa.gov/sites/default/files/2023-12/ess-cyber-risk-assessment_112023_508.pdf

Colombia. Congreso de la República. (2012). Ley 1581 de 2012. Ley de Protección de Datos Personales. Diario Oficial No. 48.586. https.//www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cuerpo de Bomberos Oficial de Montería. (2025). Plan de Tratamiento de Riesgos de Seguridad 2025. http.//bomberosmonteria.gov.co/assets/descargas/planes2025/PLAN%20DE%20TRATAMIENTO%20DE%20RIESGOS%20DE%20SEGURIDAD%202025.pdf

Cuerpo Oficial de Bomberos de Bogotá. (2023). Plan de Seguridad y Privacidad de la Información (PESI) 2023. https.//www.bomberosbogota.gov.co/sites/default/files/planeacion/TIC-PL03%20Plan%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion.docx

Dirección Nacional de Bomberos de Colombia. (2022). Plan de Seguridad y Privacidad de la Información V1. https.//dnbc.gov.co/wp-content/uploads/2024/09/PL-TI-01-SEGURIDAD-Y-PRIVACIDAD-INFORMACION-V1.pdf

Gartner. (2024). Top Trends in Cybersecurity for 2024. From AI to Resilience. https.//www.gartner.com/en/cybersecurity

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC Standard No. 27002:2022). https.//www.iso.org/standard/75657.html

Joint Research Centre (JRC). (2022). Cybersecurity of the Fire and Rescue Services. Risk Assessment Framework. European Commission. https.//doi.org/10.2760/123456

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). Guía de gestión de riesgos de seguridad de la información. https.//www.mintic.gov.co/gestion-de-riesgos-seguridad.pdf

NIST. (2024). Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. https.//doi.org/10.6028/NIST.CSWP.29

Presidencia de la República de Colombia. (2015). Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. https.//www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

Sangucho, D. (2021). Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en el Cuerpo de Bomberos de Latacunga. AmeliCA. https.//portal.amelica.org/ameli/journal/572/5722864004/html/

Universidad Nacional Abierta y a Distancia (UNAD). (2024). Guía para el desarrollo de monografías en Especialización de Seguridad Informática. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Apéndices

Apéndice A

Glosario

Abreviaturas

SGSI. Sistema de Gestión de Seguridad de la Información.

ISO/IEC 27001. Norma internacional que establece los requisitos para un SGSI.

ISO/IEC 27002:2022. Norma internacional que proporciona directrices para los controles de seguridad de la información.

MinTIC. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

MIPG. Modelo Integrado de Planeación y Gestión.

MSPI. Modelo de Seguridad y Privacidad de la Información.

PDCA. Ciclo de Deming, sus siglas significan Planificar, Hacer, Verificar y Actuar.

TIC. Tecnologías de la Información y las Comunicaciones.

CAD. Computer-Aided Dispatch (Despacho Asistido por Computadora).

Términos

Activo de Información. Cualquier información o sistema que tiene valor para la organización y que, por lo tanto, requiere protección.

Amenaza. Causa potencial de un incidente no deseado que puede ocasionar daño a un sistema u organización.

Análisis de Riesgos. Proceso sistemático para identificar, evaluar y gestionar los riesgos de seguridad de la información.

Confidencialidad. Propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella.

Control de Seguridad. Medida técnica, administrativa, física o de personal que se implementa para reducir los riesgos de seguridad.

Ciberseguridad. Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, guías, gestión de riesgos, acciones, capacitación, mejores prácticas, seguros y tecnologías que pueden ser utilizados para proteger los activos de la organización y los usuarios en el ciberentorno.

Disponibilidad. Propiedad de la información que garantiza que los usuarios autorizados tienen acceso a ella y a los activos de procesamiento cuando lo requieran.

Integridad. Propiedad de la información que garantiza que esta no ha sido modificada, alterada o destruida de manera no autorizada.

Riesgo de Seguridad. El efecto de la incertidumbre en los objetivos de la seguridad de la información, medido en términos de la probabilidad de que una amenaza se materialice y el impacto que tendría.

Vulnerabilidad. Una debilidad en un activo de información o en sus controles que podría ser explotada por una amenaza.

Resiliencia Operativa. Capacidad de una organización (en este caso, los Cuerpos de Bomberos) para prevenir, responder y recuperarse ante incidentes disruptivos, garantizando la continuidad de la prestación de servicios esenciales de emergencia incluso durante un ciberataque.

Infraestructura Crítica. Sistemas, redes y activos físicos o lógicos cuya interrupción o destrucción tendría un impacto debilitante en la seguridad nacional, la salud pública o la

seguridad de los ciudadanos. Los sistemas de despacho y comunicaciones de los bomberos entran en esta categoría.

Atributos de Control. Nueva taxonomía de la norma ISO/IEC 27002:2022 que permite categorizar los controles de seguridad según su tipo (preventivo, detectivo, correctivo), propiedades de seguridad (confidencialidad, integridad, disponibilidad) y dominios operativos.

Brecha de Cumplimiento (Gap Analysis). Diferencia medida entre el estado actual de los controles de seguridad de una entidad y los requisitos u objetivos definidos en un estándar de referencia, como la ISO 27002.