Protección de datos sensibles en entornos digitales a partir de la implementación de los estándares ISO 27001 e ISO 27002 para la seguridad de la información

Leidy Tatiana Espinel Suancha

Asesor

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Dedico este proyecto a mi familia, por su amor incondicional y apoyo en cada paso de mi formación. A mis profesores, por compartir su conocimiento y motivarme a seguir aprendiendo. Y a mis amigos, por su compañía y aliento en los momentos difíciles.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mis tutores, por su orientación y paciencia a lo largo de este trabajo. A mis compañeros, por su colaboración y espíritu de equipo. También agradezco a mi familia por su apoyo incondicional y motivación constante. Finalmente, a todas las personas que, de una u otra forma, contribuyeron al éxito de este proyecto, gracias.

Resumen

Este proyecto de investigación se enfoca en desarrollar y aplicar un completo marco de seguridad de la información para hacer frente a las amenazas actuales y futuras en entornos digitales. El objetivo del marco propuesto es asegurar la protección de datos sensibles y garantizar la continuidad operativa de las organizaciones frente a posibles incidentes de seguridad.

Las normas de seguridad de la información, como ISO 27001 y 27002, desempeñan un papel fundamental en la mitigación de riesgos cibernéticos específicos, como accesos no autorizados y filtraciones de datos sensibles en entornos digitales. La implementación de estas normativas permite a las organizaciones establecer controles rigurosos de acceso, asegurando que solo personal autorizado pueda manipular información crítica. Además, fomentan el uso de mecanismos de cifrado y autenticación robusta para minimizar la exposición de datos ante ataques como ransomware y phishing. La ausencia de estos marcos puede derivar en brechas de seguridad que comprometan la integridad y disponibilidad de los sistemas, afectando tanto la operatividad como la reputación de las empresas.

Palabras clave: Marco Integral, Seguridad de la Información, Implementación

Abstract

This research project focuses on developing and applying a comprehensive information security framework to address current and future threats in digital environments. The proposed framework aims to ensure the protection of sensitive data and guarantee the operational continuity of organizations in the face of potential security incidents.

Information security standards, such as ISO 27001 and 27002, play a fundamental role in mitigating specific cybersecurity risks, such as unauthorized access and data breaches in digital environments. Implementing these standards allows organizations to establish strict access controls, ensuring that only authorized personnel can handle critical information. Additionally, they promote the use of encryption mechanisms and robust authentication to minimize data exposure to attacks such as ransomware and phishing. The absence of these frameworks can lead to security breaches that compromise the integrity and availability of systems, affecting both the operational capacity and reputation of companies.

Keywords: Comprehensive Framework, Information Security, Implementation

Tabla de contenido

Lista de Figuras

Lista de Tablas

Glosario

Amenaza: Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales, activos organizacionales o individuos a través de un sistema de información mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio (National Institute of Standards and Technology, 2006).

Ataque Informático: Acción intencionada llevada a cabo por un actor malicioso para explotar vulnerabilidades y causar daño o acceso no autorizado a sistemas y datos (Instituto Nacional de Ciberseguridad, 2021).

Ciberseguridad: Conjunto de políticas, medidas y prácticas técnicas orientadas a proteger redes, sistemas y datos frente a accesos indebidos, daños o ataques digitales (Computer Security Resource Center, 2025).

Confidencialidad: Principio de seguridad de la información que garantiza que la información no se ponga a disposición ni se divulgue a personas, entidades o procesos no autorizados. Se trata de proteger la confidencialidad de los datos. Para que la información sea confidencial, deben implementarse controles adecuados para evitar el acceso o la divulgación no autorizados (Barker, 2025).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una persona natural, identificada o identificable, como nombre, documento o dirección (Congreso de Colombia, 2014).

Datos Sensibles: Categoría especial de datos personales que, por su naturaleza, afectan la intimidad del titular o pueden generar discriminación, como la salud, creencias religiosas u orientación política (Congreso de Colombia, 2014).

Disponibilidad: Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran (Instituto Nacional de Ciberseguridad, 2021).

Habeas Data: Derecho constitucional que otorga a las personas la facultad de conocer, actualizar, rectificar o eliminar la información que sobre ellas repose en bases de datos públicas o privadas (Corte Constitucional, 2011).

Incidente de Seguridad: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información (Instituto Nacional de Ciberseguridad, 2021).

Integridad: Propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales (Instituto Nacional de Ciberseguridad, 2021).

ISO 27001: Norma internacional que establece los requisitos que las organizaciones deben cumplir para proteger la confidencialidad, integridad y disponibilidad de su información. Está diseñada para ser aplicable a organizaciones de todo tipo y tamaño, y su principio fundamental es un enfoque basado en el riesgo para la seguridad de la información (Barker, 2025).

ISO 27002: Norma internacional que proporciona un conjunto detallado de controles de seguridad de la información para ayudar a las organizaciones a implementar y gestionar su Sistema de Gestión de la Seguridad de la Información (SGSI). Es un documento de orientación que complementa la norma de certificación ISO 27001 (Barker, ISO 27002:2022, 2025).

Ley de Protección de Datos: Marco normativo que regula el tratamiento de la información personal en Colombia, estableciendo principios, derechos y obligaciones para proteger la privacidad de los ciudadanos (Congreso de Colombia, 2014).

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información (Instituto Nacional de Ciberseguridad, 2021).

Phishing: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo (Instituto Nacional de Ciberseguridad, 2021).

Política de Seguridad: Decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos (Instituto Nacional de Ciberseguridad, 2021).

Ransomware: Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella (Instituto Nacional de Ciberseguridad, 2021).

Resiliencia: Capacidad de una organización de resistir ante una situación adversa, como, por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa (Instituto Nacional de Ciberseguridad, 2021).

Riesgo: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su

actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado (Instituto Nacional de Ciberseguridad, 2021).

RGPD: Acrónimo de Reglamento General de Protección de Datos, ley que protege los datos personales de las personas en la Unión Europea (UE). Otorga a las personas un mayor control sobre su propia información. Las empresas deben seguir normas estrictas para la recopilación, el almacenamiento y el uso de datos personales. Esta ley garantiza que las empresas sean transparentes y honestas sobre su gestión de la información personal (Barker, 2025).

SGSI (Sistema de Gestión de Seguridad de la Información): Marco estructurado de políticas, procesos y controles que permite gestionar y mejorar de manera continua la seguridad de los datos en una organización (Instituto Nacional de Ciberseguridad, 2021).

Tratamiento de datos: Cualquier operación realizada sobre datos personales, como la recolección, almacenamiento, uso, circulación o supresión (Congreso de Colombia, 2014).

Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto (Instituto Nacional de Ciberseguridad, 2021).

Introducción

La protección de la información es fundamental para proteger datos sensibles y asegurar el correcto funcionamiento de las organizaciones, especialmente en un entorno donde aumentan las amenazas digitales y la dependencia de tecnologías donde se hace necesaria la adopción de estándares internacionales que aseguren una gestión eficaz de los riesgos.

Este proyecto propone un marco de seguridad apoyado en los estándares ISO 27001 e ISO 27002, con la finalidad de mejorar la seguridad de la información, reducir vulnerabilidades y proteger el cumplimiento de las regulaciones vigentes. Se analizarán los principales riesgos y la normativa aplicable en Colombia, además de diseñar un modelo de implementación que garantice la privacidad, exactitud y accesibilidad de la información de los datos.

Aplicar estos estándares ayuda a reducir las consecuencias de los incidentes de seguridad, evitar sanciones regulatorias y preservar la confianza de clientes y socios. Según (Giraldo, 2020), las empresas tecnológicas han sido blanco frecuente de ciberataques, lo que resalta la necesidad de contar con protocolos efectivos de respuesta ante incidentes. Además, la investigación de (Córdova & Remicio, 2022) destaca que la ausencia de políticas de seguridad organizadas incrementa el riesgo de exposición ante amenazas como ransomware y phishing, afectando la operatividad y generando pérdidas económicas.

A través de este estudio, se busca aportar soluciones que permitan a las organizaciones mejorar su postura de protección, mejorar el manejo de los riesgos y disminuir las posibilidades de que ocurran incidentes que pongan en peligro la información y el funcionamiento de la empresa.

Planteamiento del Problema

Actualmente, las amenazas cibernéticas son constantes y ponen en riesgo la privacidad, exactitud y disponibilidad de los datos sensibles dentro de las organizaciones. La falta de un marco integral de seguridad de la información puede generar vulnerabilidades, brechas de seguridad y pérdidas económicas, afectando tanto la continuidad de las operaciones como la reputación corporativa. Entre los riesgos más comunes se encuentran los ataques de ransomware, el phishing y la explotación de debilidades en la infraestructura tecnológica. Además, la falta de una estrategia adecuada de gestión de incidentes puede agravar las consecuencias de estos ataques. Según (Córdova & Remicio, 2022), "la falta de un sistema de gestión de seguridad de la información basado en estándares como ISO 27001 puede llevar a incumplimientos regulatorios y pérdida de confianza por parte de clientes y partes interesadas".

Es crucial diseñar e implementar un marco integral de seguridad que mitigue estos riesgos y garantice la protección de los activos de información. (AFFIA, MATULEVICIUS, & NOLTE, 2020) resaltan que "los incidentes de seguridad cibernética están en aumento, lo que subraya la importancia de adoptar estrategias efectivas para prevenir y mitigar el impacto de estas amenazas”. Por lo que la adopción de la norma ISO 27001 permite establecer un enfoque basado en la gestión de riesgos, fortaleciendo la resiliencia organizacional. Surge la necesidad de responder a la pregunta: ¿Cómo diseñar y poner en práctica un sistema completo de seguridad de la información que responda de manera efectiva a las amenazas presentes y futuras en ambientes digitales, garantizando la protección de datos sensibles y la continuidad del funcionamiento de las organizaciones?

Justificación

Esta monografía se fundamenta en la necesidad de diseñar e implementar un marco de trabajo sólido que permita enfrentar de manera eficaz las amenazas digitales presentes y emergentes, garantizando la confidencialidad de los datos y la continuidad operativa de las organizaciones. La creciente frecuencia de incidentes cibernéticos y la importancia estratégica que ha adquirido la información en la economía digital refuerzan la urgencia de adoptar mecanismos de gestión que salvaguarden los activos críticos y aseguren la perdurabilidad de las operaciones. Como destaca (Estacio, 2023), la madurez en la gestión de la seguridad de la información es un factor crítico para los centros de datos, ya que permite evaluar de forma integral los riesgos y establecer mecanismos de respuesta ante incidentes. En este mismo sentido, (Rodríguez, Méndez, & Méndez, 2023) muestran que la aplicación de ISO 27001 en el comercio electrónico ofrece un marco sistemático que no solo protege la información sensible, sino que también fortalece la confianza de los clientes.

El desarrollo de esta investigación se apoya en marcos normativos internacionales, como las normas ISO 27001 e ISO 27002, cuya adopción en diversos sectores ha demostrado ser fundamental para mitigar amenazas y garantizar la resiliencia cibernética. Según (Ndegeya, 2022), adaptar estas normas a pequeñas y medianas empresas representa un reto, pero también una oportunidad para incrementar su viabilidad frente a ciberataques. Asimismo, autores como (Minaya, Minaya, Intriago, & Intriago, 2023) resaltan la utilidad de las normas y estándares en auditoría como instrumentos clave para optimizar la seguridad informática y cumplir con regulaciones vigentes.

Más allá del plano técnico, la presente monografía busca aportar un análisis académico comparativo que integre estas referencias normativas con las realidades de sectores

empresariales y gubernamentales que contribuyen a la producción de conocimiento en el campo de la seguridad de la información, a la vez que proporciona orientaciones prácticas que pueden ser adoptadas por diferentes tipos de organizaciones.

Desde la dimensión social, la investigación cobra relevancia porque la protección de la información impacta directamente en los derechos de los ciudadanos. Tal como señalan (Córdova & Remicio, 2022), la ausencia de cumplimiento con estándares de seguridad en contextos educativos y empresariales ha derivado en filtraciones y fraudes que deterioran la confianza en los entornos digitales. Casos similares se observan en el sector público, donde la falta de normativas claras ha comprometido la privacidad de datos ciudadanos (Jara & Jorquera, 2021). Estos escenarios evidencian que la seguridad de la información no es únicamente un asunto corporativo, sino un bien común que protege la estabilidad social y económica.

Por todo lo anterior, esta monografía busca generar un aporte tanto académico como práctico, ofreciendo lineamientos metodológicos que fortalezcan la gestión de la seguridad de la información en diferentes sectores. Su finalidad es colaborar en la consolidación de un ecosistema digital confiable y de una sociedad más segura frente a las amenazas cibernéticas emergentes.

Objetivos

Objetivo General

Desarrollar un marco de trabajo para la protección de datos sensibles en entornos digitales mediante la aplicación de los estándares ISO 27001 e ISO 27002 para mejorar la seguridad de la información.

Objetivos Específicos

Identificar los riesgos y vulnerabilidades comunes en la protección de datos sensibles en entornos digitales a partir de una revisión documental.

Revisar la normativa vigente que establece los lineamientos y regula el manejo de datos sensibles en entornos digitales en Colombia.

Crear un marco de trabajo a partir de las directrices nacionales y de los estándares ISO 27001 e ISO 27002 que permitan establecer controles, procedimientos y políticas en entornos digitales para la protección de datos sensibles

Marco Referencial

Marco Conceptual

Protección de Datos Sensibles

La protección de datos sensibles es esencial para las instituciones, ya que los ciberataques y accesos no autorizados ponen en riesgo la privacidad, la imagen y la estabilidad económica de las entidades. La digitalización ha optimizado procesos, pero también ha incrementado la vulnerabilidad frente a amenazas.

Autores como (Caicedo, 2024) y (Ruiz & Aguirre, 2020) destacan que estos datos requieren un tratamiento diferenciado, pues comprometen derechos fundamentales como la intimidad y la no discriminación. De ahí que no baste con medidas técnicas, sino que se requiera de políticas internas, protocolos de acceso y mecanismos de control que fortalezcan la confianza de los titulares de la información. En Colombia, este principio se encuentra respaldado por la Ley 1581 de 2012 y sus decretos reglamentarios, que exigen adoptar medidas proporcionales al nivel de riesgo.

Seguridad de la Información

La seguridad de la información comprende el conjunto de medidas, políticas y controles destinados a garantizar que los activos informativos se mantengan protegidos, accesibles y confiables. Según la (ISO/IEC 27000, 2018), este proceso se articula mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que integra la gestión de riesgos, la definición de controles técnicos y administrativos, y la capacitación de los colaboradores.

(Rodríguez, Méndez, & Méndez, 2023) subrayan que hoy la seguridad de la información no solo protege los datos, sino que constituye un factor estratégico de competitividad, al permitir que las

empresas innoven con confianza, refuercen su resiliencia y cumplan con las exigencias regulatorias nacionales e internacionales.

Gestión de Riesgos

La gestión de riesgos constituye el eje estratégico de cualquier programa de seguridad de la información, ya que permite identificar, evaluar y mitigar las amenazas que podrían afectar los activos digitales de una empresa. (CiberSafety, 2024)sostiene que una gestión adecuada posibilita anticiparse a escenarios adversos y optimizar el uso de recursos, evitando reacciones improvisadas.

(AFFIA, MATULEVICIUS, & NOLTE, 2020) recomiendan metodologías basadas en amenazas críticas, pues facilitan priorizar los riesgos con mayor impacto en la continuidad del negocio. En el ámbito internacional, guías como MAGERIT en España y el NIST SP 800-30 en Estados Unidos ofrecen metodologías estructuradas que pueden adaptarse a diversos contextos.

Controles de Seguridad

Los controles de seguridad son mecanismos diseñados para reducir riesgos y proteger los sistemas de información frente a amenazas. Estos abarcan desde medidas administrativas y procedimientos internos hasta soluciones tecnológicas como firewalls, sistemas de detección de intrusos o cifrado de datos.

La ISO 27002 enfatiza que su efectividad depende tanto de la tecnología como de la integración con la cultura organizacional y el compromiso de la alta dirección, garantizando así una defensa proactiva ante un entorno digital en constante cambio, definiendo así los tipos de control en preventivo, detectivo y correctivo.

Estándares Internacionales (ISO 27001 e ISO 27002)

Los estándares ISO 27001 e ISO 27002 se han consolidado como referentes internacionales en seguridad de la información. ISO 27001 proporciona un marco de gestión basado en riesgos mediante un SGSI, mientras que ISO 27002 ofrece controles concretos para reforzar la protección de los datos.

(Araujo, 2021) señala que su adopción no solo fortalece los procesos internos, sino que permite demostrar cumplimiento frente a terceros, generando confianza en mercados competitivos. No obstante, su implementación enfrenta retos como los costos iniciales, la resistencia cultural al cambio y la falta de concienciación entre los colaboradores. Aun así, constituyen un puente entre las exigencias normativas y las prácticas organizacionales, alineándose con marcos internacionales como el GDPR en Europa y las legislaciones locales de protección de datos.

Leyes Normativas

La seguridad de la información no puede comprenderse sin considerar su dimensión normativa, que regula el tratamiento responsable de los datos y sanciona las prácticas que los pongan en riesgo. En Colombia, destacan las siguientes normas:

Ley 1581 de 2012 – Protección de Datos Personales: Establece los principios generales para el tratamiento de datos personales, garantizando derechos fundamentales como la intimidad y el hábeas data. Obliga a implementar medidas de seguridad que eviten accesos no autorizados, pérdidas o alteraciones de la información (Congreso de Colombia, 2014)

Decreto 1377 de 2013 – Reglamentación de la Ley 1581: Precisa aspectos como la autorización previa, expresa e informada del titular, y define responsabilidades de responsables y encargados. Refuerza la obligación de contar con políticas claras y transparentes en la gestión de datos personales. (Presidencia de la República de Colombia, 2013)

Decreto 886 de 2014 – Registro Nacional de Bases de Datos (RNBD): Ordena a las organizaciones registrar sus bases de datos ante la Superintendencia de Industria y Comercio, consolidando la vigilancia sobre el cumplimiento de la Ley 1581. (Congreso de Colombia, 2014)

Ley 1273 de 2009 – Delitos Informáticos: Modifica el Código Penal colombiano para tipificar delitos informáticos, sancionando conductas como el acceso no autorizado, la interceptación de comunicaciones y la alteración de sistemas. Reafirma la protección de la información como un bien jurídico esencial. (Congreso de Colombia, 2009)

Fundamentos y Prácticas Clave para la Protección de Datos Sensibles

Se fundamenta en los principios esenciales para proteger los datos sensibles, abarcando conceptos importantes como la privacidad, exactitud y acceso oportuno a la información por lo que (Rodríguez, Méndez, & Méndez, 2023), "la confidencialidad asegura que la información esté accesible solo para aquellos autorizados a tener acceso a ella, la integridad garantiza que la información sea precisa y completa, y la disponibilidad asegura que la información esté disponible y utilizable cuando sea necesario".

También incluye la gestión de riesgos, que consiste en detectar, analizar y reducir posibles amenazas a la información de la empresa. Según (AFFIA, MATULEVICIUS, & NOLTE, 2020), "la gestión de riesgos en seguridad de la información es crucial para proteger activos digitales y garantizar la continuidad del negocio frente a amenazas cibernéticas".

Otros aspectos clave dentro del marco conceptual son las normas de seguridad, los mecanismos para controlar el acceso, la protección mediante cifrado de la información y la administración de incidentes. (Córdova & Remicio, 2022) mencionan que "las políticas de seguridad establecen directrices y procedimientos para proteger la información sensible, mientras que los controles de acceso aseguran que solo usuarios autorizados puedan acceder a los datos".

Mientras que se enfatiza la importancia de la gestión de incidentes, auditoría de seguridad y monitoreo continuo en la implementación de ISO 27001 destacando que una gestión efectiva de incidentes requiere protocolos claros, asignación de responsabilidades y herramientas de análisis forense para mitigar riesgos. Asimismo, resalta que las auditorías internas, son esenciales para evaluar la eficacia del SGSI y garantizar el cumplimiento normativo. En cuanto al monitoreo continuo, subraya la necesidad de herramientas como IDS y SIEM para detectar amenazas en tiempo real y responder proactivamente. Proponiendo así que la enseñanza de ISO 27001 debe ir más allá de la teoría, enfocándose en su aplicación práctica para formar profesionales capacitados en seguridad informática.

Marco Teórico

Basándose en teorías y modelos vinculados a la protección de la información y al manejo de riesgos. Según (Minaya, Minaya, Intriago, & Intriago, 2023), "las teorías de gestión de riesgos en seguridad de la información se basan en principios de evaluación de amenazas y vulnerabilidades para implementar controles adecuados y mitigar riesgos".

También se incluyen modelos de seguridad informática como COBIT e ITIL, que ofrecen buenas prácticas para administrar los servicios de TI y proteger la información. (Penagos, Rentería, Ibargüen, García, & Castro, 2022) mencionan que "la adopción de modelos como COBIT y ITIL ayuda a las organizaciones a establecer un sistema robusto de gestión de la seguridad de la información y a cumplir con estándares y regulaciones".

Proteger los datos sensibles es fundamental para las organizaciones ante el incremento de ataques cibernéticos y accesos indebidos. La aplicación de las normas ISO/IEC 27001 e ISO/IEC 27002 facilita la gestión de la seguridad de la información mediante un Sistema de Gestión de Seguridad de la Información (SGSI) y controles específicos para mitigar amenazas. Su adopción

no solo mejora la seguridad y el cumplimiento normativo, sino que también fortalece la confianza de los usuarios. No obstante, ponerlo en práctica presenta dificultades como la falta de sensibilización y los gastos relacionados.

Para una protección efectiva, es fundamental desarrollar estrategias que integren estos estándares con un ambiente empresarial orientado a la seguridad, promoviendo la concienciación y el compromiso de los empleados. La utilización de tecnologías avanzadas, como la inteligencia artificial (IA), junto con métodos como MAGERIT, mejora la identificación y bloqueo de amenazas, reforzando el manejo de riesgos y la capacidad de recuperación frente a incidentes de ciberseguridad.

La inteligencia artificial juega un papel fundamental en la protección de la información, ya que permite identificar ataques en tiempo real y evitar amenazas. Sin embargo, su uso también presenta retos relacionados con la privacidad y el manejo de riesgos (Chavez, Joel, & Mendoza, 2023). Las investigaciones indican que los sistemas de detección de intrusos basados en IA aumentan la exactitud y el desempeño, y que la combinación de big data con IA fortalece la seguridad en las empresas. A pesar de esto, su eficacia depende de una gestión cuidadosa de los riesgos involucrados.

Asimismo, la aplicación de normas internacionales como ISO/IEC 27000 e ITIL es crucial para la protección de activos de información y la gestión de riesgos, lo que mejora la postura de seguridad y garantiza el cumplimiento regulatorio (Ndegeya, 2022).

Según (Altamirano, 2019), Las metodologías para el análisis y gestión de riesgos, como MAGERIT, STRIDE, OCTAVE, ISO/IEC 27005 y NIST SP 800-30, son esenciales para proteger la información, ya que ofrecen un proceso organizado para identificar, evaluar y manejar los riesgos en los sistemas de información. Estas metodologías no funcionan de forma

independiente, sino que se complementan con normas internacionales como ISO/IEC 27001:2016 y NIST SP 800-53, que brindan pautas específicas para administrar la seguridad de la información en las organizaciones.

Incorporar estas metodologías en los procesos de seguridad permite evaluar los riesgos de manera constante y aplicar controles efectivos para reducir las posibles amenazas. Además, automatizar la detección y gestión de riesgos facilita la supervisión regular de las medidas de seguridad, mejorando la eficiencia en la respuesta ante incidentes y optimizando las estrategias de protección.

Marco Legal

Proteger los datos sensibles en ambientes digitales es crucial para asegurar la privacidad, exactitud y disponibilidad de la información. La norma ISO/IEC 27001 proporciona un marco para establecer un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que la ISO/IEC 27002 ofrece controles específicos, como la administración de accesos, protección de datos y manejo de incidentes (Araujo, 2021) y (Holloway, 2025). Estas normas están en sintonía con regulaciones internacionales como el GDPR en Europa, la CCPA en Estados Unidos y leyes en América Latina, que buscan fortalecer la seguridad de la información tanto en el sector público como privado.

Además de los estándares ISO, otros marcos como el NIST Cybersecurity Framework, COBIT 5 y PCI DSS contribuyen a fortalecer la protección de datos en infraestructuras críticas (Dua, Shah, & AbdAllah, 2024). El incumplimiento de estas normativas puede acarrear sanciones económicas y dañar la reputación de las organizaciones.

En Colombia, la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 establecen los principios y lineamientos para el tratamiento de datos personales, mientras que la Ley 1273

de 2009 tipifica delitos informáticos como el acceso abusivo, la interceptación y el daño informático. Según el Manual de Tratamiento de Datos Personales (Superintendencia de Sociedades, 2024) y el marco normativo de la Superintendencia de Industria y Comercio refuerzan la necesidad de políticas internas claras, confidencialidad y consentimiento informado, complementados por guías internacionales como la del (Instituto Nacional de Ciberseguridad, 2020) que aportan metodologías y prácticas. El incumplimiento normativo genera sanciones, y mayor riesgo de brechas de seguridad; al implementar un SGSI alineado con las normativas resulta clave para mitigar riesgos, proteger derechos y reforzar la cultura de protección de datos.

Riesgos y Vulnerabilidades Comunes en la Protección de Datos Sensibles en Entornos Digitales

A continuación, se presenta un listado de los principales riesgos y vulnerabilidades que deben ser considerados en la seguridad de datos sensibles delicados en medios digitales. Estas amenazas han sido identificadas en estudios recientes y afectan tanto a pequeñas y medianas empresas como a entidades públicas y privadas. Su presencia afecta directamente los principios clave de la seguridad informativa: confidencialidad, integridad y disponibilidad.

Riesgos: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado (Instituto Nacional de Ciberseguridad, 2021)

Tipos de Riesgos:

1. Accesos no Autorizados y Robo de Datos: Uno de los riesgos más frecuentes es el acceso indebido a información crítica, ya sea por actores externos o internos. Esto suele deberse a contraseñas débiles, configuraciones incorrectas o falta de controles de acceso. Según (López, 2024), muchas organizaciones no implementan mecanismos de autenticación robustos, lo que permite que usuarios no autorizados accedan a datos sensibles, generando filtraciones masivas, extorsión o daño reputacional, especialmente en sectores como el financiero o gubernamental.

2. Ausencia de Gestión Estructurada de Activos de Información: La falta de un inventario claro y actualizado de activos digitales (bases de datos, servidores, aplicaciones) impide a las organizaciones saber qué información deben proteger, dónde se encuentra y quién es

responsable de ella. (Dua, Shah, & AbdAllah, 2024) destacan que esta deficiencia genera puntos ciegos que pueden ser fácilmente explotados por atacantes, incrementando el riesgo de exposición de datos sensibles.

3. Deficiente Clasificación de la Información: Muchas organizaciones no diferencian entre información confidencial y datos menos críticos, lo que impide aplicar medidas proporcionales de protección. Esta clasificación inadecuada lleva a una gestión uniforme de la seguridad, ineficaz para proteger activos de alto valor, como datos personales o propiedad intelectual (Dua, Shah, & AbdAllah, 2024).

4. Carencia de Controles Técnicos y Organizacionales: Según (El-Hajj & Mirza, 2024), muchas pequeñas y medianas empresas no cuentan con controles mínimos como cifrado de datos, autenticación multifactor (MFA), respaldos periódicos o herramientas de detección de intrusos (IDS/IPS). A nivel organizativo, también es común la ausencia de políticas claras, segregación de funciones y planes de respuesta ante incidentes, lo que disminuye la capacidad de respuesta y recuperación ante eventos de seguridad.

5. Falta de Formación y Concienciación del Personal: El factor humano representa una de las principales debilidades. Empleados mal capacitados pueden ser víctimas de engaños como el phishing, compartir contraseñas o manipular indebidamente información crítica. (López, 2024) resalta que la ausencia de una cultura de ciberseguridad incrementa significativamente la probabilidad de incidentes, siendo esencial establecer programas permanentes de formación y sensibilización.

6. Riesgo Legal y Responsabilidad Estatal: (Jara & Jorquera, 2021) advierten que en el sector público la falta de medidas adecuadas de ciberseguridad puede configurar una "falta de servicio", generando responsabilidad civil del Estado ante los ciudadanos afectados. Esta

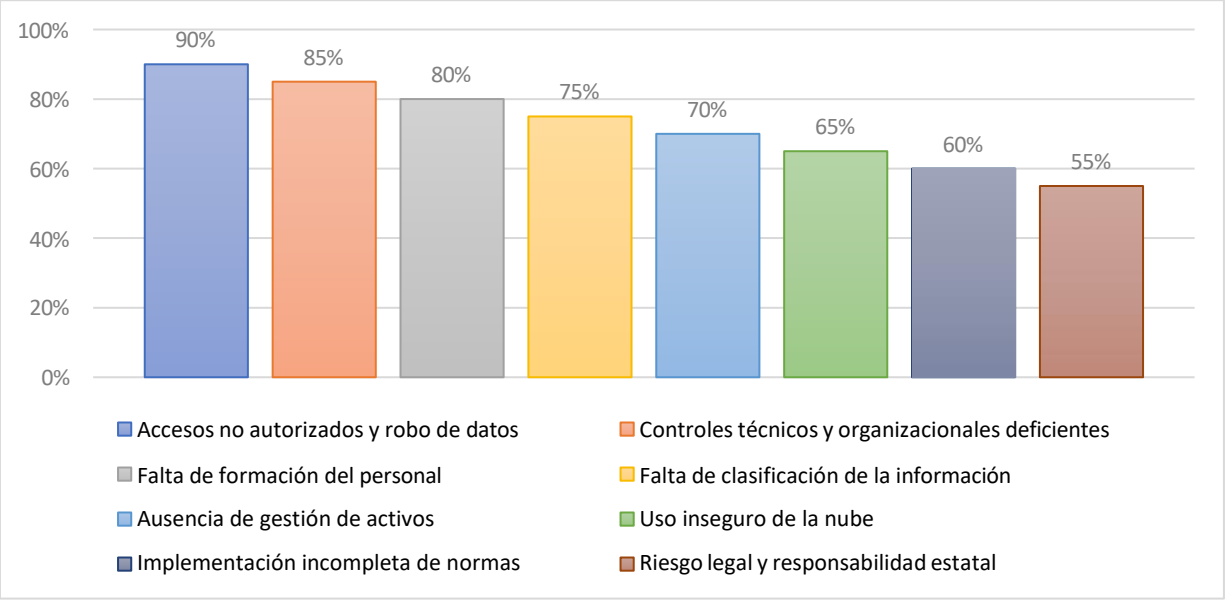
situación evidencia la necesidad urgente de implementar estándares como ISO/IEC 27001 en instituciones públicas para proteger adecuadamente los datos personales que manejan.

7. Implementación Incompleta o Deficiente de Marcos Normativos: La adopción parcial de normas como ISO 27001 o el NIST Cybersecurity Framework genera brechas que pueden ser explotadas por atacantes. (El-Hajj & Mirza, 2024) sostienen que muchas organizaciones, especialmente con recursos limitados, implementan estos marcos sin el acompañamiento adecuado, generando una falsa percepción de seguridad y vulnerabilidades latentes.

8. Alta Dependencia de Servicios en la Nube sin Controles Adecuados: El uso creciente de plataformas en la nube ha traído nuevos riesgos. (Carrillo, Jaramillo, Cabrera, Abad, & Torres, 2025) señalan que muchas organizaciones no aplican configuraciones seguras, como cifrado de datos en tránsito o en reposo, control de accesos ni segmentación por roles. Esto expone los datos a brechas internas o externas si no se alinea con marcos como ISO o NIST.

Figura 1

Grafica de Riesgos en la Protección de Datos Sensibles



Nota: Elaboración propia de los principales riesgos en la protección de datos sensibles, destacando el acceso no autorizado, la falta de controles y la limitada formación del personal en base con (López, 2024), (Dua, Shah, & AbdAllah, 2024), (El-Hajj & Mirza, 2024), (Jara & Jorquera, 2021), (Carrillo, Jaramillo, Cabrera, Abad, & Torres, 2025), (Instituto Nacional de Ciberseguridad, 2020) y (Ruiz & Aguirre, 2020).

Amenazas: Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales, activos organizacionales o individuos a través de un sistema de información mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio (National Institute of Standards and Technology, 2006).

Tipos de Amenazas

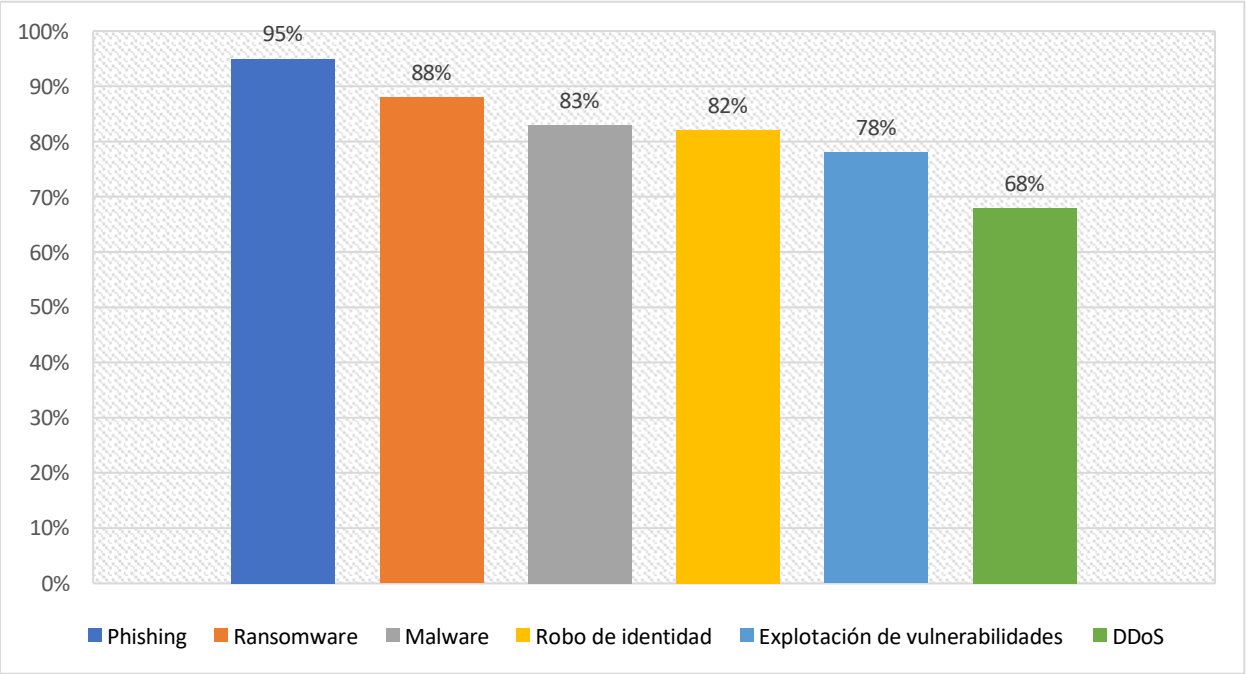
Además de las condiciones organizacionales y técnicas, existen amenazas específicas que comprometen la protección de datos sensibles, entre ellas destacan:

- Phishing: Ataques de suplantación de identidad por correo electrónico o mensajería, diseñados para obtener credenciales o datos confidenciales.
- Ransomware: Secuestro de datos mediante cifrado, exigiendo pagos para su liberación. Puede afectar gravemente la disponibilidad y operación de una organización.
- Malware: Programas maliciosos que roban, destruyen o espían información sensible dentro de los sistemas.
- Ataques DDoS: Saturación de servicios para dejar sistemas inoperativos, lo que puede generar interrupciones que derivan en otros ataques.
- Explotación de vulnerabilidades: Uso de fallos en software o sistemas desactualizados para obtener acceso no autorizado.

- Robo de identidad: Obtención y uso de información personal para realizar fraudes, suplantación o acceso indebido a sistemas protegidos.

Figura 2

Amenazas en la protección de datos sensibles



Nota. Elaboración propia con base en (Instituto Nacional de Ciberseguridad, 2020), (Congreso de Colombia, 2009), (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023, 2024) y (Norton Security, 2018). La figura muestra las principales amenazas que afectan la protección de datos sensibles, destacando el phishing y el ransomware como las más frecuentes.

Vulnerabilidades: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto (Instituto Nacional de Ciberseguridad, 2021).

Tipos de Vulnerabilidades de Acuerdo con los Factores de Exposición Común en Ciberseguridad

1. Falta de políticas y controles internos:

La ausencia de políticas formales, protocolos de respuesta y control interno es un factor recurrente en la exposición a amenazas. La *Guía Técnica Metodológica* de (López, 2024) señala que muchas entidades carecen de estructuras organizativas maduras para la seguridad, lo cual afecta directamente la eficacia de los controles implementados.

2. Configuraciones incorrectas o por defecto:

Configuraciones mal ajustadas (por ejemplo, cabeceras HTTP, cookies inseguras, falta de políticas de seguridad del navegador) representan una puerta abierta para ataques como XSS o secuestro de sesiones. Según el informe del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024) estos errores son muy comunes en sitios web y sistemas sin revisiones periódicas.

3. Uso de software obsoleto o sin parches:

El uso de versiones antiguas de PHP, Apache, Bootstrap, jQuery, etc., con vulnerabilidades conocidas, continúa siendo una práctica extendida. Según el informe del COLCERT IN-20250507-020 del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025) , estas versiones obsoletas aumentan significativamente la superficie de ataque y facilitan la explotación mediante técnicas como la ejecución remota de código (RCE) y ataques de Cross-site scripting (XSS).

4. Ausencia de cifrado o protocolos inseguros

El uso continuo de versiones obsoletas como SSL v2/v3 o TLS 1.0/1.1 compromete la seguridad de los datos, en particular su confidencialidad e integridad, lo cual es especialmente

crítico en sectores como el financiero y de salud. Según el informe del COLCERT IN-20250505-019 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024), estas vulnerabilidades facilitan ataques de tipo Man-in-the-Middle (MITM), comprometiendo la seguridad en sectores críticos como el financiero y de salud.

5. Gestión deficiente de identidades y accesos:

Fallos como contraseñas débiles, privilegios mal asignados o ausencia de autenticación multifactor (MFA) siguen presentes en infraestructuras críticas exponiendo a las organizaciones a riesgos significativos. Según el informe del COLCERT IN-20250507-020 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024), muchas aplicaciones carecen de políticas de contraseñas robustas y de mecanismos de autenticación fuertes, lo que facilita accesos no autorizados y compromete la seguridad de los sistemas.

6. Dependencia de terceros sin validación previa:

El uso de servicios tercerizados o librerías externas sin auditoría previa de seguridad, como ocurre con plugins de WordPress o versiones antiguas de jQuery, expone a las organizaciones a vulnerabilidades de cadena de suministro. Según el informe del COLCERT IN-20250507-020 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024), estas dependencias sin validación previa pueden ser explotadas por actores maliciosos para comprometer la seguridad de las organizaciones.

Identificación y Clasificación de Riesgos y Vulnerabilidades en la Protección de Datos Sensibles

Es un proceso esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información, permitiendo a las organizaciones prevenir incidentes que comprometan sus activos críticos.

Según la "Política de Administración de Riesgos" del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024), la identificación sistemática de peligros, ya sean físicos, químicos, biológicos o derivados de la infraestructura y procesos, permite evaluar su probabilidad y severidad. Este enfoque facilita la implementación de controles eficaces que se ajusten al nivel de riesgo, aplicable también al entorno informático para prevenir vulnerabilidades estructurales en los sistemas de información. Además, se destaca la importancia de actualizar periódicamente estos análisis en función de cambios organizacionales o incidentes relevantes, asegurando una gestión dinámica y preventiva de los riesgos.

Por otra parte, (Monge, 2023) nos proporciona el análisis académico comparativo de las metodologías MAGERIT y NIST SP 800-30 realizado en la *Universidad Politécnica Salesiana* la cual subraya la necesidad de aplicar metodologías especializadas para la gestión de riesgos en sistemas de tecnología de la información. Este estudio destaca que la adecuada identificación de amenazas, vulnerabilidades y activos sensibles, como bases de datos, redes y servidores, permite a las instituciones anticiparse a incidentes de ciberseguridad, optimizar recursos y garantizar la continuidad operativa. Ambas metodologías analizadas ofrecen estructuras detalladas para clasificar los activos y evaluar el impacto y la probabilidad de los riesgos, lo cual facilita la implementación de salvaguardas específicas y eficaces. La clasificación de vulnerabilidades no solo es estratégica, sino imprescindible para reducir la exposición frente a amenazas constantes y sofisticadas.

Teniendo presente que la protección de datos sensibles depende directamente de la capacidad de una organización para identificar y clasificar los riesgos y vulnerabilidades que los comprometen. Diversos análisis, como los reportados por COLCERT, INCIBE y NORTON,

permiten establecer un conjunto común de debilidades y amenazas que se repiten con frecuencia en sectores públicos y privados.

Uno de los hallazgos más relevantes corresponde a la alta incidencia de ataques por phishing, que según Norton representa entre el 30 y 35 % de los incidentes reportados. Este tipo de ataque, basado en ingeniería social, afecta especialmente a sectores con alto volumen de usuarios (como salud, educación o gobierno), al explotar la falta de verificación de identidad en comunicaciones digitales.

El ransomware es otro de los riesgos críticos señalados por Norton y respaldado por los informes de COLCERT, con un crecimiento reportado del 25 % en los últimos ciclos analizados. Este tipo de malware tiene la capacidad de cifrar información crítica, paralizar servicios y exigir pagos para recuperar el acceso, afectando seriamente la disponibilidad y la confidencialidad de los datos.

Desde el análisis de vulnerabilidades reflejado en el informe COLCERT IN-20250505-019 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024) se ha clasificado más de 22.000 en un año, de las cuales un 4.3 % fueron críticas, el 20.11 % altas, el 29.5 % medias y el 46 % bajas. Estas cifras no solo muestran el volumen de fallos explotables, sino también la necesidad de priorización en su tratamiento. Las más comunes incluyen errores de configuración, uso de versiones obsoletas de software y falta de mecanismos de cifrado actualizados, como lo documentan los artículos técnicos analizados.

INCIBE, por su parte, destaca la deficiencia en la gestión de accesos y privilegios, como uno de los factores internos más recurrentes que exponen a las organizaciones. Esto incluye la ausencia de políticas de control de cuentas, el uso de contraseñas débiles o repetidas, y la falta de autenticación multifactor (MFA). Además, la dependencia de servicios de terceros sin validación

previa de sus estándares de seguridad representa una puerta abierta para ataques indirectos a través de la cadena de suministro.

Entre los riesgos identificados, también se encuentran los ataques de denegación de servicio (DDoS), que aunque menos frecuentes, afectan especialmente a entidades gubernamentales y plataformas públicas, al impedir el acceso a servicios esenciales. COLCERT ha documentado el aumento de estos incidentes, que afectan hasta un 20 % de ciertos sectores, comprometiendo la disponibilidad operativa en momentos críticos.

La clasificación de estos riesgos debe hacerse con base en su impacto sobre los principios de la seguridad de la información:

- Confidencialidad, cuando hay fuga o acceso no autorizado a datos personales, financieros o institucionales.
- Integridad, cuando los datos son modificados de forma intencional o por malware sin el consentimiento de su propietario.
- Disponibilidad, cuando el acceso a la información se ve interrumpido por ataques, fallos técnicos o cifrado malicioso.

Los informes revisados coinciden en que la mayoría de los incidentes podrían haberse evitado mediante controles preventivos básicos: cifrado de información sensible, implementación de políticas de seguridad, formación del personal y monitoreo constante de los sistemas. La falta de estos controles refleja, más que un problema tecnológico, una debilidad estructural en la gestión institucional de la seguridad.

Por lo que los riesgos y vulnerabilidades que comprometen la protección de datos sensibles son conocidos y prevenibles. La información extraída de fuentes como Norton,

INCIBE y COLCERT ofrecen evidencia de cómo se puede sustentar decisiones estratégicas que reduzcan la exposición y fortalezcan la postura de seguridad organizacional.

Análisis de Tendencias y Patrones Comunes en Ciberataques y Fallas de Seguridad

Como bien sabemos las amenazas han evolucionado de manera significativa en los últimos años. A partir del análisis de las tendencias identificadas por NORTON, INCIBE y COLCERT, se pueden reconocer patrones clave en la frecuencia, impacto y sofisticación de los ataques cibernéticos.

Principales Tipos de Ciberataques y su Impacto

Los ataques más comunes detectados por estas entidades incluyen phishing, ransomware, malware, ataques DDoS, explotación de vulnerabilidades y robo de identidad. Si bien existen diferencias en los enfoques de cada organización, se observan similitudes en las amenazas predominantes.

1. Phishing: El phishing es uno de los ataques más comunes, representando entre el 30 % y el 35 % de los incidentes detectados por entidades como INCIBE y NORTON. Este consiste en la suplantación de identidad de entidades legítimas mediante correos electrónicos, mensajes de texto o sitios web falsos para engañar a los usuarios y obtener credenciales, datos bancarios o información personal.

Entornos afectados:

- Infraestructuras en la nube: acceso no autorizado a repositorios y máquinas virtuales.
- Redes corporativas: intrusión a través de credenciales robadas.
- Sistemas financieros**:** transferencias fraudulentas y vaciado de cuentas.

- Plataformas educativas y de salud: robo de historiales médicos o expedientes académicos.

(López, 2024) destaca que el phishing se ha sofisticado con modalidades como *spear phishing* (altamente dirigido) y *whaling* (contra directivos). Un caso documentado por INCIBE relata cómo un hospital español sufrió la exposición de datos de pacientes tras un ataque de phishing a su personal administrativo, lo que puso en riesgo la confidencialidad y disponibilidad del sistema de gestión de citas.

Otro caso encontrado en el documento de (Giraldo, 2020) en el cual detalla cómo el phishing es una de las principales amenazas en empresas de TI, con recomendaciones de mitigación como autenticación multifactor y simulaciones de ataque.

2. Ransomware: El ransomware es un software malicioso que cifra archivos o sistemas completos para exigir un rescate económico a cambio de su liberación COLCERT y Norton han reportado un aumento del 25 % en su incidencia, especialmente en hospitales, entidades financieras y administraciones públicas.

Su impacto es devastador para la disponibilidad los sistemas quedan inutilizados y, en muchos casos, para la integridad, cuando los datos son alterados o eliminados.

Los entornos más afectados incluyen:

- Salud: cancelación de cirugías y bloqueo de historiales clínicos (INCIBE).
- Gobierno: suspensión de trámites digitales y servicios ciudadanos.
- Finanzas: interrupción de plataformas de pago.
- Educación: inaccesibilidad de aulas virtuales y bibliotecas digitales.

En el estudio de *Thames Security Shredding (TSS)*, una empresa de seguridad privada, se evidenció cómo un ataque de ransomware paralizó por completo sus operaciones, lo que obligó a

restaurar los sistemas desde copias de seguridad y a reconfigurar las redes (BSI ISO/IEC 27001 , 2012). A partir de este caso, el informe *Protecting Small and Medium Enterprises* recomienda medidas preventivas como la segmentación de redes, la implementación de copias de seguridad offline y la realización de simulacros de respuesta, con el fin de minimizar el impacto de este tipo de incidentes (El-Hajj & Mirza, 2024).

También otro caso encontrado es la del artículo de *COLCERT,* se documenta el impacto del ransomware Makop y Crysis en Colombia, con empresas forzadas a suspender operaciones y pagar rescates (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023)

3. Malware: El malware incluye una variedad de programas maliciosos como troyanos, gusanos, spyware y adware diseñados para infiltrarse en sistemas y ejecutar acciones dañinas (*INCIBE* (Instituto Nacional de Ciberseguridad, 2020)). Aunque su proporción ha disminuido frente al ransomware, todavía representa entre el 18 % y el 25 % de los incidentes.

Afecta de forma simultánea a la confidencialidad (robo de datos), integridad (alteración de registros) y disponibilidad (bloqueo o destrucción de sistemas). Según (Martelo, Tovar, & Maza, 2018) el malware también puede actuar como *backdoor*, facilitando ataques posteriores.

En (NortonLifeLock, 2020) se señala que este tipo de amenaza puede infiltrarse a través de adjuntos maliciosos, descargas inseguras o vulnerabilidades no corregidas, y que su detección temprana requiere EDR y monitoreo continuo. Un caso registrado en INCIBE (Instituto Nacional de Ciberseguridad, 2020) muestra cómo una entidad financiera latinoamericana sufrió pérdidas millonarias por malware bancario que permitió transferencias fraudulentas.

Entornos afectados:

- Redes corporativas
- Plataformas educativas

- Sistemas operativos empresariales

Uno de los casos encontrado en el artículo (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024) de *COLCERT* reporta el uso de malware como parte de campañas dirigidas con XSS y ejecución remota, particularmente en plataformas web y servicios SaaS

4. Ataques DDoS: Los ataques DDoS utilizan redes de dispositivos comprometidos (*botnets*) para sobrecargar servidores y dejar fuera de servicio sitios web o aplicaciones por otra parte COLCERT ha registrado un crecimiento sostenido de este tipo de ataques, llegando a un 20 % de incidencia en ciertos sectores.

Su principal impacto es sobre la disponibilidad, impidiendo el acceso legítimo a servicios críticos. Entre los entornos más afectados están:

- Portales gubernamentales.
- Plataformas de comercio electrónico.
- Sistemas hospitalarios y de educación a distancia.

En *INCIBE* se documenta el caso de un banco europeo que sufrió un ataque DDoS que bloqueó operaciones en línea durante horas. Investigaciones posteriores revelaron que el DDoS fue usado como distracción para realizar fraude digital simultáneo, demostrando que a menudo se combina con otros ataques.

También de acuerdo con el caso expuesto en (Jara & Jorquera, 2021) describe cómo ataques DDoS pueden comprometer servicios públicos esenciales, afectando a ciudadanos y expidiendo responsabilidades legales del Estado chileno.

5. Explotación de vulnerabilidades: Ataques que aprovechan errores o fallos en software y sistemas para obtener acceso no autorizado o ejecutar código malicioso. *COLCERT(2023)* analiza vulnerabilidades críticas como Log4Shell, que han sido explotadas

para comprometer servidores sin interacción del usuario. Aunque menos común, sigue siendo un método efectivo para comprometer sistemas sin necesidad de interacción del usuario. Se mantiene en torno al 5-7% de los ataques detectados.

Este ataque se produce cuando los ciberdelincuentes aprovechan fallos de seguridad en software, configuraciones incorrectas o sistemas sin parches (El-Hajj & Mirza, 2024) y (Holloway, 2025) Es uno de los vectores más peligrosos porque puede usarse para introducir malware, ransomware o extraer datos sin necesidad de interacción del usuario.

Afecta a los tres pilares de la seguridad: confidencialidad, integridad y disponibilidad, dependiendo de la vulnerabilidad explotada. INCIBE (Instituto Nacional de Ciberseguridad, 2020) describe un incidente en el que la falta de actualización de un servidor expuesto permitió el despliegue masivo de ransomware en una red corporativa.

Las buenas prácticas documentadas en Guía Técnica Metodológica de (López, 2024) incluyen auditorías de seguridad, escaneo continuo de vulnerabilidades y aplicación inmediata de parches críticos, siguiendo marcos como CIS Benchmarks y NIST SP800-30.

De acuerdo con la publicación (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023) de *COLCERT* nos documenta vulnerabilidades como Log4Shell y CVE-2023-3519, ampliamente explotadas en 2023, con pérdidas significativas por espionaje y caída de servicios.

Log4Shell (CVE-2021-44228): Es una vulnerabilidad crítica descubierta en la biblioteca Log4j de Apache, ampliamente utilizada para registrar eventos en aplicaciones Java. Esta falla permite a un atacante ejecutar código de forma remota en el sistema afectado simplemente enviando datos especialmente diseñados que se registran con Log4j, lo que puede resultar en el

control total del sistema, robo de información, instalación de malware o ataques de ransomware, sin necesidad de autenticación previa.

CVE-2023-3519: Es una vulnerabilidad crítica que afecta a los dispositivos Citrix NetScaler ADC y Gateway. Esta falla permite a un atacante no autenticado explotar un desbordamiento de búfer, lo que puede dar lugar a la ejecución remota de código en el sistema afectado. Dada su naturaleza, esta vulnerabilidad representa un riesgo severo, ya que puede ser utilizada para tomar control completo de infraestructuras críticas sin necesidad de credenciales.

6. Robo de identidad: El robo de identidad implica el uso no autorizado de información personal para cometer fraude o suplantación de acuerdo con (NortonLifeLock, 2020), (Instituto Nacional de Ciberseguriad INCIBE, 2016),. Puede incluir datos como número de identificación, credenciales de acceso, información financiera o historiales médicos.

Impacta principalmente la confidencialidad, aunque también la integridad, cuando los registros oficiales son alterados para favorecer al atacante. *INCIBE* (Instituto Nacional de Ciberseguridad, 2020) expone un caso en el que datos médicos robados fueron usados para realizar reclamaciones fraudulentas a compañías de seguros.

Los sectores más afectados incluyen:

- Banca y finanzas: apertura de cuentas y créditos fraudulentos.
- Salud: reclamaciones médicas ilegales.
- Educación: falsificación de expedientes académicos.

Las medidas recomendadas en (NortonLifeLock, 2020) incluyen autenticación multifactor, cifrado de datos personales y monitoreo constante del uso de información sensible.

Evolución de los Ciberataques

El análisis de la evolución de los ciberataques en los últimos cinco años muestra que los ataques más sofisticados y dirigidos han reemplazado las amenazas más genéricas:

1. Phishing ha aumentado constantemente desde 2019, pasando del 20% al 35% de los incidentes reportados. El auge del teletrabajo y la digitalización ha facilitado la propagación de estos ataques.

2. Ransomware ha crecido un 150% en los últimos cinco años, convirtiéndose en una de las principales amenazas para empresas e infraestructuras críticas.

3. Los ataques DDoS han duplicado su incidencia desde 2019, especialmente con el auge de botnets y servicios de ataque por encargo.

4. El malware ha reducido su impacto, ya que los ciberdelincuentes han adoptado métodos más rentables como el ransomware y el phishing.

Patrones Comunes en las Fallas de Seguridad

El análisis también muestra que las fallas de seguridad que permiten estos ataques suelen estar relacionadas con:

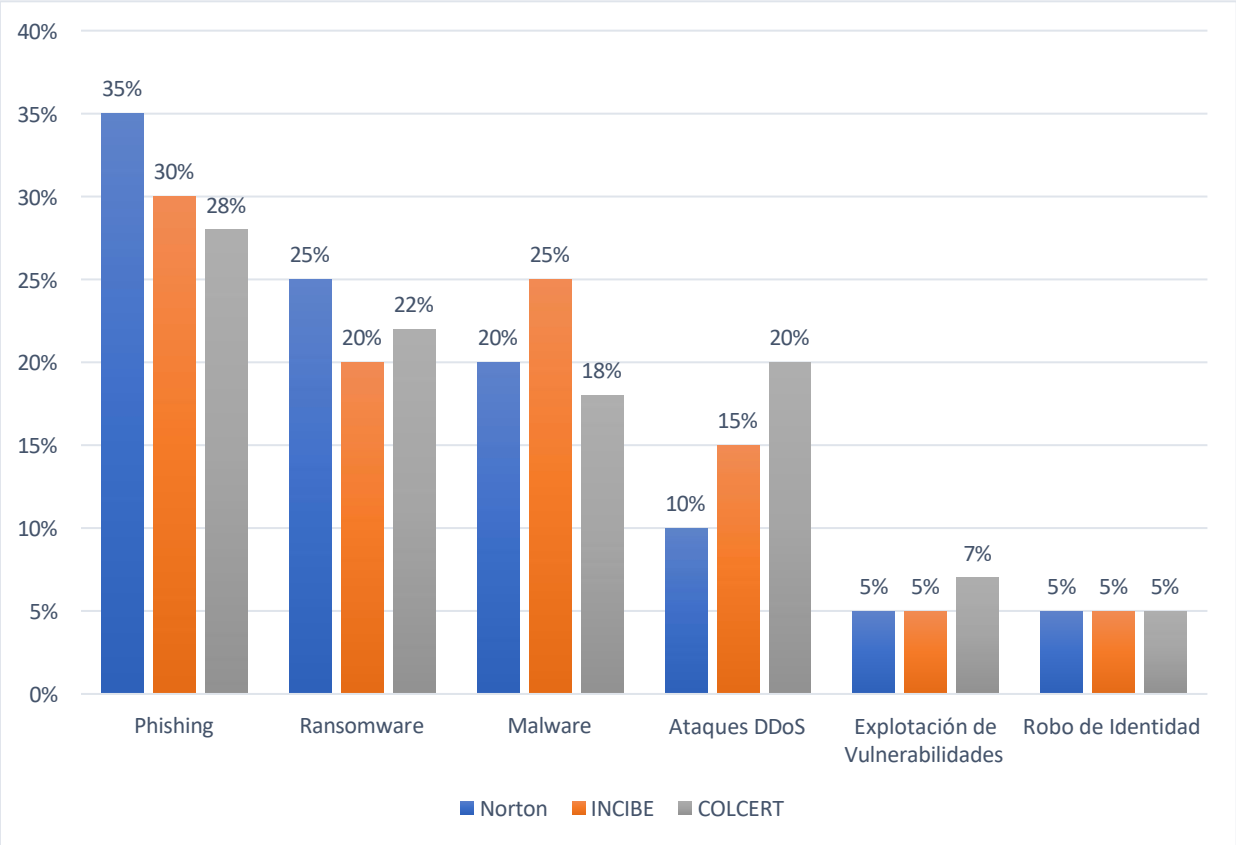
- Errores humanos y falta de concienciación, lo que facilita ataques de phishing y robo de identidad.
- Sistemas desactualizados con vulnerabilidades conocidas, explotadas en ataques de malware y ransomware.
- Falta de controles de seguridad en infraestructuras críticas, lo que aumenta el impacto de ataques DDoS y explotación de vulnerabilidades.

El análisis basado en los reportes de Norton, INCIBE y COLCERT evidencia que los ciberataques han evolucionado hacia métodos más sofisticados y dirigidos. La prevención y respuesta ante incidentes debe centrarse en la protección contra phishing, ransomware y ataques

DDoS, con énfasis en la concienciación de los usuarios y la aplicación de medidas de seguridad proactivas ya que a continuación se muestra como estas organizaciones por medio de un gráfico de las tendencias de los ciberatacantes.

Figura 3

Tendencias de ciberataques (%)



Nota: Elaboración propia con base en comparación porcentual de ciberataques más comunes según (Norton Security, 2018), (Instituto Nacional de Ciberseguridad, 2020), (López, 2024) y (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024). La figura muestra las principales tendencias de ciberataques, donde el phishing y el ransomware presentan los mayores porcentajes de incidencia.

Normativa y lineamientos de regulación el manejo de datos sensibles en entornos digitales en Colombia

La protección de datos sensibles es una preocupación central en la seguridad de la información, especialmente en un entorno digital donde las amenazas cibernéticas evolucionan constantemente. Diferentes enfoques han sido propuestos en estudios recientes para abordar esta problemática, desde la adopción de estándares internacionales hasta la aplicación de técnicas avanzadas de seguridad. La seguridad de los datos se basa en la implementación de protocolos de seguridad y técnicas avanzadas de cifrado que aseguren la confidencialidad e integridad de la información. La adopción de estándares internacionales como ISO/IEC 27001 permite establecer un marco de referencia sólido para gestionar adecuadamente la seguridad de los datos sensibles, reduciendo el riesgo de accesos no autorizados y garantizando la resiliencia de los sistemas de información. Este estudio también resalta la necesidad de auditorías periódicas y un enfoque basado en riesgos, lo que permite evaluar continuamente la efectividad de los controles de seguridad y realizar ajustes en función de nuevas amenazas. En este contexto, se recomienda la segmentación de redes y la implementación de sistemas de detección y prevención de intrusiones para reforzar la seguridad perimetral y evitar accesos no autorizados.

Por otro lado, (Gruschka, Mavroeidis, Vishi, & Jensen, 2018), se destaca la importancia del análisis de riesgos como un componente esencial en la protección de datos. Este estudio enfatiza que una estrategia efectiva no solo debe centrarse en controles técnicos, sino también en una evaluación continua de las amenazas y vulnerabilidades. Se recomienda el uso de metodologías como MAGERIT y OCTAVE, que permiten identificar los activos más críticos dentro de una organización y priorizar su protección. Además, se señala la relevancia de la anonimización y la encriptación como herramientas clave para minimizar la exposición de datos

en caso de una brecha de seguridad. Mientras que la encriptación protege los datos mediante algoritmos criptográficos, la anonimización permite eliminar o modificar información personal para que no pueda ser vinculada directamente a un individuo. Estas técnicas son fundamentales en sectores como la banca, la salud y la administración pública, donde la protección de datos personales es crítica. Otro aspecto clave del documento es la necesidad de controles de acceso basados en roles, limitando la exposición de los datos al garantizar que solo usuarios con los privilegios adecuados puedan acceder a determinada información. También se menciona la importancia de una política de gestión de incidentes que incluya procedimientos específicos para responder a ataques cibernéticos y minimizar el impacto en la organización.

Según (Sangaroonsilp, Khanh, & Ghose, 2023) aborda la protección de datos desde una perspectiva normativa y regulatoria. Se resalta la necesidad de cumplir con marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) y las directrices establecidas en ISO/IEC 27002. Este estudio subraya la importancia de la gestión de identidades, la auditoría de accesos y la aplicación de mecanismos de respuesta ante incidentes, elementos clave para garantizar la seguridad y privacidad de la información en organizaciones gubernamentales y empresariales. Entre los controles más importantes que menciona se encuentran la implementación de autenticación multifactor para reducir el riesgo de accesos no autorizados, el monitoreo y auditoría de accesos para detectar anomalías y el cifrado de extremo a extremo para proteger la información en tránsito y en reposo. Además, el estudio enfatiza que la protección de datos no depende únicamente de la tecnología, sino también de la concienciación y capacitación del personal. Muchas brechas de seguridad ocurren debido a errores humanos, por lo que las organizaciones deben invertir en formación continua y en la adopción de políticas de seguridad bien definidas.

En conjunto, estos estudios evidencian que la protección de datos sensibles no puede abordarse desde un único enfoque, sino que requiere la combinación de estándares internacionales, análisis de riesgos y cumplimiento normativo. La adopción de ISO/IEC 27001 e ISO/IEC 27002 proporciona un marco sólido para la gestión de la seguridad de la información, mientras que técnicas como la anonimización, el cifrado y los controles de acceso refuerzan la protección de los datos frente a amenazas. Además, el cumplimiento de regulaciones como el GDPR garantiza que las organizaciones operen bajo principios éticos y legales que protejan la privacidad de los usuarios. Para fortalecer la seguridad de los datos sensibles, es crucial que las organizaciones implementen una estrategia integral que incluya tecnología avanzada, capacitación continua y monitoreo activo de amenazas, asegurando así la resiliencia ante ataques cibernéticos y la protección efectiva de la información crítica.

Tabla 1

Análisis Comparativo de la Implementación de Controles ISO 27001 frente a Deficiencias Organizacionales

Área de Seguridad	Mejores Prácticas en ISO 27001	Deficiencias Comunes en las Organizaciones
Gestión de Riesgos	Implementación de un SGSI basado en ISO 27005 para mitigar amenazas y vulnerabilidades.	Falta de un marco estructurado para identificar, evaluar y mitigar riesgos de ciberseguridad.
Gestión de Incidentes	Procedimientos formales para detección, análisis y respuesta ante incidentes.	Respuesta reactiva sin procedimientos documentados ni equipos especializados.
Auditoría de Seguridad	Auditorías internas periódicas según ISO 19011 para evaluar el SGSI.	Falta de auditorías internas o externas, dificultando la detección de brechas de seguridad.

Área de Seguridad	Mejores Prácticas en ISO 27001	Deficiencias Comunes en las Organizaciones
Monitoreo de Amenazas	Implementación de SIEM, IDS/IPS y análisis de registros en tiempo real.	Dependencia de medidas básicas sin monitoreo continuo ni herramientas avanzadas.
Control de Acceso	Aplicación del principio de mínimos privilegios, autenticación multifactor y gestión centralizada.	Uso de contraseñas débiles, cuentas compartidas y falta de control de accesos privilegiados.
Protección de Datos Sensibles	Cifrado de datos en tránsito y almacenamiento, políticas de clasificación de información.	Almacenamiento sin cifrar, sin segmentación adecuada ni restricciones de acceso.
Capacitación en Seguridad	Formación continua en seguridad y concienciación sobre ingeniería social.	Falta de cultura de ciberseguridad, aumentando la vulnerabilidad ante phishing y ransomware.
Evaluación de Vulnerabilidades	Pruebas de penetración y escaneos de vulnerabilidades periódicos.	Falta de evaluaciones proactivas; detección de vulnerabilidades solo tras incidentes.
Gestión de Proveedores	Evaluación de seguridad en terceros mediante acuerdos y auditorías.	Falta de controles de seguridad en proveedores, generando brechas en la cadena de suministro.

Nota: Elaboración propia a partir de la comparación de las mejores prácticas de seguridad recomendadas por la ISO 27001 y las deficiencias más comunes en las organizaciones según (Giraldo, 2020), (Córdova & Remicio, 2022), (Jevelin & Faza, 2023) y (Al-Abdullah, Yayla, & Al-Atoum, 2024).

Principales Leyes y Regulaciones Aplicables al Tratamiento de Datos Sensibles

En Colombia, la gestión de los datos sensibles está regulada por diversas normativas legales que buscan salvaguardar la privacidad y los derechos fundamentales de los ciudadanos. El artículo 15 de la Constitución Política reconoce el derecho de toda persona a acceder, actualizar y corregir los datos personales que se encuentren en bases de datos. Este principio fue desarrollado por (Ruiz & Aguirre, 2020) la Ley 1581 de 2012, la cual establece los lineamientos y principios fundamentales para el manejo de la información personal, incluyendo la transparencia, la seguridad y la confidencialidad. Según esta ley, los datos sensibles son aquellos relacionados con aspectos íntimos del individuo o que, en caso de uso indebido, podrían dar lugar a actos de discriminación, como por ejemplo la información sobre raza, afiliación política, religión, estado de salud o vida sexual.

De acuerdo con el (Congreso de Colombia, 2009) Ley 1273 de 2009 fortalece la protección de la información digital en Colombia al incorporar nuevos delitos informáticos en el Código Penal. Esta normativa sanciona acciones como el acceso no autorizado a sistemas, la interceptación ilegal de datos, la alteración o destrucción de información y el uso de programas maliciosos, con el objetivo de preservar la integridad y confidencialidad de los datos digitales. A su vez, el Decreto 886 de 2014 impone la obligación de inscribir las bases de datos en el Registro Nacional de Bases de Datos (RNBD), gestionado por la Superintendencia de Industria y Comercio, con el fin de promover la transparencia en el tratamiento de la información y facilitar su supervisión.

El Decreto 52 de 2017, aunque enfocado en la seguridad y salud en el trabajo, establece lineamientos para la protección de los datos relacionados con la salud de los trabajadores, los cuales se consideran información sensible y deben ser manejados con estrictas medidas de

seguridad. La Circular Única de la Superintendencia de Industria y Comercio, por su parte, proporciona directrices claras sobre el tratamiento de datos personales, unificando criterios para su aplicación y garantizando el cumplimiento de la normativa vigente.

Análisis de los Requisitos y Principios Establecidos en la Normativa Vigente

El cumplimiento de estos marcos normativos implica la adopción de una serie de medidas técnicas, organizativas y jurídicas que aseguren la protección de la información y el adecuado tratamiento de los datos sensibles. En este sentido, la normativa colombiana establece que las entidades responsables del tratamiento de datos deben garantizar su seguridad, evitar accesos no autorizados y prevenir cualquier forma de alteración, pérdida o divulgación indebida de la información. Para ello, las organizaciones deben implementar políticas de protección de datos que incluyan mecanismos de control de acceso, cifrado de información, auditorías periódicas y planes de respuesta ante incidentes de seguridad.

Las empresas y entidades gubernamentales que manejan datos personales están obligadas a aplicar el principio de confidencialidad, lo que implica que la información solo puede ser utilizada por personal autorizado y exclusivamente para los fines para los cuales fue recopilada. Esto significa que el acceso a los datos debe estar restringido mediante mecanismos de autenticación segura y que cualquier transferencia de información debe realizarse bajo estrictas medidas de seguridad. Además, es fundamental que los encargados del tratamiento de datos cuenten con protocolos que les permitan identificar y gestionar posibles brechas de seguridad de manera rápida y eficiente, minimizando así el impacto en los titulares de los datos.

El principio de transparencia también juega un papel clave en la protección de los datos personales. La normativa exige que las organizaciones permitan que los titulares accedan a la información recopilada sobre ellos y que puedan ejercer su derecho de rectificación o

eliminación cuando consideren que sus datos han sido tratados de manera incorrecta. Para garantizar este derecho, las entidades deben establecer canales de comunicación adecuados que permitan a los ciudadanos presentar solicitudes relacionadas con el acceso, actualización o eliminación de su información personal.

Además, el Decreto 886 de 2014 establece la obligatoriedad de inscribir y mantener actualizadas las bases de datos en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio. Este registro busca garantizar un manejo adecuado de la información y permitir a las autoridades ejercer control y supervisión sobre el tratamiento de los datos personales. La inscripción en el RNBD implica que las empresas y entidades deben reportar el tipo de datos que manejan, la finalidad del tratamiento, las medidas de seguridad implementadas y los mecanismos utilizados para garantizar los derechos de los titulares. También se exige que esta información sea actualizada de manera periódica, asegurando que cualquier cambio en el tratamiento de los datos sea reportado oportunamente a la Superintendencia.

El cumplimiento de estas disposiciones no solo protege la privacidad de los ciudadanos, sino que también fortalece la confianza en el uso de la información y reduce los riesgos asociados a la vulneración de datos personales. Las entidades que gestionan información sensible deben adoptar una cultura de seguridad y cumplimiento normativo que garantice el respeto de los derechos de los titulares y minimice la posibilidad de sanciones por parte de las autoridades de control.

Sanciones y Responsabilidades Derivadas del Incumplimiento Normativo

Las sanciones por no cumplir con las normas de protección de datos personales pueden ser bastante severas, ya que buscan garantizar que las organizaciones manejen la información de

manera segura. La Ley 1581 de 2012 establece un régimen sancionatorio con multas que pueden llegar hasta 2.000 salarios mínimos legales vigentes. Estas sanciones son impuestas por la Superintendencia de Industria y Comercio (SIC), entidad encargada de hacer cumplir la normativa.

Además de las multas de la SIC puede aplicar sanciones administrativas, como la suspensión temporal de las actividades de tratamiento de datos por un período de hasta seis meses. Esto ocurre cuando se detectan infracciones graves que comprometan la seguridad de la información o si la entidad no toma las medidas correctivas necesarias tras una advertencia. En los casos más críticos, cuando hay incumplimientos reiterados o una afectación masiva a los derechos de los titulares, la SIC puede ordenar el cierre definitivo de la entidad responsable del tratamiento de datos.

Por otra parte, la Ley 1273 de 2009 introdujo modificaciones al Código Penal colombiano para castigar penalmente a quienes accedan, alteren o divulguen datos personales sin autorización. Dependiendo de la gravedad del delito y del daño causado, las penas pueden ir de 48 a 120 meses de prisión, además de multas que pueden alcanzar los 1.500 salarios mínimos. Algunos de los delitos más graves en esta materia incluyen el acceso abusivo a sistemas informáticos, la violación de datos personales, la interceptación ilegal de información y el uso de software malicioso para obtener datos sin permiso.

El incumplimiento de estas normas no solo conlleva sanciones económicas y penales, sino que también afecta la reputación de las empresas y puede hacer que los clientes pierdan confianza en el manejo de su información. Una violación de datos puede derivar en demandas, pérdidas económicas por indemnizaciones y un daño a la imagen institucional, lo que puede afectar las oportunidades de negocio y dificultar las relaciones comerciales.

Para evitar estos riesgos, las empresas deben establecer políticas de protección de datos efectivas que garanticen el cumplimiento de la normativa. Es clave contar con programas de cumplimiento que incluyan la capacitación del personal, auditorías periódicas y la actualización constante de las medidas de seguridad.

Las auditorías permiten detectar vulnerabilidades y verificar si las prácticas de tratamiento de datos cumplen con los estándares exigidos por la ley. Tecnologías como el cifrado de información, la autenticación multifactor y la anonimización de datos ayudan a reducir el riesgo de exposición de información sensible. También es esencial contar con protocolos de respuesta ante incidentes de seguridad para reaccionar de manera rápida y mitigar el impacto en caso de una brecha de datos, notificando tanto a las autoridades como a los titulares afectados.

Cumplir con estas normativas no solo evita sanciones, sino que también fortalece la confianza de los clientes y mejora la reputación de las organizaciones, reduciendo riesgos asociados a un mal manejo de la información.

Comparación de la Normativa Colombiana con Estándares Internacionales de Protección de Datos

Tabla 2

Comparación entre Normas Internacionales y Normas Colombianas sobre Protección de Datos Personales

Criterio	Normas Internacionales	Normas Colombianas
Base legal	• GDPR (UE): Reglamento General de Protección de Datos. • ISO/IEC 27001: Gestión de seguridad de la información. • NIST Privacy Framework (EE.UU.).	• Ley 1581 de 2012: Protección de datos personales. • Decreto 1377 de 2013: Reglamenta la Ley 1581.

Criterio	Normas Internacionales	Normas Colombianas
Protección de datos personales	• GDPR: Define principios de protección, derechos del titular y obligaciones del responsable. • CCPA (EE.UU.): Protección de datos en California.	Ley 1581 de 2012: Establece principios como confidencialidad, transparencia y seguridad.
Datos sensibles	GDPR protege datos como raza, religión, salud y orientación sexual con estrictos controles.	Ley 1581 de 2012: Define datos sensibles y limita su tratamiento sin autorización explícita.
Derechos del titular	Derecho al olvido, portabilidad, acceso y rectificación (GDPR).	Derecho a conocer, actualizar, rectificar y suprimir información (Ley 1581).
Registro de bases de datos	No obligatorio en GDPR, pero sí en algunas regulaciones nacionales.	Decreto 886 de 2014: Registro obligatorio en el RNBD (Superintendencia de Industria y Comercio).
Sanciones por incumplimiento	• GDPR: Multas de hasta 4% de la facturación anual global. • CCPA: Sanciones económicas y demandas colectivas.	SIC impone multas y sanciones administrativas.
Delitos informáticos	Convención de Budapest: Marco internacional para perseguir ciberdelitos.	Ley 1273 de 2009: Penaliza delitos informáticos en Colombia (acceso abusivo, daño informático, uso de malware).
Seguridad de la información	• ISO/IEC 27001: Estándar internacional de gestión de seguridad. • NIST SP 800-53: Controles de seguridad para sistemas de información.	Circular Única SIC: Lineamientos de seguridad para tratamiento de datos.
Protección de datos en salud	HIPAA (EE.UU.): Normativa para la protección de información médica.	Decreto 52 de 2017: Regula el manejo de datos de salud en el ámbito laboral.
Transferencia internacional de datos	GDPR exige garantías adecuadas (Cláusulas Contractuales Tipo, Privacy Shield antes de su anulación).	Decreto 1377 de 2013: Regula la transferencia internacional de datos con restricciones.

Nota. Elaboración propia a partir de la comparación entre las prácticas recomendadas por la ISO 27001 y las debilidades más frecuentes observadas en las organizaciones.

Marco de Trabajo a Partir de los Estándares ISO 27001 E ISO 27002 para la Seguridad de la Información i Tratamiento de Datos en Entornos Digitales

Introducción

La seguridad de la información es una necesidad estratégica para las organizaciones modernas, no solo por su vinculación directa con la protección de datos sensibles, sino también por el cumplimiento normativo y la confianza de los usuarios. Las constantes amenazas digitales como el ransomware, el phishing o la explotación de vulnerabilidades han expuesto con crudeza las limitaciones de estructuras de seguridad poco formales, improvisadas o sin un respaldo normativo claro.

Para enfrentar esta realidad, diversos estudios académicos y técnicos recopilados en esta revisión proponen adoptar un marco de trabajo sustentado en estándares internacionales como ISO/IEC 27001 y ISO/IEC 27002. Este enfoque no solo estandariza los procesos internos relacionados con la seguridad, sino que también brinda herramientas concretas para el tratamiento de datos en entornos digitales, conforme a principios de gestión de riesgos, mejora continua y gobernanza institucional.

Uno de los pilares en la construcción de este marco proviene del análisis de la tesis de (Giraldo, 2020), que propone un modelo de ciberseguridad específicamente diseñado para empresas de servicios informáticos. Esta investigación utiliza como base la norma ISO 27005:2018 para identificar activos críticos, evaluar riesgos y proponer controles alineados con la ISO/IEC 27001 y el NIST SP800-53, con el fin de mejorar el manejo de incidentes de ciberseguridad.

De manera complementaria, la tesis de Remicio Córdova ofrece un abordaje más institucional, centrado en el diseño de políticas, la asignación de roles organizacionales y la

implementación progresiva de controles administrativos y técnicos. Su aplicación práctica en una entidad pública que muestra cómo es posible adaptar los estándares ISO a contextos con limitaciones presupuestarias o recursos humanos limitados.

El marco también se fundamenta en los casos de estudio reales de organizaciones como Fredrickson International (BSI ISO/IEC 27001, 2012) y Thames Security (BSI ISO/IEC 27001 , 2011), documentados en informes de BSI (British Standards Institution). Ambos muestran cómo, a través de la implementación de ISO 27001, fue posible:

- Establecer un SGSI formal que integrara seguridad física, lógica y organizacional.
- Adaptar las políticas de seguridad a los procesos existentes.
- Mejorar la respuesta ante incidentes de seguridad gracias a controles más estrictos y al monitoreo continuo.
- Aumentar la confianza de clientes y socios mediante la certificación formal.

A nivel normativo, (López, 2024) destaca en la Guía Técnica Metodológica en Seguridad y Ciberseguridad como uno de los documentos más completos orientados al contexto colombiano. Esta guía adopta ISO 27001 y 27002 como base, y propone una serie de recomendaciones prácticas, tales como:

- Auditorías internas periódicas.
- Evaluación de la madurez organizacional.
- Establecimiento de indicadores clave de seguridad.
- Gestión de incidentes desde un enfoque proactivo y no reactivo.

Al mismo tiempo, se identifican factores recurrentes de exposición que justifican aún más la implementación de un marco estructurado. Según los informes analizados por *COLCERT* (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024) *y la presentación de*

COLCERT (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025), muchos incidentes de seguridad están vinculados a:

- Configuraciones incorrectas de sistemas y aplicaciones web.
- Uso de software obsoleto o sin parches de seguridad.
- Falta de cifrado adecuado.
- Gestión deficiente de accesos y privilegios.
- Tercerización de servicios sin validación de sus estándares de seguridad.

Estas condiciones, sumadas a la escasa cultura organizacional sobre ciberseguridad, evidencian la necesidad de pasar de un enfoque correctivo a uno preventivo y normativamente sustentado.

Alcance

Está diseñado para servir como una guía práctica aplicable a cualquier organización que gestione información sensible o datos personales, ya sea en formato digital o físico, abarcando desde pequeñas empresas hasta entidades públicas y privadas de gran escala en sectores críticos como salud, educación, gobierno o finanzas. Su cobertura incluye todos los procesos, sistemas y personas involucradas en la recolección, almacenamiento, uso y protección de datos, con el objetivo de asegurar el cumplimiento de la normativa vigente y la alineación con las mejores prácticas internacionales en seguridad de la información.

Objetivo

ofrecer a las organizaciones una ruta clara y bien estructurada para proteger su información y la de sus usuarios, minimizando riesgos y fortaleciendo la confianza.

Este marco busca que la seguridad de la información no se vea solo como un requisito legal, sino

como una cultura organizacional que prioriza la confidencialidad, integridad y disponibilidad de los datos.

Se basa en estándares reconocidos como ISO/IEC 27001 e ISO/IEC 27002, así como en la ley 1581 de 2012 (Congreso de Colombia, 2012), para que cada medida y control implementado tenga respaldo normativo y efectividad comprobada en la práctica.

La adopción de este marco, además de facilitar el cumplimiento normativo, ofrece beneficios estratégicos como la reducción de incidentes, la optimización de procesos internos, y la generación de confianza en clientes, usuarios y entes reguladores.

Es una responsabilidad esencial para las organizaciones, que deben garantizar la seguridad de sus activos frente a riesgos crecientes y cada vez más complejos. Para lograrlo, no basta con implementar herramientas tecnológicas: es necesario contar con un enfoque estructurado que permita identificar amenazas, establecer controles efectivos y definir políticas claras que orienten la gestión de la seguridad en todos los niveles.

Este marco de trabajo responde a esa necesidad; reúniendo directrices normativas reconocidas internacionalmente, como las establecidas en las normas ISO/IEC 27001 y 27002, y las articula con prácticas operativas adaptables a distintos contextos organizacionales. A partir de un diagnóstico inicial, que incluye la identificación de activos sensibles y la evaluación de riesgos, se propone un conjunto coherente de controles técnicos, físicos y administrativos, acompañado de políticas institucionales y procedimientos definidos dentro los que podemos encontrar:

Componentes del Marco de Trabajo

Procedimientos Operativos Obligatorios

Según la Ley 1581 de 2012, toda entidad que trate datos personales debe pedir y guardar la autorización clara del titular antes de usarlos; custodiar ese permiso en papel o en formato digital de forma segura; manejar la información siguiendo principios como legalidad, finalidad, veracidad, transparencia, seguridad y confidencialidad; y responder a las solicitudes, quejas o reclamos de las personas dentro de los plazos que fija la norma, asegurando siempre sus derechos sobre la información por lo cual se estable lo siguiente:

1. Formato de autorización de tratamiento de datos personales

Cuando una entidad necesita manejar los datos personales de una persona, debe pedirle autorización por escrito o por medios equivalentes.

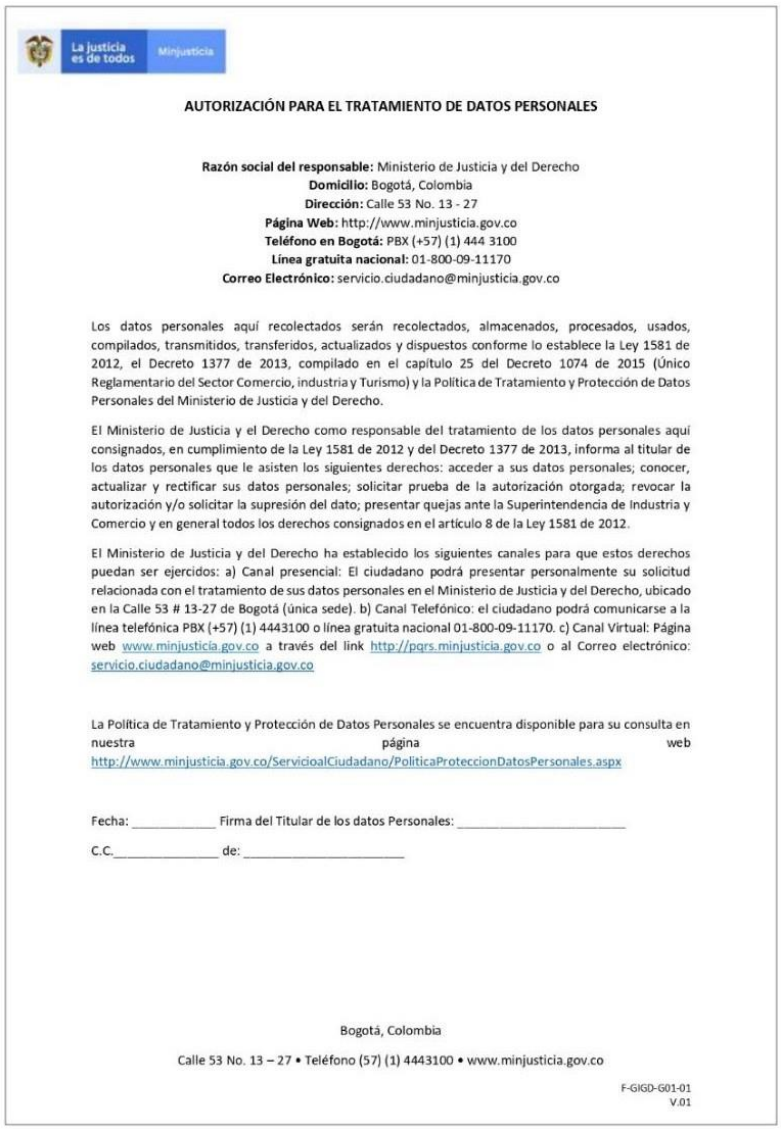
En el formato de autorización se incluyen:

- Quién es el responsable: nombre de la entidad, dirección, teléfono, correo y página web.
- Para qué se usarán los datos: por ejemplo, envío de información, prestación de un servicio o trámites administrativos.
- Derechos del titular: acceso, corrección, eliminación, prueba de autorización, revocatoria y queja ante la SIC (Ley 1581 de 2012).
- Canales para ejercer esos derechos: atención presencial, teléfono, correo electrónico y página web.
- Firma y fecha del titular como prueba de consentimiento.

Es importante guardar esta autorización como evidencia, ya sea en papel o en formato digital. Si la persona dio su autorización de manera verbal, también se deben conservar los soportes, como grabaciones. A continuación, podrás ver un ejemplo ilustrativo en la *Imagen 1*.

Figura 4

Modelo del Ministerio de Justicia Incluye estos Campos y Canales de Contacto



La justicia es de todos | Minjusticia

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Razón social del responsable: Ministerio de Justicia y del Derecho
Domicilio: Bogotá, Colombia
Dirección: Calle 53 No. 13 - 27
Página Web: http://www.minjusticia.gov.co
Teléfono en Bogotá: PBX (+57) (1) 444 3100
Línea gratuita nacional: 01-800-09-11170
Correo Electrónico: servicio.ciudadano@minjusticia.gov.co

Los datos personales aquí recolectados serán recolectados, almacenados, procesados, usados, compilados, transmitidos, transferidos, actualizados y dispuestos conforme lo establece la Ley 1581 de 2012, el Decreto 1377 de 2013, compilado en el capítulo 25 del Decreto 1074 de 2015 (Único Reglamentario del Sector Comercio, industria y Turismo) y la Política de Tratamiento y Protección de Datos Personales del Ministerio de Justicia y del Derecho.

El Ministerio de Justicia y el Derecho como responsable del tratamiento de los datos personales aquí consignados, en cumplimiento de la Ley 1581 de 2012 y del Decreto 1377 de 2013, informa al titular de los datos personales que le asisten los siguientes derechos: acceder a sus datos personales; conocer, actualizar y rectificar sus datos personales; solicitar prueba de la autorización otorgada; revocar la autorización y/o solicitar la supresión del dato; presentar quejas ante la Superintendencia de Industria y Comercio y en general todos los derechos consignados en el artículo 8 de la Ley 1581 de 2012.

El Ministerio de Justicia y del Derecho ha establecido los siguientes canales para que estos derechos puedan ser ejercidos: a) Canal presencial: El ciudadano podrá presentar personalmente su solicitud relacionada con el tratamiento de sus datos personales en el Ministerio de Justicia y del Derecho, ubicado en la Calle 53 # 13-27 de Bogotá (única sede). b) Canal Telefónico: el ciudadano podrá comunicarse a la línea telefónica PBX (+57) (1) 4443100 o línea gratuita nacional 01-800-09-11170. c) Canal Virtual: Página web www.minjusticia.gov.co a través del link http://pqrs.minjusticia.gov.co o al Correo electrónico: servicio.ciudadano@minjusticia.gov.co

La Política de Tratamiento y Protección de Datos Personales se encuentra disponible para su consulta en nuestra página web http://www.minjusticia.gov.co/ServicioalCiudadano/PoliticaProteccionDatosPersonales.aspx

Fecha: _____ Firma del Titular de los datos Personales: _____

C.C._____ de: _____

Bogotá, Colombia

Calle 53 No. 13 – 27 • Teléfono (57) (1) 4443100 • www.minjusticia.gov.co

F-GIGD-G01-01
V.01

Nota. Menciona consentimiento informado conforme a la Ley 1581 de 2012, incluye derechos, prueba de autorización, revocatoria, y canales presencial, telefónico o virtual encontrado en Anexo_N_1_Autorizacion_tratamiento_de_datos.pdf

2. Registro y almacenamiento seguro del consentimiento

El permiso que una persona da para usar sus datos debe guardarse de forma segura.

- En digital: se almacena en sistemas protegidos, con acceso restringido, y siempre con fecha, hora y una copia de la autorización (por ejemplo, formularios web o correos).
- En físico: se archiva el formulario firmado en un gabinete o archivo de gestión con llave y control de acceso.
- Evidencias: si la autorización fue por llamada o chat, se guarda la grabación o captura, con número de radicado para rastreo.

Todo esto se hace para cumplir con la Ley 1581, que obliga a conservar la autorización y proteger la información contra pérdidas o accesos no autorizados.

3. Principios de recolección de datos personales

Cada vez que se pidan y usen datos personales, la ley exige seguir estos principios:

- Legalidad: todo debe hacerse de acuerdo con la ley.
- Finalidad: el uso de los datos debe tener un propósito legítimo y claro.
- Libertad: los datos solo se usan si la persona dio su consentimiento previo, salvo excepciones legales.
- Veracidad o calidad: la información debe ser exacta y actualizada.
- Transparencia: el titular puede saber en todo momento qué datos suyos tiene la entidad y para qué los usa.
- Acceso y circulación restringida: no se puede dar acceso a cualquiera.
- Seguridad: se deben aplicar medidas técnicas y organizativas para proteger los datos.

- Confidencialidad: quienes manejan los datos deben guardar reserva, incluso cuando dejen de trabajar en la entidad.

4. Atención de consultas, quejas y reclamos según plazos de la Ley 1581

Las personas tienen derecho a preguntar, reclamar o pedir cambios sobre sus datos.

El proceso funciona así:

- Recepción: cuando llega la solicitud, se registra y se asigna un número de radicado.
- Consultas (preguntas sobre la información): la entidad debe responder en 10 días hábiles, y si necesita más tiempo, puede prorrogar hasta 5 días más avisando al titular.
- Reclamos (corrección, eliminación o inconformidad):
  - Si falta información, se pide al titular que la complete en 5 días hábiles; si no responde en 2 meses, se da por desistida.
  - En máximo 2 días hábiles desde que entra el reclamo, se marca en la base de datos la leyenda “reclamo en trámite” y se suspende el uso del dato, excepto para guardarlo.
  - Se debe responder en máximo 15 días hábiles, con posibilidad de prorrogar 8 días más avisando al titular.
- Escalamiento: si la persona no queda satisfecha o no recibe respuesta, puede acudir a la Superintendencia de Industria y Comercio.

Este proceso debe quedar documentado en una bitácora o registro interno, guardando copia de la respuesta y del trámite completo.

Fundamentos Normativos

Las normas ISO/IEC 27001 y 27002 constituyen el marco internacional más reconocido para la protección de la información. La primera se enfoca en la implementación y certificación

de un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que la segunda provee lineamientos prácticos para aplicar controles de seguridad específicos.

Ambas están alineadas con otras regulaciones internacionales como el GDPR y el NIST CSF, y permiten establecer un enfoque basado en riesgos, centrado en la confidencialidad, integridad y disponibilidad de la información.

Diagnóstico Inicial

Identificación de Activos y Datos Sensibles: La identificación y clasificación de datos sensibles constituye el primer paso crítico en la implementación de cualquier estrategia de seguridad de la información. Sin un inventario claro de qué información existe, dónde se encuentra y qué nivel de protección requiere, cualquier control posterior pierde eficacia. Los documentos revisados coinciden en que este proceso debe ser sistemático, documentado y actualizado periódicamente para responder a cambios en la organización y en el entorno tecnológico.

De acuerdo con la Ley 1581 de 2012, artículo 5, se consideran datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, entre ellos: origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, datos de salud, vida sexual y datos biométricos. Estos tipos de datos, por su nivel de criticidad, deben estar sujetos a controles reforzados de confidencialidad, trazabilidad y acceso restringido.

En paralelo, deben identificarse otros activos de información que, si bien no encajan en la definición legal de “datos sensibles”, sí resultan estratégicos o confidenciales para la organización, como datos financieros, propiedad intelectual, historiales académicos o información contractual.

A. Inventario de activos

1. Definición del Alcance: Incluye todos los repositorios de información, ya sean físicos o digitales, que contengan datos sensibles por lo que a continuación se abarca:

Bases de Datos Internas (ERP, CRM, historiales clínicos, expedientes académicos, sistemas contables).

Aplicaciones Críticas (plataformas de banca en línea, portales de atención al cliente, sistemas de gestión hospitalaria).

Dispositivos de Almacenamiento (servidores, equipos de escritorio, portátiles, discos externos, memorias USB).

Entornos en la nube (IaaS, PaaS, SaaS) contratados a proveedores externos como AWS, Azure o Google Cloud.

2. Metodología que se Recomienda de Acuerdo con las Siguientes Investigaciones:

(Araujo, A. (2021) y Harvey, A. (2024)) proponen mantener un registro centralizado de activos donde cada elemento tenga un responsable asignado.

INCIBE sugiere incluir información sobre la ubicación, propietario, tecnología asociada, criticidad y fecha de última actualización.

De acuerdo con ((Dua, Shah, & AbdAllah, 2024) se plantea usar herramientas de gestión de activos automatizada que permitan detectar nuevos sistemas o repositorios no registrados (“shadow IT”).

B. Clasificación por Nivel de Criticidad

Una vez inventariados los activos, es fundamental clasificarlos según el nivel de sensibilidad de los datos que contienen y el impacto que supondría una brecha de seguridad.

1. Criterios Propuestos por (Holloway, 2025) y adaptados por INCIBE:

- Público: Información que puede ser divulgada sin riesgo (ej. comunicados de prensa).
- Interno: Uso exclusivo dentro de la organización, sin datos personales ni estratégicos (ej. manuales internos).
- Confidencial: Contiene datos personales, financieros o corporativos que requieren medidas de protección (ej. nóminas, contratos, registros médicos).
- Restringido: Información de máxima criticidad cuya divulgación tendría un impacto grave en la continuidad del negocio o en el cumplimiento legal (ej. claves criptográficas maestras, planes estratégicos, bases de datos completas de clientes).

2. Evaluación de Impacto: La clasificación se determina valorando el efecto sobre:

- Confidencialidad (riesgo de divulgación no autorizada).
- Integridad (riesgo de modificación no autorizada).
- Disponibilidad (riesgo de pérdida o indisponibilidad).

C. Etiquetado y Trazabilidad

La clasificación no es suficiente si no se hace visible y trazable dentro del ciclo de vida de la información.

Etiquetado:

(Holloway, 2025) sugiere el uso de etiquetas físicas (para documentos impresos) y metadatos digitales (para archivos electrónicos).

INCIBE recomienda herramientas de Data Loss Prevention (DLP) que permitan aplicar etiquetas automáticas basadas en el contenido y contexto.

Trazabilidad:

Registrar cada acceso, copia, modificación y transferencia de la información sensible.

El uso de sistemas de auditoría y logging permite identificar anomalías y responder rápidamente a incidentes.

(Dua, Shah, & AbdAllah, 2024) destaca la importancia de integrar la trazabilidad con soluciones SIEM para correlacionar eventos y detectar fugas o accesos indebidos en tiempo real.

Identificación de amenazas y evaluación de riesgos: Utilizando metodologías como las descritas en ISO/IEC 27005 y apoyándose en marcos como NIST SP800-30 o análisis CVSS, se deben considerar amenazas como:

- Phishing, malware, ransomware
- Configuraciones incorrectas
- Accesos no autorizados
- Fallos humanos y dependencia de terceros inseguros.

Diseño del Esquema de Control

a. Controles técnicos

Tabla 3

Tipos de controles técnicos a tener presentes

Control	Descripción	Casos
Cifrado en tránsito	TLS 1.3 o superior para comunicaciones internas y externas	INCIBE propone cifrado extremo a extremo en teletrabajo
Cifrado en reposo	AES-256 en bases de datos, discos y copias de seguridad	Norton cifra datos de clientes en reposo y tránsito
Gestión de acceso basado en roles (RBAC)	Principio de mínimo privilegio	Caso Fredrickson International: segmentación por roles

Control	Descripción	Casos
Autenticación multifactor (MFA)	Refuerzo de seguridad en accesos a sistemas críticos	Thames Security adoptó MFA para accesos remotos
Prevención de fuga de datos (DLP)	Monitorización y bloqueo de transferencias no autorizadas	INCIBE recomienda DLP en endpoints y nube
Segmentación de red	Separación de redes críticas y administrativas	Implementada en entornos hospitalarios según ISO 27002
Registro y monitoreo continuo	SIEM con alertas y auditorías	Thames Security implementó monitoreo 24/7
Cifrado en tránsito	TLS 1.3 o superior para comunicaciones internas y externas	INCIBE propone cifrado extremo a extremo en teletrabajo

Nota. Elaboración propia que nos proporciona controles de seguridad de la información y casos de aplicación con base en referentes internacionales de ciberseguridad.

b. Controles físicos

Los controles físicos reducen la probabilidad de accesos no autorizados a infraestructuras críticas.

Acceso restringido a centros de datos mediante autenticación biométrica o tarjetas inteligentes, con registro de entradas y salidas.

Cámaras de videovigilancia que permitan monitoreo constante, respaldadas por registros de acceso físicos.

Sistemas de alimentación ininterrumpida (UPS) y climatización redundante para evitar daños por cortes de energía o sobrecalentamiento.

Protección contra incendios y humedad mediante sensores, extintores especializados y sistemas de supresión automáticos.

c. Controles administrativos

Los controles administrativos constituyen la base organizativa de la seguridad de la información, ya que establecen políticas, procedimientos y responsabilidades claras.

Política de seguridad de la información debe estar documentada, revisada periódicamente y aprobada por la alta dirección, garantizando su alineación con objetivos estratégicos y normativas aplicables.

Procedimientos de gestión de incidentes deben definir roles, canales de comunicación y tiempos de respuesta, minimizando el impacto de cualquier evento adverso.

Acuerdos de confidencialidad (NDA) para empleados, proveedores y terceros refuerza la protección de datos sensibles y reduce riesgos de filtraciones.

Capacitación periódica en seguridad de la información y concienciación frente a phishing y fuga de datos.

La evaluación periódica de proveedores asegura que estos cumplan con estándares internacionales como ISO 27001 y con regulaciones de privacidad como GDPR, evitando brechas originadas por terceros.

Monitoreo y Respuesta a Incidentes

La detección temprana y la respuesta eficiente ante incidentes es clave para minimizar daños.

Sistemas SIEM/SOC que centralizan y analizan eventos de seguridad, emitiendo alertas en tiempo real.

Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) probados al menos una vez al año, para asegurar la operatividad en escenarios críticos.

Simulacros de Ciberataques que entrenan al personal para actuar rápidamente y en coordinación.

Protocolos de Notificación de Brechas alineados con el GDPR y la Ley 1581, que en Colombia exige notificar de forma inmediata a la SIC en caso de incidentes con datos personales.

Marco Normativo de Referencia

Un marco robusto de seguridad se apoya en estándares y regulaciones consolidadas:

ISO/IEC 27001: Define los requisitos para implementar, mantener y mejorar un SGSI basado en gestión de riesgos.

ISO/IEC 27002: Proporciona directrices para implementar controles técnicos, físicos y administrativos.

GDPR / Ley 1581: Establecen las obligaciones legales para el tratamiento y protección de datos personales en la UE y en Colombia, respectivamente.

NIST SP 800-53: Ofrece un catálogo de controles de seguridad y privacidad aplicable a sistemas de información gubernamentales y corporativos.

Políticas Institucionales

La definición y formalización de políticas institucionales es un pilar clave para garantizar la correcta gestión de la seguridad de la información y la protección de datos sensibles. Según ISO/IEC 27001 y ISO/IEC 27002, estas políticas deben ser aprobadas por la alta dirección, comunicadas a todos los empleados y revisadas periódicamente para asegurar su vigencia y adecuación a cambios normativos o tecnológicos.

Entre las políticas fundamentales se destacan:

Política de Privacidad y Confidencialidad: Establece las directrices para el tratamiento de datos personales y corporativos, alineada con el GDPR y la Ley 1581 de 2012 en Colombia.

Política de uso Aceptable de Recursos Tecnológicos: Define el uso permitido de sistemas, redes, dispositivos móviles y aplicaciones, con el fin de prevenir incidentes y abusos.

Política de Continuidad del Negocio: Regula la planificación y ejecución de estrategias para mantener operaciones críticas ante incidentes, incluyendo planes de recuperación ante desastres.

Política de Gestión de Incidentes y Notificación de Brechas: Especifica los pasos a seguir para detectar, contener, investigar y notificar incidentes de seguridad, cumpliendo con plazos legales.

Procedimientos de Onboarding y Offboarding: Garantizan que las altas y bajas de usuarios en los sistemas se gestionen de forma segura, evitando accesos no autorizados.

Estas políticas no solo cumplen una función normativa, sino que actúan como guías operativas para toda la organización, reduciendo riesgos derivados de malas prácticas y mejorando la capacidad de respuesta ante incidentes.

Enfoque Flexible y Adaptativo

Este marco debe ser:

Escalable: aplicable tanto a PYMEs como a grandes corporaciones

Modular: adaptable según sector (salud, educación, finanzas, gobierno)

Iterativo: con mejora continua a través del ciclo Plan-Do-Check-Act (PDCA)

- Planificar: definir objetivos y controles
- Hacer: implementar y operar controles
- Verificar: evaluar mediante auditorías y métricas

- Actuar: corregir y mejorar

Soporte Empírico y Casos Relevantes

Los estudios de Fredrickson International y Thames Security demuestran cómo la implementación de ISO 27001 permitió reforzar la seguridad y generar confianza con clientes. Entre los principales desafíos se encontró la necesidad de adaptar las políticas internas y capacitar al personal.

Recomendaciones Finales

- Integrar auditorías internas periódicas
- Evaluar continuamente el nivel de madurez del SGSI
- Asegurar la trazabilidad y monitoreo de toda actividad en sistemas críticos
- Validar a proveedores y servicios tercerizados antes de su integración

Conclusiones

El análisis realizado permitió reconocer los principales riesgos y vulnerabilidades que comprometen la seguridad de los datos sensibles, entre ellos accesos no autorizados, phishing, ransomware y malware. Al clasificar estas amenazas se hizo posible priorizar controles como el cifrado y la autenticación robusta, así como fortalecer la capacitación del personal, acciones que reflejan un cumplimiento efectivo del propósito de diagnosticar la situación actual de exposición.

A partir de ello, el estudio de tendencias reveló cómo los ciberataques han evolucionado hacia formas más sofisticadas y dirigidas, afectando con mayor intensidad sectores como salud, finanzas y gobierno. Factores recurrentes como la falta de políticas, el uso de sistemas obsoletos y la dependencia de proveedores externos sin evaluación de seguridad mostraron que la gestión organizacional requiere ser reforzada de manera preventiva y no solo reactiva.

En el plano normativo, se evidenció que el marco legal colombiano, encabezado por la Ley 1581 de 2012 y sus decretos, establece principios sólidos en torno a la confidencialidad, la transparencia y la seguridad de la información. Dichos lineamientos constituyen la base para que las organizaciones garanticen el respeto por los derechos de los titulares y eviten sanciones, al tiempo que se fortalecen la confianza y la legitimidad en el uso de los datos.

La comparación con los estándares internacionales permitió advertir que, aunque la normativa nacional ofrece un marco de referencia robusto, persisten vacíos en la aplicación práctica de controles técnicos y de gestión. En este punto, los lineamientos de las normas ISO 27001 e ISO 27002 se presentan como un complemento esencial, al brindar directrices claras para estructurar un sistema de seguridad de la información basado en riesgos que responda a exigencias globales y locales.

Finalmente, el diseño del marco de trabajo apoyado en estas normas internacionales consolidó un esquema adaptable a distintos sectores y tamaños de organización, integrando procedimientos, políticas y controles de carácter técnico, físico y administrativo. Este modelo favorece la mejora continua, la consolidación de una cultura institucional de ciberseguridad y una mayor capacidad de respuesta ante incidentes, lo que refleja el cumplimiento integral de la propuesta planteada desde el inicio de la investigación.

En conjunto, el recorrido de esta investigación evidencia que la protección de datos sensibles en entornos digitales no puede entenderse de manera aislada, sino como un proceso integral que parte de la identificación de riesgos y su relación con tendencias emergentes, se apoya en marcos normativos nacionales, se enriquece con la comparación frente a estándares internacionales y finalmente se materializa en un modelo de trabajo estructurado. De este modo, la aplicación de ISO 27001 e ISO 27002 se consolida como la estrategia más efectiva para garantizar la confidencialidad, integridad y disponibilidad de la información, al tiempo que fortalece la resiliencia organizacional y asegura la continuidad operativa. Con ello se confirma que la seguridad de la información trasciende el mero cumplimiento legal y se posiciona como un eje estratégico de confianza, sostenibilidad y competitividad para las organizaciones.

Referencias Bibliográficas

Affia, A.-A. O., Matulevicius, R., & Nolte, A. (2020). *Security Risk Management in E- commerce Systems: A Threat-driven Approach.* Obtenido de https://doi.org/10.22364/bjmc.2020.8.2.02

Al-Abdullah, M., Yayla, A., & Al-Atoum, M. S. (15 de Diciembre de 2024). *Teaching Case: Combining Standards to Conduct Risk Assessment at SecureEnd Solutions.* https://jise.org/Volume35/n4/JISE2024v35n4pp461-466.pdf

Altamirano, D. L. (27 de Junio de 2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso.* https://www.redalyc.org/journal/6378/637869113010/html/

Araujo, A. (2021). *ISO 27001: Tu primer paso hacia la protección de datos.* https://blog.hackmetrix.com/iso27001-tu-primer-paso-hacia-la-proteccion-de-datos/

Barker, S. (11 de Septiembre de 2025). *Glosario de Término ISO 27001.* https://hightable.io/iso-27001-glossary-of-terms/

Barker, S. (11 de Septiembre de 2025). *ISO 27001:2013.* https://hightable.io/iso- 27001-glossary-of-terms/iso-270012013/

Barker, S. (11 de Septiembre de 2025). *ISO 27002:2022.* https://hightable.io/iso- 27001-glossary-of-terms/iso-270022022/

BSI ISO/IEC 27001 . (01 de Agosto de 2011). *ISO/IEC 27001 Information Security Management Thames Security Shredding (TSS) Ltd.* https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case- study-Thames-Security-UK-EN.pdf?epslanguage=en-MY

BSI ISO/IEC 27001 . (01 de Agosto de 2012). *ISO/IEC 27001 Information Security Management Thames Security Shredding (TSS) Ltd.* https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case- study-Thames-Security-UK-EN.pdf?epslanguage=en-MY

BSI ISO/IEC 27001. (2012). *BSI ISO/IEC 27001 case study: Fredrickson International.* Obtenido de https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-Fredrickson-International-EN-UK.pdf

Caicedo, L. (2024). *Regulación de Datos Sensibles en Colombia: Alcance y Aplicación.* Obtenido de https://www.compliance.com.co/regulacion-de-datos-sensibles-en-colombia-alcance-y-aplicacion/

Carrillo, V. J., Jaramillo, H. D., Cabrera, S. A., Abad, E. M., & Torres, V. A. (07 de Marzo de 2025). *Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM TOGAF*. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=7170391

Chavez, F. J., Joel, P. G., & Mendoza, d. l. (21 de Agosto de 2023). *El papel de la inteligencia artificial en la seguridad de la información: una revisión de su aplicación en la industria cibernética.* https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/25390/20003

CiberSafety. (05 de Diciembre de 2024). *¿Qué es la gestión de riesgos en la seguridad informática?* Obtenido de https://cibersafety.com/gestion-riesgo-seguridad-informatica/

Computer Security Resource Center. (26 de Septiembre de 2025). *Glosario de términos clave de seguridad de la información.* https://csrc.nist.gov/glossary?index=C

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

Congreso de Colombia. (17 de Octubre de 2012). *LEY ESTATUTARIA 1581 DE 2012.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (13 de Mayo de 2014). *Decreto 886.* https://sedeelectronica.sic.gov.co/sites/default/files/normatividad/Decreto_886_2014.pdf

Córdova, S. J., & Remicio, C. W. (2022). *Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.* https://repositorio.upci.edu.pe/bitstream/handle/upci/634/Tesis_REMICIO_CORDOVA..pdf?sequence=1&isAllowed=y

Corte Constitucional. (2011). *Proyecto de Ley Estatutaria de Habeas Data y Protección de Datos Personales.* https://www.corteconstitucional.gov.co/relatoria/2011/c- 748-11.htm

Dua, S., Shah, P., & AbdAllah, E. G. (2024). *Navigating the Digital Landscape: Enhancing Small.* Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en

El-Hajj, M., & Mirza, Z. A. (2024). *Protección de pequeñas y medianas empresas: un marco y una herramienta especializados de evaluación de riesgos de ciberseguridad.* https://doi.org/10.3390/electronics13193910

Estacio, C. K. (2023). *Modelo de evaluación de seguridad de la información en centros de datos.* https://dialnet.unirioja.es/descarga/articulo/9046150.pdf

Giraldo, M. Y. (2020). *Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad.* https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5550/Yenifer_Zulay_Giraldo_Montes_2021.pdf?sequence=8&isAllowed=y

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (20 de Noviembre de 2018). *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR.* https://arxiv.org/pdf/1811.08531

Holloway, D. (6 de Agosto de 2025). *La guía definitiva de la norma ISO 27002.* https://es.isms.online/iso-27002/#:~:text=ISO%2027002%20proporciona%20un%20conjunto%20de%20referencia%20de,implementaci%C3%B3n%20basada%20en%20las%20mejores%20pr%C3%A1cticas%20reconocidas%20internacionalmente.

Instituto Nacional de Ciberseguriad INCIBE. (28 de Septiembre de 2016). *Guía de privacidad y seguridad en Internet.* https://www.incibe.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf

Instituto Nacional de Ciberseguridad. (2020). *PROTECCIÓN DE LA INFORMACIÓN.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Instituto Nacional de Ciberseguridad. (2021). *Glosario de términos de ciberseguridad.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ISO/IEC 27000. (2018). *INTERNATIONAL STANDARD ISO/IEC 27000.* https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027000-2018.pdf

Jara, F. N., & Jorquera, C. A. (Junio de 2021). *La responsabilidad de la Administración del Estado por incidentes de ciberseguridad.* https://rchdt.uchile.cl/index.php/RCHDT/article/view/58776/67520

Jevelin, & Faza, A. (29 de Noviembre de 2023). *Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification.* https://journal-isi.org/index.php/isi/article/view/572/272

Kaelble, S., Gurzeev, R., & Potekhin, D. (2023). *External Exposure & Attack Surface Management For Dummies.* Obtenido de https://www.cycognito.com/documents/white-papers/External-Exposure-and-Attack-Surface-Management-For-Dummies-CyCognito-Edition-v2.pdf

López, V. C. (2024). *Guía Técnica Metodológica en Seguridad y Ciberseguridad: Un enfoque práctico, caso de estudio.* https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=10747613

Martelo, R. J., Tovar, L. C., & Maza, D. A. (Febrero de 2018). *Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en.* Obtenido de https://scielo.conicyt.cl/pdf/infotec/v29n1/0718-0764-infotec-29-01-00003.pdf

Minaya, M. M., Minaya, M. R., Intriago, N. M., & Intriago, N. J. (21 de Junio de 2023). *Normas Y Estándares En Auditoría: Una Revisión De Su Utilidaden La Seguridad Informática.* https://www.editorialalema.org/index.php/pentaciencias/article/view/700/975

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *Alerta de seguridad: Campaña de ransomware Makop y Crysis en Colombia (COLCERT-AL-2810-054).* https://colcert.gov.co/800/articles-397349_documento_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *Alerta Principales vulnerabilidades explotadas en 2023 COLCERT AL-1511-056.* https://colcert.gov.co/800/articles-398633_documento_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *INFORME DE GESTIÓN Año 2024.* Obtenido de https://www.mintic.gov.co/portal/715/articles-399819_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *Informe Vulnerabilidades Detectadas 2024 Colcert In-20250505-019.* https://www.colcert.gov.co/800/articles-400805_documento_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025). *Técnico Semanal Vulnerabilidades críticas detectadas (1 al 6 de mayo de 2025) COLCERT IN-20250507-020.* https://www.colcert.gov.co/800/articles-401060_documento_1.pdf Monge, L. Z. (2023). *Analisis Comparativo de Metodologías de Análisis de Riesgos Magerit VS Nist SP 800-30.* https://dspace.ups.edu.ec/bitstream/123456789/26671/1/UPS-CT011070.pdf

National Institute of Standards and Technology. (2006). *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems .* https://csrc.nist.gov/publications

Ndegeya, R. U. (2022). *Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs.* https://www.diva- portal.org/smash/get/diva2:1670976/ATTACHMENT01.pdf

Norton Security. (2018). *Protección total para pequeñas empresas.* https://pcgamermexico.com/u/CDNORTON21416109.pdf

NortonLifeLock. (Enero de 2020). *Aviso de privacidad global de NortonLifeLock.* Obtenido de https://www.nortonlifelock.com/us/en/privacy/global-privacy-statement/spanish/

Penagos, M. J., Rentería, G. K., Ibargüen, M. Y., García, P. V., & Castro, R. F. (21 de Diciembre de 2022). *Implementación De Políticas De Seguridad.* https://revistas.uss.edu.pe/index.php/ING/article/view/2271/2783

Presidencia de la República de Colombia. (2013). *DECRETO 1377 DE 2013.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Rodríguez, G. D., Méndez, F. R., & Méndez, F. A. (2023). *Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática.* https://scispace.com/pdf/seguridad-de-la-informacion-en-el-comercio-electronico-283svzy2.pdf

Ruiz, G. M., & Aguirre, O. D. (2020). *Seguridad Informática: Relación E Impacto Frente A La Ley De Protección De Datos Personales (Ley 1581 De 2012)* https://repository.unad.edu.co/bitstream/handle/10596/35057/mpruizga.pdf?sequence=3&isAllowed=y

Sangaroonsilp, P., Khanh, H. D., & Ghose, A. (10 de Febrero de 2023). *On Privacy Weaknesses and Vulnerabilities in Software Systems.* https://arxiv.org/pdf/2112.13997

Superintendencia de Sociedades. (24 de Julio de 2024). *MANUAL Interno De Políticas Y* . https://www.supersociedades.gov.co/documents/107391/3463418/GC-M-003_ManualTratamientoDatosPersonales.pdf