



# Seguridad cibernética y amenazas actuales

xxxxxxxxxx  
xxxxxxxxxx  
xxxxxxxxxx

**Autores:**  
Angie Daniela Giraldo  
Andhry Vanessa Chavarro Moyano

## Resumen

El artículo aborda la creciente relevancia de la ciberseguridad en un mundo cada vez más dependiente de la tecnología digital, con un enfoque particular en Colombia. Destaca cómo la transformación digital ha incrementado la vulnerabilidad ante ciberataques, afectando tanto a organizaciones como a ciudadanos. Amenazas como el phishing, malware y ransomware han generado pérdidas económicas y comprometen la estabilidad de infraestructuras críticas como la salud y la banca. Aunque el país ha avanzado con iniciativas como la Estrategia Nacional de Ciberseguridad y Ciberdefensa y la creación del Centro Cibernético Policial, persisten desafíos significativos en términos de capacitación de profesionales, concienciación pública y desarrollo de infraestructuras tecnológicas robustas.

El documento subraya la importancia de la educación y la colaboración entre sectores público y privado para enfrentar las amenazas cibernéticas. La formación de talento especializado, el fortalecimiento de la legislación y el impulso de una cultura organizacional enfocada en la seguridad son claves para mitigar riesgos. Finalmente, se recalca que la ciberseguridad no es solo un desafío técnico, sino también una cuestión de confianza y estabilidad social, que requiere un esfuerzo conjunto entre gobiernos, empresas y ciudadanos para construir un entorno digital seguro y resiliente.

### Palabras claves:

Ciberseguridad, Ciberataques, Phishing, Ransomware, Transformación digital, Estrategia Nacional de Ciberseguridad.

## Abstract

The article addresses the growing relevance of cybersecurity in a world increasingly dependent on digital technology, with a particular focus on Colombia. It highlights how digital transformation has increased vulnerability to cyberattacks, affecting both organizations and citizens. Threats such as phishing, malware, and ransomware have caused economic losses and jeopardized the stability of critical infrastructures like healthcare and banking. Although the country has made progress with initiatives such as the National Cybersecurity and Cyberdefense Strategy and the creation of the Cyber Police Center, significant challenges remain in terms of professional training, public awareness, and the development of robust technological infrastructures.

The document emphasizes the importance of education and collaboration between the public and private sectors to address cyber threats. Developing specialized talent, strengthening legislation, and fostering an organizational culture focused on security are key to mitigating risks. Finally, it underscores that cybersecurity is not only a technical challenge but also a matter of trust and social stability, requiring a collective effort by governments, businesses, and citizens to build a safe and resilient digital environment.

### Keywords:

Cybersecurity, Cyberattacks, Phishing, Ransomware, Digital Transformation, National Cybersecurity Strategy.

# Introducción

La tecnología ha revolucionado el mundo y nuestra forma de vivir, usualmente vista con optimismo. No obstante, es crucial reconocer que junto a sus beneficios surgen desafíos importantes. La tecnología se ha convertido en una herramienta esencial para las empresas y un elemento estratégico fundamental para la economía de cualquier país, trayendo consigo cambios significativos en los ámbitos económico, social, cultural, militar, político y educativo de Colombia. Sin embargo, también ha dado lugar a ciber amenazas. Es importante comprender el impacto de eventos como apagones de computadores o ataques a procesos industriales, que afectan gravemente a las naciones de manera digital y virtual. El nuevo concepto de guerra se basa en armas digitales, difíciles de detectar. Es crucial comprender que a mayor desarrollo de una sociedad, mayor es su dependencia de la tecnología y de los sistemas de información y comunicaciones, lo que incrementa su vulnerabilidad y el riesgo de sufrir incidentes de seguridad en la información e infraestructura crítica. En Colombia, se ha adoptado una estrategia para prevenir y enfrentar delitos cibernéticos y minimizar el riesgo para los ciudadanos ante amenazas o incidentes cibernéticos. Esta estrategia, impulsada por el gobierno, establece los lineamientos de la Política para Ciberseguridad y Ciberdefensa, representando un avance significativo en seguridad. Es una estrategia integral que aborda los desafíos de seguridad interna y el cibercrimen que pueden surgir dentro de las comunidades o individuos que utilizan el ciberespacio en nuestra sociedad.



## Antecedentes destacados

Uno de los antecedentes más relevantes es el creciente número de ataques cibernéticos en Colombia, que ha experimentado un aumento significativo en los últimos años. Según informes, empresas y entidades gubernamentales han sido blanco de ciberataques, con consecuencias económicas y de seguridad nacional. El incidente del año 2016, cuando varios sistemas de la Registraduría Nacional del Estado Civil fueron hackeados, subraya la urgencia de fortalecer la ciberseguridad en el país. Además, la transformación digital de sectores clave como la banca, la salud y la educación ha incrementado la superficie de ataque, exponiendo vulnerabilidades críticas.

Otro antecedente crucial es la evolución de las legislaciones y normativas en ciberseguridad. La Ley 1273 de 2009, que tipifica el delito informático y protege la información y los datos, marcó un hito en el marco legal colombiano. Sin embargo, la rápida evolución de las amenazas cibernéticas ha exigido una actualización constante de estas normativas. La Estrategia Nacional de Ciberseguridad y Ciberdefensa, lanzada en 2016, ha sido un paso fundamental para consolidar una respuesta coordinada y efectiva ante las ciberamenazas.

### Razones para Realizar este Artículo

La relevancia de este artículo radica en la necesidad de comprender y divulgar el impacto de la ciberseguridad en la sociedad colombiana. La tecnología y la digitalización no solo ofrecen oportunidades de desarrollo, sino que también presentan desafíos que requieren una atención y acción inmediatas. Al abordar este tema, se busca sensibilizar a los actores clave sobre la importancia de la ciberseguridad y fomentar una cultura de prevención y protección.

Además, la proliferación de ciberataques y la creciente dependencia de la tecnología en todos los ámbitos de la vida diaria hacen imperativo contar con un conocimiento profundo de las estrategias y políticas existentes. Este artículo no solo pretende informar, sino también promover el desarrollo de capacidades y competencias en ciberseguridad, tanto a nivel institucional como individual.



## Objetivo de la Revisión

El objetivo principal de esta revisión es analizar y evaluar las estrategias y políticas de ciberseguridad implementadas en Colombia, identificando sus fortalezas y áreas de mejora. Se busca proporcionar una visión integral de los desafíos y avances en la ciberdefensa del país, ofreciendo recomendaciones para fortalecer la seguridad digital. Asimismo, se pretende concienciar a la sociedad sobre la importancia de la ciberseguridad y la necesidad de una colaboración continua entre el sector público, privado y la ciudadanía para enfrentar eficazmente las amenazas cibernéticas.

## Seguridad Cibernética y Amenazas Actuales

El mundo ha experimentado un cambio significativo con la llegada de internet, revolucionando nuestra forma de comunicarnos, trabajar e interactuar. Aunque esto ha traído numerosos beneficios, también ha generado peligros que pueden comprometer nuestra información personal y empresarial. Todos los dispositivos conectados a internet están en riesgo si no se protegen adecuadamente, lo que puede llevar a la pérdida de datos y afectar a personas cercanas.

## Amenazas de Ciberseguridad

Las amenazas de ciberseguridad son ataques dirigidos a organizaciones con diversos objetivos, como robar información sensible, interrumpir servicios o realizar acciones perjudiciales. Discutir sobre estos incidentes resulta complicado debido a la falta de información disponible públicamente y la confidencialidad mantenida por las organizaciones afectadas para proteger su reputación.

## Fuentes de Amenazas

Las empresas enfrentan amenazas cibernéticas de diversas fuentes, desde delincuentes poco sofisticados hasta actores altamente capacitados respaldados por estados-nación o el crimen organizado. Los ciberataques pueden ser muy lucrativos para los atacantes, proporcionando acceso a información valiosa o permitiendo la realización de objetivos políticos.



## Tipos de amenazas

**Phishing:** Correos electrónicos y sitios web falsos que engañan a los empleados para que revelen credenciales de acceso.

**Malware:** Software malicioso diseñado para infiltrarse y dañar sistemas informáticos.

**Hacking:** Técnicas avanzadas para explotar vulnerabilidades en sistemas y redes.

## Impacto de las amenazas

Los ataques cibernéticos no solo afectan a las organizaciones, sino también a proveedores y usuarios, pudiendo tener repercusiones en la seguridad nacional o regional. Para garantizar la seguridad de los datos, es crucial cumplir con los tres pilares fundamentales de la seguridad de la información:

**Disponibilidad:** La información debe estar accesible para los autorizados.

**Integridad:** Los datos deben mantenerse precisos y sin alteraciones.

**Confidencialidad:** Solo las personas, procesos o aplicaciones autorizadas deben acceder a la información sensible.

## Medidas de Seguridad

Contar con un oficial de seguridad informática puede prevenir muchos problemas. Este profesional se encarga de proteger la información, realizando análisis continuos de los sistemas para identificar posibles amenazas y vulnerabilidades. Aunque algunas empresas se preocupan por el costo, es crucial considerar el costo potencial de un ataque cibernético comparado con la inversión en un oficial de seguridad.

## Conciencia y Educación

La ciberseguridad no es solo una cuestión de implementar herramientas y establecer políticas, sino también de educar y concienciar a los empleados sobre la importancia de protegerse en el entorno digital. Una mayor conciencia y educación en ciberseguridad pueden ayudar a prevenir ataques y proteger los activos digitales.

## Desafíos y Avances en Colombia

El panorama actual de la ciberseguridad en Colombia presenta serios desafíos. El país ha enfrentado un incremento significativo en los ataques cibernéticos, desde robos de identidad hasta la proliferación de malware. Esta situación se debe en parte a la falta de conciencia generalizada y la ausencia de una legislación efectiva. Sin embargo, hay avances prometedores, como la creación de una agencia independiente dedicada a la seguridad cibernética y acuerdos estratégicos con el Departamento de Seguridad Nacional de Estados Unidos.

# Importancia de la Ciberseguridad

La ciberseguridad representa un desafío global que requiere una respuesta integral y coordinada. Colombia ha progresado en su lucha contra las amenazas cibernéticas, pero aún enfrenta retos importantes en términos de concientización y fortalecimiento de la infraestructura de seguridad. Es crucial que el país continúe invirtiendo en ciberseguridad, promoviendo la educación y fomentando la colaboración entre los sectores público y privado.

## Evaluación de Recursos Humanos en Ciberseguridad

La ciberseguridad se ha convertido en una prioridad para las organizaciones y gobiernos en todo el mundo, y Colombia no es la excepción. La creciente cantidad de ciberataques y la complejidad de las amenazas han generado una demanda significativa de profesionales capacitados en ciberseguridad. Esta necesidad de talento especializado es crítica para proteger los activos digitales y garantizar la integridad de los sistemas de información.

## Disponibilidad de Profesionales en Ciberseguridad

En Colombia, la disponibilidad de profesionales en ciberseguridad es aún limitada en comparación con la demanda existente. Las empresas y entidades gubernamentales buscan cada vez más expertos capaces de diseñar, implementar y gestionar estrategias de seguridad eficaces. Sin embargo, la oferta de profesionales con las competencias necesarias no ha crecido al mismo ritmo.

Esta situación ha llevado a un déficit de talento en el sector, lo que representa un desafío significativo para la seguridad digital del país. Muchas organizaciones se ven obligadas a competir por un número reducido de expertos, lo que puede incrementar los costos salariales y dificultar la retención de talento.

## Formación y capacitación

La formación y capacitación en ciberseguridad es esencial para cerrar la brecha de habilidades en este campo. En Colombia, diversas universidades y centros de formación técnica han comenzado a ofrecer programas especializados en ciberseguridad. Estos programas están diseñados para equipar a los estudiantes con las habilidades y conocimientos necesarios para enfrentar las amenazas cibernéticas actuales.

Entre las iniciativas educativas destacadas se encuentran:

**Programas Universitarios:** Varias universidades colombianas han incorporado carreras y posgrados en ciberseguridad. Estos programas incluyen asignaturas en criptografía, análisis forense digital, gestión de incidentes y legislación en ciberseguridad.

**Cursos de Certificación:** Existen numerosos cursos de certificación que permiten a los profesionales mejorar sus competencias y obtener credenciales reconocidas internacionalmente, como Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) y Certified Information Security Manager (CISM).

## Capacitación Corporativa

Muchas empresas han implementado programas de capacitación interna para su personal, con el objetivo de sensibilizar y preparar a todos los empleados en prácticas seguras de ciberseguridad. Esto incluye desde el uso adecuado de contraseñas hasta la detección de intentos de phishing.

## Demanda de Profesionales en Ciberseguridad

La demanda de profesionales en ciberseguridad en Colombia ha aumentado considerablemente en los últimos años. Las empresas, conscientes de los riesgos asociados a los ciberataques, buscan cada vez más especialistas que puedan proteger sus sistemas y datos. Sectores como la banca, telecomunicaciones, salud y gobierno son especialmente activos en la búsqueda de talento en ciberseguridad.

Este aumento en la demanda también se refleja en las oportunidades de empleo y las condiciones laborales. Los profesionales en ciberseguridad suelen recibir salarios competitivos y beneficios adicionales, lo que hace que esta carrera sea atractiva para muchos jóvenes.

## Formación y capacitación

Para abordar la escasez de profesionales en ciberseguridad, se han implementado varias iniciativas:

**Alianzas Público-Privadas:** El gobierno colombiano ha trabajado en colaboración con empresas privadas para desarrollar programas de capacitación y promoción de carreras en ciberseguridad. Estas alianzas buscan crear un ecosistema de talento robusto y sostenible.

**Becas y Subvenciones:** Se han creado programas de becas y subvenciones para estudiantes interesados en ciberseguridad, con el objetivo de incentivar el estudio de esta disciplina y apoyar a aquellos que desean especializarse.

**Eventos y Conferencias:** La organización de eventos y conferencias sobre ciberseguridad ha aumentado en Colombia. Estos eventos no solo sirven para capacitar a los profesionales, sino también para crear una red de contactos y compartir conocimientos sobre las últimas tendencias y amenazas.

**Promoción de la Carrera:** La promoción de la ciberseguridad como una carrera viable y atractiva es clave. Iniciativas en colegios y universidades que destacan la importancia y las oportunidades en este campo son esenciales para atraer a nuevos talentos. La evaluación de recursos humanos en ciberseguridad en Colombia revela una necesidad urgente de formación y desarrollo de talento especializado. Aunque se han dado pasos importantes para aumentar la oferta de profesionales capacitados, aún queda mucho por hacer para cerrar la brecha entre la oferta y la demanda. La colaboración entre el gobierno, las instituciones educativas y el sector privado será crucial para fortalecer la ciberseguridad en el país y proteger sus activos digitales en el futuro.

## Conclusiones

La ciberseguridad se ha convertido en un desafío crítico en el siglo XXI, especialmente en Colombia, donde el aumento de ciberataques ha expuesto la vulnerabilidad de infraestructuras digitales y la necesidad urgente de medidas de protección robustas. Incidentes como el phishing, ransomware y hacking han generado graves pérdidas económicas y comprometen servicios esenciales como la salud y la banca. Para enfrentar estos retos, el gobierno ha implementado iniciativas como el Centro Cibernético Policial (CCP) y la Estrategia Nacional de Ciberseguridad y Ciberdefensa, promoviendo una respuesta coordinada y fomentando la colaboración entre sectores. Sin embargo, aún se requiere mayor inversión en tecnología, capacitación profesional y conciencia pública.

La ciberseguridad también depende de marcos legales que evolucionen al ritmo de las amenazas y de una colaboración internacional para enfrentar riesgos transfronterizos. Es crucial que individuos, empresas y gobiernos trabajen juntos, desde prácticas seguras en línea hasta políticas públicas que fortalezcan un entorno digital resiliente. Solo a través de un esfuerzo colectivo y continuo podrá Colombia adaptarse a las nuevas amenazas y garantizar un futuro digital seguro, confiable y próspero para todos.



## Referencias Bibliográficas

- <https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/>
- [https://youtu.be/mHAdqq\\_7FXg?si=kTKfVEEtNPETm\\_ZP](https://youtu.be/mHAdqq_7FXg?si=kTKfVEEtNPETm_ZP)
- [https://www.airuniversity.af.edu/Portals/10/ASP%20Spanish/Journals/Volume-29\\_Issue-1/2017\\_1\\_09\\_caceres\\_s.pdf](https://www.airuniversity.af.edu/Portals/10/ASP%20Spanish/Journals/Volume-29_Issue-1/2017_1_09_caceres_s.pdf)
- <https://es.linkedin.com/pulse/ciberseguridad-en-colombia-2021-seis-ataques-y-jeimy-cano-ph-d-cfe>
- <https://www.larepublica.co/alta-gerencia/practicas-de-los-trabajadores-que-ponen-en-peligro-la-ciberseguridad-de-una-empresa-3690130>
- <https://fenixpuntonet.com/articulos/ciber-seguridad-en-colombia-file:///home/chronos/u-4c1ce031fb1bc715bc361696e9efb9a583c68015/MyFiles/Downloads/Dialnet-EstadoActualDeLaPoliticaPublicaDeCiberseguridadYCib-7496888.pdf>
- <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y>
- <https://ti724.com/ciberseguridad-en-colombia-desafios-y-avances-en-la-era-digital/>
- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC). (2023). Informe sobre la Estrategia Nacional de Ciberseguridad y Ciberdefensa. Disponible en: [www.mintic.gov.co](http://www.mintic.gov.co)
- Centro Cibernético Policial (CCP). (2022). Informe anual sobre la demanda de profesionales en ciberseguridad en Colombia. Policía Nacional de Colombia. Disponible en: [www.ccp.gov.co](http://www.ccp.gov.co)
- Observatorio Colombiano de Ciberseguridad. (2023). Estudio sobre la oferta y demanda de talento en ciberseguridad en Colombia. Disponible en: [www.observatoriociberseguridad.co](http://www.observatoriociberseguridad.co)
- Gartner. (2022). Top Security and Risk Management Trends. Disponible en: [www.gartner.com](http://www.gartner.com)
- ISACA. (2023). State of Cybersecurity Report. Disponible en: [www.isaca.org](http://www.isaca.org)
- Symantec. (2023). Internet Security Threat Report. Disponible en: [www.symantec.com](http://www.symantec.com)
- Universidad de los Andes. (2023). Programa de Maestría en Seguridad de la Información y Ciberseguridad. Disponible en: [www.uniandes.edu.co](http://www.uniandes.edu.co)
- Kaspersky Lab. (2023). Global IT Security Risks Survey. Disponible en: [www.kaspersky.com](http://www.kaspersky.com)
- CompTIA. (2023). Cybersecurity Workforce Study. Disponible en: [www.comptia.org](http://www.comptia.org)