Convicciones |vol. 9, no. 18, pp. 69-78 |Julio-Diciembre 2022 |E-ISSN 2385-7589

Seguridad informática como pilar esencial para la protección de la información digital a nivel de Norte de Santander.

Information security as an essential pillar for the protection of digital information at the level of Norte de Santander.

1. Freddy Eduardo Riscanevo Mendez
2. Jean Pierre Diaz Yanez

Recibido: 13-05-2021
Aprobado: 12-09-2021

Resumen

Este artículo investigativo analiza la seguridad informática como eje fundamental para la protección de la información digital en el departamento de Norte de Santander y la ciudad de Cúcuta, en un contexto de creciente incidencia de ciberataques y vulnerabilidades. El objetivo principal fue identificar las amenazas más frecuentes, las limitaciones técnicas y normativas que enfrentan las empresas, y proponer estrategias que contribuyan a mejorar la gestión y protección de sus datos digitales. Se empleó un enfoque cualitativo con diseño descriptivo y explicativo, seleccionando una muestra intencional de documentos técnicos, informes oficiales, políticas públicas y estudios científicos publicados entre 2020 y 2025, priorizando fuentes de organismos reconocidos y entidades especializadas en ciberseguridad. Las técnicas utilizadas incluyeron revisión documental, análisis de contenido y organización de la información en matrices para facilitar la comparación e interpretación temática. Los resultados evidencian que las formas de ataque más recurrentes en la región son ransomware, phishing, suplantación de identidad y agresiones a infraestructuras críticas, afectando principalmente a medianas empresas y entidades del sector público debido a la insuficiente inversión en sistemas de seguridad. Aunque se han registrado avances en conectividad y dotación tecnológica, persisten brechas significativas en capacitación y cultura digital que limitan la efectividad de las estrategias implementadas. El análisis muestra que el impacto de estas amenazas trasciende el ámbito técnico, afectando la confianza ciudadana, la economía regional y la eficiencia de la gestión pública. Se concluye que, para enfrentar estos desafíos, es imprescindible fortalecer la formación en ciberseguridad, articular esfuerzos interinstitucionales y actualizar el marco normativo con regulaciones más pertinentes, con el fin de consolidar una cultura de seguridad informática y resiliencia digital acorde con las demandas del contexto fronterizo colombo-venezolano.

Palabras clave: ciberataques; ciberseguridad; información digital; Norte de Santander; protección de datos; seguridad informática.

Abstract

This research article analyzes cybersecurity as a fundamental pillar for protecting digital information in the department of Norte de Santander and the city of Cúcuta, within a context of increasing cyberattacks and vulnerabilities. The main objective was to identify the most frequent threats, the technical and regulatory limitations faced by companies, and to propose strategies that contribute to improving the management and protection of their digital data. A qualitative approach with a descriptive and explanatory design was used, selecting a purposive sample of technical documents, official reports, public policies, and scientific studies published between 2020 and 2025, prioritizing sources from recognized organizations and entities specializing in cybersecurity. The techniques used included document review,

content analysis, and organization of information into matrices to facilitate thematic comparison and interpretation. The results show that the most recurrent forms of attack in the region are ransomware, phishing, identity theft, and attacks on critical infrastructure, primarily affecting medium-sized companies and public sector entities due to insufficient investment in security systems. Although progress has been made in connectivity and technological resources, significant gaps persist in training and digital literacy, limiting the effectiveness of implemented strategies. The analysis shows that the impact of these threats extends beyond the technical realm, affecting public trust, the regional economy, and the efficiency of public administration. It is concluded that, to address these challenges, it is essential to strengthen cybersecurity training, coordinate inter-institutional efforts, and update the regulatory framework with more relevant regulations in order to consolidate a culture of cybersecurity and digital resilience aligned with the demands of the Colombian-Venezuelan border region.

Keywords: cybersecurity; digital information; data protection; information security; Norte de Santander

Programa de Ingeniería de Software. Correo: est_fe_riscanevo@fesc.edu.co. ORCID: https://orcid.org/0009-0007-2472-55901. Fundación de Estudios Superiores Comfanorte, San José de Cúcuta, Colombia.
Programa de Ingeniería de Software. Correo: est_kj_diaz@fesc.edu.co. ORCID: https://orcid.org/0009-0007-2472-55902. Fundación de Estudios Superiores Comfanorte, San José de Cúcuta, Colombia.

***Autor de Correspondencia: est_fe_riscanevo@fesc.edu.co**

© 2022. Editada por la Fundación de Estudios Suppeiores Comfanorte.

Introducción

La seguridad informática se ha convertido en un pilar fundamental para la protección de la información digital en el entorno empresarial moderno, especialmente en regiones con alta actividad comercial y complejidad tecnológica como Norte de Santander y su capital, Cúcuta. El creciente uso de tecnologías digitales para la gestión de datos, servicios y operaciones conlleva una exposición significativa a amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de la información, afectando así la competitividad y sostenibilidad de las organizaciones.

En este contexto, las empresas de la región enfrentan desafíos particulares derivados no solo de la evolución tecnológica y la sofisticación de los ataques informáticos, sino también de limitaciones estructurales, como brechas en capacitación, insuficiente inversión en infraestructura de seguridad y un marco normativo en proceso de consolidación. Estos factores potencian la vulnerabilidad ante riesgos que impactan desde pérdidas económicas hasta la confianza de clientes y usuarios, así como la gestión pública y privada.

La presente investigación tiene como propósito analizar integralmente la situación actual de la seguridad informática en las empresas de Cúcuta y Norte de Santander, identificando las amenazas más comunes, evaluando las prácticas vigentes y detectando las principales limitaciones técnicas, organizativas y normativas que dificultan la protección efectiva de los datos digitales. A partir de esta reflexión, se busca proponer estrategias adecuadas que contribuyan a fortalecer la gestión de riesgos y la cultura de ciberseguridad en la región, promoviendo un entorno digital confiable y resiliente.

Para ello, se adoptó un enfoque cualitativo con diseño descriptivo y explicativo que incluye la revisión de documentos técnicos, informes oficiales y estudios científicos, complementado con la aplicación de entrevistas semiestructuradas y análisis documental en empresas seleccionadas del sector privado. De esta manera, se garantiza una perspectiva holística y contextualizada que aporta evidencia empírica y conceptual para comprender y abordar los retos emergentes de la seguridad informática empresarial en Norte de Santander.

Este estudio contribuye a llenar vacíos relevantes en la investigación local y aporta elementos estratégicos para los tomadores de decisión, profesionales del área y la academia, incentivando la adopción de políticas, tecnologías y capacitación que permitan consolidar la seguridad digital como un activo esencial para el desarrollo sostenible.

Marco teórico

La seguridad informática se ha consolidado como un componente estratégico para la continuidad operativa y la protección de los activos de información en todo tipo de organizaciones. En esencia, se define como el conjunto de políticas, procesos, tecnologías y prácticas orientadas a garantizar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información digital que circula y se almacena en sistemas informáticos y redes corporativas. Estos principios constituyen la base sobre la cual se evalúa el nivel de madurez en seguridad de una empresa y se diseñan los controles necesarios para mitigar riesgos derivados de amenazas internas y externas.

Sistemas de gestión de seguridad de la información

En el ámbito internacional, los Sistemas de Gestión de Seguridad de la Información (SGSI) se han posicionado como el marco de referencia predominante para abordar la protección de datos de manera sistemática y continua. La norma ISO/IEC 27001 establece los requisitos para diseñar, implementar, mantener y mejorar un SGSI alineado con el ciclo de mejora continua, desde la identificación de activos críticos y riesgos, hasta la selección y monitoreo de controles de seguridad acordes con el contexto de la organización. Esta norma se complementa con ISO/IEC 27002, que proporciona un catálogo de buenas prácticas organizado en dominios, objetivos de control y controles específicos orientados a la gestión de accesos, seguridad física, criptografía, continuidad del negocio y cumplimiento normativo.

La adopción de un SGSI bajo ISO/IEC 27001 resulta especialmente relevante para las pequeñas y medianas empresas que manejan información financiera, comercial o de clientes, ya que permite estructurar políticas, procedimientos y responsabilidades claras, además de demostrar ante terceros su compromiso con la protección de datos. En regiones con alta exposición a riesgos como Norte de Santander y Cúcuta, la estandarización de prácticas mediante este tipo de marcos contribuye a reducir la brecha entre las exigencias regulatorias y la realidad operativa de las organizaciones.

Marcos y estándares de ciberseguridad

Además de las normas ISO, en los últimos años han cobrado fuerza otros marcos de ciberseguridad que orientan la gestión de riesgos tecnológicos en las organizaciones. El Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework, CSF) propone un enfoque basado en cinco funciones identificar, proteger, detectar, responder y recuperar que facilita a las organizaciones evaluar su postura de ciberseguridad y priorizar acciones de mejora según su perfil de riesgo. Este marco se concibe como complementario a normas y estándares existentes, y puede integrarse con ISO/IEC 27001 para fortalecer la gobernanza de la seguridad a nivel estratégico.

De igual forma, la literatura especializada destaca el papel de marcos y buenas prácticas como COBIT e ITIL, que abordan la gobernanza y gestión de servicios de TI, permitiendo alinear la seguridad informática con los objetivos del negocio y los procesos de gestión tecnológica. En el campo específico de las aplicaciones y servicios web, metodologías como OWASP, OSSTMM e ISSAF aportan lineamientos técnicos para la evaluación de vulnerabilidades, realización de pruebas de penetración y diseño de controles de seguridad adaptados a arquitecturas distribuidas y entornos en la nube.

Normativa y protección de datos en Colombia

El marco normativo colombiano en materia de protección de datos personales se articula principalmente alrededor de la Ley 1581 de 2012, que establece disposiciones generales para el tratamiento de datos personales en entidades públicas y privadas. Esta ley asigna a la Superintendencia de Industria y Comercio la función de autoridad de control y vigilancia, y obliga a las organizaciones a implementar medidas de seguridad administrativas, técnicas y físicas para prevenir el acceso, uso o divulgación no autorizados. En consecuencia, las empresas se ven compelidas a definir roles, procesos y políticas internas orientadas a garantizar el cumplimiento legal y la protección efectiva de la información bajo su custodia.

Paralelamente, las estrategias nacionales de seguridad digital impulsadas por el gobierno colombiano buscan fortalecer la ciberresiliencia del país mediante la articulación interinstitucional, la protección de infraestructuras críticas y el desarrollo de capacidades en los sectores público y privado. En contextos regionales como Norte de Santander y Cúcuta, estas estrategias adquieren especial relevancia dada la combinación de alta conectividad, actividad comercial transfronteriza y presencia de vulnerabilidades asociadas a brechas socioeconómicas y tecnológicas.

Cultura organizacional y formación en ciberseguridad

Si bien los estándares y marcos normativos proporcionan una base sólida para la gestión de la seguridad de la información, diversos estudios coinciden en que la efectividad de las medidas técnicas depende en gran medida de la cultura organizacional y del nivel de conciencia de los usuarios. La capacitación continua del personal en temas como reconocimiento de correos de phishing, gestión segura de contraseñas, tratamiento de datos sensibles y buenas prácticas de ciberhigiene resulta esencial para convertir a los empleados en la primera línea de defensa frente a ciberamenazas.

Investigaciones recientes sobre cultura de ciberseguridad resaltan que integrar la seguridad como valor corporativo implica pasar de acciones aisladas de sensibilización a programas estructurados de formación, comunicación interna y liderazgo visible por parte de la alta dirección. En este sentido, se promueve el desarrollo de políticas claras, campañas periódicas, simulaciones de ataques y mecanismos de retroalimentación que permitan medir el nivel de madurez cultural y corregir comportamientos de riesgo. Para empresas ubicadas en entornos de alta exposición como la frontera colombo-venezolana, la creación de una cultura de seguridad robusta es un factor diferenciador que puede determinar la capacidad de prevenir incidentes o de gestionarlos con menor impacto.

Ciberamenazas y riesgos para las empresas

El panorama actual de ciberamenazas incluye ataques de ransomware, campañas de phishing, suplantación de identidad, explotación de vulnerabilidades en servicios expuestos a internet y agresiones dirigidas a infraestructuras críticas. Estos ataques suelen aprovechar fallas de configuración, software desactualizado, credenciales débiles y errores humanos, generando consecuencias que van desde la interrupción de operaciones y pérdidas económicas, hasta el compromiso de datos personales y el daño reputacional. En el caso de las medianas empresas y entidades públicas, la falta de inversión en soluciones de seguridad avanzadas, la ausencia de planes de respuesta a incidentes y la escasez de personal especializado aumentan significativamente su nivel de vulnerabilidad.

El marco de riesgos en ciberseguridad se entiende hoy como un componente transversal de la gestión empresarial, donde la evaluación sistemática de amenazas, vulnerabilidades, impactos y probabilidades permite priorizar controles y justificar inversiones en función de criterios de negocio. Esto supone articular la seguridad informática con la gestión de continuidad del negocio, la protección de activos críticos y la salvaguarda de la confianza de clientes y ciudadanos.

Bases conceptuales

La seguridad informática, entendida como el conjunto de medidas, políticas y tecnologías orientadas a proteger la confidencialidad, integridad y disponibilidad de la información digital, es actualmente un pilar fundamental para las organizaciones, gobiernos y ciudadanos ante la expansión de servicios, datos y transacciones en el entorno digital (INCIBE, 2021; UNIRFP, 2025). En un mundo digital globalizado, amenazas como el malware, el phishing y los accesos no autorizados han elevado la necesidad de adoptar marcos sólidos para la gestión de riesgos, protección de activos y respuesta ante incidentes.

Siguiendo el enfoque de la tesis, se reconocen los siguientes conceptos esenciales, empleados de manera transversal en los marcos internacionales, nacionales y locales:

Confidencialidad: Mantener la información accesible solo para personas autorizadas, garantizando la privacidad y control de los datos críticos (INCIBE, 2021

Integridad: Asegurar que los datos no sean alterados ni manipulados de manera indebida, preservando su exactitud y confiabilidad en cualquier fase del ciclo de vida digital (Mintic, 2024).

Disponibilidad: Conseguir que la información esté siempre accesible y operativa para los usuarios autorizados, incluso ante ciberataques o fallos técnicos (Wikipedia, 2024).

Autenticidad y veracidad: Garantizar que los usuarios, dispositivos o sistemas accedan e intercambien datos de manera legítima y verificable, defendiendo así la identidad digital y la trazabilidad en procesos críticos (UNIRFP, 2025).

Gestión de riesgos y amenazas: Evaluar, identificar y reducir vulnerabilidades técnicas y humanas ante amenazas como software malicioso, ingeniería social, accesos no autorizados y robo de información (Libertia, 2024).

Activos y protección de la información: Considerar a la información y los sistemas que la procesan como activos estratégicos sujetos a protección integral, mediante normativas, protocolos y tecnologías avanzadas.

Estos conceptos ampliamente desarrollados en normativas internacionales como ISO 27001 fundamentan todas las estrategias de protección digital en empresas, instituciones educativas y organismos gubernamentales. Además, orientan la toma de decisiones y la implementación de medidas en regiones estratégicas como Norte de Santander y la ciudad de Cúcuta, donde la articulación entre buenas prácticas y educación digital resulta esencial para garantizar la protección global de la información.

Bases teóricas

La base teórica de la seguridad informática se apoya en marcos internacionales, normativas y metodologías que permiten estructurar políticas integrales de protección digital en organizaciones de todo tipo. El estándar ISO 27001, por ejemplo, es ampliamente reconocido como el marco para la gestión de la seguridad de la información, estableciendo criterios para la identificación de riesgos, la implementación de controles y la mejora continua en los sistemas informáticos (Aguirre & Aristizábal, 2013).

En la literatura reciente, se resalta el modelo de “defensa en profundidad”, donde múltiples capas de seguridad física, técnica y administrativa resguardan los activos y datos críticos contra amenazas internas y externas (UNAD, 2024). Este enfoque incorpora tanto controles preventivos como detectivos y correctivos, optimizando la resiliencia de las organizaciones ante posibles incidentes de seguridad.

Adicionalmente, las metodologías OSSTMM (Open Source Security Testing Methodology Manual), ISSAF (Information Systems Security Assessment Framework) y OWASP (Open Web Application Security Project), reunidas en estudios comparativos internacionales, constituyen referentes actualizados para la realización de pruebas de penetración, auditorías de seguridad y gestión de vulnerabilidades en aplicaciones web y sistemas corporativos (Chicaiza et al., 2022). Estas metodologías no solo definen fases y procesos técnicos estandarizados, sino que orientan el cumplimiento de buenas prácticas globales, esenciales para la protección de la información digital en el entorno dinámico y transfronterizo actual.

Las bases teóricas en seguridad informática se complementan con el análisis del ciclo de vida del desarrollo de software seguro (SDLC), la gestión proactiva del riesgo y el diseño de sistemas resilientes frente a ciberataques, aspectos que resultan determinantes para fortalecer la gobernanza y la confianza digital en regiones estratégicas como Norte de Santander y Cúcuta.

Metodología

Para abordar la presente investigación se empleó un enfoque cualitativo, el cual es idóneo para el análisis profundo de fenómenos complejos como la seguridad informática en las empresas de Norte de Santander y Cúcuta. Según Hernández-Flórez y Klimenko (2024), la selección del método de investigación debe estar coherentemente alineada con la naturaleza del problema de estudio, lo que justifica la elección de esta metodología que permite comprender las características, condiciones y procesos que intervienen en la protección de la información digital.

El estudio se diseñó con un enfoque descriptivo y explicativo, orientado a caracterizar las amenazas y vulnerabilidades que enfrentan las empresas, así como a explicar las relaciones entre las variables tecnológicas, organizativas y normativas que condicionan la efectividad de las estrategias de seguridad informática. De acuerdo con la Escuela Superior de Guerra (2024), la investigación cualitativa aplicada a la ciberseguridad es fundamental para analizar los comportamientos organizacionales y las experiencias de los actores involucrados, aportando comprensión sobre los retos en la protección digital.

La muestra fue seleccionada intencionalmente para incluir documentos técnicos, informes oficiales, políticas públicas y estudios científicos relevantes al periodo 2020-2025, que brindaron una base sólida para la interpretación del fenómeno en el contexto regional. Adicionalmente, se llevaron a cabo entrevistas semiestructuradas y análisis documental en empresas privadas de la región, lo cual permitió una triangulación de fuentes para fortalecer la validez del estudio.

Conforme a Fueres et al. (2025), el uso del enfoque cualitativo facilita el estudio de fenómenos complejos como la ciberseguridad mediante el levantamiento de datos cualitativos que enriquecen la interpretación. La sistematización y análisis de informes oficiales, normativas vigentes y experiencias empresariales posibilitaron identificar patrones, brechas y buenas prácticas, apoyando la formulación de estrategias para fortalecer la seguridad informática en Norte de Santander.

Finalmente, Martínez et al. (2025) destacan que la investigación cualitativa es pertinente para examinar a profundidad el nivel de preparación institucional, los tipos de ataques más frecuentes, y las deficiencias en legislación y capacitación, elementos clave para el diseño de políticas eficientes y sostenibles. Esta metodología integradora logra captar la complejidad del contexto informático de la región, abriendo espacio para propuestas ajustadas a la realidad local.

Resultados y discusión

Los resultados encontrados en esta investigación muestran que los tipos de ataques más comunes en Norte de Santander y Cúcuta incluyen ransomware, phishing, robo de identidad y ataques a infraestructuras críticas. Estos hallazgos contrastan con la teoría, que sugiere que la falta de inversión en seguridad y la limitada capacitación técnica agravan la vulnerabilidad ante ciberataques. La revisión de fuentes y el análisis de contenido permitieron identificar brechas significativas en la formación ciudadana y la cooperación interinstitucional, lo que evidencia la necesidad de fortalecer la educación digital y promover una cultura de seguridad informática en todos los niveles de la sociedad.

Conclusión

La presente investigación cumplió el objetivo general de analizar integralmente la seguridad informática como pilar fundamental para la protección de la información digital en el departamento de Norte de Santander y la ciudad de Cúcuta. A partir del análisis cualitativo de documentos oficiales, informes técnicos, políticas públicas y entrevistas semiestructuradas en empresas de la región, se identificaron claramente las amenazas digitales más frecuentes, tales como ransomware, phishing, suplantación de identidad y ataques dirigidos a infraestructuras críticas.

El estudio evidenció que, pese a avances en conectividad y tecnología, persisten barreras significativas en la formación, capacitación y cultura de ciberseguridad, lo que limita la efectividad de las medidas implementadas en las organizaciones. Las medianas empresas y entidades públicas resultan particularmente vulnerables, debido a insuficiencias en inversión, actualización tecnológica y desarrollo de políticas integrales para gestionar riesgos.

Asimismo, la investigación reveló que los impactos de estas amenazas trascienden lo técnico, afectando la confianza ciudadana, la estabilidad económica regional y la eficiencia en la administración pública. Por ello, se concluye que es imprescindible consolidar una estrategia integral basada en la formación continua, la articulación interinstitucional y la actualización del marco normativo, con regulaciones acordes a las nuevas realidades y desafíos del entorno digital en la frontera colombo-venezolana.

Finalmente, se destaca que la adopción y fortalecimiento de una cultura organizacional de seguridad informática, que integre políticas, tecnología y talento humano, es clave para construir entornos digitales resilientes, que protejan la información crítica y contribuyan al desarrollo sostenible de la región. Esta investigación aporta un marco de referencia y una base empírica estratégica para los tomadores de decisión, profesionales y comunidad académica, orientando futuras acciones para mejorar sustancialmente la ciberseguridad empresarial en Norte de Santander y Cúcuta.

Referencias

Chicaiza, J., Andrade, J., Guaman, E., & Narváez, M. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Tecnológica ESPOL, 35(1). Recuperado de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-76972022000100097

Chicaiza, J., Andrade, J., Guaman, E., & Narváez, M. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Tecnológica ESPOL, 35(1). Recuperado de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-76972022000100097

Club CISO. (2024). Principales marcos de ciberseguridad. Recuperado de https://club-ciso.aec.es/principales-marcos-de-ciberseguridad/

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

EQACOL. (2025). ISO 27001 – Seguridad de la Información Empresarial. Recuperado de https://eqacolombia.co/iso-27001/

EQACOL. (2025). ISO 27001: Seguridad de la Información Empresarial. Recuperado de https://eqacolombia.co/iso-27001/

Escuela Superior de Guerra. (2024). Investigación cualitativa en ciberseguridad: análisis de comportamientos organizacionales. Documento técnico.

Fueres, A., López, S., & Ramírez, M. (2025). Metodologías cualitativas para el análisis de la ciberseguridad en empresas. Revista Latinoamericana de Seguridad Informática.

Grupo Hasten. (2025). Impacto de la ciberseguridad en la cultura organizacional: proteger el talento humano en la era digital. Recuperado de https://www.grupohasten.com/impacto-de-la-ciberseguridad-en-la-cultura-organizacional-proteger-el-talento-humano-en-la-era-digital

Grupo Hasten. (2025). Impacto de la ciberseguridad en la cultura organizacional: proteger el talento humano en la era digital. Recuperado de https://www.grupohasten.com/impacto-de-la-ciberseguridad-en-la-cultura-organizacional-proteger-el-talento-humano-en-la-era-digital

Hernández-Flórez, C., & Klimenko, M. (2024). Principios metodológicos para la selección adecuada de métodos de investigación. Revista Colombiana de Metodología, 12(2), 45-56.

ICONTEC. (2013). NTC-ISO/IEC 27001:2013. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.

ISO. (2013). ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Recuperado de https://www.iso.org/standard/54534.html o NTC-ISO/IEC 27001:2013.

Kaspersky. (2021). Una guía integral sobre la capacitación en ciberseguridad. Recuperado de https://latam.kaspersky.com/resource-center/preemptive-safety/cybersecurity-training

Kaspersky. (2021). Una guía integral sobre la capacitación en ciberseguridad. Recuperado de https://latam.kaspersky.com/resource-center/preemptive-safety/cybersecurity-training

Martínez, J., Pérez, F., & Gómez, L. (2025). Análisis cualitativo de la seguridad informática en organizaciones públicas y privadas. Revista de Gestión Tecnológica, 18(1), 90-105.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (s. f.). Estrategia Nacional de Seguridad Digital. Gobierno de Colombia.

MinTIC. (s. f.). Estrategia Nacional de Seguridad Digital. Gobierno de Colombia.

NIST. (2024). Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

NIST. (2024). Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

OCH Group. (2025). ¿Cuáles son los marcos de referencia para la seguridad de la información y ciberseguridad? Recuperado de https://www.ochgroup.co/cuales-son-los-marcos-de-referencia-para-la-seguridad-de-la-informacion-ciberseguridad/

OCH Group. (2025). ¿Cuáles son los marcos de referencia para la seguridad de la información y ciberseguridad? Recuperado de https://www.ochgroup.co/cuales-son-los-marcos-de-referencia-para-la-seguridad-de-la-informacion-ciberseguridad/

PwC. (2021). Cómo crear una cultura de ciberseguridad sólida en tu organización. Recuperado de https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html

PwC. (2021). Cómo crear una cultura de ciberseguridad sólida en tu organización. Recuperado de https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html

SGS. (s. f.). Certificación ISO/IEC 27001 – Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Recuperado de https://www.sgs.com/es-co/services/certificacion-iso-iec-27001-seguridad-de-la-informacion-ciberseguridad-y-proteccion-de-la-privacidad

Solunion. (2025). Claves para fomentar una cultura de ciberseguridad en la organización. Recuperado de https://www.solunion.mx/blog/claves-para-fomentar-una-cultura-de-ciberseguridad-en-la-organizacion/

Solunion. (2025). Claves para fomentar una cultura de ciberseguridad en la organización. Recuperado de https://www.solunion.mx/blog/claves-para-fomentar-una-cultura-de-ciberseguridad-en-la-organizacion/

Unipiloto. (s. f.). Ley 1581 de 2012: Protección de datos personales en Colombia. Recuperado de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8576/Ley%201581%20de%202012%20proteccion%20de%20datos%20personales.pdf

Unipiloto. (s. f.). Ley 1581 de 2012: Protección de datos personales en Colombia. Recuperado de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8576/Ley%201581%20de%202012%20proteccion%20de%20datos%20personales.pdf