Evaluación de la complejidad técnica y su incidencia en la seguridad de los procesos digitales en una organización del sector público en Bogotá

Franklin González Sierra

Asesor

Christian Hernán Obando Ibarra

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2026

Dedicatoria

A mi familia, por su apoyo incondicional y por ser la motivación constante para alcanzar cada meta.

Agradecimientos

A Dios, por darme la fortaleza y sabiduría en este proceso.

A mi familia, por su comprensión y compañía en cada etapa de este camino académico.

A mi tutor y a la Universidad Nacional Abierta y a Distancia – UNAD, por la orientación y las herramientas brindadas para el desarrollo de este trabajo.

Resumen

La presente monografía tiene como propósito evaluar cómo la complejidad técnica incide en la seguridad de los procesos digitales y sistemas de información utilizados por una organización del sector público en Bogotá. La investigación se desarrolla a partir de un enfoque cualitativo y de carácter documental, mediante la revisión de literatura especializada, normatividad vigente, estándares internacionales y buenas prácticas en ciberseguridad. El estudio busca comprender los factores técnicos y organizacionales que incrementan la complejidad en la gestión de dichos procesos digitales, así como las vulnerabilidades que esta puede generar en los principios de confidencialidad, integridad y disponibilidad de la información. A partir del análisis realizado, se plantean recomendaciones estratégicas que podrían servir como referencia para la formulación de políticas internas de ciberseguridad, contribuyendo al fortalecimiento de la gestión de la seguridad informática en entidades públicas con estructuras tecnológicas dependientes o similares.

Palabras clave: ciberseguridad, complejidad técnica, procesos digitales, sector público, seguridad informática.

Abstract

This monograph aims to evaluate how technical complexity impacts the security of digital processes and information systems used by a public sector organization in Bogotá. The research employs a qualitative and documentary approach, reviewing specialized literature, current regulations, international standards, and cybersecurity best practices. The study seeks to understand the technical and organizational factors that increase the complexity of managing these digital processes, as well as the vulnerabilities this complexity can generate in the principles of confidentiality, integrity, and availability of information. Based on the analysis, strategic recommendations are proposed that could serve as a reference for formulating internal cybersecurity policies, contributing to strengthening information security management in public entities with dependent or similar technological structures.

Keywords: cybersecurity, digital processes, information security, public sector, technical complexity.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En el entorno actual, las organizaciones del sector público enfrentan una creciente dependencia de los procesos digitales y sistemas de información para la gestión de datos institucionales, la ejecución de trámites administrativos y la prestación de servicios a la ciudadanía. Esta transformación digital, aunque ha optimizado múltiples tareas, también ha incrementado la complejidad técnica de las infraestructuras tecnológicas, generando nuevos desafíos para la gestión de la seguridad informática y la protección de los activos digitales.

La complejidad técnica se manifiesta en la interconexión de múltiples plataformas, la coexistencia de tecnologías heredadas con herramientas más modernas, la falta de personal especializado y la ausencia de procesos estandarizados de mantenimiento y control. En las entidades públicas, esta situación puede agravarse debido a estructuras organizacionales limitadas, ausencia de áreas internas dedicadas a tecnología o dependencia de proveedores y plataformas externas, lo que aumenta la vulnerabilidad ante amenazas cibernéticas y fallas operativas.

La ciberseguridad, entendida como el conjunto de prácticas, políticas y tecnologías destinadas a proteger los sistemas y la información frente a accesos no autorizados o incidentes, cobra una relevancia estratégica en este contexto. La gestión de la seguridad en entornos digitales requiere no solo herramientas técnicas, sino también una comprensión integral de los factores que determinan la complejidad y su impacto en la confidencialidad, integridad y disponibilidad de la información.

Esta monografía tiene como propósito evaluar cómo la complejidad técnica incide en la seguridad de los procesos digitales de una organización del sector público en Bogotá, a partir de un análisis documental sustentado en la literatura especializada, la normativa vigente y los

estándares internacionales en materia de ciberseguridad. Con base en este estudio, se plantean recomendaciones estratégicas que podrían servir como referencia para la formulación de políticas internas orientadas al fortalecimiento de la seguridad informática institucional.

El documento se organiza en cuatro apartados principales, cada uno orientado al cumplimiento de un objetivo específico. El primero aborda el estado actual de la seguridad informática y de los procesos digitales de la organización e identifica los factores que contribuyen a la complejidad técnica. El segundo presenta el análisis comparativo entre las prácticas y controles de la organización y los estándares y buenas prácticas nacionales e internacionales, con el fin de reconocer brechas. El tercero profundiza en las limitaciones técnicas, organizacionales y de gestión detectadas en la entidad. El cuarto expone las recomendaciones estratégicas derivadas del análisis y examina su pertinencia como referencia para la formulación de políticas internas. Finalmente, se presentan las conclusiones generales, las limitaciones del estudio y las futuras líneas de investigación. Como materiales complementarios, el póster académico se presenta en el Apéndice A y el video de sustentación de la propuesta en el Apéndice B.

Planteamiento del Problema

En el contexto actual, las organizaciones del sector público en Colombia se encuentran en plena senda de transformación digital, adoptando procesos digitales y sistemas de información para la gestión documental, la tramitación administrativa, la continuidad operativa y la atención a la ciudadanía. Sin embargo, esta evolución tecnológica también ha incrementado la complejidad técnica de las infraestructuras y entornos digitales, ya que múltiples plataformas, servidores, bases de datos, redes y aplicaciones deben interactuar de forma interconectada, elevando los riesgos asociados a la seguridad de la información.

La complejidad técnica se manifiesta cuando los componentes tecnológicos requieren integraciones, actualizaciones frecuentes e interoperabilidad con sistemas heredados, en contextos caracterizados por limitaciones organizacionales y ausencia de áreas internas de tecnología que supervisen los procesos digitales. Esta situación genera vulnerabilidades ante errores de configuración, fallas humanas, ataques cibernéticos, interrupciones del servicio o accesos no autorizados, afectando la confidencialidad, la integridad y la disponibilidad de la información institucional.

En el contexto colombiano, este riesgo presenta una alta materialidad, como lo evidencian las cifras recientes. En Colombia se registraron 77.666 denuncias por cibercrimen en 2024, lo que representa un aumento del 23 % respecto a 2023. En Bogotá se concentraron 23.490 casos de hurto por medios informáticos, acceso abusivo a sistemas o violación de datos personales (Cámara Colombiana de Informática y Telecomunicaciones [CCIT], 2025). Además, según un informe de COLCERT y Fortinet, durante 2024 se registraron más de 36.000 millones de intentos de ciberataques en el país, lo que posiciona a Colombia entre los más afectados de

América Latina (Dorado, 2025). Estas cifras evidencian la creciente exposición y criticidad del riesgo en el entorno digital.

De acuerdo con Alejos (2025), Fuentes y Ponce (2025) y Muñoz et al. (2025), los efectos de la complejidad técnica se acentúan debido a limitaciones organizacionales como la falta de direcciones de tecnología, la carencia de políticas internas de ciberseguridad, los presupuestos reducidos y la limitada capacitación del personal. Estas condiciones dificultan la implementación de controles efectivos, el monitoreo de vulnerabilidades y la respuesta oportuna ante incidentes de seguridad.

En la organización objeto de estudio, una entidad del sector público adscrita al Ministerio de Hacienda, la gestión tecnológica depende en gran medida de la infraestructura, políticas y servicios ministeriales. Actualmente, no dispone de sistemas automatizados propios ni de un área de tecnología interna, lo que limita su autonomía en materia de seguridad digital. No obstante, se encuentra en proceso de construcción de su Plan Estratégico de Tecnologías de la Información (PETI) y de políticas institucionales relacionadas con la gestión documental, el manejo de datos y la seguridad de la información.

Por lo tanto, resulta necesario analizar cómo la complejidad técnica, asociada a la dependencia tecnológica y a las limitaciones organizacionales, incide en la seguridad de los procesos digitales de la organización. A partir de ello, se busca generar recomendaciones estratégicas que orienten la formulación de políticas internas de ciberseguridad y fortalezcan la gestión institucional. En consecuencia, la pregunta central de investigación se plantea así:

¿De qué manera la complejidad técnica incide en la seguridad de los procesos digitales de una organización del sector público en Bogotá, y qué recomendaciones estratégicas podrían formularse para orientar la creación de políticas internas de ciberseguridad?

Justificación

La transformación digital que experimentan las organizaciones del sector público en Colombia ha impulsado la adopción de procesos digitales y sistemas de información que facilitan la gestión de trámites, la interoperabilidad entre plataformas institucionales y el almacenamiento de información crítica. No obstante, esta evolución tecnológica también ha incrementado la complejidad técnica de los entornos digitales, generando nuevos desafíos en materia de seguridad de la información y ciberseguridad institucional.

Según el Centro Cibernético Policial y la Cámara Colombiana de Informática y Telecomunicaciones, durante 2024 se reportaron más de 77.000 denuncias por delitos informáticos, con Bogotá como la ciudad que concentró la mayor cantidad de incidentes (CCIT, 2025; Centro Cibernético Policial, 2025). A su vez, Fortinet (2024) registró más de 36.000 millones de intentos de ciberataques en Colombia, lo que sitúa al país entre los más afectados de América Latina. Estas cifras evidencian la creciente exposición de las entidades públicas y privadas frente a riesgos digitales, lo que hace necesario fortalecer la gobernanza tecnológica y la gestión de la seguridad en todos los niveles institucionales.

En el sector público colombiano, estas problemáticas se intensifican debido a limitaciones organizacionales y a la dependencia tecnológica de entidades superiores. A ello se suman la ausencia de áreas especializadas en tecnología, la limitada capacitación del personal y la falta de políticas internas de ciberseguridad. Estas condiciones incrementan las vulnerabilidades de las instituciones frente a amenazas informáticas, especialmente cuando manejan información sensible o dependen de plataformas compartidas para su operación. En este contexto, la complejidad técnica, entendida como la dificultad de gestionar entornos digitales

interconectados y dependientes se configura como un factor de riesgo para la confidencialidad, la integridad y la disponibilidad de la información institucional.

La organización objeto de estudio representa un caso significativo dentro de este contexto. Como entidad adscrita al Ministerio de Hacienda, depende de su infraestructura tecnológica y no cuenta con un área propia de tecnologías de la información. Aunque dispone de herramientas digitales para el cumplimiento de sus funciones misionales, la falta de autonomía tecnológica y la ausencia de políticas internas formalizadas dificultan la gestión integral de la seguridad informática.

Analizar esta situación permite comprender cómo la complejidad técnica, derivada de la dependencia tecnológica y de las limitaciones organizacionales, incide en la seguridad institucional. Asimismo, facilita la formulación de recomendaciones estratégicas orientadas al fortalecimiento de la protección de la información y la gestión digital.

Desde el punto de vista académico, este trabajo aporta a la comprensión de la relación entre complejidad técnica y seguridad digital en el sector público, un campo de estudio aún limitado en el contexto colombiano. Además, ofrece una aproximación metodológica basada en análisis documental que puede servir de referencia para futuras investigaciones sobre gestión de ciberseguridad en entidades públicas con estructuras tecnológicas similares.

En el plano institucional, los resultados de esta monografía proporcionan insumos para la formulación de políticas internas de ciberseguridad y la toma de decisiones estratégicas orientadas al fortalecimiento de la gestión tecnológica. Finalmente, desde una perspectiva social y gubernamental, el estudio contribuye al fortalecimiento de la cultura de seguridad digital en el sector público, en coherencia con las metas de la Política Nacional de Seguridad Digital (2023–2030) y las estrategias de transformación digital del Estado colombiano.

Objetivos

Objetivo General

Evaluar cómo la complejidad técnica incide en la seguridad de los procesos digitales y sistemas de información utilizados por una organización del sector público en Bogotá, con el fin de generar recomendaciones estratégicas que podrían servir como referencia para la formulación de políticas internas de ciberseguridad.

Objetivos Específicos

Analizar el estado actual de la seguridad informática y los procesos digitales de la organización, identificando los factores técnicos y organizacionales que contribuyen a la complejidad en su gestión.

Comparar las políticas, controles y prácticas actuales de seguridad informática de la organización con los estándares y buenas prácticas nacionales e internacionales en ciberseguridad, para identificar brechas y oportunidades de mejora en la gestión institucional.

Identificar las principales limitaciones técnicas, organizacionales y de gestión que inciden en la seguridad informática de la organización, considerando su dependencia tecnológica y estructura administrativa.

Formular recomendaciones estratégicas orientadas a fortalecer la confidencialidad, integridad y disponibilidad de la información, que puedan servir como referencia para la elaboración de políticas internas y planes de mejora en ciberseguridad.

Delimitación del Estudio

El presente estudio se desarrolla en el contexto de una organización del sector público ubicada en la ciudad de Bogotá, seleccionada por su relevancia institucional y por representar el tipo de entidad que, aun cuando utiliza procesos digitales y sistemas de información para el cumplimiento de sus funciones misionales, no cuenta con una dirección de tecnología propia ni con políticas formales de ciberseguridad. Por razones de confidencialidad y protección de la información, el nombre de la organización no se menciona explícitamente.

En cuanto a su delimitación temporal, la monografía se sustenta en información recopilada entre los años 2023 y 2025, periodo caracterizado por el fortalecimiento de las políticas de transformación digital y seguridad cibernética en Colombia, así como por un incremento sostenido en los incidentes de ciberseguridad reportados a nivel nacional.

La delimitación temática se centra en el análisis de la relación entre la complejidad técnica y la seguridad de los procesos digitales en una organización pública que depende tecnológicamente de otra entidad estatal. No se realiza la implementación de estrategias ni la aplicación de controles técnicos, sino un análisis documental y evaluativo basado en literatura especializada, normativa vigente y estándares internacionales de ciberseguridad. El propósito principal es evaluar cómo la complejidad técnica incide en la seguridad institucional y formular recomendaciones estratégicas que sirvan como referencia para la creación de políticas internas de ciberseguridad.

De esta manera, el estudio se circunscribe al ámbito académico y de análisis teórico, sin involucrar acciones prácticas o intervenciones directas sobre la infraestructura tecnológica de la organización. Los resultados buscan generar un aporte conceptual y estratégico que sirva como

guía para futuras investigaciones y procesos de mejora institucional en entidades públicas con estructuras tecnológicas dependientes o similares.

Marco de Referencia

Antecedentes

A nivel internacional, la seguridad de los procesos digitales y los sistemas de información en organizaciones públicas ha cobrado creciente relevancia debido al aumento de ciberataques dirigidos a entidades gubernamentales y a infraestructuras críticas. En este sentido, la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) (2023) señalan que más del 70 % de los países de América Latina carecen de estrategias consolidadas de ciberseguridad que integren tanto la gestión tecnológica como la formación del talento humano. Esta falta de madurez institucional genera vulnerabilidades en los entornos digitales, especialmente en aquellos con estructuras tecnológicas complejas, fragmentadas o dependientes de terceros. Asimismo, la cooperación público-privada constituye un componente relevante para consolidar capacidades institucionales de ciberseguridad (Arteaga, 2021).

Por su parte, el Instituto Nacional de Estándares y Tecnología, mediante su Marco de Ciberseguridad (NIST CSF 2.0, 2023), propone un enfoque basado en la gestión del riesgo que enfatiza la identificación de activos críticos y la reducción de la complejidad técnica como mecanismo preventivo. De manera complementaria, la norma ISO/IEC 27001:2022 recomienda establecer controles de seguridad sustentados en el conocimiento del entorno digital, la actualización continua y la capacitación del personal. Estas referencias constituyen un punto de partida para analizar la relación entre la complejidad técnica y la ciberseguridad institucional en el contexto colombiano.

En el ámbito nacional, la transformación digital del Estado ha avanzado significativamente durante la última década. Como parte de este proceso, el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Política Nacional de

Seguridad Digital 2023–2030, resalta la importancia de fortalecer la resiliencia digital de las entidades públicas, mejorar la gobernanza de la seguridad de la información y reducir la dependencia tecnológica mediante la adopción de buenas prácticas y estándares internacionales.

En cuanto al panorama de amenazas, durante 2024 se registraron más de 77.000 denuncias por delitos informáticos en Colombia, lo que representa un incremento del 23 % frente al año anterior, según datos de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT, 2025). A esta situación se suma que Fortinet (2024) reportó más de 36.000 millones de intentos de ciberataques en el país, lo que posiciona a Colombia como uno de los más afectados en América Latina. Estas cifras evidencian la creciente exposición de las entidades públicas a riesgos digitales y la necesidad de fortalecer su gestión de la seguridad tecnológica.

De acuerdo con el Centro Cibernético Policial (2025), muchas instituciones estatales aún carecen de estructuras sólidas de ciberseguridad y presentan altos niveles de dependencia tecnológica de terceros, lo que incrementa la complejidad técnica de sus entornos digitales. En esta misma línea, la Estrategia de Transformación Digital del Estado 2023–2026, impulsada por la Presidencia de la República (2024), plantea la necesidad de fortalecer la interoperabilidad de las plataformas institucionales, garantizando simultáneamente la gestión del riesgo tecnológico y la protección de la información gubernamental En el sector salud público colombiano, Rosero Córdoba (2024) también destaca la utilidad de los marcos de ciberseguridad y las buenas prácticas para proteger información sensible y fortalecer la continuidad institucional.

En este contexto, la organización objeto de estudio, una entidad del sector público ubicada en Bogotá y adscrita al Ministerio de Hacienda, representa un caso ilustrativo de los desafíos que enfrentan múltiples instituciones estatales. A pesar de emplear herramientas y plataformas digitales para el desarrollo de sus funciones misionales, no cuenta con una dirección

de tecnología propia ni con políticas internas formalizadas de ciberseguridad, lo que genera una dependencia de la infraestructura ministerial y limita su autonomía en la gestión de la seguridad de la información.

La complejidad técnica en este escenario se refleja en la coexistencia de plataformas heterogéneas, procesos digitales distribuidos y una limitada capacidad de control sobre los sistemas. Sin una estructura tecnológica interna que articule la gestión de riesgos, esta situación puede derivar en vulnerabilidades no gestionadas, comprometiendo la confidencialidad, la integridad y la disponibilidad de la información institucional.

Si bien en Colombia existen políticas, normativas y estudios sobre seguridad digital, estos se han centrado principalmente en el fortalecimiento de la infraestructura tecnológica o en la capacitación del talento humano. Sin embargo, son escasos los análisis que abordan la relación entre la complejidad técnica, la dependencia tecnológica y la seguridad institucional en entidades públicas sin autonomía tecnológica. Este vacío académico y práctico justifica el desarrollo de la presente monografía, cuyo propósito es analizar cómo la complejidad técnica incide en la seguridad de los procesos digitales y proponer recomendaciones estratégicas que orienten la formulación de políticas internas de ciberseguridad en el sector público colombiano.

Marco Conceptual

Complejidad Técnica

La complejidad técnica se refiere al grado de dificultad que presentan los sistemas tecnológicos y procesos digitales para ser diseñados, operados, integrados y mantenidos. Según Törngren y Grogan (2018), la complejidad técnica aumenta a medida que los entornos digitales incorporan más componentes, interconexiones y dependencias entre plataformas. En el ámbito organizacional, esta complejidad puede estar asociada a la coexistencia de tecnologías heredadas

y modernas, la falta de estandarización en los procesos o la escasez de personal especializado. En las entidades públicas, la complejidad técnica suele verse amplificada por infraestructuras heterogéneas, dependencia de proveedores externos y limitaciones presupuestales para el mantenimiento tecnológico. De acuerdo con la Organización de los Estados Americanos (OEA, 2023), la gestión inadecuada de la complejidad técnica es una de las principales causas de vulnerabilidades en los sistemas de información de las instituciones estatales, ya que dificulta el control integral de los activos digitales y la identificación de riesgos de seguridad.

En esta monografía, el término complejidad técnica se entiende como el conjunto de factores tecnológicos, estructurales y de gestión que dificultan la administración, monitoreo y protección de los procesos digitales y sistemas de información institucionales, incrementando la exposición de la organización a incidentes de ciberseguridad.

Procesos Digitales y Sistemas de Información

Según Hashemi-Pour et al. (2023), los procesos digitales son aquellas actividades institucionales que se desarrollan mediante el uso de herramientas tecnológicas, plataformas en línea o sistemas de información que permiten la gestión y almacenamiento de datos. Estos sistemas pueden incluir aplicaciones de gestión documental, bases de datos, plataformas de comunicación o herramientas que ejecutan tareas automatizadas, como respaldos o autenticaciones.

En el sector público, la automatización ha permitido optimizar procesos administrativos, mejorar la trazabilidad de la información y agilizar los servicios al ciudadano. Sin embargo, también ha incrementado la dependencia tecnológica y ha ampliado la superficie de exposición ante amenazas cibernéticas (GBA Latam, s. f.). La Política Nacional de Seguridad Digital (MinTIC, 2024) advierte que la automatización y digitalización sin una adecuada gestión de la

seguridad pueden generar puntos críticos de vulnerabilidad, especialmente cuando los sistemas dependen de terceros, carecen de monitoreo o no cuentan con políticas de actualización y respaldo. Por tanto, en este estudio, los procesos digitales se conciben como los conjuntos de herramientas, plataformas y flujos de información que soportan la operación institucional, cuya protección resulta esencial para garantizar la continuidad operativa y la seguridad de los datos.

Ciberseguridad y Seguridad de la Información

La ciberseguridad se define como el conjunto de políticas, procedimientos y tecnologías destinadas a proteger los sistemas, redes y datos frente a ataques, daños o accesos no autorizados (ISO/IEC 27032:2023). Incluye tanto aspectos técnicos como cortafuegos, antivirus y cifrado, como organizacionales, por ejemplo, políticas de control de acceso, capacitación del personal y planes de contingencia. De acuerdo con el NIST (2023), la ciberseguridad debe concebirse desde un enfoque de gestión del riesgo, que contemple los principios de confidencialidad, integridad y disponibilidad (CIA) de la información. Estos tres pilares son fundamentales para la seguridad digital:

- Confidencialidad: garantizar que solo las personas autorizadas accedan a la información.
- Integridad: asegurar que los datos no sean modificados de forma indebida.
- Disponibilidad: mantener la información y los sistemas accesibles cuando se necesiten.

En el contexto del sector público colombiano, la Presidencia de la República (2024), mediante la Estrategia de Transformación Digital del Estado 2023–2026, resalta la importancia de que todas las entidades fortalezcan sus capacidades en ciberseguridad, adoptando estándares internacionales y promoviendo una cultura organizacional de seguridad digital.

Relación entre Complejidad Técnica y Ciberseguridad

Diversos estudios han evidenciado que, a mayor complejidad técnica, mayor es el riesgo de fallas o vulnerabilidades en la infraestructura digital. Esto se debe a que la interdependencia entre sistemas y la falta de claridad en las responsabilidades de gestión aumentan las probabilidades de errores de configuración y de brechas de seguridad (Törngren y Grogan, 2018; OEA, 2023). En el caso de las organizaciones públicas, la complejidad técnica no gestionada puede afectar directamente los tres pilares de la seguridad de la información (CIA), al dificultar la protección de los datos, el control de accesos y la continuidad de los procesos institucionales. Por ello, analizar esta relación es fundamental para comprender los riesgos derivados de la digitalización y dependencia tecnológica, y para formular recomendaciones estratégicas que fortalezcan la gobernanza de la seguridad digital en el sector público colombiano.

Gobernanza de la Seguridad de la Información

La gobernanza de la seguridad de la información se entiende como el conjunto de estructuras, procesos y mecanismos de liderazgo mediante los cuales una organización garantiza que la gestión de la seguridad digital esté alineada con sus objetivos institucionales (ISACA, 2023). No se limita a implementar controles técnicos, sino que involucra la definición de roles y responsabilidades, la asignación de recursos, y el seguimiento a la gestión del riesgo tecnológico. Según el MinTIC (2024), la gobernanza digital en el sector público colombiano implica integrar la seguridad de la información dentro del Modelo Integrado de Planeación y Gestión (MIPG), promoviendo la responsabilidad compartida entre las áreas administrativas, directivas y operativas. Este enfoque permite que las decisiones sobre seguridad no dependan exclusivamente de personal técnico, sino que se conviertan en parte de la estrategia organizacional. En entidades que no cuentan con una dirección de tecnología propia, como la organización objeto de este

estudio, la gobernanza de la seguridad de la información cobra especial relevancia, pues facilita la definición de prioridades, roles y políticas internas, contribuyendo a reducir los efectos de la complejidad técnica y a fortalecer la coordinación institucional. De esta manera, una gobernanza efectiva constituye el eje para desarrollar una cultura de ciberseguridad sostenible y resiliente frente a los desafíos del entorno digital. En instituciones públicas, la articulación entre gobierno de TI y gestión del riesgo también contribuye a fortalecer la toma de decisiones y el control tecnológico (Molina Oviedo, 2020).

Marco Teórico

Fundamentación Teórica de la Complejidad Técnica

El concepto de complejidad técnica surge del campo de la ingeniería de sistemas y se refiere a la interacción de múltiples componentes tecnológicos interdependientes que deben funcionar de manera coordinada para lograr un propósito específico. Según Törngren y Grogan (2018), la complejidad técnica se manifiesta cuando los sistemas presentan una gran cantidad de elementos, conexiones, software y procesos, lo que incrementa la dificultad para controlarlos y mantenerlos estables.

La complejidad puede clasificarse en dos dimensiones principales: estructural y dinámica. La complejidad estructural está relacionada con la cantidad de componentes y sus interrelaciones, mientras que la dinámica se refiere al comportamiento cambiante de los sistemas a lo largo del tiempo (Arévalo y Luz, 2016). En entornos organizacionales, una alta complejidad técnica implica una mayor posibilidad de fallos, vulnerabilidades y errores de configuración, especialmente cuando no existen procedimientos claros de control o supervisión.

En las organizaciones del sector público, esta complejidad se ve amplificada por la coexistencia de tecnologías heredadas y modernas, la dependencia de proveedores externos, la

falta de estandarización documental y las limitaciones presupuestales (OEA, 2023). Comprender la complejidad técnica permite identificar los factores estructurales que aumentan los riesgos tecnológicos y establecer medidas de gobernanza que fortalezcan la seguridad digital institucional.

Teorías sobre la Seguridad de la Información y la Ciberseguridad

La seguridad de la información se sustenta teóricamente en el modelo CIA (Confidencialidad, Integridad y Disponibilidad), base de estándares internacionales como ISO/IEC 27001:2022 e ISO/IEC 27032:2023. Este modelo establece que toda política o medida de seguridad debe garantizar que la información sea accesible únicamente para personas autorizadas, se mantenga íntegra y permanezca disponible cuando se requiera (ISO, 2023).

El Instituto Nacional de Estándares y Tecnología (NIST, 2023) complementa este enfoque mediante el Cybersecurity Framework. Este marco propone cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. En conjunto, estas etapas representan un ciclo de mejora continua que permite gestionar riesgos tecnológicos y responder de forma efectiva ante incidentes.

Desde una perspectiva teórica, la ciberseguridad no se limita al uso de herramientas tecnológicas; implica también un enfoque integral de gestión del riesgo (Rainer y Prince, 2021). Dicho enfoque articula factores humanos, organizacionales y técnicos, y reconoce que las vulnerabilidades más críticas suelen derivarse de la falta de políticas institucionales, la escasa capacitación del personal o la ausencia de una cultura organizacional de seguridad.

En consecuencia, la teoría moderna de la ciberseguridad plantea la necesidad de una gestión integral. Esta debe involucrar tanto la infraestructura tecnológica como el comportamiento del personal y la toma de decisiones institucionales.

Enfoques de Digitalización y Transformación en el Sector Público

La digitalización de procesos en el sector público forma parte de la teoría de la transformación digital. Esta busca mejorar la eficiencia, la transparencia y la sostenibilidad de la gestión pública mediante el uso de tecnologías inteligentes (OECD, 2022). Este proceso implica la automatización parcial de tareas, la integración de plataformas y la gestión electrónica de la información. Sin embargo, diversos autores advierten que la digitalización sin una adecuada planificación técnica y de seguridad puede generar nuevos riesgos, tales como la dependencia tecnológica de terceros, la pérdida de control sobre los procesos, o la vulnerabilidad de sistemas interconectados (Cano y Monsalve, 2023).

La Estrategia de Transformación Digital del Estado 2023–2026 (Presidencia de la República, 2024) plantea que las entidades públicas deben fortalecer su infraestructura digital y sus capacidades de ciberseguridad antes de ampliar su grado de automatización. Por tanto, el éxito de la digitalización no depende únicamente de la tecnología, sino también del liderazgo institucional, la gobernanza y la gestión del riesgo. En el caso de organizaciones públicas sin área tecnológica propia, como la entidad objeto de este estudio, la dependencia de la infraestructura ministerial representa un reto adicional, pues limita la autonomía técnica y la capacidad de respuesta ante incidentes de seguridad digital.

Teoría de la Gobernanza de la Seguridad de la Información

La gobernanza de la seguridad de la información se basa en los principios del modelo COBIT 2019 desarrollado por ISACA (2023), el cual define la gobernanza como la responsabilidad de la alta dirección para garantizar que el uso de la tecnología esté alineado con los objetivos estratégicos de la organización. Este modelo establece que la gobernanza debe integrar tres componentes esenciales: dirección, evaluación y monitoreo. La dirección se encarga

de establecer políticas y objetivos claros; la evaluación revisa los riesgos y el cumplimiento normativo; y el monitoreo verifica que las decisiones sean efectivas y coherentes con la estrategia institucional.

En el contexto de la ciberseguridad, la gobernanza implica definir estructuras organizacionales que asignen responsabilidades claras sobre la gestión de riesgos, la protección de la información y la respuesta ante incidentes (MinTIC, 2024). La falta de gobernanza puede derivar en decisiones reactivas, descoordinación entre áreas y debilidad en los controles institucionales. Para las organizaciones públicas que no cuentan con una dirección de tecnología, la gobernanza de la seguridad de la información se convierte en un mecanismo esencial para mitigar la complejidad técnica, establecer roles de responsabilidad compartida y fomentar una cultura organizacional de seguridad que trascienda los aspectos técnicos. De esta manera, la gobernanza se convierte en el puente entre la complejidad tecnológica y la gestión estratégica de la ciberseguridad.

Los enfoques teóricos descritos permiten comprender cómo la complejidad técnica se relaciona con la seguridad digital en el contexto del sector público colombiano. En primer lugar, la complejidad técnica plantea un desafío constante para la gestión de la ciberseguridad, ya que incrementa la cantidad de puntos de falla, la dependencia tecnológica y la dificultad para mantener el control integral de los activos digitales (Törngren y Grogan, 2018). En segundo lugar, la teoría de la gobernanza de la seguridad ofrece el marco conceptual para analizar cómo las decisiones institucionales pueden mitigar dichos riesgos, aun cuando no exista una dirección de tecnología formal. Finalmente, la aplicación de los modelos de seguridad basados en el riesgo (NIST, 2023; ISO, 2023) proporcionan una base sólida para evaluar la madurez de las prácticas organizacionales y formular recomendaciones estratégicas que fortalezcan la resiliencia digital.

En conjunto, el presente estudio se fundamenta en un enfoque teórico integrador que articula la gestión de la complejidad técnica, la gobernanza institucional y los principios de ciberseguridad. Este enfoque permite comprender de manera holística los desafíos de la protección digital en el sector público colombiano, particularmente en entidades con estructuras tecnológicas dependientes o en proceso de consolidación.

Marco Legal

El marco legal establece las disposiciones normativas y políticas que orientan la gestión de la seguridad de la información y la ciberseguridad en las organizaciones. En el contexto colombiano, tanto los instrumentos internacionales como las leyes nacionales constituyen la base sobre la cual se deben desarrollar las estrategias institucionales de protección digital.

Normativa Internacional

En el ámbito internacional, se destacan las normas ISO/IEC 27001:2022 y ISO/IEC 27032:2023, publicadas por la Organización Internacional de Normalización (ISO). La primera define los lineamientos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que la segunda ofrece directrices específicas para la protección del ciberespacio y la gestión coordinada de incidentes. De igual manera, el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF 2.0, 2023) propone un enfoque basado en la gestión del riesgo, estructurado en cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Este modelo promueve la identificación de activos críticos, la evaluación de amenazas y la mitigación de vulnerabilidades. Tanto las normas ISO como el NIST CSF constituyen referentes internacionales adoptados por múltiples gobiernos e instituciones públicas para fortalecer la resiliencia digital y la gestión de la seguridad.

Normativa Nacional

En Colombia, la legislación relacionada con la ciberseguridad y la seguridad de la información ha evolucionado significativamente en los últimos años. Entre las normas más relevantes se destacan:

- Ley 1273 de 2009, que modifica el Código Penal colombiano para tipificar los delitos informáticos y proteger los datos, sistemas y redes de información.
- Ley 1581 de 2012: Establece el régimen general de protección de datos personales, garantizando los derechos de privacidad y confidencialidad de los ciudadanos.
- Decreto 620 de 2020, por el cual se establecen lineamientos para la gestión de la seguridad digital en las entidades del Estado, con el propósito de fortalecer la confianza en los servicios digitales y promover una cultura de seguridad.
- Política Nacional de Seguridad Digital 2023–2030 (MinTIC, 2024), que plantea acciones estratégicas para prevenir, detectar y responder ante incidentes de ciberseguridad, impulsando la coordinación interinstitucional y la madurez digital del Estado.
- Estrategia de Transformación Digital del Estado 2023–2026 (Presidencia de la República, 2024), que promueve la interoperabilidad y seguridad de los sistemas y servicios digitales del sector público colombiano.

Estas normas reflejan el compromiso del Estado colombiano con la consolidación de una gobernanza digital sólida y con la reducción de los riesgos derivados de la complejidad técnica y operativa de los entornos digitales institucionales.

El cumplimiento de este marco legal no solo garantiza la conformidad normativa de las entidades públicas, sino que también contribuye a la generación de confianza ciudadana, a la protección de los datos institucionales y a la resiliencia operativa frente a las amenazas digitales.

En el caso de la organización objeto de estudio, la adopción de estas disposiciones representa una oportunidad estratégica para fortalecer la gestión de la seguridad informática, establecer políticas internas coherentes con las mejores prácticas internacionales y reducir los efectos negativos de la complejidad técnica en sus procesos digitales y sistemas de información.

Diseño Metodológico

Enfoque de Investigación

El presente estudio se desarrolla bajo un enfoque cualitativo de tipo descriptivo y analítico, ya que busca evaluar cómo la complejidad técnica incide en la seguridad de los procesos digitales y los sistemas de información en una organización del sector público en Bogotá. Este enfoque permite interpretar los fenómenos desde una perspectiva contextual, comprendiendo las relaciones entre los factores técnicos, organizacionales y de gestión que afectan la seguridad institucional. La investigación se desarrolla bajo la modalidad monográfica con revisión documental, apoyada en la sistematización de información teórica, normativa y técnica proveniente de fuentes académicas, institucionales y especializadas en ciberseguridad y gobernanza digital.

Tipo de Investigación

El tipo de investigación es documental y descriptivo, ya que se fundamenta en la recopilación, análisis e interpretación de información secundaria. Según Hernández Sampieri et al. (2014), la investigación documental busca recopilar y analizar información existente para generar conclusiones y propuestas fundamentadas. En este caso, la información se obtiene de informes institucionales, normas, políticas nacionales, artículos científicos y documentos técnicos del ámbito de la seguridad digital.

Alcance de la Investigación

El estudio tiene un alcance descriptivo y evaluativo, pues se orienta a comprender y analizar la relación entre la complejidad técnica y la gestión de la seguridad informática en una organización pública de Bogotá. No se busca implementar soluciones técnicas ni intervenir directamente en los sistemas automatizados, sino evaluar las condiciones actuales, identificar

factores críticos y formular recomendaciones estratégicas que sirvan como referencia para la elaboración de políticas internas de ciberseguridad. Asimismo, el alcance temporal se extiende entre los años 2023 y 2025, periodo en el cual se recopila información documental actualizada sobre políticas nacionales de seguridad digital, transformación tecnológica y buenas prácticas internacionales.

Fuentes de Información

Para el desarrollo de la investigación se consultaron fuentes primarias y secundarias:

Fuentes Primarias: revisión de documentos institucionales de acceso público (manuales, políticas, informes de gestión, planes estratégicos, diagnósticos técnicos, entre otros).

Fuentes Secundarias: artículos científicos, tesis, libros especializados, informes técnicos, marcos normativos y estándares internacionales como ISO/IEC 27001, ISO/IEC 27032, NIST CSF y COBIT 2019, además de políticas nacionales como la Política Nacional de Seguridad Digital 2023–2030 y la Estrategia de Transformación Digital del Estado 2023–2026.

Técnicas e Instrumentos de Recolección de Información

Las principales técnicas de recolección de información son:

- Análisis documental: revisión sistemática de fuentes académicas, normativas e institucionales para identificar conceptos, prácticas y marcos de referencia.
- Análisis comparativo: contraste entre la situación actual de la organización y las buenas prácticas establecidas por los estándares internacionales de ciberseguridad.
- Matriz de análisis: herramienta que permitirá organizar la información en función de tres ejes: complejidad técnica, gestión de seguridad y gobernanza institucional.

Fases de Desarrollo de la Investigación

A continuación, se describen las fases que guiarán la ejecución del proyecto:

Fase 1. Diagnóstico del Estado Actual de la Organización

El propósito de esta fase es analizar el estado actual de la seguridad informática y los sistemas digitales de la organización, identificando los factores que contribuyen a la complejidad técnica. Las actividades a desarrollar incluyen la revisión detallada de la estructura tecnológica y de los procesos digitalizados de la entidad, con el propósito de comprender su funcionamiento y nivel de integración. En este proceso se identifican los principales componentes técnicos, así como las interdependencias existentes entre los distintos sistemas de información. Además, se realiza un análisis de los incidentes y vulnerabilidades más comunes en entidades públicas que cuentan con infraestructuras automatizadas, lo que permite reconocer posibles riesgos y puntos críticos. Finalmente, se elabora un diagnóstico integral sobre la situación actual de la seguridad digital institucional, sirviendo como base para el desarrollo de estrategias de mejora y fortalecimiento.

Fase 2. Análisis Comparativo con Estándares y Buenas Prácticas

El propósito es comparar las políticas, controles y prácticas actuales de la organización con los estándares nacionales e internacionales de ciberseguridad. Las actividades a desarrollar contemplan la selección de los estándares y marcos de referencia más pertinentes, tales como ISO 27001, ISO 27032, NIST, COBIT y la Política Nacional de Seguridad Digital. Posteriormente, se elaborará una matriz comparativa entre la situación actual de la organización y los requisitos o buenas prácticas establecidos por dichos estándares. Finalmente, se procederá a identificar las brechas, fortalezas y oportunidades de mejora, con el fin de orientar estrategias que fortalezcan la gestión de la ciberseguridad institucional.

Fase 3. Identificación de Limitaciones Técnicas y Organizacionales

El propósito es reconocer los factores que limitan la gestión efectiva de la seguridad digital, tanto desde la infraestructura técnica como desde la gobernanza institucional. Las actividades a realizar incluyen la clasificación de los hallazgos obtenidos en el diagnóstico según tres categorías principales: técnica, organizacional y de gestión. Posteriormente, se evaluará el impacto potencial que las limitaciones identificadas podrían tener sobre la seguridad de la información. Finalmente, se priorizan las debilidades críticas que deban abordarse mediante la formulación o actualización de políticas internas, con el propósito de fortalecer la postura de ciberseguridad de la organización.

Fase 4. Formulación de Recomendaciones Estratégicas

El propósito es proponer acciones orientadas al fortalecimiento de la ciberseguridad institucional. Las actividades a realizar incluyen la redacción de las recomendaciones fundamentadas en los hallazgos obtenidos durante las fases anteriores, garantizando que las acciones sugeridas respondan a las necesidades detectadas. Asimismo, se busca que dichas propuestas estén alineadas con el marco legal vigente y con las políticas nacionales en materia de seguridad digital. Finalmente, se valida la coherencia entre las estrategias formuladas y los objetivos institucionales, con el fin de asegurar su viabilidad y pertinencia dentro del contexto organizacional.

Criterios de Análisis

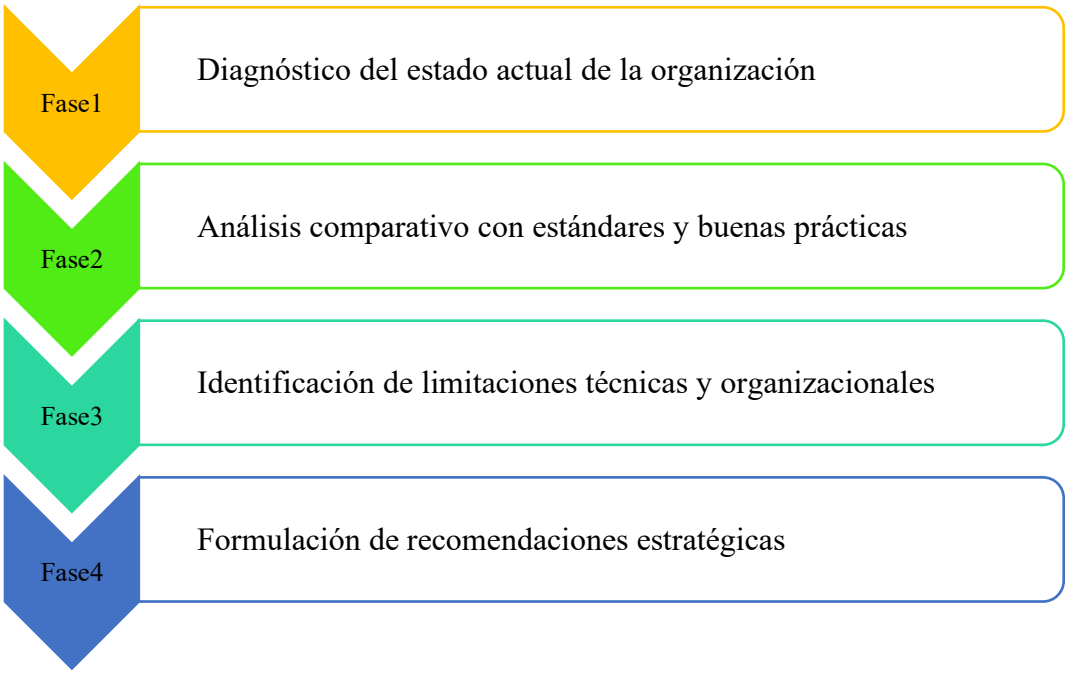
Los resultados del estudio se analizarán de manera cualitativa, relacionando los hallazgos de cada fase con los objetivos específicos. Se buscará establecer correspondencias entre la complejidad técnica, las limitaciones organizacionales y la madurez en seguridad informática, generando conclusiones que fundamenten las recomendaciones finales.

Consideraciones Éticas

El estudio respetará los principios éticos de confidencialidad y uso responsable de la información. No se divulgarán nombres ni datos sensibles de la organización. Toda la información institucional utilizada será de acceso público o anonimizada, garantizando el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.

Figura 1

Diagrama de Fases del Diseño Metodológico de la Monografía



Nota. El diagrama representa las cuatro fases planteadas para el desarrollo metodológico de la monografía.

Para garantizar la organización y el cumplimiento de estas fases, se propone el siguiente cronograma tentativo de actividades. Este cronograma servirá como guía para planificar el desarrollo del proyecto, distribuir adecuadamente los tiempos y asegurar el avance progresivo en el logro de los objetivos específicos. Además, permitirá realizar un seguimiento ordenado de

cada fase, identificar posibles ajustes y mantener la coherencia metodológica del estudio durante todo el proceso investigativo.

Tabla 1

Cronograma de Actividades por Mes

Fase / Actividad principal	Descripción principal
Fase 1. Diagnóstico del Estado Actual de la Organización	
Revisión de literatura y documentos institucionales	Búsqueda y análisis de fuentes académicas, normativas y técnicas sobre ciberseguridad, gobernanza digital y gestión de sistemas de información en el sector público. Permite establecer el marco de referencia conceptual para el diagnóstico inicial.
Identificación de factores de complejidad técnica.	Análisis de los procesos digitalizados y de los sistemas de información de la organización, considerando su nivel de integración, interoperabilidad, mantenimiento y dependencias técnicas. Se busca identificar los aspectos que incrementan la complejidad técnica.
Análisis de incidentes y riesgos frecuentes en el sector público	Sistematización de datos nacionales e internacionales sobre vulnerabilidades, incidentes de ciberseguridad y amenazas comunes en entidades públicas colombianas. Se utiliza esta información para contextualizar los riesgos que podrían afectar a la organización.
Fase 2. Análisis Comparativo con Estándares y Buenas Prácticas	
Selección de estándares y marcos de referencia	Identificación y elección de los estándares más relevantes para el análisis, tales como ISO/IEC 27001, ISO/IEC 27032, NIST, COBIT 2019, la Política Nacional de Seguridad Digital 2023–2030 y la Estrategia de Transformación Digital del Estado 2023–2026.
Elaboración de matriz comparativa	Construcción de una matriz que contraste las políticas, controles y prácticas actuales de la organización con los lineamientos establecidos en los estándares seleccionados. Permite evidenciar el nivel de cumplimiento o la ausencia de ciertos controles.
Identificación de brechas y fortalezas.	Evaluación de las diferencias entre la situación actual y las buenas prácticas internacionales. Se determinan las brechas

Fase / Actividad principal	Descripción principal
	existentes, las fortalezas institucionales y las oportunidades de mejora en la gestión de la seguridad informática.
Fase 3. Identificación de Limitaciones Técnicas y Organizacionales	
Clasificación de limitaciones	Análisis de los hallazgos del diagnóstico y la comparación para agrupar las limitaciones según tres categorías: técnica (infraestructura, mantenimiento), organizacional (ausencia de políticas o roles) y de gestión (procesos y controles).
Evaluación del impacto de las limitaciones	Estudio cualitativo de cómo las limitaciones detectadas afectan la seguridad institucional, la confidencialidad, la integridad y la disponibilidad de la información. Permite estimar el nivel de riesgo asociado a cada limitación.
Priorización de factores críticos	Selección de los aspectos más relevantes o urgentes que deben ser abordados mediante políticas, estrategias o acciones institucionales. Esta priorización servirá como base para formular las recomendaciones estratégicas.
Fase 4. Formulación de Recomendaciones Estratégicas	
Diseño de propuestas y lineamientos	Elaboración de recomendaciones orientadas al fortalecimiento de la ciberseguridad institucional, con base en los hallazgos de las fases previas y en las buenas prácticas internacionales.
Validación con el marco legal y políticas nacionales	Verificación de que las recomendaciones propuestas estén alineadas con la normativa colombiana (Ley 1273 de 2009, Ley 1581 de 2012, Decreto 620 de 2020, Política Nacional de Seguridad Digital 2023–2030, entre otras).
Redacción de conclusiones y revisión final	Integración de los resultados obtenidos, las recomendaciones estratégicas y las conclusiones del estudio. Incluye la revisión general del documento y la formulación de sugerencias para investigaciones futuras.

Nota. El cronograma presenta la distribución mensual de las actividades correspondientes a las cuatro fases de la investigación.

Análisis del Estado Actual de la Seguridad Informática y la Infraestructura Tecnológica Institucional

El proceso de modernización digital en las entidades públicas colombianas ha avanzado de manera constante durante la última década, impulsado por políticas nacionales, iniciativas de transformación digital y la creciente demanda ciudadana de servicios eficientes, transparentes y accesibles. Este escenario ha llevado a que múltiples instituciones incorporen sistemas de información, plataformas digitales y procesos automatizados para la gestión administrativa, operativa y financiera. Sin embargo, dicho progreso también ha incrementado la exposición a vulnerabilidades, riesgos tecnológicos y amenazas cibernéticas, especialmente en aquellas organizaciones que presentan limitaciones organizacionales y dependencia tecnológica para la gestión de sus sistemas de información.

En este contexto, el presente apartado analiza el estado actual de la seguridad informática y la infraestructura tecnológica institucional, tomando como caso de estudio la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF), entidad del sector público adscrita al Ministerio de Hacienda y Crédito Público. Para ello, se aborda inicialmente el entorno tecnológico del sector público colombiano y los niveles de madurez en ciberseguridad, con el fin de contextualizar las condiciones generales en las que operan las entidades estatales.

Posteriormente, el análisis se centra en la URF, identificando los principales factores organizacionales y tecnológicos que inciden en la complejidad técnica de su entorno digital, tales como la dependencia de infraestructura tecnológica externa, la ausencia de un área interna de tecnologías de la información y la falta de políticas formales de ciberseguridad. Estos elementos permiten comprender cómo dichas condiciones influyen en la gestión de la seguridad de la información y en la protección de los procesos digitales institucionales.

Entorno Tecnológico de las Entidades Públicas en Colombia

El sector público colombiano ha avanzado de manera significativa en la implementación de tecnologías de la información como parte de la Estrategia de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Estas iniciativas han promovido el uso de plataformas interoperables, la digitalización de trámites y el desarrollo de sistemas orientados a mejorar la eficiencia administrativa y ofrecer mejores servicios a la ciudadanía. No obstante, el nivel de digitalización y la calidad de la infraestructura tecnológica varían ampliamente entre entidades.

En muchas organizaciones persisten infraestructuras heterogéneas, sistemas antiguos o desactualizados, limitaciones organizacionales y dependencia de proveedores externos para operar o mantener sistemas críticos. Estas condiciones generan brechas operativas y afectan la capacidad institucional para proteger la información y responder a incidentes tecnológicos.

Rodríguez (2021) señala que, aunque la digitalización de procesos judiciales y administrativos ha mejorado la eficiencia y el acceso a los servicios, también ha evidenciado vacíos importantes en la protección de datos, la gestión de vulnerabilidades y la estandarización de controles de seguridad. Tales vacíos se asocian, en gran medida, con la escasez de personal especializado, la fragmentación de las plataformas y la falta de políticas de seguridad actualizadas.

De acuerdo con Bueno Munar (2022), las instituciones estatales enfrentan desafíos significativos en materia de infraestructura, gobernanza tecnológica y capacitación interna. En particular, las entidades que no cuentan con áreas propias de tecnología, o que dependen de servicios informáticos tercerizados, presentan mayores riesgos debido a la falta de control directo sobre activos críticos. Esta situación es especialmente visible en unidades técnicas o

administrativas adscritas a ministerios y organismos del nivel central, donde la gestión tecnológica depende de infraestructuras externas.

En este contexto, la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF) se enmarca dentro de este tipo de organizaciones, ya que su operación tecnológica depende de la infraestructura del Ministerio de Hacienda. Esta condición limita el control directo sobre los sistemas de información y contribuye a la generación de complejidad técnica, lo que incide en la gestión de la seguridad informática y en la protección de los procesos digitales institucionales.

Estado Actual de la Seguridad Informática en el Sector Público

La Política Nacional de Seguridad Digital (MinTIC, 2024) reconoce que la mayoría de las instituciones estatales presentan niveles de madurez bajos o intermedios en la gestión de la ciberseguridad. Los principales desafíos se relacionan con la gestión del riesgo, la protección de infraestructuras críticas y la limitada disponibilidad de talento humano especializado. En este sentido, el informe de Fortinet (2024) indica que el 68 % de las organizaciones en América Latina reportan dificultades para contratar personal en ciberseguridad, lo que se traduce en una mayor dependencia de consultores externos y en una capacidad limitada de respuesta ante incidentes.

Jiménez y López (2023) señalan que, si bien Colombia cuenta con un marco normativo robusto que incluye la Ley 1273 de 2009, la Ley 1581 de 2012 y el Decreto 620 de 2020, su aplicación práctica sigue siendo heterogénea. En muchas entidades, los protocolos de seguridad no se actualizan de manera periódica y las medidas de prevención se implementan de forma reactiva, una vez ocurridos los incidentes.

En esta misma línea, Polania Amaya (2025) destaca que, aunque el país ha fortalecido su marco legal en ciberseguridad desde 2012, la implementación efectiva de estas políticas depende de factores organizacionales como la capacitación del personal, la claridad en la asignación de responsabilidades y la existencia de estructuras de gobernanza tecnológica. La ausencia de estos elementos incrementa la complejidad técnica y dificulta la gestión adecuada de la seguridad digital.

En el caso de la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF), estas condiciones se reflejan en la ausencia de un área interna de tecnologías de la información y en la dependencia de la infraestructura tecnológica del Ministerio de Hacienda. Esta situación limita la capacidad institucional para implementar controles de seguridad, gestionar riesgos de manera autónoma y responder oportunamente ante incidentes, lo que ubica a la entidad en un nivel de madurez básico o intermedio en materia de ciberseguridad.

Tabla 2

Nivel de Madurez de la Ciberseguridad en Entidades Públicas Colombianas

Nivel de Madurez	Características Principales	Situación Observada en la Mayoría de Entidades
Inicial	No existen políticas de seguridad formales ni asignación de responsabilidades.	Varias entidades pequeñas y unidades adscritas a ministerios.
Básico	Se aplican controles mínimos de seguridad; acciones reactivas.	La mayoría de entidades públicas locales y regionales.
Intermedio	Existen políticas institucionales y capacitación ocasional del personal.	Entidades de nivel central con proyectos de digitalización.
Avanzado	Políticas actualizadas y monitoreo permanente.	Pocas entidades (Superfinanciera, MinTIC, DIAN).

Nota. Basado en los criterios de madurez del MinTIC (2024) y adaptado al contexto del estudio.

Factores de Complejidad Técnica Identificados

A partir de la revisión documental y del análisis del contexto institucional, se identifican los principales factores que incrementan la complejidad técnica en los sistemas digitales de las entidades públicas colombianas. Asimismo, estos factores se evidencian en la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF), lo que permite comprender su incidencia en la seguridad de los procesos digitales:

1. Infraestructura tecnológica heterogénea: Se refiere a la coexistencia de sistemas antiguos y nuevas plataformas sin una integración adecuada, lo que dificulta la interoperabilidad y el control de seguridad (Bueno Munar, 2022). En el caso de la URF, este factor se manifiesta en el uso de múltiples plataformas institucionales proporcionadas por el Ministerio de Hacienda, sobre las cuales la entidad no tiene control directo, lo que incrementa la complejidad en la gestión de la información.

2. Dependencia de terceros: Corresponde a la contratación o uso de servicios tecnológicos externos sin supervisión técnica interna, lo que genera brechas en la gestión de riesgos (Betancourt, 2025). En la URF, la dependencia de la infraestructura tecnológica del Ministerio de Hacienda limita la autonomía institucional para gestionar la seguridad informática y dificulta la implementación de controles propios.

3. Falta de personal especializado: Hace referencia al déficit de profesionales en ciberseguridad y administración de sistemas, lo que limita la capacidad de respuesta ante incidentes (Fortinet, 2024). En este sentido, la URF no cuenta con un área interna de tecnologías de la información, lo que restringe la capacidad de monitoreo, mantenimiento y gestión de riesgos tecnológicos.

4. Ausencia de gobernanza tecnológica: Se relaciona con la falta de liderazgo, estructura organizacional y coordinación en la gestión de las tecnologías de la información (Jiménez y López, 2023). En la URF, esta situación se evidencia en la inexistencia de una estructura formal de gobernanza TI, lo que dificulta la definición de responsabilidades, la implementación de políticas y la toma de decisiones estratégicas en materia de ciberseguridad.

5. Escasa cultura organizacional de seguridad: Hace referencia al bajo nivel de concienciación del personal sobre la importancia de la ciberseguridad, así como a la percepción de esta como un gasto y no como una inversión (Rodríguez, 2021). En la URF, la ausencia de políticas internas formalizadas y de procesos de capacitación continua limita la consolidación de una cultura de seguridad institucional.

Asimismo, Rozo Díaz (2024) resalta que la falta de auditorías periódicas y de simulaciones de respuesta ante ataques cibernéticos permite que las vulnerabilidades persistan durante largos períodos, aumentando el riesgo de exposición de datos institucionales. Estos

factores no solo representan desafíos técnicos, sino también limitaciones organizacionales y estratégicas, ya que afectan la toma de decisiones y la confianza en los sistemas digitales. En la misma línea, Ávalos et al. (2023) señalan que la ausencia de políticas internas claras y de mecanismos de seguimiento dificulta la implementación de controles de seguridad sostenibles.

Tabla 3

Factores de Complejidad Técnica en Entidades Públicas Colombianas

Factor de Complejidad Técnica	Descripción / Causa	Consecuencia en la Seguridad Informática
Infraestructura heterogénea	Coexistencia de sistemas antiguos y modernos sin integración.	Dificulta la interoperabilidad y el monitoreo de seguridad.
Dependencia de terceros	Servicios tecnológicos externos sin supervisión interna.	Brechas en la gestión de riesgos y vulnerabilidad ante fallos externos.
Falta de personal especializado	Falta de profesionales en ciberseguridad y soporte técnico.	Aumenta el tiempo de respuesta ante incidentes.
Ausencia de gobernanza tecnológica	Falta de liderazgo y coordinación institucional.	Falta de políticas claras y control interno débil.
Escasa cultura de seguridad	Bajo compromiso del personal con las prácticas seguras.	Riesgo de errores humanos y accesos indebidos.

Nota. Información elaborada con base en Munar (2022), Betancourt (2025), Jiménez y López (2023), Rodríguez (2021), Fortinet (2024) y la Política Nacional de Seguridad Digital (MinTIC, 2024).

En el contexto colombiano, esta situación se agrava por factores como la alta rotación de personal y las limitaciones organizacionales en la gestión tecnológica. En el caso de la URF, estos elementos refuerzan la dependencia tecnológica y la dificultad para ejercer control sobre los sistemas de información. Por tanto, gestionar la complejidad técnica implica no solo la actualización de los sistemas, sino también el fortalecimiento de las capacidades institucionales, la definición de estructuras de gobernanza tecnológica y la implementación de procesos de monitoreo continuo. Estas acciones contribuyen a mitigar vulnerabilidades y a consolidar una

gestión de la seguridad de la información más efectiva y alineada con las necesidades institucionales.

Complejidad Técnica y Ciberseguridad Institucional

Diversos autores coinciden en que la complejidad técnica es uno de los principales factores que incrementa la vulnerabilidad de las entidades públicas frente a ciberataques (Törngren y Grogan, 2018; Gómez, 2020). La fragmentación de sistemas, la falta de documentación técnica y la rotación de personal dificultan la gestión y el seguimiento de incidentes. En este sentido, Lopera (2025) señala que la creciente automatización en las entidades públicas, sin una adecuada planificación, amplifica el riesgo cibernético, especialmente cuando no existen mecanismos efectivos de gobernanza digital. Esto se refleja en que una proporción significativa de los incidentes informáticos reportados en Colombia se relaciona con configuraciones erróneas, accesos indebidos o fallas en la gestión de credenciales.

De acuerdo con el Centro Cibernético Policial (2024), se registraron más de 30.000 denuncias por delitos informáticos en Bogotá, lo que evidencia la necesidad de fortalecer los mecanismos de protección digital en las instituciones estatales. Estas cifras confirman que el entorno digital en el país es cada vez más complejo y exige mayores capacidades institucionales para la gestión de la ciberseguridad.

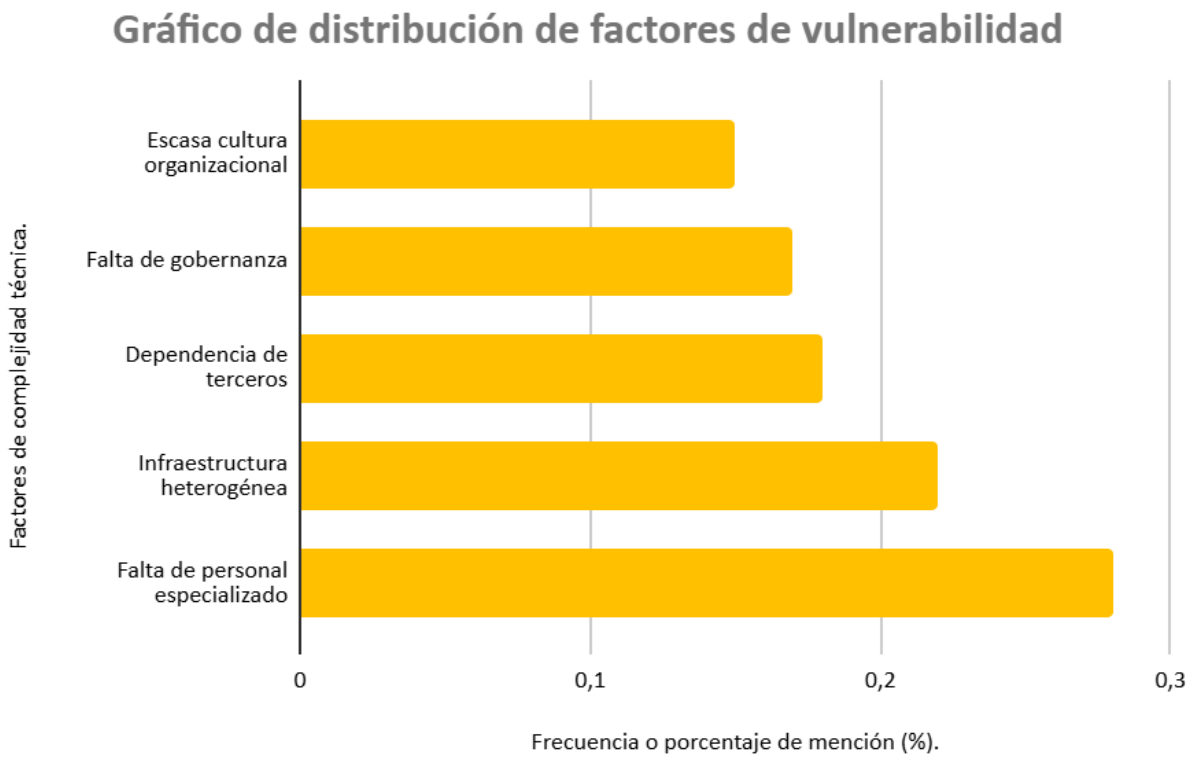
Según la Figura 2, el déficit de talento humano y la heterogeneidad tecnológica representan una proporción significativa de las causas de la complejidad técnica en las entidades públicas colombianas, lo que indica que los principales riesgos están asociados a la capacidad operativa y a la infraestructura tecnológica.

El análisis realizado evidencia que las organizaciones del sector público operan en un entorno caracterizado por limitaciones organizacionales, dependencia tecnológica y una

infraestructura heterogénea. La complejidad técnica surge principalmente de la interdependencia de sistemas, la falta de estandarización de procesos y la ausencia de políticas internas claras y actualizadas de seguridad, lo que dificulta la protección de los sistemas automatizados y aumenta la exposición a incidentes cibernéticos.

Figura 2

Principales Factores de Complejidad Técnica en Entidades Públicas Colombianas



Nota. Información elaborada con base en Rodríguez-Márquez (2021), Betancourt Zúñiga (s. f.), Jiménez-Almeira y López (2023), Munar (2022), Fortinet (2024) y la Política Nacional de Seguridad Digital (MinTIC, 2024).

En este contexto, el fortalecimiento de la gobernanza de la seguridad de la información y la adopción de buenas prácticas internacionales, como las propuestas por NIST, ISO/IEC 27001

y COBIT, resultan fundamentales para mitigar los riesgos derivados de la complejidad técnica y mejorar la gestión de la seguridad informática.

En el caso de la Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF), se evidencia la coexistencia de plataformas tecnológicas heterogéneas, la ausencia de un área interna de tecnologías de la información y la falta de políticas formales de ciberseguridad. Estos factores, sumados a la dependencia de la infraestructura tecnológica del Ministerio de Hacienda y a la ausencia de una estructura de gobernanza digital, configuran un entorno de alta complejidad técnica que impacta directamente la seguridad de la información institucional.

En consecuencia, la URF presenta limitaciones para implementar controles de seguridad, gestionar riesgos de manera autónoma y responder oportunamente ante incidentes. Este diagnóstico permite identificar las principales debilidades tecnológicas y organizacionales y constituye la base para desarrollar estrategias orientadas al fortalecimiento de la ciberseguridad institucional en los apartados siguientes.

Análisis Comparativo de Políticas, Controles y Prácticas de Seguridad Informática en una Organización del Sector Público Frente a Estándares y Buenas Prácticas de Ciberseguridad

La ciberseguridad en el sector público colombiano enfrenta desafíos significativos debido a la rápida evolución tecnológica, la diversidad de plataformas digitales y la limitada disponibilidad de personal especializado. En este contexto, resulta fundamental realizar un análisis comparativo que permita identificar brechas entre las políticas y controles de seguridad implementados en las organizaciones estatales y las buenas prácticas nacionales e internacionales.

El propósito de este apartado es comparar las políticas, controles y prácticas actuales de seguridad informática de una organización del sector público en Bogotá con estándares reconocidos a nivel mundial, tales como la ISO/IEC 27001:2022, el NIST Cybersecurity Framework (2023) y el modelo COBIT 2019, así como con lineamientos nacionales como la Política Nacional de Seguridad Digital 2023–2030 (MinTIC, 2024). A través de esta comparación, se busca identificar las brechas existentes, las fortalezas institucionales y las oportunidades de mejora en la gestión de la seguridad de la información y de la infraestructura tecnológica institucional.

Este apartado presenta el análisis aplicado a la organización del sector público objeto de estudio, describiendo su situación actual en materia de seguridad informática, identificando brechas frente a estándares internacionales y estableciendo elementos que fundamentan la formulación de recomendaciones estratégicas. A diferencia del apartado anterior, de carácter contextual y descriptivo, este apartado se centra en la realidad operativa de la entidad, sin mencionar su nombre por razones de confidencialidad.

Estándares y Buenas Prácticas Internacionales en Ciberseguridad

Los marcos internacionales proporcionan estructuras metodológicas para gestionar los riesgos de ciberseguridad y asegurar la confidencialidad, integridad y disponibilidad de la información. Entre los más relevantes se destacan:

ISO/IEC 27001:2022

La norma ISO/IEC 27001 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su propósito es garantizar la confidencialidad, integridad y disponibilidad de la información, mediante políticas, controles y procesos documentados (Rivera y Cruzatty, 2025). Sus principales controles incluyen:

- Política de seguridad de la información.
- Evaluación y tratamiento de riesgos.
- Control de accesos.
- Seguridad en las operaciones y continuidad del negocio.
- Capacitación y concientización del personal.

En el contexto público colombiano, Camargo y Pinzón (2022) sostienen que la adopción de ISO 27001 contribuye a fortalecer la transparencia y la confianza ciudadana, aunque la mayoría de entidades aún no cuentan con una certificación formal.

NIST Cybersecurity Framework (CSF 2.0, 2024)

El NIST CSF 2.0, desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., propone cinco funciones esenciales: Identify, Protect, Detect, Respond, y Recover, las cuales permiten gestionar el riesgo cibernético de manera integral. Así pues, Pérez, Velásquez y Silva (2023) destacan que este marco es adaptable y sirve como referencia para organizaciones

públicas que no poseen un departamento de TI estructurado, ya que ofrece lineamientos prácticos y graduales de implementación.

COBIT 2019

El marco COBIT 2019, desarrollado por ISACA, se enfoca en la gobernanza y gestión de la información y la tecnología empresarial. Su objetivo es asegurar que la tecnología aporte valor y reduzca los riesgos. Por ende, Álvarez (2024) señala que COBIT promueve la definición de roles y responsabilidades, la gestión de riesgos tecnológicos y la medición del desempeño, aspectos que suelen ser débiles en las entidades públicas colombianas.

CIS Critical Security Controls (v8)

Este conjunto de controles prácticos definidos por el Center for Internet Security (CIS) prioriza la protección técnica de los sistemas, como la gestión de activos, vulnerabilidades, privilegios de usuario y respuesta a incidentes. Su aplicación contribuye a reducir significativamente la exposición a los ataques más comunes.

ISO/IEC 27032:2023

Complementa el estándar ISO 27001 al enfocarse en la cooperación entre sectores y la protección del ciberespacio frente a amenazas globales, promoviendo la colaboración entre actores públicos, privados y ciudadanos.

En conjunto, estos marcos de referencia son utilizados como guía para el fortalecimiento de la ciberseguridad institucional en entidades públicas y privadas a nivel mundial, y sirven como base para comparar el nivel de madurez de la organización objeto de estudio frente a las mejores prácticas internacionales.

Lineamientos Normativos y Políticas Nacionales de Ciberseguridad en Colombia

Colombia ha consolidado en los últimos años un marco normativo y político destinado a fortalecer la seguridad digital del Estado y proteger la información pública frente a los crecientes riesgos cibernéticos. Estas disposiciones establecen los principios, responsabilidades y mecanismos de gestión que deben adoptar las entidades del sector público para garantizar la protección de sus activos tecnológicos y de información.

Política Nacional de Seguridad Digital (MinTIC, 2023–2030)

Este instrumento constituye el eje central de la estrategia nacional de ciberseguridad. Promueve la resiliencia digital del Estado, la coordinación interinstitucional y la protección de las infraestructuras críticas. Además, impulsa la adopción de estándares internacionales como ISO/IEC 27001, NIST CSF y COBIT 2019, y la creación de capacidades técnicas en las entidades públicas para la gestión del riesgo tecnológico. El MinTIC (2024) resalta la necesidad de que cada institución desarrolle políticas internas de seguridad digital, garantizando la continuidad de los servicios públicos y la protección de la información gubernamental.

Documento CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital

Este documento establece las acciones estratégicas para fomentar una cultura de seguridad digital en el país. Entre sus objetivos se encuentran: mejorar la gestión del riesgo cibernético, fortalecer la gobernanza digital y aumentar la capacidad de respuesta ante incidentes. También orienta la formación de talento humano especializado en ciberseguridad, aspecto que sigue siendo un reto en las entidades estatales (Molina, 2020).

Ley 1581 de 2012 – Protección de Datos Personales

Esta ley establece los principios y procedimientos para garantizar la protección de los datos personales en el territorio nacional. Obliga a las entidades públicas a implementar medidas

técnicas y administrativas para evitar la pérdida, alteración o acceso no autorizado a la información de los ciudadanos. Su aplicación es especialmente relevante en instituciones que manejan bases de datos sensibles sin una estructura formal de seguridad informática (Congreso de la República de Colombia, 2012).

Ley 1273 de 2009 – Delitos Informáticos

Modifica el Código Penal colombiano para incluir delitos asociados al acceso abusivo a sistemas informáticos, la interceptación de datos y la violación de información personal o confidencial. Esta ley constituye la base jurídica que sanciona las acciones ilícitas relacionadas con la seguridad digital, y complementa las políticas preventivas impulsadas por el estado (Congreso de la República de Colombia, 2009).

Estrategia de Transformación Digital del Estado 2023–2026

Liderada por la Presidencia de la República, busca promover la interoperabilidad de los sistemas gubernamentales, la digitalización de trámites y la adopción de tecnologías seguras en las entidades públicas. Esta estrategia subraya la importancia de incorporar la ciberseguridad desde la planeación tecnológica institucional y de alinear los proyectos digitales con la Política Nacional de Seguridad Digital (Departamento Nacional de Planeación, 2024).

Situación Actual de la Organización en Materia de Seguridad Informática

La organización analizada es una entidad pública ubicada en Bogotá que depende administrativamente de un organismo del nivel central. Sus procesos misionales y administrativos se apoyan en diversas plataformas digitales para la gestión documental, la comunicación interna, la administración financiera y el seguimiento operativo. Sin embargo, el análisis realizado evidencia que la entidad presenta bajos niveles de madurez en seguridad informática, derivados de limitaciones de infraestructura, ausencia de políticas internas y una

fuerte dependencia tecnológica de servicios tercerizados. Los principales hallazgos identificados son los siguientes:

1. Ausencia de un área interna de tecnología

La entidad no cuenta con una unidad de TI propia. Las actividades de soporte, mantenimiento y administración de sistemas dependen totalmente de un proveedor externo. Esta situación dificulta la supervisión de incidentes, el control de cambios, la trazabilidad de las configuraciones y la gestión de riesgos tecnológicos.

2. Infraestructura tecnológica heterogénea

Conviven plataformas institucionales alojadas en servidores externos, aplicaciones ofimáticas basadas en la nube y sistemas locales antiguos que continúan operando debido a las necesidades de algunos procesos administrativos. La falta de integración y estandarización complica la administración y genera vulnerabilidades operativas.

3. Ausencia de políticas formales de ciberseguridad

No existen documentos institucionales sobre:

- Clasificación de la información
- Control de accesos
- Gestión de incidentes
- Continuidad del negocio,
- Gestión de riesgos tecnológicos.

Las prácticas actuales son operativas y no obedecen a un marco de gobernanza definido.

4. Controles básicos sin estandarización

El uso de contraseñas, restricciones de acceso y permisos diferenciados existe, pero no sigue lineamientos documentados, no se revisa periódicamente y no hay procesos formales de auditoría interna.

5. Capacitación limitada

El personal no recibe formación periódica en ciberseguridad. Las prácticas avanzadas (phishing, ingeniería social, identificación de incidentes, manejo adecuado de información sensible) no son conocidas por la mayoría de los funcionarios.

6. Dependencia de terceros para incidentes

Cuando ocurre un incidente técnico o de seguridad, la entidad depende exclusivamente del proveedor externo. Esto prolonga los tiempos de respuesta y reduce la capacidad institucional para gestionar riesgos.

Análisis Comparativo con Estándares y Buenas Prácticas Internacionales

Con el fin de identificar brechas y oportunidades de mejora, se realizó una comparación directa entre los controles de seguridad existentes en la organización y los controles propuestos por estándares internacionales de ciberseguridad, tales como ISO/IEC 27001:2022, ISO/IEC 27032:2023, NIST Cybersecurity Framework 2.0 (2024), COBIT 2019 y CIS Critical Security Controls v8.

El análisis se estructuró a partir de cuatro dimensiones clave: gobernanza, gestión del riesgo, controles de seguridad y gestión del personal. Para cada una de estas dimensiones, se contrastaron las prácticas actuales de la organización con los controles definidos en los marcos de referencia, con el propósito de identificar el nivel de alineación, las brechas existentes y las oportunidades de fortalecimiento institucional. Este enfoque permite evidenciar de manera explícita las diferencias entre los controles implementados actualmente y aquellos recomendados

por las buenas prácticas internacionales, facilitando la evaluación del nivel de madurez en ciberseguridad de la organización.

En la Tabla 4 se presenta una síntesis de esta comparación, destacando los aspectos clave en los que la organización presenta un menor grado de cumplimiento o requiere desarrollo adicional.

Tabla 4

Comparación de Controles de Seguridad: Situación Actual vs Estándares Internacionales

Control de seguridad	Implementación actual	Control según estándar	Brechas identificada
Gobernanza y políticas internas	No existen políticas formales ni roles definidos.	ISO 27001, COBIT 2019, Decreto 620/2020.	Crear políticas institucionales, definir roles, establecer un comité de seguridad.
Gestión del riesgo	No se realiza identificación, valoración ni documentación de riesgos digitales.	ISO 27005, NIST CSF (Identify).	Implementar un proceso de gestión de riesgos y definir controles prioritarios.
Control de accesos	Buenas prácticas informales, sin auditoría ni estándares.	CIS v8, ISO 27001 (Anexo A.5)	Estandarizar permisos, documentar privilegios, establecer revisiones periódicas.
Gestión de incidentes	No existe un procedimiento ni un equipo interno; depende del proveedor externo.	NIST CSF (Respond), ISO 27035.	Crear un protocolo interno, definir escalamiento y registrar incidentes.
Continuidad del negocio	No hay plan de continuidad ni recuperación ante desastres.	ISO 22301, ISO 27001 A.17.	Elaborar y probar un plan de continuidad, realizar simulacros.
Capacitación y cultura organizacional	Capacitación mínima; no hay programas regulares.	NIST CSF (Protect), CIS v8 – Awareness.	Implementar campañas periódicas, simulaciones de phishing, capacitaciones.
Gestión de proveedores	Alta dependencia tecnológica sin acuerdos de niveles de servicio específicos para seguridad.	ISO 27036, COBIT APO10.	Incluir cláusulas de seguridad, establecer métricas y revisiones periódicas.

Nota. Información elaborada con base en ISO/IEC 27001:2022, ISO/IEC 27032:2023, NIST CSF 2.0, COBIT 2019 y CIS Controls v8 y Política Nacional de Seguridad Digital (MinTIC, 2023).

Interpretación del Análisis Comparativo

El análisis comparativo de controles de seguridad evidencia que la organización presenta un nivel de madurez básico, con brechas significativas frente a los estándares internacionales evaluados. En términos generales, se observa una baja alineación entre los controles implementados actualmente y aquellos recomendados por marcos como ISO/IEC 27001, NIST CSF, COBIT 2019 y CIS Controls v8.

En la dimensión de gobernanza, la ausencia de políticas formales y de una estructura organizacional definida limita la implementación de controles estratégicos, lo cual contrasta con los lineamientos establecidos en ISO 27001 y COBIT. En cuanto a la gestión del riesgo, la inexistencia de procesos formales impide identificar, evaluar y mitigar amenazas de manera proactiva, en contraste con lo propuesto por NIST CSF (función Identify) y la norma ISO 27005.

Respecto a los controles técnicos, si bien existen prácticas básicas como el uso de contraseñas y restricciones de acceso, estas no se encuentran estandarizadas ni alineadas con controles específicos como los definidos en CIS Controls v8 o el Anexo A de ISO 27001. Asimismo, la gestión de incidentes y la continuidad del negocio presentan vacíos críticos frente a estándares como ISO 27035 e ISO 22301.

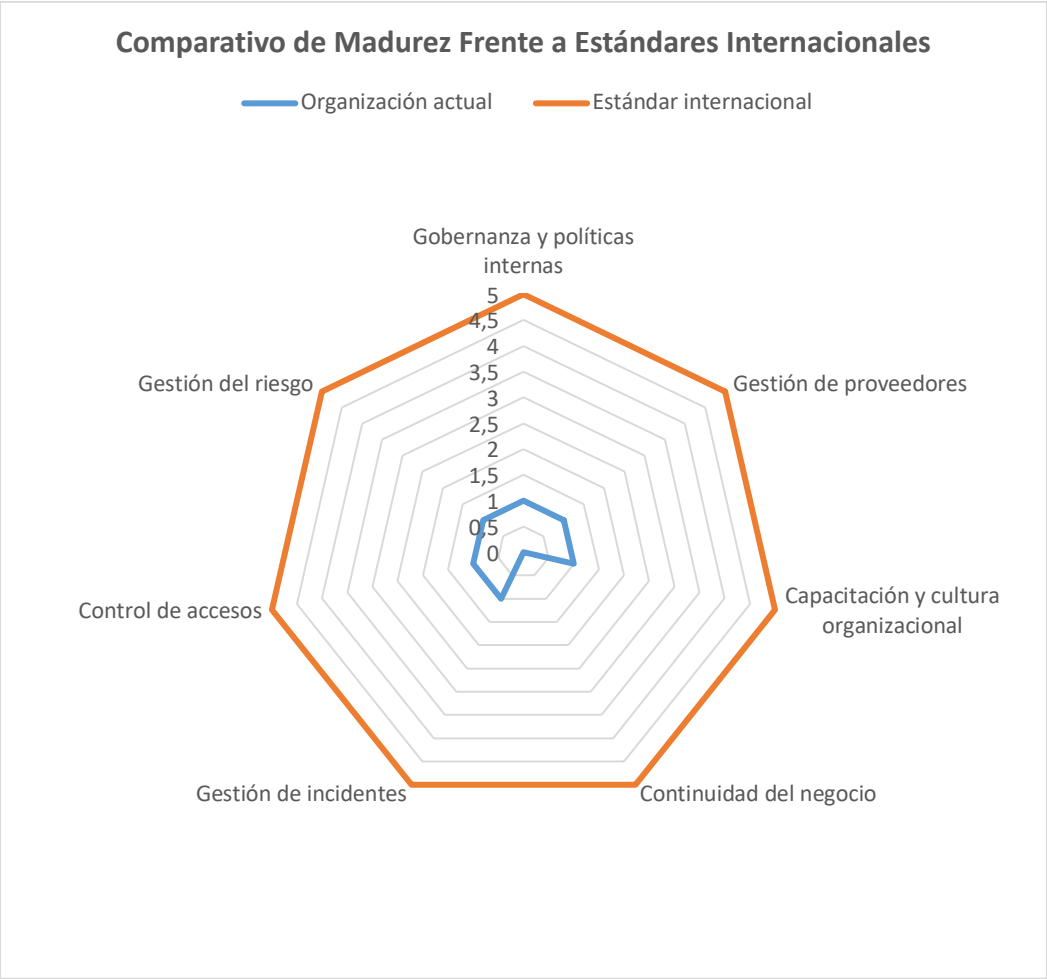
Finalmente, en la dimensión de gestión del personal, la ausencia de programas estructurados de capacitación contrasta con las recomendaciones de concientización y formación continua establecidas en los marcos internacionales. En conjunto, estas brechas evidencian la necesidad de fortalecer los controles de seguridad de manera progresiva, mediante la adopción de un enfoque basado en estándares, que permita mejorar la capacidad institucional para prevenir, detectar y responder a incidentes de ciberseguridad.

Adicionalmente, es importante señalar que la brecha identificada entre los controles actuales y los estándares internacionales no solo responde a limitaciones técnicas, sino también a factores organizacionales y de gestión. En el caso de la organización analizada, la ausencia de una estructura formal de gobernanza de tecnologías de la información y la dependencia de proveedores externos inciden directamente en la falta de implementación de controles alineados con buenas prácticas. Esta situación evidencia que la adopción de estándares como ISO/IEC 27001 o NIST CSF no depende exclusivamente de recursos tecnológicos, sino también de la capacidad institucional para definir políticas, asignar responsabilidades y establecer procesos de seguimiento. En este sentido, la complejidad técnica identificada en el apartado anterior se refleja en la dificultad para operacionalizar controles de seguridad de manera estructurada y sostenible.

Como se observa en la Figura 3, la organización presenta niveles de madurez bajos en todos los dominios evaluados, especialmente en gobernanza tecnológica, respuesta a incidentes y gestión de riesgos. Esta brecha significativa frente a los estándares internacionales evidencia la necesidad de adoptar políticas institucionales, mecanismos de gestión del riesgo y procesos de capacitación que permitan avanzar hacia una postura de seguridad más sólida.

Figura 3

Comparativo de Madurez en Ciberseguridad entre la Organización y los Estándares Internacionales



Nota. Comparación elaborada con base en ISO/IEC 27001:2022, NIST (2023), COBIT 2019 y CIS v8.

Plan de Implementación Gradual para el Fortalecimiento de la Ciberseguridad Institucional

Con base en las brechas identificadas en el análisis comparativo de controles de seguridad, se propone un plan de implementación gradual estructurado en tres fases. Este plan

prioriza el fortalecimiento progresivo de la gobernanza, la gestión del riesgo y los controles técnicos, alineado con estándares internacionales como ISO/IEC 27001, NIST CSF y COBIT 2019.

La propuesta responde directamente a las debilidades detectadas en la organización, particularmente en la ausencia de políticas formales, la limitada gestión del riesgo, la dependencia tecnológica de terceros y la falta de capacidades internas en ciberseguridad. Su implementación permite avanzar de un enfoque reactivo hacia un modelo preventivo, estructurado y sostenible.

Tabla 5

Fases del Plan de Implementación para el Fortalecimiento de la Ciberseguridad Institucional

Fase	Objetivo	Acciones principales	Resultado esperado
Fase 1 – Fortalecimiento normativo y de gobernanza (0-6 Meses)	Establecer los lineamientos institucionales mínimos para la gestión de la seguridad de la información y crear la estructura básica de gobernanza interna.	- Elaborar y aprobar políticas internas de seguridad (clasificación de la información, control de accesos, gestión de incidentes, uso aceptable). - Definir roles y responsabilidades en materia de seguridad digital. - Crear el Comité de Seguridad de la Información. • Iniciar el proceso básico de gestión de riesgos siguiendo ISO 27005 o NIST CSF (Identify). - Formalizar acuerdos operativos mínimos con proveedores tecnológicos.	- Existencia de políticas formales aprobadas - Roles y responsabilidades definidos - Primer mapa de riesgos identificado - Base inicial de gobernanza establecida
Fase 2 – Fortalecimiento técnico y operativo (6–12 meses)	Implementar controles esenciales para reducir vulnerabilidades y mejorar la capacidad de respuesta ante incidentes.	- Implementar controles prioritarios del CIS v8 (gestión de activos, control de privilegios, protección de endpoints). - Establecer un procedimiento interno de gestión de incidentes basado en ISO 27035.	- Controles técnicos básicos implementados - Procedimientos documentados de incidentes - Accesos controlados y auditables

Fase	Objetivo	Acciones principales	Resultado esperado
		- Estandarizar y auditar los accesos de usuarios y permisos sobre información crítica. - Implementar planes de respaldo y pruebas periódicas. - Integrar cláusulas de seguridad en los contratos con proveedores y establecer métricas de cumplimiento. - Crear o fortalecer un equipo interno responsable de la seguridad de la información.	- Reducción de vulnerabilidades operativas
Fase 3 – Madurez institucional (12–24 meses)	Consolidar las capacidades de ciberseguridad, mejorar la autonomía institucional y garantizar la continuidad operativa.	- Implementar un Plan de Continuidad del Negocio y de Recuperación ante Desastres (BCP–DRP). - Establecer monitoreo continuo de eventos de seguridad. - Realizar auditorías internas anuales alineadas con ISO 27001. - Desarrollar un ciclo de mejora continua para la gestión de riesgos y la actualización de controles.	- Sistema de gestión de seguridad más estructurado - Capacidad de respuesta autónoma - Continuidad operativa garantizada - Cultura organizacional de seguridad consolidada

Nota. Información elaborada con base en ISO 27001:2022, NIST CSF 2.0 y COBIT 2019.

La implementación progresiva de este plan permitirá que la organización evolucione desde un modelo reactivo hacia un enfoque preventivo y basado en la gestión del riesgo. Asimismo, facilita la alineación de los controles de seguridad con estándares internacionales y fortalece la capacidad institucional para prevenir, detectar y responder a incidentes de ciberseguridad.

Desde una perspectiva estratégica, el éxito del plan dependerá no solo de la adopción de herramientas tecnológicas, sino también del compromiso institucional, la asignación de responsabilidades y la consolidación de una cultura organizacional orientada a la seguridad de la

información. En este sentido, la gobernanza, la capacitación del personal y el monitoreo continuo se constituyen en elementos clave para garantizar la sostenibilidad de las acciones propuestas.

Limitaciones Técnicas, Organizacionales y de Gestión que Inciden en la Seguridad Informática

A partir del análisis comparativo realizado previamente, se identificó que la organización objeto de estudio presenta brechas significativas frente a los estándares internacionales y nacionales de ciberseguridad. Estas brechas no se originan únicamente en factores tecnológicos, sino también en carencias estructurales, organizacionales y de gestión, que limitan la adopción efectiva de prácticas seguras y sostenibles.

Limitaciones Técnicas

Las limitaciones técnicas se relacionan con la infraestructura tecnológica, el soporte operativo, la interoperabilidad de plataformas y la disponibilidad de herramientas adecuadas para la gestión de la seguridad digital. Leguizamón y Galindo (2021) señalan que muchas instituciones públicas colombianas operan con sistemas legados y plataformas desactualizadas, lo que incrementa las vulnerabilidades y dificulta la implementación de políticas modernas de seguridad. De igual forma, Ávalos, Castilla y Gordillo (2023) identifican que la dependencia de proveedores externos para el soporte técnico genera una falta de control sobre la administración de los activos tecnológicos.

En el caso de la organización estudiada, no existe un equipo interno especializado que administre de manera integral los sistemas informáticos. La infraestructura se compone de equipos y plataformas heterogéneas, muchas de ellas sin actualizaciones periódicas. Rivas Turcios y Esquivel Mejía (2025) advierten que la ausencia de herramientas automatizadas para la detección y monitoreo de incidentes incrementa el riesgo operativo y retrasa la respuesta ante ciberataques. Aunque se realizan copias de seguridad externas, no existen pruebas regulares de restauración, lo cual constituye una debilidad crítica. Asimismo, Medina (2023) indica que la

falta de interoperabilidad entre sistemas institucionales genera duplicidad de información, retrasa procesos administrativos y aumenta la complejidad operativa.

En síntesis, las limitaciones técnicas están relacionadas con la infraestructura, la arquitectura tecnológica, las herramientas disponibles y los mecanismos de protección digital con los que cuenta la organización. Entre las principales se identifican:

a. Infraestructura tecnológica fragmentada

La organización utiliza plataformas digitales que dependen completamente de los servicios del Ministerio al cual está adscrita. Esto genera un ecosistema tecnológico heterogéneo en el que coexisten aplicaciones institucionales, sistemas heredados y herramientas externas sin una integración plena. Esta fragmentación dificulta la trazabilidad, el monitoreo y la identificación de riesgos de seguridad.

b. Ausencia de políticas técnicas de control

No existen lineamientos formales sobre:

- actualización de software,
- gestión de parches,
- uso de contraseñas,
- cifrado de información,
- respaldo de datos,
- control de accesos.

Esto implica que las configuraciones técnicas dependen de prácticas individuales y no de protocolos institucionales.

c. Falta de herramientas de monitoreo y alertamiento

La organización no cuenta con:

- sistemas SIEM,
- mecanismos centralizados de logs,
- herramientas de detección de intrusiones,
- monitoreo en tiempo real.

La visibilidad del estado de seguridad es mínima, lo que obstaculiza la detección temprana de incidentes.

d. Dependencia total de proveedores y del Ministerio

Cualquier ajuste técnico, mantenimiento, actualización o corrección debe solicitarse al Ministerio de Hacienda, pues la organización no cuenta con personal especializado propio. Esto genera tiempos de atención prolongados y una limitada capacidad de reacción.

Limitaciones Organizacionales

Las limitaciones organizacionales se vinculan con la estructura interna, la cultura institucional y la ausencia de liderazgo en temas de seguridad digital. Villa et al. (2023) señalan que la mayoría de entidades públicas carecen de estructuras administrativas formales para la gestión de TI, lo que lleva a que las decisiones de seguridad recaigan en personal no especializado. Esta situación se replica en la organización analizada, donde no existe una unidad de tecnología definida ni un responsable institucional de ciberseguridad. Asimismo, Peña (2022) advierte que la falta de gobernanza tecnológica y liderazgo institucional genera desarticulación entre las áreas administrativas y técnicas, dificultando la coordinación y la priorización de recursos. Estas limitaciones se relacionan con la estructura interna, la asignación de responsabilidades, los procesos administrativos y la disponibilidad de recursos.

a. Inexistencia de un área de tecnología interna

La organización no cuenta con una oficina de TI, un responsable de seguridad de la información ni un comité que articule los temas tecnológicos. Esto provoca vacíos en:

- liderazgo,
- supervisión,
- planeación estratégica,
- toma de decisiones.

b. Falta de gobernanza digital clara

No existe un modelo de gobernanza que defina roles como:

- custodios de la información,
- propietarios de procesos,
- responsables de seguridad digital,
- administradores de accesos.

Esta ausencia dificulta la claridad en las responsabilidades y la rendición de cuentas.

c. Escasa cultura institucional de seguridad

Los funcionarios no cuentan con prácticas estandarizadas relacionadas con:

- protección de contraseñas,
- manejo seguro de información,
- almacenamiento adecuado de documentos,
- prevención del phishing

La ciberseguridad se percibe como un asunto técnico, y no como una responsabilidad transversal.

d. Procesos manuales y falta de integración

Muchos procedimientos administrativos siguen siendo manuales, lo que incrementa:

- la posibilidad de errores,
- la duplicación de datos,
- la falta de trazabilidad en actividades críticas.

Limitaciones de Gestión

Las limitaciones de gestión se refieren a la planificación, asignación de recursos y control de los procesos de mejora continua en materia de seguridad digital. Ávalos et al. (2023) señalan que una de las mayores debilidades del sector público es la falta de políticas y procedimientos documentados de ciberseguridad, así como la inexistencia de indicadores que midan su efectividad. En la organización analizada, no existen planes estratégicos de seguridad ni políticas formales de gestión de riesgos tecnológicos. La ausencia de auditorías y de seguimiento institucional debilita la capacidad para priorizar acciones preventivas. Medina (2023) sostiene que la baja prioridad que se otorga a la ciberseguridad dentro de la planificación institucional deriva en una gestión reactiva frente a los incidentes.

Por otro lado, Villa et al. (2023) subrayan que la falta de presupuesto y personal capacitado en seguridad digital impide avanzar hacia niveles de madurez más altos. En la entidad estudiada, Las limitaciones de gestión están asociadas a la planeación, la toma de decisiones, las políticas internas y el cumplimiento normativo

a. Ausencia de políticas internas de seguridad

No existe un conjunto formal de políticas institucionales que regulen:

- seguridad digital
- uso aceptable de la información
- clasificación de datos
- continuidad del negocio

- tratamiento de incidentes

La organización depende casi por completo de las políticas del Ministerio, pero no tiene lineamientos propios adaptados a su realidad.

b. Falta de un modelo de gestión del riesgo tecnológico

No hay un proceso sistemático para:

- identificar vulnerabilidades,
- evaluar su impacto,
- priorizar amenazas,
- asignar recursos de mitigación.

Sin gestión del riesgo no es posible tomar decisiones estratégicas informadas.

c. Ausencia de un plan de continuidad del negocio

No existen directrices sobre:

- recuperación ante desastres,
- procedimientos de respaldo,
- restauración de servicios críticos,
- tiempos máximos de recuperación (RTO / RPO).

Esto aumenta la vulnerabilidad ante fallas técnicas o incidentes de ciberseguridad.

d. Capacitación limitada en seguridad digital

Aunque la entidad recibe lineamientos del Ministerio, no desarrolla programas de capacitación propios. Esto acentúa la dependencia tecnológica y limita la apropiación de buenas prácticas por parte del personal.

Tabla 6

Principales Limitaciones que Afectan la Seguridad Informática en la Organización

Tipo de Limitación	Descripción / Evidencia	Impacto en la Seguridad Informática
Técnica	Infraestructura tecnológica fragmentada: coexistencia de sistemas heredados, aplicaciones del Ministerio y plataformas externas sin integración centralizada.	Incrementa la vulnerabilidad y el tiempo de respuesta ante incidentes.
Tecnica	Ausencia de herramientas de monitoreo y alertamiento: no existen sistemas SIEM, IDS/IPS o análisis centralizado de logs.	Reduce la capacidad de detectar incidentes oportunamente y aumenta el riesgo de ataques no identificados.
Tecnica	Dependencia total de proveedores y del Ministerio para actualizaciones, soporte técnico y gestión operativa.	Limita la capacidad de respuesta ante incidentes y genera retrasos críticos al depender de terceros.
Organizativo	Inexistencia de un área de TI o responsable de seguridad dentro de la entidad.	Falta de liderazgo, coordinación y supervisión en temas de ciberseguridad.
Organizativo	Escasa cultura institucional de seguridad: prácticas insuficientes de protección de contraseñas, manejo de datos y prevención de ataques.	Mayor probabilidad de incidentes por error humano o desconocimiento de riesgos.
Organizativo	Procesos manuales y baja integración digital, lo que produce duplicidad de información y baja trazabilidad.	Incrementa el riesgo de pérdida o manipulación no intencionada de información sensible.
De gestion	Ausencia de políticas internas de seguridad de la información, como uso aceptable, clasificación de datos o plan de contingencia.	Falta de lineamientos claros para la protección de activos digitales y cumplimiento normativo.
De gestion	Falta de un modelo formal de gestión del riesgo tecnológico.	La organización opera sin identificar amenazas prioritarias, sin evaluación de impacto ni medidas de mitigación.
De gestion	No existe un plan de continuidad del negocio ni procedimientos de recuperación ante desastres (RTO/RPO).	Alta vulnerabilidad ante fallas técnicas, incidentes cibernéticos o interrupciones prolongadas del servicio.
De gestion	Capacitación limitada en seguridad digital, dependiente únicamente de lineamientos generales externos.	Los funcionarios no adoptan buenas prácticas, aumentando la exposición a ataques como phishing, malware o fuga de datos.

Nota. Información elaborada con base en Leguizamón y Galindo (2021), Rivas Turcios y Esquivel Mejía (2025), Villa et al. (2023), Peña Barranco (2022), Ávalos et al. (2023), Medina (2023) y observaciones del caso de estudio.

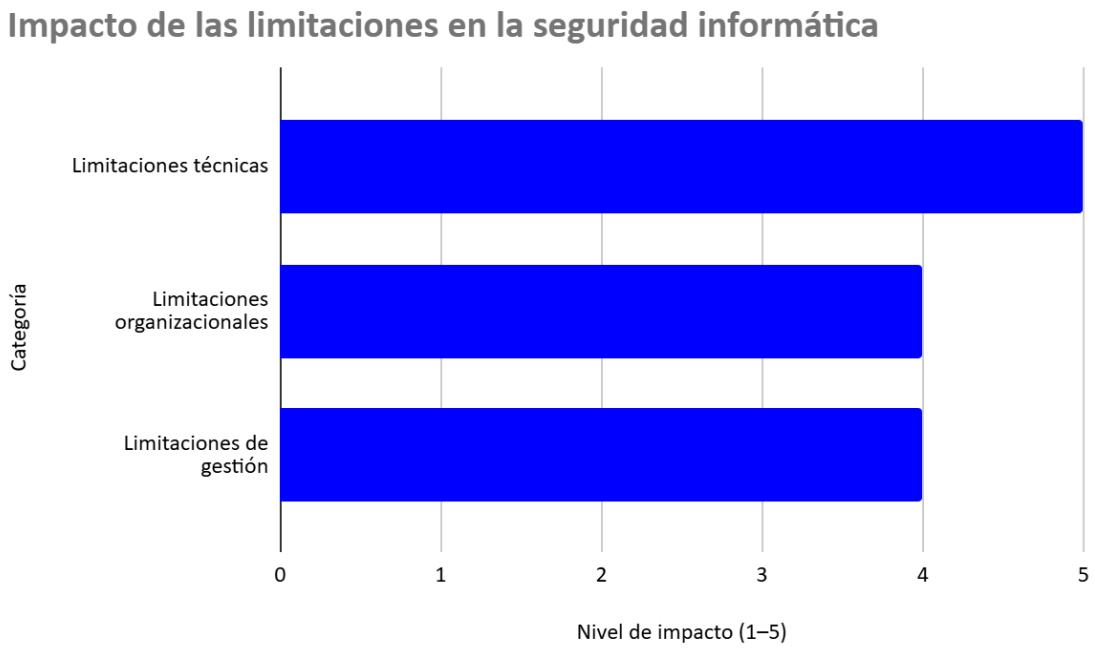
El análisis demuestra que la seguridad informática de la organización está condicionada por tres factores clave:

- Limitaciones técnicas: infraestructura fragmentada, ausencia de herramientas de monitoreo y dependencia total de proveedores.
- Limitaciones organizacionales: falta de gobernanza digital y debilidades en la cultura institucional de seguridad.
- Limitaciones de gestión: inexistencia de políticas internas, ausencia de gestión del riesgo y falta de un plan de continuidad.

Con base en el análisis de las limitaciones técnicas, organizacionales y de gestión, se elaboró una representación visual que permite sintetizar el nivel de impacto que cada categoría ejerce sobre la seguridad informática de la organización. Este ejercicio busca facilitar la comprensión de los factores más críticos y su relación con la vulnerabilidad institucional, evidenciando que las debilidades no solo se originan en el ámbito tecnológico, sino también en aspectos estructurales y administrativos que afectan la capacidad de respuesta y resiliencia digital.

Figura 4

Nivel de Impacto de las Limitaciones Técnicas, Organizacionales y de Gestión en la Seguridad Informática



Nota. Resultados obtenidos a partir del análisis documental desarrollado en el estudio.

La Figura 4 presenta una síntesis de las limitaciones que afectan la seguridad informática en la organización. Se observa que las limitaciones técnicas presentan el mayor nivel de impacto (valor cercano a 5), lo que indica que las deficiencias en infraestructura, herramientas o recursos tecnológicos afectan de forma significativa la seguridad informática institucional. Las limitaciones organizacionales y las de gestión muestran un impacto ligeramente menor (alrededor de 4), aunque siguen siendo factores críticos que pueden comprometer la efectividad de las políticas y los controles de seguridad. En conjunto, los resultados evidencian que la seguridad informática no solo depende de los recursos tecnológicos, sino también de la gestión adecuada y del compromiso organizacional para mitigar las vulnerabilidades.

El análisis realizado evidencia que las limitaciones que afectan la seguridad informática de la organización no se originan únicamente en la infraestructura tecnológica, sino que responden a un conjunto de factores estructurales, organizacionales y de gestión que incrementan su exposición al riesgo digital. La ausencia de un área responsable de tecnología, la dependencia casi total de proveedores externos, la falta de políticas internas y un modelo incipiente de gestión del riesgo demuestran que el problema central no es tecnológico, sino de gobernanza institucional. Asimismo, la baja cultura de seguridad y la escasez de procesos estandarizados dificultan la adopción de buenas prácticas y reducen la capacidad de detectar y responder oportunamente a incidentes. Superar estas limitaciones requiere una estrategia integral que articule fortalecimiento organizacional, definición clara de responsabilidades, desarrollo de capacidades internas y la implementación gradual de controles alineados con los estándares internacionales de ciberseguridad.

Recomendaciones Estratégicas para el Fortalecimiento de la Ciberseguridad Institucional

El análisis realizado a lo largo del estudio permitió identificar brechas significativas en materia de gobernanza, gestión del riesgo, control de accesos, continuidad del negocio, capacitación y supervisión de proveedores. Estas brechas afectan directamente la confidencialidad, integridad y disponibilidad de la información institucional. Por ello, este apartado presenta un conjunto de recomendaciones estratégicas orientadas a fortalecer la madurez de la organización en seguridad de la información y servir como referencia para la formulación de políticas internas y planes de mejora.

Las recomendaciones se agrupan en tres ejes fundamentales: (1) Gobernanza y políticas institucionales, (2) Gestión del riesgo y respuesta a incidentes, y (3) Desarrollo de capacidades internas y cultura organizacional. Cada eje responde directamente a las limitaciones identificadas en el análisis previo y se articula con estándares internacionales como ISO/IEC 27001:2022, NIST CSF 2.0, COBIT 2019 y CIS v8.

Además, las acciones propuestas cumplen con la normativa nacional vigente, incluyendo la Ley 1273 de 2009, la Ley 1581 de 2012, el Decreto 620 de 2020 y la Política Nacional de Seguridad Digital 2023–2030.

Eje 1 – Gobernanza y políticas institucionales

El primer eje se centra en crear las bases organizacionales para una gestión de seguridad sólida y sostenible. Actualmente, la organización presenta ausencia de políticas internas, falta de roles definidos y un modelo de seguridad reactivo. Para superar estas brechas se propone:

Recomendaciones estratégicas

1. Creación de un Comité Institucional de Seguridad de la Información.

- Integrado por directivos, área jurídica, talento humano y líderes de proceso.
- Responsables de la toma de decisiones, priorización de riesgos y seguimiento a las políticas.
- Alineado con el Modelo Integrado de Planeación y Gestión (MIPG).

2. Diseño e implementación de un Marco Interno de Seguridad de la Información.

Debe incluir:

- Política de Seguridad de la Información.
- Política de Gestión de Riesgos Digitales.
- Política de Uso Aceptable de Recursos Informáticos.
- Política de Continuidad del Negocio y Recuperación ante Desastres.

Estas políticas deben ser aprobadas por la alta dirección y actualizadas cada año.

3. Definición formal de roles y responsabilidades.

- Responsable institucional de seguridad de la información (equivalente a un CISO institucional, aunque sea delegado).
- Responsables de custodia de información por proceso.
- Líder de continuidad operativa.

4. Integración de la seguridad de la información al planeamiento institucional.

- Incluir metas de seguridad digital en el Plan de Acción Institucional.
- Incorporar indicadores de desempeño en seguridad.

Eje 2 – Gestión del riesgo y Respuesta Ante Incidentes

El diagnóstico mostró ausencia de metodologías de riesgo, inexistencia de inventarios, controles débiles de acceso y falta de protocolos de incidentes. Este eje busca fortalecer la postura de defensa institucional.

Recomendaciones estratégicas

1. Implementación de un proceso formal de gestión del riesgo digital.

Basado en ISO/IEC 27005 o NIST CSF, incluye:

- Inventario de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Valoración del riesgo institucional.
- Plan de tratamiento del riesgo con responsables y fechas.

2. Fortalecimiento del control de accesos.

- Políticas de contraseñas robustas.
- Eliminación de cuentas inactivas.
- Asignación de permisos por rol (principio de mínimo privilegio).
- Registro de accesos críticos.

3. Establecimiento del Protocolo Institucional de Respuesta a Incidentes.

Debe contemplar:

- Clasificación de incidentes.
- Rutas de comunicación y reporte.
- Procedimientos de contención y mitigación.
- Registro centralizado de incidentes.
- Acciones posts-incidentes (lecciones aprendidas).

4. Elaboración del Plan de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP).

Incluye:

- Identificación de procesos críticos.
- Definición de RTO (tiempo máximo de recuperación) y RPO (pérdida máxima tolerable).
- Procedimientos alternos para garantizar continuidad operativa.
- Simulacros dos veces al año.

5. Supervisión de proveedores tecnológicos.

- Revisar contratos y exigir cláusulas de seguridad y confidencialidad.
- Monitorear los tiempos de respuesta, niveles de servicio y controles aplicados por el proveedor.
- Solicitar evidencias de buenas prácticas (por ejemplo, cumplimiento ISO 27001 del proveedor).

Eje 3 – Desarrollo de Capacidades y Cultura Organizacional

El análisis evidenció escasa cultura de seguridad y falta de programas de formación, lo cual es una de las principales causas de incidentes en entidades públicas.

Recomendaciones estratégicas

1. Programa permanente de capacitación y sensibilización.

- Formación básica para todo el personal (phishing, contraseñas, protección de datos).
- Capacitación avanzada para quienes gestionan información sensible.
- Campañas trimestrales de cultura organizacional en seguridad digital.

2. Definición de un plan anual de formación en ciberseguridad.

- Vinculado al Plan Institucional de Capacitación (PIC).
- Priorizar competencias en gestión del riesgo, manejo seguro de información y continuidad operativa.

3. Creación de una guía de buenas prácticas de seguridad digital.

- Orientada a usuarios no técnicos.
- Incluir lineamientos sobre uso de correo, documentos sensibles, movilidad, autenticación y manejo de incidentes.

4. Promoción de una cultura de corresponsabilidad.

- Recordatorios institucionales mensuales.
- Mensajes de la alta dirección resaltando la importancia de la seguridad.
- Reconocimiento a buenas prácticas.

Las recomendaciones estratégicas formuladas en este apartado se organizan en tres ejes que responden directamente a las brechas identificadas en la organización: gobernanza institucional, gestión del riesgo y fortalecimiento de capacidades internas. Cada eje integra acciones prioritarias que permiten orientar la toma de decisiones y guiar el diseño de políticas internas de seguridad de la información. A continuación, se presenta una síntesis general de estas recomendaciones.

Tabla 7

Síntesis de Recomendaciones Estratégicas por Eje de Acción

Eje Estratégico	Objetivo Principal	Recomendaciones Clave
Gobernanza y políticasinstitucional.	Establecer una estructura organizacional y normativa que permita gestionar la seguridad de la información de forma planificada, consistente y alineada con los marcos internacionales.	• Crear el Comité Institucional de Seguridad de la Información. • Diseñar e implementar un Marco Interno de Seguridad (políticas de seguridad, riesgos, uso aceptable, continuidad). • Definir roles y responsabilidades (responsable institucional de seguridad, custodios de información, líder de continuidad). • Integrar objetivos e indicadores de seguridad en la planeación estratégica institucional.
Gestión del riesgo y respuesta ante incidentes.	Fortalecer la capacidad institucional para prevenir, detectar, mitigar y recuperar incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.	• Implementar un proceso formal de gestión del riesgo digital (inventario de activos, valoración y tratamiento). • Robustecer los controles de acceso (mínimo privilegio, cuentas inactivas, contraseñas robustas). • Crear el Protocolo Institucional de Respuesta a Incidentes. • Elaborar el Plan de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP). • Fortalecer el control y supervisión de proveedores tecnológicos, incorporando cláusulas de seguridad y niveles de servicio.
Capacidades Internas y Cultura Organizacional	Desarrollar competencias técnicas y promover una cultura de seguridad que reduzca el riesgo humano y fortalezca la protección institucional de forma sostenible.	• Implementar un programa permanente de sensibilización y capacitación. • Incluir la formación en ciberseguridad dentro del Plan Institucional de Capacitación (PIC). • Crear una guía de buenas prácticas de seguridad para usuarios. • Establecer iniciativas de cultura organizacional y corresponsabilidad (campañas internas, mensajes de la dirección, recordatorios).

Nota. Síntesis construida con base en ISO/IEC 27001, ISO 27005, NIST CSF 2.0, ISO 27035, COBIT 2019 y Política Nacional de Seguridad Digital (MinTIC, 2023–2030).

La tabla anterior consolida los lineamientos esenciales para fortalecer la seguridad digital de la organización, articulando acciones de corto, mediano y largo plazo que contribuyen al

mejoramiento progresivo de la confidencialidad, integridad y disponibilidad de la información. Estas recomendaciones constituyen la base para el desarrollo de políticas internas, planes de mejora y procesos de gobernanza alineados con los estándares internacionales de ciberseguridad.

Verificación de Alineación Normativa

Las recomendaciones propuestas cumplen con el marco normativo colombiano aplicable a la protección de la información y la seguridad digital en entidades públicas. Específicamente, se alinean con los siguientes instrumentos:

- Ley 1273 de 2009: protección de datos y penalización de accesos no autorizados.
- Ley 1581 de 2012: principios y obligaciones en el tratamiento de datos personales.
- Decreto 620 de 2020: lineamientos para la seguridad digital en el Estado y gestión del riesgo tecnológico.
- Política Nacional de Seguridad Digital 2023–2030: fortalecimiento de capacidades, gobernanza y resiliencia digital.
- Estrategia de Transformación Digital 2023–2026: integración segura de la tecnología, interoperabilidad y protección de activos.

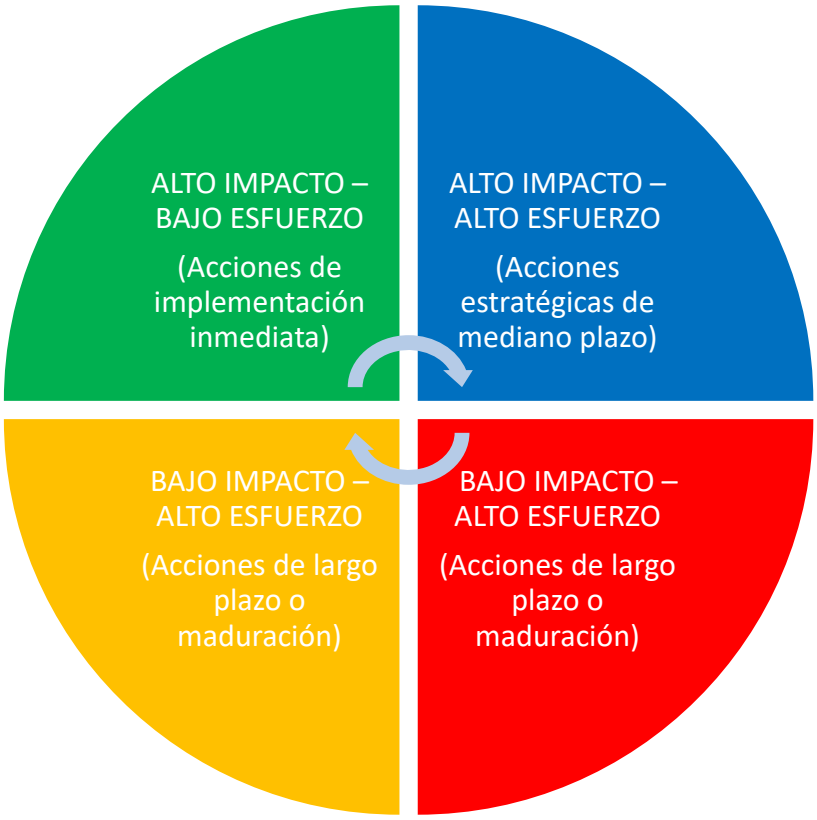
La coherencia con estas normas garantiza que las acciones propuestas puedan incorporarse formalmente dentro del marco institucional sin contravenir disposiciones legales vigentes y contribuyendo a elevar el nivel de madurez en seguridad digital.

Priorización Estratégica de Recomendaciones (Matriz Impacto–Esfuerzo)

Para complementar las recomendaciones estratégicas propuestas y facilitar su aplicación práctica dentro de la organización, se elaboró una matriz de priorización basada en los criterios de impacto y esfuerzo.

Figura 5

Matriz de Priorización de Recomendaciones Estratégicas (Impacto vs. Esfuerzo)



Nota. Priorización construida con base en el análisis de brechas institucionales y en los marcos ISO 27001:2022, NIST CSF 2.0, COBIT 2019 y CIS v8.

Esta matriz permite clasificar las acciones según su relevancia institucional y los recursos necesarios para su implementación, lo cual contribuye a definir un orden lógico y gradual de ejecución. De esta manera, la organización podrá enfocar primero las iniciativas de mayor beneficio y menor complejidad, avanzando progresivamente hacia intervenciones de mediano y largo plazo.

Descripción de los Cuadrantes de Priorización

Cuadrante 1: Alto Impacto / Bajo Esfuerzo. (Acciones de implementación inmediata)

- Creación del Comité Institucional de Seguridad de la Información.
- Actualización de políticas y lineamientos internos.
- Definición de roles y responsabilidades relacionados con la seguridad de la información.
- Elaboración del inventario de sistemas, datos y proveedores tecnológicos.

Cuadrante 2: Alto Impacto / Alto Esfuerzo. (Acciones estratégicas de mediano plazo)

- Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Integración progresiva de plataformas y sistemas digitales.
- Diseño e implementación del Plan de Continuidad del Negocio y Recuperación ante Desastres.
- Adopción de controles avanzados: MFA, monitoreo, hardening, gestión de vulnerabilidades.

Cuadrante 3: Bajo Impacto / Bajo Esfuerzo. (Acciones complementarias de apoyo)

- Capacitaciones iniciales en buenas prácticas digitales.
- Campañas institucionales de sensibilización.
- Actualización general de contraseñas, privilegios y accesos básicos.

Cuadrante 4: Bajo Impacto / Alto Esfuerzo (Acciones de maduración a largo plazo)

- Automatización y optimización de procesos digitales.
- Implementación de herramientas SIEM o servicios SOC (si aplica).
- Migración progresiva hacia arquitectura Zero Trust.

- Consolidación gradual de un equipo interno de TI o reforzamiento de la capacidad técnica institucional.

En conjunto, este estudio permitió comprender cómo la complejidad técnica, la ausencia de gobernanza digital y las limitaciones institucionales se convierten en factores determinantes que afectan la seguridad informática en las entidades públicas colombianas. A partir del análisis del caso seleccionado y de la comparación con los principales estándares internacionales, se evidenció la necesidad urgente de fortalecer la gestión de la ciberseguridad mediante políticas claras, capacidades internas y la adopción progresiva de buenas prácticas. Si bien el alcance metodológico fue documental, los hallazgos ofrecieron una base sólida para orientar acciones institucionales y futuras investigaciones. Con ello, se espera que los resultados aquí expuestos contribuyan al fortalecimiento de la seguridad digital en el sector público y sirvan como referencia para la construcción de estrategias que promuevan una gestión más segura, madura y resiliente de la información institucional.

Conclusiones

La investigación permitió determinar que la complejidad técnica incide de manera directa y significativa en la seguridad de los procesos digitales de la organización analizada, al incrementar la exposición a vulnerabilidades, dificultar la gestión de riesgos y limitar la capacidad institucional para prevenir, detectar y responder ante incidentes de ciberseguridad. Esta incidencia se manifiesta principalmente en la fragmentación de los sistemas, la dependencia tecnológica de terceros, la ausencia de un área interna de tecnologías de la información y la falta de políticas formales de seguridad, lo que configura un entorno con bajo nivel de control y alta probabilidad de fallos operativos y de seguridad.

El análisis realizado permitió evidenciar que la organización opera en un entorno digital caracterizado por una alta complejidad técnica, derivada de factores como la infraestructura tecnológica heterogénea, la limitada gobernanza institucional y las restricciones organizacionales. Estos elementos generan un nivel de madurez bajo en ciberseguridad y un incremento significativo en la exposición a riesgos, situación que coincide con las problemáticas identificadas en otras entidades del sector público colombiano.

La comparación entre los controles actuales de la organización y los establecidos en estándares internacionales como ISO/IEC 27001:2022, NIST CSF 2.0, COBIT 2019 y CIS Controls v8 evidenció brechas relevantes en gobernanza, gestión del riesgo, control de accesos, monitoreo de incidentes, continuidad del negocio y cultura organizacional. Aunque existen controles básicos en operación, estos se aplican de manera reactiva y sin un marco de gestión estructurado, lo que limita la efectividad de la seguridad de la información.

Asimismo, se identificaron limitaciones organizacionales, técnicas y de gestión que afectan directamente la seguridad institucional, tales como la falta de roles definidos, la ausencia

de procedimientos documentados, la inexistencia de métricas de seguridad y la carencia de mecanismos formales de seguimiento. Estos hallazgos evidencian que la problemática no es exclusivamente tecnológica, sino también estratégica y administrativa.

En respuesta a la problemática identificada, se formularon recomendaciones estratégicas orientadas a la creación y fortalecimiento de políticas internas de ciberseguridad, estructuradas en tres ejes principales: (i) fortalecimiento de la gobernanza institucional mediante la definición de roles, políticas y estructuras de decisión; (ii) implementación de un enfoque de gestión del riesgo alineado con estándares internacionales; y (iii) desarrollo de capacidades organizacionales, incluyendo capacitación del personal, formalización de procesos y mejora en la gestión de incidentes. Estas recomendaciones permiten orientar la construcción de un modelo de seguridad más estructurado, coherente y sostenible.

Finalmente, se concluye que el fortalecimiento de la seguridad de los procesos digitales en la organización requiere un enfoque integral que articule la gestión de la complejidad técnica con la gobernanza institucional y la adopción de buenas prácticas internacionales. La seguridad de la información no depende únicamente de herramientas tecnológicas, sino de la capacidad organizacional para gestionar riesgos, coordinar procesos, asignar responsabilidades y consolidar una cultura de seguridad digital. Avanzar en estas líneas permitirá mejorar la resiliencia institucional, garantizar la protección de la información y responder de manera más efectiva a los desafíos del entorno digital en el sector público colombiano.

Limitaciones del Estudio y Futuras Líneas de Investigación

El presente estudio permitió analizar la relación entre la complejidad técnica y la seguridad de los procesos digitales en una organización del sector público; sin embargo, presenta algunas limitaciones asociadas al enfoque metodológico y a las condiciones de acceso a la información.

En primer lugar, la investigación se desarrolló bajo un enfoque cualitativo, de tipo documental y descriptivo. En consecuencia, no se realizaron validaciones empíricas mediante pruebas técnicas especializadas, como auditorías de seguridad, pruebas de penetración o análisis forense digital. Esta limitación restringe la verificación directa del nivel de eficacia de los controles existentes y del grado real de exposición a vulnerabilidades en la infraestructura tecnológica de la entidad.

En segundo lugar, el análisis de la organización se basó en información secundaria y en la caracterización general de sus condiciones tecnológicas y organizacionales. Debido a criterios de confidencialidad institucional, no fue posible identificar explícitamente la entidad ni profundizar en aspectos operativos específicos. Aunque esto limita el nivel de detalle del estudio de caso, también favorece la aplicabilidad de los resultados, en la medida en que las brechas identificadas responden a patrones comunes en entidades públicas con alta complejidad técnica y dependencia tecnológica.

Asimismo, la ausencia de interacción directa con actores institucionales (como entrevistas o encuestas a funcionarios) impidió incorporar percepciones internas sobre la cultura de seguridad, la gestión de incidentes y la toma de decisiones en materia de ciberseguridad. Este aspecto podría enriquecer el análisis al complementar la visión documental con evidencia práctica del entorno organizacional.

Por otra parte, es importante considerar que la ciberseguridad es un campo dinámico, en el que las amenazas, tecnologías, estándares y marcos normativos evolucionan constantemente. En este sentido, los resultados obtenidos representan un diagnóstico contextual que podría requerir actualización frente a cambios en el entorno tecnológico o en las políticas nacionales e internacionales.

A partir de estas limitaciones, se proponen futuras líneas de investigación orientadas a: (i) la aplicación de metodologías cuantitativas para medir el nivel de madurez en ciberseguridad mediante indicadores y métricas; (ii) la realización de auditorías técnicas que permitan validar los controles implementados; (iii) el desarrollo de estudios comparativos entre entidades públicas con diferentes niveles de complejidad técnica; y (iv) la implementación y evaluación de planes piloto de fortalecimiento en gobernanza de la seguridad de la información, con el fin de medir su impacto en la reducción de brechas y vulnerabilidades.

Referencias Bibliográficas

Alejos, A. A. V. (2025). *Gestión tecnológica en la digitalización de servicios públicos gubernamentales: El caso del Municipio de Querétaro*. https://ri-ng.uaq.mx/handle/123456789/11875

Álvarez, Y. S. N. (2024). *Desafíos en la gobernanza de pymes mineras colombianas: Gestión de TI y ciberseguridad como factores críticos*. En Actas del Congreso de Investigación, Desarrollo e Innovación (pp. 82–98). https://revistas.unicyt.org/index.php/actasidi-unicyt/article/view/221

Arévalo, B., & Luz, E. (2016). *La comprensión de las organizaciones empresariales y su ambiente como sistemas de complejidad creciente: Rasgos e implicaciones*. Ingeniería, 21(3), 363–377. http://www.scielo.org.co/scielo.php?pid=S0121-750X2016000300008&script=sci_arttext

Arteaga, F. (2021). *Ciberseguridad: La consolidación de la cooperación público-privada. Real Instituto Elcano.* https://media.realinstitutoelcano.org/wp-content/uploads/2022/03/comentario-arteaga-ciberseguridad-la-consolidacion-de-la-cooperacion-publico-privada.pdf

Ávalos Mendoza, M. R., Castilla Tasaico, J. L., & Gordillo López, C. P. (2023). *Diseño de un modelo de gestión en seguridad digital para la aplicación en entidades peruanas del sector público*. https://repositorio.esan.edu.pe/items/b111397c-5702-4dd8-8ea1-018635e9f28b

Betancourt Zúñiga, J. (2025). *Importancia del uso de marcos de trabajo para la gestión de riesgos de ciberseguridad en organizaciones de salud del sector público en Colombia.* https://repository.unad.edu.co/handle/10596/70927

Bueno Munar, L. D. (2022). *Ciberseguridad en Colombia, avances y retos* [Trabajo de grado, Universidad Militar Nueva Granada]. Repositorio Institucional UMNG. https://hdl.handle.net/10654/41303

Cámara Colombiana de Informática y Telecomunicaciones. (2025, marzo 28). *Balance de ciberseguridad 2024: Desafíos y prevención para un entorno digital seguro.* https://www.ccit.org.co/noticias/balance-de-ciberseguridad-2024-desafios-y-prevencion-para-un-entorno-digital-seguro/

Camargo, E. A. R., & Pinzón, M. A. R. (2022). *La importancia de la seguridad de la información en el sector público en Colombia. Revista Ibérica de Sistemas y Tecnologías de Información*, (46), 87–99. https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

Cano, W. D., & Monsalve Machado, S. (2023). *Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual (Trabajo de grado).* https://repository.upb.edu.co/handle/20.500.11912/11318

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Departamento Nacional de Planeación. (2024). *Estrategia nacional digital de Colombia.* https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

Dorado, D. (2025, junio 25*). Colombia, entre los países más atacados por cibercriminales en América Latina.* Latinpyme. https://latinpyme.com/colombia-entre-los-paises-mas-atacados-por-cibercriminales-en-america-latina/

Fuentes, G. E. F., & Ponce, O. I. C. (2025). *Estrategia de resiliencia digital basada en el NIST RMF*. https://repositorio.unitec.edu/items/c629d3a9-1f1b-4fb5-83c3-8f83653d5f0f

GBA Latam. (s. f.). *Gobierno y transformación digital: Cómo la tecnología está optimizando la administración pública*. https://gbalatam.com/gobierno-y-transformacion-digital-como-la-tecnologia-esta-optimizando-la-administracion-publica/

Hashemi-Pour, C., Lawton, G., & Gillis, A. S. (2023). *Digital process automation (DPA). TechTarget*. https://www.techtarget.com/searchcio/definition/digital-process-automation

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). Metodología de la investigación (6ª ed.). McGraw-Hill.

Instituto Nacional de Estándares y Tecnología (NIST). (2023). *Cybersecurity framework 2.0.* https://www.nist.gov/cyberframework

ISACA. (2019). *COBIT 2019: Framework for governance and management of enterprise IT.*

Jiménez, G. A., & López, D. E. (2023). *Ciberseguridad y seguridad integral: Un análisis reflexivo sobre el avance normativo en Colombia.* RISTI, (E62), 16–31.

Leguizamón López, E. M., & Galindo Higuera, D. A. (2021). *Revisión de mejores prácticas de gestión para sistemas de información en Colombia.* https://repository.universidadean.edu.co/entities/publication/cad0ed07-fa25-4cfd-9af6-6908b4b9841d

Lopera Rodríguez, A. (2025). *Ciberseguridad en ciudades inteligentes.* https://bibliotecadigital.udea.edu.co/entities/publication/406a2be9-8639-4e83-b913-b59b9716897b

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023*). Manual de seguridad y privacidad de la información.*

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *Política nacional de seguridad digital 2023–2030.*

Molina Oviedo, A. (2020). *Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: caso de estudio Universidad Popular del Cesar* [Trabajo de maestría, Universidad del Norte]. Repositorio Institucional de la Universidad del Norte. https://manglar.uninorte.edu.co/handle/10584/10394

Muñoz, J. J. M., Delgado, N. Y. Q., & González, M. Á. N. (2025). *Modelo de gestión de riesgos en infraestructura tecnológica.* Ciencia y Desarrollo, 28(2), 133–147.

Organización de los Estados Americanos & Banco Interamericano de Desarrollo. (2023). *Ciberseguridad: Avances y desafíos en América Latina y el Caribe.*

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022.*

Organización Internacional de Normalización. (2023). *ISO/IEC 27032:2023.*

Pérez, T. V., Velásquez, A. M. P., & Silva, H. F. C. (2023). *Adopción de prácticas de gobierno y gestión en entidades públicas*. Aglala, 14(2), 101–116.

Polania Amaya, K. (2025). *Ciberseguridad dentro del marco normativo colombiano desde 2012* [Trabajo de grado, Universidad Libre]. Repositorio Institucional Universidad Libre. https://repository.unilibre.edu.co/handle/10901/31856

Policía Nacional de Colombia. (2025). *Informe anual de cibercriminalidad 2024.*

Presidencia de la República de Colombia. (2024). *Estrategia de transformación digital del Estado colombiano 2023–2026.*

Rainer, R. K., & Prince, B. (2021). *Introduction to information systems.* Wiley.

Rivas Turcios, C. L., & Esquivel Mejía, W. F. (2025). *Desarrollo de una metodología para la gestión de incidentes en seguridad informática con aplicación de la ISO 27001 y*

protocolos NIST para el Hospital María [Tesis de maestría, Universidad Tecnológica Centroamericana]. Repositorio UNITEC. https://repositorio.unitec.edu/items/10a9bce1-791f-47ed-a26f-0541532ae551

Rivera, F. E. C., & Cruzatty, J. E. Á. (2025). *Propuesta de la normativa ISO/IEC para la gobernanza de ciberseguridad.* Sinergia Académica, 8(5), 656–677.

Rodríguez, M. P. (2021). *Ciberseguridad en la justicia digital: Recomendaciones para el caso colombiano.* Revista UIS Ingenierías, 20(3), 19–45.

Rosero Córdoba, J. E. (2024). *Recomendar las mejores prácticas en el sector salud basadas en frameworks de ciberseguridad aplicables a hospitales del sector público en Colombia* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/61501

Rozo Díaz, J. F. (2024). *La importancia del hacking en la ciberseguridad a nivel organizacional en entidades de orden público en Colombia* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/50279

Törngren, M., & Grogan, P. T. (2018). *How to deal with the complexity of future cyber-physical systems? Designs*, 2(4). https://doi.org/10.3390/designs2040040

Villa, L. R. M., Saavedra, C. C. P., Reyes, N. M., & Arandia, N. Y. M. (2023). *Evaluación de la madurez digital en municipios de Colombia. Revista de Ciencia Latina*, 7(6), 4763–4790.

Apéndices

Apéndice A

Póster Académico de la Monografía

El póster académico se encuentra disponible en el siguiente enlace:

https://drive.google.com/file/d/1S3Qe5rkMd-bMsmIMfdKd2bc3NM7RQ6sp/view?usp=sharing

Apéndice B

Video de Sustentación de la Propuesta

El video de sustentación se encuentra disponible en el siguiente enlace:

https://drive.google.com/file/d/1LCbznk2GcM8KATfgvYgY0tr67-GoWQ3a/view?usp=sharing