2025

ANÁLISIS

PROSPECTIVO EN MATERIA DE CIBERSEGURIDAD

CRC
COMISIÓN DE REGULACIÓN DE COMUNICACIONES

www.crcom.gov.co

@CRCCol /CRCCol /CRCCol CRCCOL @CRCCol

//COL

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMITÉ DE COMISIONADOS DE COMUNICACIONES

Claudia Ximena Bustamante Osorio
Comisionada y Directora Ejecutiva

Lina María Duque del Vecchio
Comisionada

Felipe Augusto Díaz Suaza
Comisionado

Javier Gutiérrez Afanador
Comisionado

EQUIPO DE TRABAJO

Sandra Milena Rico Vera
Andrés Ricardo Sanabria Garay
Germán Darío Rodríguez Ávila

Diana Paola Morales Mora
Coordinadora de Prospectiva Estratégica e Innovación

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

AGRADECIMIENTOS

La Comisión de Regulación de Comunicaciones (CRC) agradece a todas las entidades, organizaciones y personas que participaron en la elaboración de este documento. Su conocimiento, disposición y aportes han sido fundamentales para enriquecer el análisis y fortalecer las recomendaciones presentadas.

En particular, se reconoce la participación de representantes del sector de telecomunicaciones, la academia, la industria, la sociedad civil y las entidades públicas, cuyas experiencias y propuestas permitieron consolidar un trabajo incluyente y pertinente para los diversos actores del ecosistema digital.

Asimismo, la CRC expresa su reconocimiento a los expertos nacionales e internacionales que contribuyeron con sus conocimientos y experiencia al desarrollo de este documento técnico sobre ciberseguridad. Se destaca especialmente la activa intervención de quienes formaron parte de las mesas sectoriales durante el primer semestre de 2025, cuyo compromiso resultó esencial para la obtención de resultados relevantes.

Finalmente, se valora la colaboración de los distintos profesionales y organizaciones que, mediante su apoyo y aportes, hicieron posible la consolidación de los análisis expuestos. Su participación ha sido clave para abordar los retos actuales en materia de ciberseguridad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

INTRODUCCION

La Comisión de Regulación de Comunicaciones (CRC) presenta este estudio como parte integral de la visión prospectiva establecida en la ***Agenda Regulatoria 2025-2026****. El documento responde a una de las actividades estratégicas:* ***«Retos de seguridad en el ecosistema digital»****, el cual recoge las opiniones del sector mediante un proceso de escucha activa realizado en mesas sectoriales con actores relevantes del sector público y privado, expertos internacionales en ciberseguridad y representantes académicos, así como organizaciones especializadas en seguridad digital. Además, el estudio se ha enriquecido por medio de una exhaustiva investigación orientada a promover el* ***desarrollo de capital humano****, fomentar la colaboración e incentivar la investigación y la inversión en soluciones más eficientes.*

Hoy, la ciberseguridad trasciende y no es una cuestión reservada para expertos: es un imperativo estratégico que atraviesa todos los sectores y afecta profundamente a la sociedad. Por eso, este documento representa una invitación a elevar nuestra conciencia colectiva y fomentar acciones contundentes ante amenazas cibernéticas cada vez más avanzadas, incentivando la formación, el fortalecimiento de competencias y la adopción de buenas prácticas en materia de seguridad digital.

La CRC presenta este documento abierto que contiene análisis y recomendaciones con el fin de proporcionar una guía fundamentada en experiencias, tendencias relevantes y conocimientos especializados. Se promueve un enfoque de «toda la sociedad» que involucra al sector público, privado, académico y a la sociedad civil, fomentando la colaboración intersectorial. La ciberseguridad se entiende como una responsabilidad colectiva, esencial para consolidar un ecosistema digital confiable y resiliente.

Este documento es un llamado a la acción para fortalecer la ciberseguridad, promueve la educación y evolución de habilidades, el trabajo colaborativo, la conformación de redes de cooperación y la exploración de nuevas capacidades para hacer frente a amenazas cibernéticas cada vez más sofisticadas. El mundo de la ciberseguridad es un campo de batalla de alto riesgo, y los desafíos nunca han sido tan grandes. A medida que la tecnología se vuelve más inteligente, rápida e integrada, los ciberdelincuentes avanzan al mismo ritmo, adaptando sus tácticas para aprovechar cada vulnerabilidad.

Este documento inicia con un análisis exhaustivo sobre el estado actual y los desafíos futuros de la ciberseguridad, con especial énfasis en el sector de telecomunicaciones y la protección de infraestructuras críticas para el año 2026. Se aborda la evolución de amenazas, vectores de ataque, normativas internacionales y nacionales, así como estrategias de defensa inteligente basadas en inteligencia artificial y colaboración multisectorial.

El documento señala que el año 2026 será un punto de inflexión donde convergen tendencias tecnológicas como la democratización de la inteligencia artificial (IA), la computación cuántica y la expansión de la superficie de ataque debido a la hiperconectividad. Destaca los retos como la promoción de una cultura sólida de ciberseguridad (cibercultura), la preparación para la seguridad cuántica, la protección energética, el uso creciente de IA tanto para defensa como para ataques, la evolución del *ransomware* y la adaptación normativa en entornos OT/IT (Tecnologías Operativas/ Tecnologías de la Información).

Se destaca que el factor humano constituye el eslabón más vulnerable en la seguridad de la información. Por ello, para 2026, las organizaciones apostarán por la capacitación, realización de simulacros y establecimiento de culturas de concientización orientadas a mitigar riesgos asociados a errores humanos o técnicas de manipulación social. La formación continua y el empoderamiento del personal resultan fundamentales para fortalecer la resiliencia organizacional.

Durante el próximo año, la visibilidad, la adaptabilidad y el juicio humano serán lo más importante. La IA amplificará tanto la amenaza como la defensa, pero la tecnología por sí sola no será la salvación. La verdadera ventaja provendrá de las personas: entenderlas, protegerlas y empoderarlas para tomar decisiones más inteligentes en un mundo donde los atacantes y la IA evolucionan lado a lado.

El documento profundiza en la importancia de la cultura de ciberseguridad, que se basa en valores, comportamientos y actitudes compartidas que motivan a los empleados a proteger la organización. Se identifican tres niveles: liderazgo, grupo e individual. La formación constante, la comunicación abierta, el empoderamiento y la responsabilidad compartida son esenciales para una cultura resiliente. Se resaltan las dificultades por la escasez de talento y la complejidad operativa como desafíos

La computación cuántica representa una amenaza real para los sistemas de cifrado actuales, especialmente en redes 5G y dispositivos IoT. Se destaca la necesidad de migrar hacia criptografía post-cuántica (PQC), implementar tecnologías como *Quantum Key Distribution* (QKD) y fomentar la cooperación sectorial para gestionar los riesgos. Además, se menciona la internet cuántica como una nueva red global segura basada en principios cuánticos. Estados Unidos ha fijado 2035 como fecha límite para la transición a PQC y la GSMA ha emitido recomendaciones para operadores de telecomunicaciones.

El crecimiento de centros de datos para IA implica un aumento significativo en la demanda energética, lo que afecta la independencia tecnológica y la soberanía digital. La transformación digital en el sector energético conlleva la convergencia IT/OT, exponiendo infraestructuras críticas a ciberataques cada vez más sofisticados, como los dirigidos a redes eléctricas y sistemas operativos OT. Se subraya la importancia de estrategias coordinadas para proteger la continuidad operativa

La IA se integrará de forma natural en la vida cotidiana y en la industria, facilitando tanto la defensa como ataques más sofisticados, incluyendo *deepfakes* y *malware* polimórfico. El *ransomware* evolucionará hacia modelos automatizados, con *bots* de extorsión que negocian rescates y campañas

mimetizadas con actividades legítimas. La normativa, como NIS2 y DORA en Europa, exigirá medidas de resiliencia y copias de seguridad inmutables
Se destaca el endurecimiento normativo global, con directivas como NIS2, leyes de IA, y regulaciones de divulgación de incidentes que exigen monitoreo continuo, evidencia de resiliencia y responsabilidad directa de la alta dirección. La gobernanza integrada IT/OT y la ciberseguridad medible en tiempo real serán estándares clave

La digitalización global ha incrementado la superficie de ataque y la sofisticación de las amenazas, que ahora operan mediante grupos organizados y con apoyo de IA. Se reportan miles de millones de intentos de escaneo y explotación de vulnerabilidades, con Asia Pacífico y América Latina como regiones destacadas. En Colombia, los *endpoints* presentan alta exposición a *malware* y *botnets*, especialmente en el sector telecomunicaciones, que concentra gran parte de los ataques

Se identifican vectores que abarcan infraestructura física y lógica, virtualización y nube, redes abiertas, dispositivos finales e IoT, cadena de suministro y ataques impulsados por IA generativa. La apertura y desagregación de redes, junto con la proliferación de dispositivos IoT inseguros, amplían la superficie de ataque. La cadena de suministro es un riesgo crítico, con ataques indirectos que impactan múltiples operadores. La IA amplifica la sofisticación y escala de los ataques, incluyendo *deepfakes* y campañas automatizadas

La expansión de la superficie de ataque afecta la integridad, disponibilidad y confianza en las redes de telecomunicaciones, esenciales para servicios críticos. Los costos de cumplimiento y operación aumentan, y la reputación de los operadores puede verse afectada por brechas de seguridad. Se evidencian desigualdades regulatorias y de capacidad entre operadores grandes y pequeños, especialmente en zonas rurales. La tensión entre innovación y seguridad exige marcos proporcionales y basados en riesgos

Se revisa el marco internacional para la protección de infraestructuras críticas cibernéticas, destacando la Unión Europea con directivas como NIS2, CER, DORA y CRA, y Estados Unidos con la CISA y regulaciones específicas. Canadá, México, Brasil, Chile y Argentina también han desarrollado marcos regulatorios y estrategias nacionales. En Colombia, el Decreto 338 de 2022 y documentos CONPES establecen un modelo de gobernanza de seguridad digital, identificación de infraestructuras críticas y servicios esenciales, gestión de riesgos y respuesta a incidentes. Se enfatiza la necesidad de coordinación multisectorial y cooperación internacional.

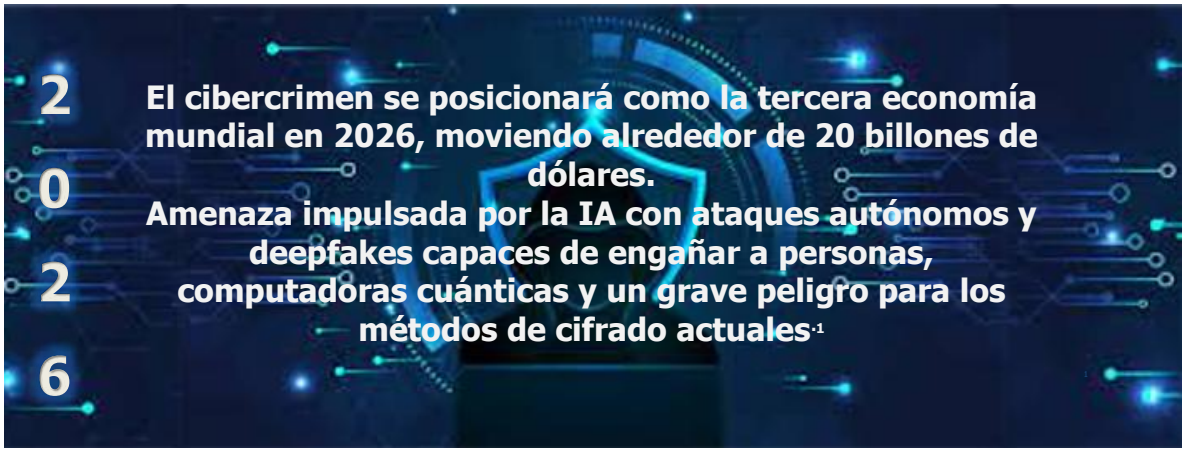
Se evidencia la asimetría entre la rapidez de los ataques y la lentitud en la detección y respuesta, con atacantes actuando en minutos y defensores tardando días. Se resaltan tres pilares para la defensa inteligente: redes colaborativas de intercambio de información (como FIRST y CSIRT Américas), inteligencia de amenazas con estándares técnicos (STIX, TAXII) y el papel estratégico de la IA para detección proactiva, defensa automatizada, cumplimiento normativo y aprendizaje adaptativo. La IA reduce significativamente los tiempos de detección y contención de brechas, y disminuye los costos asociados.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En el contexto actual de acelerada transformación digital y amenazas en evolución continua, es fundamental adoptar un enfoque integral y prospectivo de la ciberseguridad que contemple tanto los aspectos tecnológicos como los humanos. Mediante la colaboración entre sectores, una inversión constante en innovación y la adaptación a nuevas normativas y riesgos, las organizaciones podrán robustecer su resiliencia y asegurar la protección de activos críticos dentro del ecosistema digital global. La capacidad de anticipar y responder de manera proactiva a los desafíos emergentes será determinante para alcanzar niveles sostenibles de seguridad durante los próximos años.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. RETOS EN CIBERSEGURIDAD 2026



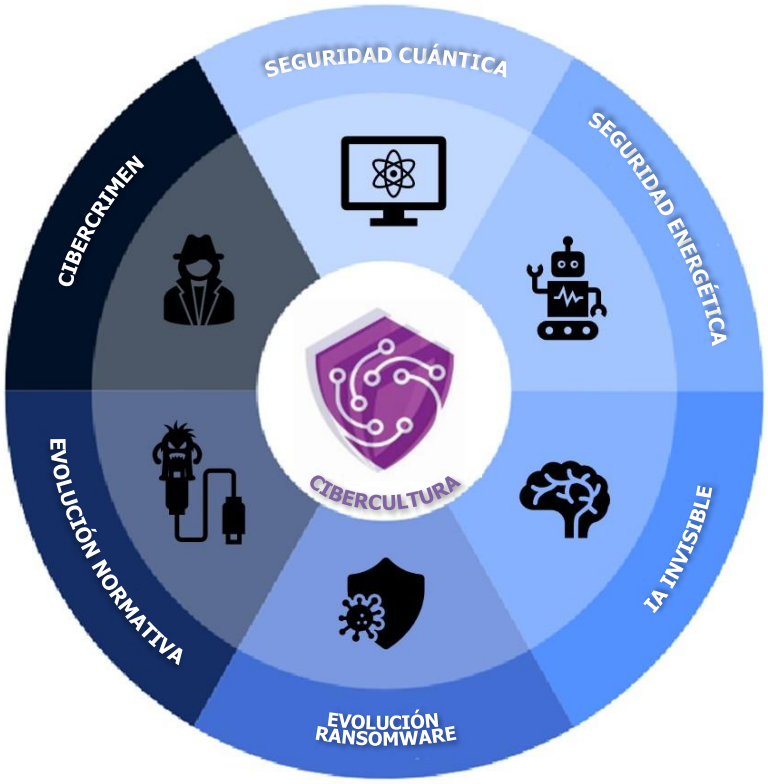
Las empresas y los gobiernos a nivel mundial desarrollan diferentes estrategias para mitigar las amenazas de los ciber ataques, sin embargo, cada año también surgen nuevos actores y tácticas de vulneración que requieren la mejora continua en las estrategias de seguridad. A continuación, se abordarán los principales retos de la ciberseguridad para 2026 (Gráfico 1.1), entre los que se destacan, la importancia de promover una sólida cultura como eje de la seguridad digital, que las organizaciones se preparen ante las repercusiones que la computación cuántica podría tener sobre los actuales sistemas de cifrado, así como prestar especial atención a la protección y el consumo energético, factores cada vez más relevantes en el contexto tecnológico actual. Asimismo, el uso creciente de la inteligencia artificial y el aprendizaje automático, tanto en el ámbito de la defensa como en el de los posibles ataques, es otro aspecto clave a considerar.

Por último, cabe señalar la constante evolución de ataques como el *ransomware* y la importancia de una normativa en el desafiante entorno OT/IT, áreas que serán fundamentales para mitigar los riesgos ante ciberataques.

[1] The 8 Biggest AI Trends For 2026 That Everyone Must Be Ready For Now. Disponible en: https://bernardmarr.com/the-8-biggest-ai-trends-for-2026-that-everyone-must-be-ready-for-now/
The 7 Cyber Security Trends Of 2026 That Everyone Must Be Ready For. Disponible en: https://www.forbes.com/sites/bernardmarr/2025/09/26/the-7-biggest-cyber-security-trends-of-2026-that-everyone-must-be-ready-for

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 1.1 Retos en ciberseguridad 2026



Fuente: Elaboración propia

1.1 CIBERCULTURA (FACTOR HUMANO)

Los delincuentes descubren a menudo que resulta más sencillo engañar, sobornar o chantajear a las personas para que revelen credenciales de acceso que intentar superar sofisticadas barreras tecnológicas de seguridad. Como respuesta, en el 2026 las empresas invertirán en el eslabón más débil en la infraestructura de seguridad que suele ser el factor humano y formarán a los trabajadores para que sean conscientes de las amenazas, realizarán simulaciones de ataques de ingeniería social y fomentarán culturas de concienciación en seguridad. Este reto será analizado en profundidad en el capítulo 2 de este documento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1.2 SEGURIDAD CUÁNTICA[2]

La computación cuántica ofrece importantes oportunidades económicas y científicas al desbloquear una potencia de cálculo sin precedentes y aunque sigue siendo incierto el plazo para alcanzar el máximo potencial de la computación cuántica, los riesgos asociados a la seguridad cuántica ya están presentes.

Es por esto que para prepararse frente a la era cuántica y antes de que sea demasiado tarde, **en 2026 la prioridad será desarrollar una cultura de ciberseguridad** a través de la capacitación del recurso humano; la identificación de vulnerabilidades como la obsolescencia de estándares actuales de cifrado utilizados para proteger redes móviles e infraestructura heredada diseñada para la computación clásica y dispositivos IoT; la migración a cifrados resistentes a la computación cuántica; la transformación de las arquitecturas de red y un enfoque con visión para gestionar redes que operan sobre tecnologías emergente (red cuántica); así como la adaptación de los modelos de negocio, pues en tanto que la industria trabaja hace una década en la interconexión de ordenadores cuánticos, también los delincuentes conocidos como «Cosechar ahora, descifrar después» *Harvest Now, Decrypt Later,* (HNDL) están interceptando y almacenando datos cifrados hoy en día, preparándose para el momento en que la tecnología cuántica permita descifrarlos, transportarlos y explotarlos.

Pioneros de la industria continúan trabajando en la interconexión de ordenadores cuánticos, un avance que podría transformar la seguridad de los datos en toda la infraestructura de telecomunicaciones. Se espera que algunos de los primeros prototipos reales de nodos de internet cuántica lleguen en un corto plazo debido a las pruebas que en varias regiones se han desarrollado. Por ejemplo, en el 2021[3] investigadores holandeses establecieron la primera red cuántica multimodo (Gráfico 1.2), conectando tres procesadores cuánticos. Además, lograron una demostración del concepto de los principales protocolos de red cuántica.

Los investigadores se centraron en añadir más bits cuánticos a su red de tres nodos y en incorporar capas de software y hardware de nivel superior. «Una vez que se hayan desarrollado todas las capas de control e interfaz de alto nivel para gestionar la red, cualquiera podrá escribir y ejecutar una aplicación de red sin necesidad de entender cómo funcionan los láseres y los criostatos. Ese es el objetivo final» comentó Matteo Pompili uno de los investigadores.

La tecnología cuántica tiene el potencial de transformar las redes de telecomunicaciones que dependen del cifrado, la transmisión de datos y la seguridad de la infraestructura, desbloqueando nuevas eficiencias en la optimización de redes, la gestión del espectro y el procesamiento ultrarrápido de datos.

---

[2] SECURING THE FUTURE, Quantum Computing´S Impact on Telecom Security. Disponible en: https://api.qcforum.org/api/files/public/upload/ec47f543-2a80-45bb-8d43-b11b5df4b5e7_Future-of-Quantum.pdf

[3] Dutch researchers establish the first entanglement-based quantum network. Disponible en: https://qutech.nl/2021/04/15/dutch-researchers-establish-the-first-entanglement-based-quantum-network/
Disponible en: https://www.youtube.com/watch?v=C4j4BZFiGgM

Gráfico 1.2 Primera red cuántica multimodo

Fuente: QuTech, https://qutech.nl/2021/04/15/dutch-researchers-establish-the-first-entanglement-based-quantum-network/

Los líderes y organizaciones deben prepararse tanto para las oportunidades como para los riesgos adoptando criptografía resistente a la computación cuántica para proteger los datos a largo plazo. El desarrollo de computadores cuánticos además de proyectarse en resolver en segundos problemas que, a los más potentes de hoy en día, les llevarían siglos, también tienen el potencial de desmantelar los métodos de cifrado de datos más avanzados, poniendo en peligro información sensible y exponiendo a las empresas al riesgo de incumplimiento de normativas de privacidad y protección de datos.

La computación cuántica representa una amenaza seria para la seguridad de las redes 5G, debido a su capacidad para romper el cifrado que protege estos sistemas. Los métodos actuales de cifrado, como *Rivest-Shamir-Adleman* (RSA), *Asymmetric cryptography* y la criptografía de curva *elíptica Elliptic Curve Cryptography* (ECC), se basan en problemas matemáticos complejos que los ordenadores cuánticos podrían resolver rápidamente.

1.2.1. Preparando las Telecomunicaciones para los retos cuánticos[4]. La computación cuántica exige a las compañías de telecomunicaciones evolucionar sus estrategias, fomentando una **cultura organizacional orientada a la protección** proactiva e integrar el cifrado poscuántico– *Post-Quantum Cryptography* (PQC) en la infraestructura de telecomunicaciones para proteger las redes de IoT y dispositivos conectados que serán especialmente vulnerables a los ataques potenciados por la computación cuántica.

[4] Global Cybersecurity Outlook 2025. Disponible en: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
SECURING THE FUTURE, Quantum Computing´S Impact on Telecom Security. Disponible en: https://api.gcforum.org/api/files/public/upload/ec47f543-2a80-45bb-8d43-b11b5df4b5e7_Future-of-Quantum.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Actores de la industria han comenzado a desarrollar y probar soluciones de seguridad resistentes a la tecnología cuántica. Una de las soluciones emergentes es la distribución cuántica de claves *Quantum Key Distribution* (QKD), que ofrece un cifrado teóricamente irrompible al detectar cualquier intento de interceptar las claves transmitidas.

La cooperación a nivel sectorial está desempeñando un papel clave en la aceleración de la transición hacia una seguridad en telecomunicaciones robusta frente a la irrupción de la tecnología cuántica. Grandes compañías globales del ámbito de las telecomunicaciones y la tecnología han constituido grupos de trabajo especializados, conformados por numerosos operadores y proveedores del sector, con el objetivo de definir pautas comunes que permitan identificar y gestionar los riesgos que plantea la computación cuántica para la industria.

Organizaciones como la *Post-Quantum Cryptography Coalition* (PQCC)[5] publican guías estratégicas para la migración, que incluyen pasos como la preparación, comprensión, planificación, ejecución, monitorización y evaluación. Esta hoja de ruta permite a las organizaciones alinear a las partes interesadas, priorizar activos, implementar soluciones y monitorear continuamente el progreso con actividades detalladas, resultados esperados y referencias a estándares de la industria para garantizar una transición segura hacia la criptografía resistente a la computación cuántica.

Otros acuerdos como el de Telefónica Tech e IBM[6] que colaboran en el desarrollo de tecnología de seguridad cuántica. La integración de *quantum-safe* de IBM en el portafolio de servicios de Telefónica Tech diseñado para mejorar las evaluaciones de riesgos que llevan a cabo los profesionales de operaciones de Telefónica Tech con el objetivo de ayudar a las organizaciones a identificar y hacer frente a las vulnerabilidades criptográficas que puedan presentar las infraestructuras. Telefónica Tech también ayudará a las organizaciones en su transición a nuevos estándares, protocolos o algoritmos criptográficos para garantizar la resiliencia y la agilidad frente a los riesgos de ciberseguridad que plantea la computación cuántica y la transición a nuevas tecnologías de cifrado.

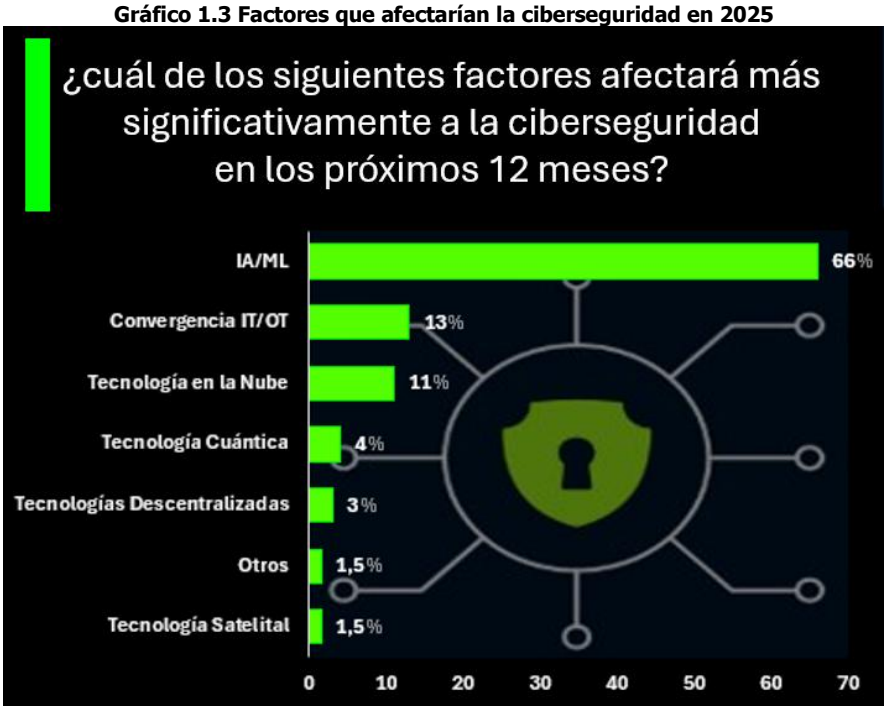
Recientemente, el Instituto Nacional de Estándares y Tecnología (NIST) publicó tres estándares de algoritmos de criptografía post-cuántica (PQC)[7], diseñados para resistir ciberataques provenientes de ordenadores cuánticos.

[5] Post-Quantum Cryptography (PQC) Migration Roadmap. Disponible en: https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf
Novedades en ciberseguridad post-cuántica: del aviso al plan de acción. Disponible en: https://www.tendencias.kpmg.es/2025/06/novedades-ciberseguridad-post-cuantica-aviso-plan-accion/
[6] Telefónica Tech e IBM colaboran en el desarrollo de tecnología de seguridad cuántica. Disponible en: https://www.redseguridad.com/actualidad/telefonica-tech-e-ibm-colaboran-en-el-desarrollo-de-la-tecnologia-de-seguridad-cuantica_20250203.html
[7] El NIST publica los tres primeros estándares de cifrado postcuántico finalizados. Disponible en: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

En septiembre de 2023, la GSMA[8] publicó un documento técnico titulado «Directrices para la Gestión de Riesgos Cuánticos para Operadores de Telecomunicaciones» con el objetivo de proponer una metodología que ayude tanto a los proveedores de servicios de telecomunicaciones como a toda la cadena de suministro del sector. Este proceso ayuda a los operadores de telecomunicaciones a evaluar riesgos, identificar vulnerabilidades, desarrollar un plan de transición hacia la criptografía post-cuántica (PQC) y el establecimiento de un marco de cripto-agilidad para adaptarse y prepararse frente a las amenazas cuánticas que pueden afectar sus redes y datos.

Adicionalmente, según una encuesta realizada por el *Global Cybersecurity Outlook* (GCO) a finales de 2024 (Gráfico 1.3), en la que participaron 321 expertos cualificados, se observa que hace apenas un año solo el 4% consideraba la computación cuántica como una amenaza inmediata para la ciberseguridad. No obstante, dado los posibles riesgos y el rápido avance del sector, en la actualidad se abordan discusiones acerca de la implementación de redes e internet cuántico y en cómo estas tecnologías están transformando el panorama de la seguridad digital.

Gráfico 1.3 Factores que afectarían la ciberseguridad en 2025



Fuente: Elaboración propia a partir de información del Foro Económico Mundial, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[8] Guidelines for Quantum Risk Management for Telco. Disponible en: https://www.gsma.com/get-involved/working-groups/gsma_resources/guidelines-for-quantum-risk-management-for-telco/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1.2.2. Desafíos en la migración post-cuántica[9]. El Instituto Nacional de Estándares y Tecnología (NIST) y la Oficina de Administración y Presupuesto (OMB) de Estados Unidos abordan de manera conjunta los desafíos técnicos, de implementación y presupuesto implicados en la transición segura de la computación cuántica.

En la Cumbre de Ciberseguridad Billington 2025, Andy Regenscheid, líder del grupo de tecnología criptográfica en NIST, indicó que esta es una transformación de magnitudes nunca vista. Por un lado, se están identificando sistemas que operan sobre criptografía vulnerable y en paralelo se están especificando las nuevas tecnologías y los nuevos algoritmos para definir el momento del despliegue.

En relación con esta transición, se señalan varios aspectos clave que merecen atención:

- El papel del gobierno durante este proceso de modernización a algoritmos PQC[10] es fundamental para garantizar una transición segura y eficiente.

- Colaboración sectorial: La migración hacia la criptografía post-cuántica no es una iniciativa independiente; es fundamental analizar cómo dar pasos hacia la modernización de manera conjunta, en la que se espera que los proveedores integren muchos de los algoritmos de criptografía post-cuántica requeridos en sus productos como parte de su ciclo regular de actualización y modernización.

- Publicación de estándares y guías: El proceso de migración requiere una estrecha cooperación entre las agencias encargadas de la ciberseguridad y aquellas responsables de la protección de la infraestructura crítica. Por ejemplo, en agosto de 2023[11], la *Cybersecurity & Infrastructure Security Agency* (CISA) junto con la *National Security Agency* (NSA) y la *National Institute of Standards and Technology* (NIST), elaboraron un documento sobre los impactos de las capacidades cuánticas y la migración hacia la criptografía post-cuántica, el cual además incluye recomendaciones para una hoja de ruta, un inventario criptográfico útil, consideraciones para entender y evaluar la cadena de suministro y cómo las organizaciones deben relacionarse con sus proveedores tecnológicos para discutir la PQC, y las responsabilidades de los proveedores de tecnología.

- Marco de cripto-agilidad: Procurar que la redacción de contratos incluya ciclos regulares de actualización y modernización, así como garantías para evitar la necesidad de una renovación completa de los sistemas cuando estos queden obsoletos.

---

[9] NIST, OMB Outline Challenges in Post-Quantum Migration. Disponible en: https://www.meritalk.com/articles/nist-omb-outline-challenges-in-post-quantum-migration/

[10] Criptografía Post-Cuántica PQC) es un tipo de algoritmo criptográfico diseñado para ser resistente a los ataques de futuras computadoras cuánticas, que tienen la capacidad de romper los sistemas de cifrado actuales (como RSA o ECC).

[11] Quantum-Readiness: Migration to Post-Quantum Cryptograph. Disponible en: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Modernización estratégica: Aprovechar esta migración a la criptografía post-cuántica puede ser una oportunidad estratégica para modernizar de manera integral otras áreas de las redes como mejoras en infraestructura, protocolos y procesos operativos, impulsando una transición más eficiente.

- Desafíos presupuestales: Las grandes modernizaciones 'de golpe' siempre van a ser, evidentemente, difíciles, debido a que la práctica más común es la elaboración de presupuestos con incrementos de un año.

- Desarrollo tecnológico: Tomarse en serio la amenaza de la computación cuántica, no implica desviar recursos de las defensas a corto plazo como la autenticación multifactor y la aplicación de parches.

- Pruebas y adaptabilidad: Debido a que cada red posee particularidades operativas propias, es esencial que la transformación hacia la criptografía post-cuántica se adapte específicamente a las necesidades y características de cada ecosistema. Para lograr un equilibrio adecuado entre seguridad y rendimiento, se recomienda implementar pruebas de los nuevos algoritmos de criptografía post-cuántica en las redes existentes e identificar problemas ocultos que, en el futuro, podrían impedir completar la migración a la criptografía post-cuántica.

En el caso de los Estados Unidos, se estableció el año 2035 como la fecha límite para completar la transición estatal hacia la criptografía post-cuántica. Esta determinación responde a la necesidad de coordinar esfuerzos entre agencias gubernamentales, proveedores tecnológicos y responsables de la infraestructura crítica.

1.2.3. La internet cuántica[12]. Más allá de las capacidades de cifrado y computación, la tecnología cuántica está sentando las bases para un nuevo tipo de red global segura. A diferencia de las redes actuales, que dependen de métodos de cifrado que los ordenadores cuánticos podrían llegar a romper, una red cuántica aprovecharía el entrelazamiento cuántico y la distribución cuántica de claves *Quantum Key Distribution* (QKD) para establecer un cifrado de extremo a extremo intrínsecamente resistente a la interceptación utilizando leyes de la mecánica cuántica, garantizando una seguridad en las comunicaciones que se mantiene intacta incluso ante adversarios cuánticos de gran potencia.

Por su parte la IEEE analiza cómo implementar cifrado homomórfico[13] (método criptográfico que permite realizar cálculos sobre datos cifrados sin necesidad de descifrarlos) con QISKIT, un entorno de desarrollo de software de libre acceso basado en Python y desarrollado por IBM[14], para trabajar con computadoras cuánticas. La investigación aborda fundamentos teóricos del cifrado homomórfico (HE), su aplicación en computación cuántica y su relevancia para la realización de cálculos preservando la privacidad.

[12] SECURING THE FUTURE, Quantum Computing´S Impact on Telecom Security. Disponible en: https://api.qcforum.org/api/files/public/upload/ec47f543-2a80-45bb-8d43-b11b5df4b5e7_Future-of-Quantum.pdf
[13] Homomorphic Encryption in Quantum Computing. Disponible en: https://ieeexplore.ieee.org/document/11012553/authors#authors
[14] Introducción a Qiskit y IBM Quantum. Disponible en: https://quantum.cloud.ibm.com/docs/es/guides

Además, examina circuitos sumadores basados en compuertas lógicas cuánticas, su implementación con QISKIT y las perspectivas para mejorar la seguridad computacional en entornos de computación en la nube. Los resultados destacan la viabilidad práctica del HE en escenarios cuánticos.

1.3 CIBERSEGURIDAD ENERGÉTICA

En el contexto actual de digitalización acelerada y avance tecnológico, la seguridad en el sector energético se convierte en un aspecto fundamental para preservar la estabilidad y la soberanía digital de los países. A continuación, se analiza, por un lado, cómo el crecimiento exponencial de los centros de datos destinados para el entrenamiento de la inteligencia artificial está redefiniendo la independencia tecnológica y energética de las naciones, así como la necesidad de garantizar la protección de sistemas críticos frente a amenazas externas. Por otro, se examina la transformación digital de los sistemas operativos y la convergencia entre IT y OT que enfrenta la industria energética, que, aunque mejora la eficiencia y la producción en la industria, también genera nuevos puntos de explotación para los ciber atacantes.

Asimismo, se abordan los desafíos presentes y futuros en materia de ciberseguridad, subrayando la relevancia de establecer estrategias integrales, coordinadas y colaborativas para proteger las infraestructuras críticas que sostienen la seguridad digital, asegurando la continuidad operativa para reducir el impacto de incidentes cibernéticos, considerando la ciberseguridad como una disciplina interconectada en lugar de tratarla como un área independiente.

1.3.1. Alta demanda de energía[15]. La disposición de centros de datos y una infraestructura energética propia otorga a los países independencia en la gestión de sus operaciones tecnológicas avanzadas. Esto no solo garantiza la capacidad de entrenar modelos de IA sin depender de recursos externos, sino que también impide que actores adversos tengan acceso a sistemas críticos que podrían poner en riesgo la ciberseguridad y la soberanía nacional.

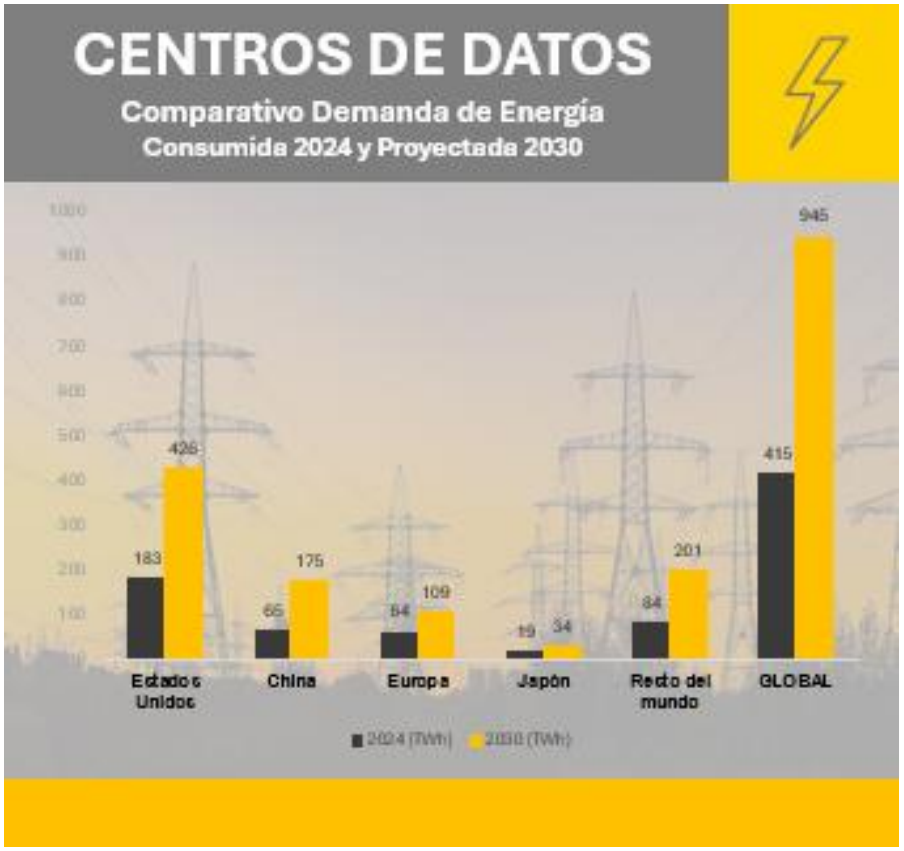
Según datos de la Agencia Internacional de Energía (IEA)[16] como se muestra en el Gráfico 1.4, en 2024 los centros de datos a nivel global consumieron un total de 415 teravatios-hora (TWh) de electricidad, lo que representa cerca del 1,5% de la demanda eléctrica mundial. Las proyecciones indican que para 2030 esta demanda se incrementará hasta alcanzar los 945 TWh, aproximándose al 3% del consumo total de electricidad a nivel global. Esta enorme huella no solo tiene que ver con almacenamiento, disponibilidad, latencia y ubicación, los centros de datos determinan el consumo de energía y quién lidera la economía tecnológica global.

La interconexión de la infraestructura de los centros de datos de inteligencia artificial con la red eléctrica busca no solo impulsar una transición hacia fuentes de energía más limpias y sostenibles o evitar que

[15] Biden signs ambitious order to bolster energy resources for AI data centers. Disponible en: https://apnews.com/article/biden-white-house-ai-artificial-intelligence-7458d9d1bb537929c5dcfb5192695223
[16] Disponible en: https://www.cargoson.com/es/blog/numero-de-centros-de-datos-por-pais

el costo derivado del aumento en la demanda energética recaiga sobre comunidades locales, sino que desde una perspectiva de ciberseguridad nacional, este tipo de proyectos adquiere una importancia estratégica al garantizar la generación interna de energía para satisfacer la creciente demanda de los centros de datos y evitar la dependencia a recursos energéticos externos para mantener la autonomía y garantizar la operación de la IA y otras tecnologías avanzadas.

Gráfico 1.4 Demanda de Energía en Centros de Datos (2024)



Fuente: Elaboración propia a partir de información de Cargoson,
https://www.cargoson.com/es/blog/numero-de-centros-de-datos-por-pais

Según lo indicó Tarun Chhabra[17], excoordinador de tecnología y seguridad nacional de los EE.UU «Los volúmenes de potencia de cálculo y electricidad necesarios para entrenar y operar los modelos más avanzados están aumentando rápidamente y se prevé que se disparen aún más», por lo que se busca garantizar que la infraestructura necesaria para las operaciones avanzadas de IA, como los centros de datos a gran escala y las nuevas instalaciones de energía limpia, se construyan de forma rápida y a gran escala.

Gráfico 1.5 centro de datos

La urgencia por encontrar fuentes más limpias y sostenibles según el Departamento de **Energía** de Estados Unidos (DOE) es porque para **2028** la cantidad de energía consumida por los centros de datos representará el **12%** de toda la electricidad del territorio.

Por otro lado, según la Agencia Internacional de Energía (AIE) el consumo para el **2024** representó el **4,4%** del consumo total de electricidad de EE.UU.

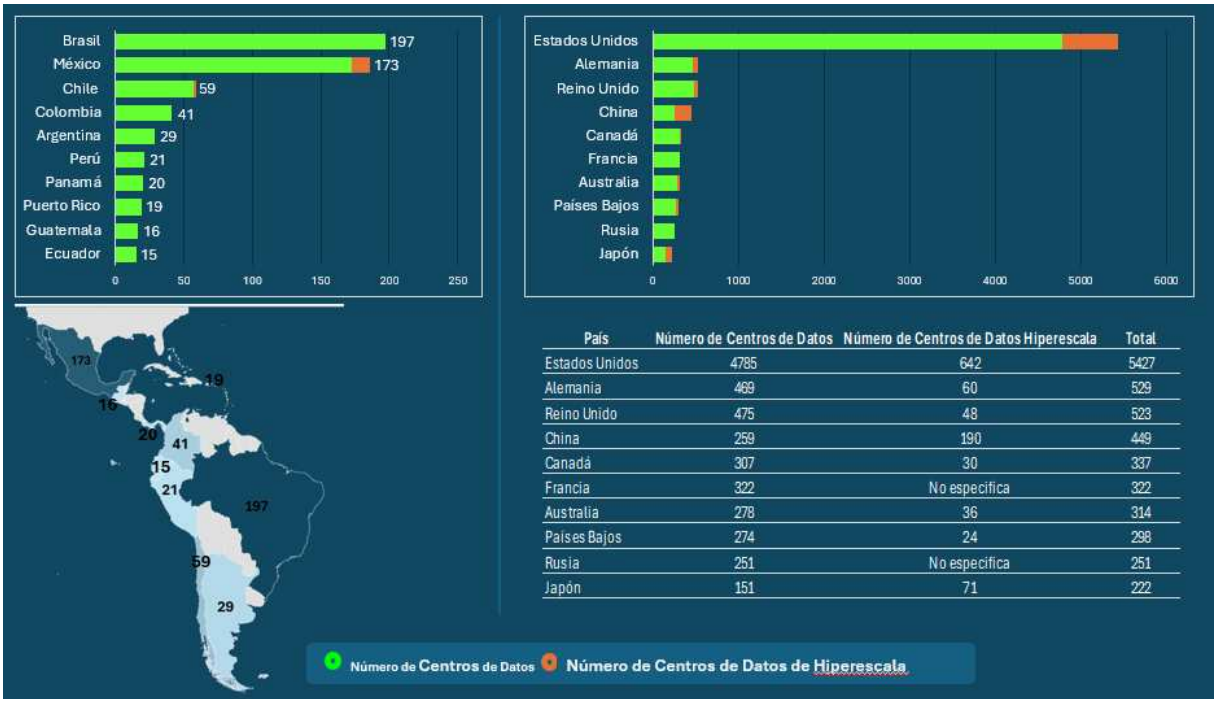
Fuente: Data Center Dynamics, https://www.datacenterdynamics.com/en/analysis/what-is-a-hyperscale-data-center/#:~:text=Estas%20empresas%20pueden%20obtener%20sus,de%20gesti%C3%B3n%20tecnol%C3%B3gica%20a%20terceros.&text=Si%20no%20est%C3%A1%20seguro%20de,la%20eficiencia%20y%20reducir%20costos.

En el año 2025, como se ilustra en el Gráfico 1.6, Estados Unidos refuerza su liderazgo global en infraestructura de centros de datos, alcanzando un total de 5.427 instalaciones, cifra que equivale a aproximadamente la mitad de todos los centros de datos existentes a nivel mundial. Por su parte, Alemania (529), Reino Unido (523) y China (449) sobresalen también por su significativa concentración de centros de datos, consolidando su posición como actores relevantes en el panorama tecnológico internacional. Otros países destacados en este sector son Canadá (337), Francia (322), Australia (314), Países Bajos (298), Rusia (251) y Japón (222), que mantienen una presencia considerable y contribuyen activamente al desarrollo de la infraestructura digital. En lo que respecta a América del Sur, Brasil lidera el ranking regional con 197 centros de datos, seguido de cerca por México (173). Chile se posiciona con 59 instalaciones, mientras que Colombia cuenta con 41, Argentina con 29 y Perú suma 21. Panamá, Puerto Rico, Guatemala y Ecuador también presentan cifras relevantes, con 20, 19, 16 y 15 centros de datos respectivamente.

[17] Biden signs ambitious order to bolster energy resources for AI data centers. Disponible en: https://apnews.com/article/biden-white-house-ai-artificial-intelligence-7458d9d1bb537929c5dcfb5192695223

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 1.6 Principales Países a Nivel Global y Sur América por Cantidad de Centros de Datos (Nov 2025)



País	Número de Centros de Datos	Número de Centros de Datos Hiperescala	Total
Estados Unidos	4785	642	5427
Alemania	469	60	529
Reino Unido	475	48	523
China	259	190	449
Canadá	307	30	337
Francia	322	No especifica	322
Australia	278	36	314
Países Bajos	274	24	298
Rusia	251	No especifica	251
Japón	151	71	222

En Sudamérica Chile cuenta con 2 de centros hiperescala. Por su parte, México con 13 en construcción, los demás países no cuentan con registro
Fuente: Elaboración propia a partir de información de Cargoson, https://www.cargoson.com/es/blog/numero-de-centros-de-datos-por-pais

De acuerdo con los datos proporcionados por *Synergy Research Group*, durante el primer trimestre de 2025 se encontraban en funcionamiento un total de 1.189 centros de datos de hiperescala[18] repartidos a nivel global. Además, se identificaron 504 nuevas instalaciones en diferentes fases de planificación y construcción. Las estimaciones para los próximos años prevén un crecimiento continuo, con la inauguración anual de entre 130 y 140 centros de datos de hiperescala. Este rápido desarrollo incrementa de manera significativa la necesidad de contar con fuentes energéticas capaces de soportar la demanda de estos complejos tecnológicos, convirtiendo la gestión energética en un reto de máxima prioridad para la industria.

Para 2026, un elemento central del discurso en torno a la protección de datos y la IA, será mejorar la eficiencia de los sistemas que alimentan y enfrían millones de computadores que procesan enormes volúmenes de datos. Así como también buscar métodos innovadores para generar energía.

[18] Un centro de datos a hiperescala es un centro de datos masivo que proporciona capacidades de escalabilidad extremas. Está diseñado para cargas de trabajo a gran escala con una infraestructura de red optimizada, una conectividad de red racionalizada y una latencia minimizada.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

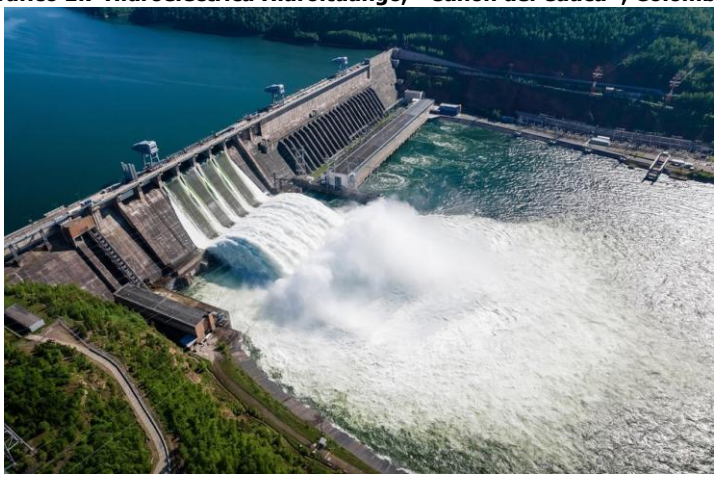
1.3.2. Explotación OT. Tradicionalmente, los sistemas IT (Tecnologías de la Información) y OT (Tecnologías Operativas) funcionaban de forma aislada y mediante la llamada «desconexión física» o «*air-gapping*» se minimizaba la exposición de los entornos OT a los riesgos cibernéticos comunes de los sistemas IT.

Sin embargo, la transformación digital cerró la brecha entre los sistemas IT y OT, impulsada por la necesidad de datos en tiempo real. Por ello el sector energético global viene experimentando una profunda transformación digital, integrando sistemas digitales avanzados para mejorar la producción y la eficiencia operativa.

Pese a esta transformación una parte significativa de los sistemas en operación y clave en los procesos de generación y distribución de energía superan los cincuenta años de antigüedad. Esta fuerte dependencia de infraestructuras y tecnologías heredadas genera importantes vulnerabilidades en materia de seguridad, ya que dificulta la implementación de soluciones avanzadas, dejando expuestas las infraestructuras críticas a amenazas cibernéticas cada vez más sofisticadas.

En los últimos años, los ciberataques dirigidos a los sistemas IT y OT han experimentado un notable aumento tanto en frecuencia como en sofisticación. De acuerdo con datos de Fortinet[19], en 2025 el 60 % de las organizaciones entre las que se encuentra el suministro de energía sufrió al menos una intrusión que impactó simultáneamente a los entornos IT y OT, cifra que supera el 49 % reportado en 2024. Este incremento refleja la creciente vulnerabilidad en sectores como el energético reconocido a nivel mundial como infraestructuras críticas, esenciales para la economía y el funcionamiento de la sociedad.

Gráfico 1.7 Hidroeléctrica Hidroituango, «Cañón del Cauca», Colombia



Fuente: https://inspenet.com/noticias/hidroelectrica-hidroituango-cys-litacion/

💡 Sin un marco de gobernanza unificado, los equipos de IT y OT suelen seguir protocolos y prioridades diferentes, lo que complica aún más las estrategias de ciberseguridad.

💡 La falta de modelos operativos claramente definidos da lugar a esfuerzos fragmentados y a una respuesta a incidentes ineficaz.

[19] 2025 State of Operational Technology and Cybersecurity. Disponible en: https://www.fortinet.com/resources/reports/state-ot-cybersecurity

En el sector energético, los ciberataques han evidenciado las debilidades existentes en las infraestructuras críticas. Un ejemplo relevante son los incidentes dirigidos contra redes eléctricas, donde se han vulnerado los sistemas de tecnología operativa (OT), originando apagones y desencadenando una serie de consecuencias negativas para ciudadanos y empresas.

Gráfico 1.8 Hidroeléctrica Hidroituango, Colombia

Fuente: https://www.eltiempo.com/colombia/medellin/hidroituango-asi-esta-el-avance-de-las-turbinas-que-deben-funcionar-en-diciembre-776530

- Debido a las grandes diferencias entre IT y OT en cuanto a objetivos, prioridades, estrategias e implementaciones, muchas industrias enfrentan retos significativos para conformar un capital humano dedicado a la ciberseguridad OT.

- Además, la naturaleza especializada de los entornos OT, con sus tecnologías y requisitos operativos únicos, dificulta que los equipos de seguridad IT tradicionales puedan supervisar y proteger eficazmente los sistemas OT.

De manera similar, los ataques de *ransomware* dirigidos a los sistemas informáticos (IT) han obligado a la desconexión preventiva de los sistemas de tecnología operativa (OT), lo que ha provocado importantes interrupciones, como escasez de combustible y problemas en el suministro energético. Estos incidentes evidencian la importancia del trabajo conjunto entre los entornos IT y OT, y cómo las vulnerabilidades en un área pueden desencadenar alteraciones a gran escala en todo el sector energético.

Mejorar la supervisión de la seguridad en OT y las capacidades de respuesta ante incidentes requiere un enfoque integral para una gobernanza sólida, tecnologías avanzadas y una gestión proactiva de riesgos.

Al integrar estas estrategias, las organizaciones pueden preparar su ciberseguridad para el futuro y garantizar el funcionamiento seguro e ininterrumpido de la infraestructura crítica, especialmente a medida que las amenazas cibernéticas se vuelven más sofisticadas.

1.4 IA INVISIBLE

Sin duda, desde hace varios años la IA ha sido la herramienta y palabra de moda. 2026 será el año en que el impacto de estos asistentes autónomos y capaces de actuar realmente se materialice y transformen profundamente el tejido industrial.

La inteligencia artificial está alcanzando un nivel de integración en nuestra vida diaria comparable a hitos históricos como la llegada de la mecánica, la electricidad o las telecomunicaciones. Esto implica que, cada vez más, pasará desapercibida, convirtiéndose en una tecnología de fondo que dejará de ser resaltada. Para las nuevas generaciones, especialmente los niños nacidos en la última década, interactuar de manera natural y fluida con dispositivos y máquinas será algo habitual; ya no lo percibirán como una innovación destacable, sino como la manera normal en que opera el mundo que les rodea.

1.4.1. Aprendizaje Automático (IA/ML). La inteligencia artificial (IA) y el aprendizaje automático (ML – *Machine Learning*) utilizada para que la detección de amenazas sea más eficiente y precisa también es empleada para crear amenazas más sofisticadas. Los agentes autónomos de IA son la nueva primera línea en el cibercrimen que permitirán ofensivas más sofisticadas, censando defensas para encontrar vulnerabilidades para lanzar intentos de ingeniería social cada vez más engañosos. Sin embargo, también ofrecen a los defensores nuevas opciones para detectar y responder de forma autónoma.

1.4.2. Deepfakes y contenido sintético. El audio y vídeo manipulados mediante *deepfake*[20] abren nuevas posibilidades para que los atacantes imiten a personas de confianza y accedan a sistemas seguros. Se han producido casos en los que empleados han sido engañados tras recibir llamadas telefónicas falsas que simulaban ser de su jefe, y a medida que esta tecnología se vuelve más sofisticada será más difícil distinguir la realidad de lo artificial y estos incidentes serán cada vez más frecuentes.

Según *Bernard Marr*[21] en 2026 hasta el 90% del contenido en línea podría ser generado de forma sintética. Sin duda, el contenido sintético tiene su lugar para analizar y extraer conclusiones de datos que se mueven demasiado rápido para que los humanos puedan gestionarlos. Sin embargo, cuando se utiliza para sustituir la percepción y la experiencia humanas, carece de legitimidad.

1.5 EVOLUCIÓN DEL RANSOMWARE[22]

Para 2026, las organizaciones deberán reconsiderar sus estrategias de resiliencia debido al incremento de ataques de *ransomware*[23] operados como servicio y respaldados por tecnología *deepfake*, utilizada para engañar la percepción humana. Estos avances elevan los riesgos asociados al robo de identidad y datos en donde la implementación de inmutabilidad y copias de seguridad segmentadas[24] se posiciona

[20] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 4.1.6.
[21] Las ocho tendencias de IA más importantes para 2026 que todos deben afrontar. Disponible en: https://forbes.es/tecnologia/801213/las-ocho-tendencias-de-ia-mas-importantes-para-2026-que-todos-deben-afrontar/
[22] SECURITY PREDICTIONS FOR 2026. Disponible en: https://documents.trendmicro.com/assets/research-reports/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026.pdf?_gl=1*dxiz24*_gcl_au*MTQwMTEwNTA2OC4xNzY0NzI3NDEz*_ga*MTk4ODk0NzI4Ni4xNzY0NzI3NDEz*_ga_PCCSVH5M9H*czE3NjQ3Mjc0NTgkbzEkZzEkdDE3NjQ3Mjc1NTUkajQ3JGwwJGgxNDYyNTUxOTM1
[23] Detalles adicionales sobre este aspecto se explorarán más adelante en el capítulo 4. VECTORES DE ATAQUE
[24] La inmutabilidad asegura que las copias no puedan ser alteradas o eliminadas, mientras que la segmentación añade capas de protección y aislamiento a las copias.

como una defensa crucial, por ejemplo, en Europa normativas como NIS2[25] y DORA[26] transforman la resiliencia de las copias de seguridad, pasando de ser una buena práctica de TI a constituir un requisito legal sujeto a sanciones económicas.

El constante cambio de la huella de eventos maliciosos y la reutilización de herramientas obligará a los defensores a centrarse en la detección basada en el comportamiento en lugar de indicadores estáticos. De igual forma, aunque el modelo principal de *ransomware* sigue siendo eficaz, la creación y el despliegue ahora son más automatizados y adaptativos, lo que acelera el hallazgo de vulnerabilidades y permite ataques más precisos en los entornos objetivo.

Los *bots* de extorsión impulsados por IA se involucrarán directamente con las víctimas en las negociaciones de rescate. Algunos grupos, como el sindicato *Global Group Ransomware*[27], ya han comenzado a experimentar con estos agentes automatizados de negociación. Se prevé que surjan otras tácticas de presión reputacional, como divulgar información manipulada o crear escándalos para forzar los pagos. Estas acciones de manipulación se basan principalmente en la generación de temor en lugar de provocar interrupciones técnicas. En muchos casos, los costos legales y el daño reputacional superan significativamente el importe del rescate solicitado.

Las campañas de *ransomware* serán cada vez más imperceptibles, mimetizándose con la actividad legítima y aprovechando la complejidad de las cadenas de suministro empresariales y los ecosistemas digitales. Las cadenas de suministro, componentes de código abierto y flujos de trabajo integrados con IA se convertirán en vías clave de acceso, permitiendo que el *ransomware* infiltre sistemas de confianza mientras se mimetiza con la actividad habitual de las empresas.

En este contexto, el *ransomware* será más agresivo y selectivo. De manera similar a otras formas de amenazas, la automatización basada en inteligencia artificial marcará una nueva etapa, abarcando desde la identificación autónoma de vulnerabilidades y la realización automatizada de pruebas de penetración, hasta el análisis sistemático de datos que permite a los atacantes priorizar objetivos, desarrollar estrategias de coacción específicas y aumentar el alcance de la extorsión de segundo orden y de alto valor (Los atacantes buscan menos objetivos, pero más rentables).

En 2026, los grupos de *ransomware* recurrirán cada vez más a la IA agentica para gestionar grandes partes del ciclo de vida del ataque sin supervisión humana. Lo que comenzó como el desarrollo de *malware* asistido por IA en 2025, como se vio en los ataques que involucraron a *FunkSec*[28], evolucionará

[25] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 5.1.1.1.
[26] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 5.1.1.3.
[27] GLOBAL GROUP's Golang Ransomware Expands Attacks Across Major Operating Systems. Disponible en: https://cyberpress.org/global-groups-golang-ransomware-expands-attacks/
[28] AI-Driven Ransomware FunkSec Targets 85 Victims Using Double Extortion Tactics. Disponible en: https://thehackernews.com/2025/01/ai-driven-ransomware-funksec-targets-85.html

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

hacia *malware* operacionalmente independiente como *LameHug*[29], marcando un salto en la automatización.

La capacidad de la IA para analizar medios no textuales, como imágenes, voz y vídeo, permite a los atacantes pasar de la simple encriptación de datos a la explotación inteligente, empleando IA para identificar y ejercer presión sobre los activos más sensibles de las víctimas.

Los marcos de *zero trust* fortalecen la seguridad ante amenazas como el *ransomware*, pero requieren medidas adicionales. Es clave formar a las personas regularmente contra la ingeniería social avanzada por IA y usar plataformas de inteligencia de amenazas para rastrear el *ransomware* y diseñar defensas eficaces que involucren análisis de impacto, copias de seguridad *offline*, manuales probados de recuperación y flujos de contingencia indispensables para garantizar la continuidad.

Así las cosas, se prevé que la **resiliencia en 2026**[30] será menos bloquear intrusión y más garantizar que la recuperación siempre sea posible a través de controles como:

- **Integrar copias de seguridad en la respuesta a incidentes:** Incorporar flujos de recuperación y acción frente al *ransomware*, de modo que las restauraciones sean inmediatas, automatizadas y no dependan de decisiones manuales.

- **Inmutabilidad:** Almacenar copias de seguridad de manera que los datos no puedan eliminarse ni modificarse, incluso con credenciales de administrador robadas.

- **Regla 3-2-1-1-0:** Mantener varias copias en diferentes tipos de soporte, una fuera de las instalaciones, otra inmutable y verificar que no haya errores de copia de seguridad mediante pruebas rutinarias de restauración.

- **Segmentar copias de seguridad:** Separar el almacenamiento primario y el almacenamiento secundario en dominios de seguridad distintos, con accesos de mínimo privilegio y protocolos seguros.

- **Automatizar pruebas de recuperación:** Ejecutar pruebas automatizadas de restauración y comprobación de integridad para asegurar que las copias de seguridad funcionen bajo condiciones reales de ataque.

[29] LameHug malware uses AI LLM to craft Windows data-theft commands in real-time. Disponible en: https://www.bleepingcomputer.com/news/security/lamehug-malware-uses-ai-llm-to-craft-windows-data-theft-commands-in-real-time/
[30] Ransomware Trends 2026. Disponible en: https://cyberpress.org/ransomware-trends-2026-how-businesses-can-build-resilience/#:~:text=Ransomware%20in%202026%20is%20driven,the%20decisive%20line%20of%20defense.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **Priorizar objetivos:** Definir los objetivos de tiempo y punto de recuperación acordes al impacto en el negocio, y probar las copias de seguridad periódicamente contra esos objetivos.

Adicionalmente para el 2026, se incorpora la **presión normativa.** Con la entrada en vigor de NIS2[31] y DORA[32], los reguladores de la UE exigen la inmutabilidad comprobable de las copias de seguridad, evidencias de recuperación listas para auditoría y plazos estrictos de notificación. El incumplimiento puede acarrear sanciones tan graves como el propio rescate.

1.6 EVOLUCIÓN NORMATIVA

La regulación y legislación han tenido dificultades para seguir el ritmo del cibercrimen. En 2026 medidas recientes como la directiva NIS2 de la UE obligará a las empresas a implementar medidas de resiliencia y la norma de la SEC de EE. UU. sobre divulgación cibernética obligarán a las empresas a informar y documentar brechas de seguridad, estas y otras acciones como el desarrollo de estándares para un hardware seguro por diseño indican que los reguladores en todo el mundo están reduciendo la brecha entre innovación y responsabilidad en respuesta a la dependencia de la sociedad en los servicios digitales para sostener tanto la vida cotidiana como el funcionamiento económico sostenido por el latido digital de operaciones (OT).

Según *Peter Sandkuijl*[33], vicepresidente del departamento de ingeniería de EMEA (*Europe, the Middle East, and Africa*) de *Check Point Software*, 2026 será el año en que la regulación deje de ser reactiva y de hecho puede evidenciarse en marcos como la Directiva NIS2 de la Unión Europea, la Ley de la IA y las normas de divulgación de incidentes de la SEC[34] en Estados Unidos, la publicación de «*Cyber Assessment Framework 4.0*»[35] (CAF) del *National Cyber Security Centre* (NCSC) y la *Ley Cyber Security and Resilience Bill*[36] (CSRB)[37] de Reino Unido, que establecen expectativas más precisas y orientadas a resultados en materia de resiliencia y comenzarán a alinearse bajo un mismo principio: «La ciberseguridad debe ser medible y demostrable en tiempo real». Esto implicará que los gobiernos exijan pruebas continuas de resiliencia y que las organizaciones demuestran controles preventivos, planes de respuesta y políticas de protección de datos de forma ininterrumpida.

La resiliencia empresarial se convierte así en el principal motor del endurecimiento normativo, incluso pese a la advertencia de que ciertos marcos regulatorios podrían obstaculizar la innovación y el crecimiento, no obstante, dichos marcos garantizan dos vertientes: (i) proporcionar evidencia a los

[31] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 5.1.1.1.
[32] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 5.1.1.3.
[33] El tsunami tecnológico 2026. Disponible en: https://www.puromarketing.com/12/216477/tsunami-tecnologico-2026-colision-entre-cuantica
[34] Detalles adicionales sobre este aspecto se explorarán más adelante en el numeral 5.1.1.4.
[35] Cyber Assessment Framework 4.0. Disponible en: https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf?utm_source=chatgpt.com
[36] Cyber Security and Resilience Bill - GOV.UK. Disponible en: https://www.gov.uk/government/collections/cyber-security-and-resilience-bill?utm_source=chatgpt.com
[37] Ley que busca fortalecer la ciber resiliencia en servicios digitales y cadenas de suministro

reguladores de que se cumplen las obligaciones legales, y (ii) que las obligaciones legales prueben a la sociedad que los servicios esenciales pueden resistir interrupciones.

La era por un cumplimiento anual terminará. Las organizaciones adoptarán monitoreo automatizado, certificaciones en tiempo real y análisis de riesgos basados en IS[38]. Las juntas directivas y los directores ejecutivos serán responsables directos de supervisar la ciberseguridad. Tras los impactos que se repiten una y otra vez a nivel global, los ejecutivos que antes consideraban la seguridad como una obligación regulatoria ahora se preguntan cuántas horas de auditoría se ahorrarán, cuánto tiempo improductivo se evitarán y con qué rapidez se abrirán los flujos de datos listos para la IA una vez que se protejan las redes.

Tanto directivos como equipos operativos han reconocido que las operaciones (OT) crean nuevas superficies de ciberataque y se han dado cuenta de la importancia de actuar, según el «*Annual State of Smart Manufacturing*[39]» de *Rockwell Automation*. La encuesta, basada en 1560 líderes del sector manufacturero de 17 países y empresas desde 100 millones hasta miles de millones de dólares, señala que el hardware seguro por diseño cobra protagonismo y que la ciberseguridad es tan importante como la productividad y los costos para medir el rendimiento.

Algunos aspectos clave concluidos de la encuesta son: Garantizar la compatibilidad de los nuevos activos entrantes, programar actualizaciones como parches IT con planes de reversión y pruebas simuladas para evitar interrupciones repentinas, e incorporar registros a nivel de dispositivos en la gestión de información para una detección temprana de eventos maliciosos.

Quizá el cambio más significativo sea la gobernanza unificada IT y OT[40]. Durante demasiado tiempo, IT se ha gestionado bajo la norma ISO 27001 y OT bajo la IEC 62443, con poca integración entre ambas. Los objetivos A1 y A2 del CAF 4.0 exigen que los directivos gobiernen ambos dominios de forma holística. Esto implica unificar los sistemas de gestión de seguridad de la información (ISMS) y los sistemas de gestión de seguridad cibernética (CSMS) dentro de un único modelo de gobernanza, incorporando la garantía mediante pruebas, auditorías, ejercicios, y asegurando que los marcos de gobernanza vayan más allá del cumplimiento para pasar a la gestión estratégica de consecuencias.

Para 2026, el estándar proyectado es que se adopten estrategias de gobernanza alineadas con el CAF, probadas mediante una garantía continua. Los límites entre IT y OT estarán reforzados mediante una zonificación robusta y un control estricto del acceso de proveedores. Los *Centros de Operaciones de Seguridad* (SOC) integrarán la telemetría de OT, los planes de actuación basados en consecuencias se pondrán a prueba y la notificación de incidentes se alineará con el régimen de comunicación de

[38] El análisis de riesgos basado en activos de información (IS, por sus siglas en inglés) es un proceso fundamental en la ciberseguridad, guiado por normas como ISO 27001/27005, que se centra en identificar, valorar y tratar amenazas y vulnerabilidades que afectan a los activos de información (datos, software, hardware, personas) para proteger su confidencialidad, integridad y disponibilidad (CID).
[39] Annual State of Smart Manufacturing. Disponible en: https://www.rockwellautomation.com/en-us/capabilities/digital-transformation/state-of-smart-manufacturing.html
[40] Operational Technology Security 2025–2026. Disponible en: https://www.techuk.org/resource/from-compliance-to-consequence-management.html

incidentes de 24 horas. La resiliencia será práctica, con copias de seguridad comprobadas y offline, y manuales de recuperación centrados en la seguridad.

1.7 CIBERCRIMEN

Los operadores modernos de *ransomware* cada vez se asemejan más a empresas legítimas. Estos actores de amenazas utilizan infraestructuras en la nube, alquilan recursos informáticos y crean empresas fantasmas para ocultar sus operaciones. El cambio constante de marca, motivado por las acciones policiales y las sanciones, les ayuda a evitar la atribución, restablecer su reputación y reclutar nuevos afiliados. Esta agilidad obliga a los defensores a cambiar el enfoque: en lugar de rastrear bandas específicas de *ransomware*, deben identificar tácticas, técnicas y procedimientos persistentes que trasciendan la identidad de cada grupo.

Las organizaciones que consigan equilibrar velocidad con gobernanza, inteligencia con ética, e innovar de forma segura, serán reconocidas por su estándar de confianza y seguridad en la nueva era del cibercrimen industrializado.

Ryan Flores[41], líder de *forward-Looking threat research* en *Trend Micro*, explicó que «2026 será recordado como el año en el que la ciberdelincuencia dejó atrás el modelo como servicio, para convertirse en una industria plenamente automatizada» y advierte que el próximo año marcará un punto de inflexión decisivo en la evolución del cibercrimen. De igual forma afirma «Estamos entrando en una etapa en la que los Agentes IA descubrirán, explotarán y monetizarán vulnerabilidades sin necesidad de intervención humana».

En 2026, aumentarán las intrusiones que se adaptan en tiempo real a las defensas, como el *malware* polimórfico, capaz de reescribirse para evitar su detección, impulsando un modelo delictivo completamente autónomo. Además, los ciberataques se enfocarán especialmente en entornos *cloud* híbridos, cadenas de suministro de software, paquetes de código abierto envenenados y manipulación de infraestructuras de IA mediante datos corruptos.

Habrá código sintético, IA manipulada y módulos defectuosos en procesos legítimos, lo que permitirá usar elementos de confianza para atacar la cadena de suministro digital desde el inicio y confundir los límites entre innovación y manipulación.

Operar con seguridad en un entorno cada vez más autónomo requerirá una estrategia basada en la visibilidad de extremo a extremo, la automatización con **validación humana** y una seguridad cultural compartida que sitúe la ciberseguridad como parte esencial de la infraestructura empresarial.

[41] The AI-fication of Cyberthreats. Disponible en: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Para 2027, se anticipa que el cibercrimen alcance una escala similar a industrias legítimas. *FortiGuard Labs* prevé mayor automatización ofensiva con IA autónoma, agentes en enjambre coordinando tareas y sofisticados ataques a cadenas de suministro enfocados en inteligencia artificial y sistemas integrados.[42]

Las organizaciones deben dejar atrás un enfoque reactivo y avanzar hacia una estrategia de resiliencia proactiva. Esto exige integrar la seguridad en cada etapa en la que se adopte la IA, en las operaciones *cloud* y en toda la cadena de suministro digital. Aquellas empresas que combinen una **supervisión humana constante**, el uso responsable de la inteligencia artificial con capacidades de defensa adaptativas, serán las que estén mejor posicionadas a la hora de afrontar este nuevo panorama.

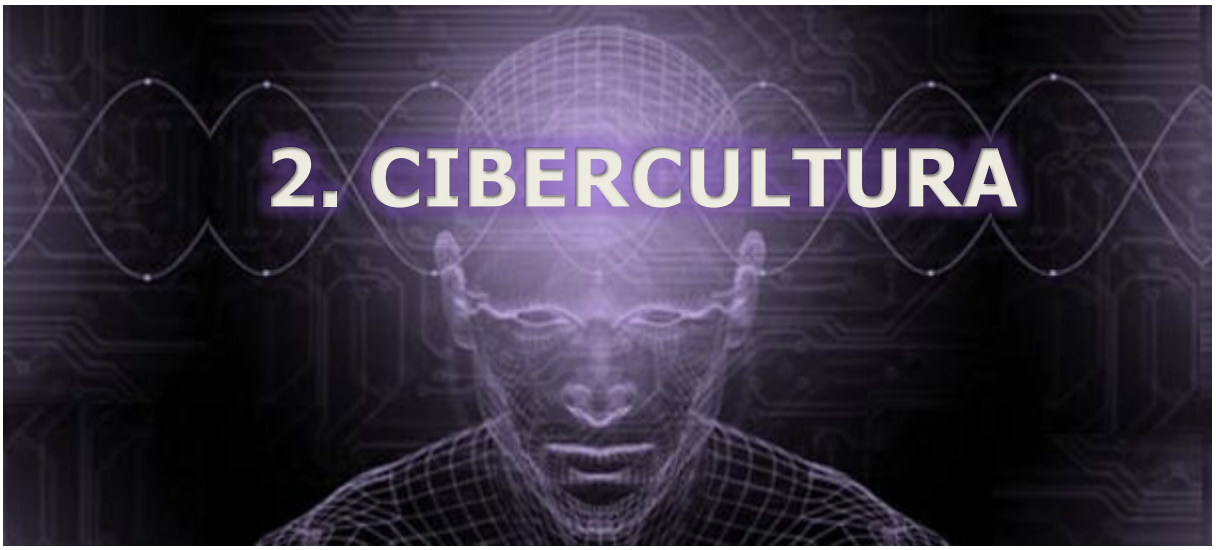
La velocidad y forma de escalar definirán la década que viene. **Las organizaciones que unifiquen la experiencia humana, la inteligencia y la automatización dentro de un único sistema de respuesta serán las que estén más capacitadas para enfrentar lo que se avecina.**

En definitiva, el panorama de la ciberseguridad es objeto de la evolución constante, exigiendo una adaptación continua por parte de cada individuo y de las organizaciones. La integración de una cibercultura como eje ayuda a desarrollar buenas prácticas de manera natural, imprescindibles para afrontar cada nuevo reto. Solo mediante el compromiso de la alta dirección, una gobernanza sólida y las personas como factor multiplicador de la defensa, se podrá garantizar la protección de los activos digitales y la resiliencia frente a las amenazas emergentes, consolidando así una estrategia robusta y orientada al futuro. A continuación, buscaremos responder **¿Por qué las personas son lo más importante?**

[42] Industrialización del cibercrimen: ¿Qué esperar en 2026?. Disponible en: https://hondanagroup.com/industrializacion-del-cibercrimen-que-esperar-en-2026/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2. CIBERCULTURA



Ciberseguridad se trata realmente de personas
Ciberseguridad es mentalidad, no solo tecnología

La rapidez con la que los agentes maliciosos emplean inteligencia artificial para desarrollar nuevas capacidades y coordinar sus operaciones representa un nivel de eficiencia notable. La superficie de ataque se ha vuelto considerablemente más dinámica, abarcando desde dispositivos móviles hasta redes, lo que requiere una visibilidad integral y la capacidad de detectar actividades maliciosas en cada punto imaginable.[43]

La cultura como nuevo perímetro: Los atacantes saben que el camino más rápido de acceso suele ser a través de un clic humano, un error o un momento de fatiga. Por eso la cultura convierte a las personas en defensoras, y no en vulnerabilidades.

[43] Building a Cyber Resilient Culture – Why people matter most. Disponible en: https://cyberfortgroup.com/building-a-cyber-resilient-culture-why-people-matter-most/#:~:text=Culture%20and%20Behaviour,another%20in%20doing%20the%20same.
Why Culture Is the First Line of Defense in the Age of Agentic AI. Disponible en: https://www.paloaltonetworks.com/perspectives/why-culture-is-the-first-line-of-defense-in-the-age-of-agentic-ai/#:~:text=It%20(%20a%20deeply%20ingrained%20security%20culture,formidable%20part%20of%20our%20collective%20security%20solution.
Your first line of defense in cybersecurity. Disponible en: https://www.cloudflare.com/the-net/security-first-culture/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Según «*The 2025 Security Awareness Training Statistics*»[44], publicado por *KeepnetLabs*, el 82% de las brechas de datos involucran algún elemento humano, ya sea por error, uso indebido o manipulación mediante ingeniería social. Además, *IBM Security*[45] asegura que «los CISO consideran el error humano como su principal riesgo de ciberseguridad».

El informe «*Voice of the* CISO 2025[46]» de *Proofpoint*, que encuestó a 1600 CISO de todo el mundo, concluyó que las personas siguen siendo el mayor riesgo con un 66%, incluso ante la creciente presión de la IA y la gestión ejecutiva. El informe de *Proofpoint* de 2024[47] mostró que el 74% de los responsables de ciberseguridad consideran el error humano como su principal amenaza, frente al 60% que lo afirmó en 2023. Con cifras iguales o superiores al 60% en los últimos tres años, queda claro que la tecnología importa en ciberseguridad, pero el factor humano determina el riesgo y la defensa.

Verizon[48] en su informe de 2025 analizó 22.052 incidentes de seguridad reales, de los cuales 12.195 fueron filtraciones de datos confirmadas que ocurrieron dentro de organizaciones de todos los tamaños y tipos, en 139 países. Los resultados revelan que:

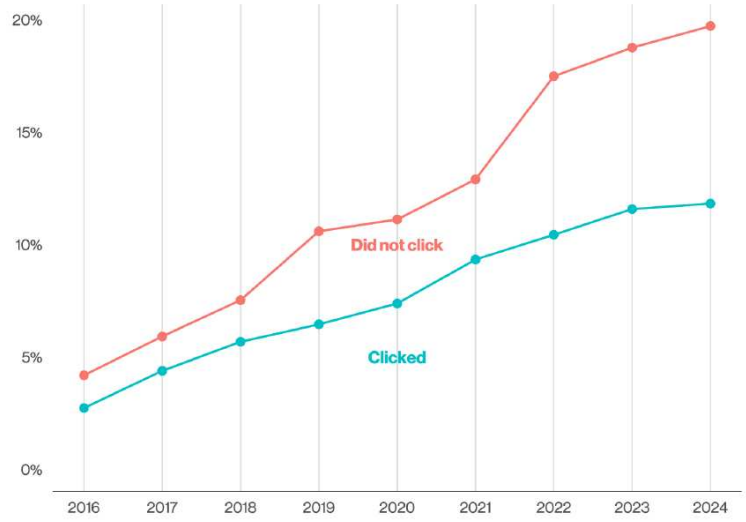
- El 60% de los incidentes de ciberseguridad implicaron el factor humano.
- El registro de credenciales robadas reveló que el 30% de los sistemas comprometidos eran dispositivos con licencia empresarial. Sin embargo, el 46% de los sistemas con credenciales corporativas comprometidos eran dispositivos personales.
- Los actores de amenazas están potenciando sus ciberataques con inteligencia artificial. El texto generado sintéticamente en correos electrónicos maliciosos se ha duplicado en los últimos dos años.
- El 15 % de los empleados accedió de forma habitual a plataformas de IA generativa desde sus dispositivos corporativos, lo que aumenta el riesgo de filtraciones de datos.

Para 2025[49], el informe abarcó la tasa de clics (Gráfico 2.1) en enlaces sospechosos en empresas con entrenamientos y simulaciones periódicas de *phishing*, concluyendo que:

[44] Security Awareness Training Statistics. Disponible en: https://keepnetlabs.com/blog/security-awareness-training-statistics
[45] Riesgo humano en ciberseguridad. Disponible en: https://www.ibm.com/es-es/think/insights/cisos-list-human-error-top-cybersecurity-risk
[46] Voice of the CISO 2025. Disponible en: https://www.proofpoint.com/sites/default/files/white-papers/pfpt-es-wp-voice-of-the-CISO-report.pdf
[47] Voice of the CISO 2024. Disponible en: https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2024-voice-ciso-report-reveals-three-quarters-cisos-identify
[48] 2025 Data Breach Investigations Report. Disponible en: https://www.verizon.com/business/resources/reports/dbir/?msockid=2a71ac0737bd62ce32c0b9de365d63c5
[49] El conjunto de datos de incidentes del DBIR 2025 ocurrieron entre el 1 de noviembre de 2023 y el 31 de octubre de 2024.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 2.1 Resultado simulacros de phishing a un clic!



Fuente: 2025 Data Breach Investigations Report

- A medida que los empleados participaron regularmente en actividades de entrenamiento, la proporción de personas que evitó hacer clic en contenidos maliciosos se incrementó de manera sostenida con el tiempo.
- Una formación constante fortalece la defensa de los equipos al crear una cibercultura proactiva, donde las personas identifican amenazas, reportan incidentes y toman decisiones que la tecnología no puede asegurar por sí sola.
- Incluso los sistemas de inteligencia artificial más avanzados no pueden replicar la intuición humana. Si bien las herramientas automatizadas son esenciales para detectar amenazas conocidas a gran escala, a menudo carecen de contexto y pensamiento crítico que sí pueden aportar empleados capacitados.
- Un miembro del equipo atento, que cuestione un correo electrónico sospechoso o reporte comportamientos inusuales, puede detectar lo que los algoritmos podrían pasar por alto y hacer la diferencia entre un incidente controlado y un ciberataque a gran escala.
- Resulta inviable lograr que absolutamente todos los empleados eviten hacer clic en enlaces sospechosos, pero al menos es fundamental que comprendan la importancia de informar cualquier actividad o contenido sospechoso. Los reportes no solo contribuyen a detectar amenazas de manera temprana, sino que permiten a la organización reaccionar y contener posibles incidentes con mayor agilidad, minimizando el impacto y fortaleciendo la postura de defensa frente a los ciberataques.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 2.2 ¿es suficiente La tecnología?

Fuente: Adaptado de https://www.linkedin.com/feed/update/urn:li:activity:7396426607999094784

Las amenazas cibernéticas están evolucionando a un ritmo sin precedentes, se producen a una escala mayor que nunca, volviéndose cada vez más sofisticadas, difíciles de detectar y las barreras lingüísticas, que antes podían ofrecer pistas sutiles de un ataque, prácticamente han desaparecido. Como respuesta, las organizaciones vienen invirtiendo fuertemente en tecnología y aunque estas herramientas son esenciales, existe una tendencia a depender en exceso únicamente de la tecnología, pasando por alto un elemento crucial en la ecuación de la ciberseguridad y es valorar a las personas como factor clave de la solución en vez de considerarlas como el origen del problema.

La tecnología es poderosa y permite la detección, automatización y defensa a gran escala. Sin embargo, la tecnología por sí sola no puede adaptarse, razonar ni preocuparse. Son las personas quienes hacen efectiva la tecnología y promueven la resiliencia, perciben lo inusual, hacen las preguntas adecuadas, escalan preocupaciones y recuperan los sistemas bajo presión.

Esta situación pone de relieve una verdad sencilla la tecnología por sí sola, por avanzada que sea, no es una solución milagrosa e incluso quienes tienen una sólida formación en el sector pueden tener dificultades para mantenerse al día con la evolución constante de los vectores de ataque. Por eso, más allá de la tecnología, no se trata solo de adquirir herramientas avanzadas ni de contar con personas brillantes dedicadas exclusivamente al equipo de seguridad. En el fondo, se trata de fomentar una cultura de seguridad sólida y profundamente resiliente.

La resiliencia cibernética no se trata solo de identificar amenazas; implica equilibrar el riesgo, el costo y el impacto operativo. Estas son decisiones matizadas que requieren comprensión, juicio humano, contexto y capacidad de priorización, cualidades que las máquinas no pueden emular completamente y que suelen determinar si un ataque tiene éxito o fracasa. Esta realidad requiere un cambio en nuestra

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

forma de pensar hacia una cultura consciente de la seguridad, donde la confianza y el empoderamiento sean la primera línea de defensa.

Como parte del desarrollo del presente estudio la CRC consultó a expertos internacionales para reflexionar sobre la eficacia de las defensas y el papel tanto del factor humano como de la tecnología. Para lo cual elaboró la siguiente pregunta que invita a analizar cómo podemos reforzar nuestras estrategias para proteger mejor a las organizaciones y a la sociedad frente al cambiante panorama del ciberdelito, considerando no solo las herramientas disponibles, sino también el desarrollo de una cultura resiliente y consciente en materia de seguridad digital.

> A lo largo del tiempo, la tecnología se ha orientado a mantenerse al ritmo del avance del ciberdelito. En tu opinión, ¿es la tecnología lo suficientemente ágil e inteligente como para cambiar esta dinámica y frenar la ofensiva de los ataques, o qué factor multiplicador debería añadirse a la ecuación para fortalecer nuestras defensas ante el ritmo evolutivo del ciberdelito? Por favor, explica tu respuesta en un párrafo.

«La tecnología es una defensa útil para mantenerse al ritmo del avance del ciberdelito; sin embargo, también debe considerarse el factor humano. Es necesario realizar campañas continuas de información y educación para los usuarios del ciberespacio hasta que la cultura de ciberseguridad se convierta en un hábito»

Susana Panes
Chief , Corporate Planning and Programming
National Telecommunications Commision
Filipinas

«Como sociedad, avanzamos poco a poco hacia dispositivos más seguros y una mayor transparencia en la comercialización de tecnologías y dispositivos conectados a nuestros hogares y equipos. Nuestras plataformas tecnológicas también están evolucionando para ofrecer mejores defensas al servicio de los consumidores. Constantemente necesitamos capacitar de manera constante a nuestra fuerza laboral para detectar y contener amenazas. Sin embargo, dado que las amenazas cibernéticas ya forman parte de nuestra vida cotidiana, los gobiernos y las empresas deberían trabajar en planes de recuperación. Si bien la ciberdefensa es útil y necesaria, la naturaleza asimétrica de la ciberseguridad implica que, tarde o temprano, un ataque tendrá éxito. Es especialmente crítico que las sociedades desarrollen planes de recuperación para infraestructuras críticas como energía, agua y telecomunicaciones. También es importante que los consumidores cuenten con planes de contingencia para casos en los que en casa fallen la cerradura o el sistema de calefacción inteligentes. Asegurar que tengamos formas de sobreponernos y superar un fallo cibernético debe formar parte de nuestra planificación».

Grace Koh
Vice President Government Relations
Ciena
Estados Unidos

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

«La tecnología sigue evolucionando rápidamente, pero los ciberdelincuentes suelen adaptarse aún más rápido, ya que operan fuera de los límites de la gobernanza, la responsabilidad y la supervisión ética. Aunque las herramientas avanzadas refuerzan nuestras defensas, la tecnología por sí sola no basta para cambiar esta tendencia. **El factor multiplicador que necesitamos es un ecosistema sostenible centrado en las personas: profesionales calificados**, estructuras de gobernanza sólidas, políticas claras e inversión a largo plazo en prácticas seguras. Este enfoque equilibrado garantiza que nuestras defensas crezcan al mismo ritmo que las amenazas a las que nos enfrentamos»

Gemma Pyne-Bailey
Cybersecurity specialist and Trainer
National Cybersecurity Coordination Centre
Sierra Leona

«Cuanto más evoluciona la tecnología, más complejas se vuelven las amenazas y más sofisticadas las técnicas de ataque. De ahí la necesidad de adaptar continuamente nuestras técnicas de defensa mediante la implantación de tecnologías de vanguardia, **el desarrollo de capacidades, la formación y las campañas de concientización**»

Racky Seye
Head of the National Cyberattack Response
National Cybersecurity Authority (DCSSI)
Senegal

«Mientras la tecnología sigue avanzando en respuesta a la sofisticada evolución de las amenazas cibernéticas, por sí sola la tecnología no es suficiente para revertir la ventaja que suelen tener los atacantes. **Los ciberdelincuentes explotan no solo debilidades tecnológicas, sino también comportamientos humanos** y deficiencias en los procesos. Por ello, el factor multiplicador que debe añadirse es un enfoque holístico y basado en la inteligencia en materia de seguridad, uno que combine tecnologías avanzadas como la detección de amenazas mediante IA, con procesos sólidos, **desarrollo continuo de habilidades y una cultura de concientización en ciberseguridad**. Solo integrando personas, procesos y tecnología podremos ralentizar de forma efectiva el avance ofensivo de los ciberataques y fortalecer nuestra ciber resiliencia tanto a nivel nacional como organizacional»

Zareefa Mustafa
Senior Manager Cybersecurity
National Information Technology Development Agency (NITDA)
Nigeria

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

«El principal desafío técnico consiste en mantener las defensas de ciberseguridad impulsadas por IA por delante de los ataques también basados en IA, como la generación de código malicioso y la ingeniería social sofisticada. Soy optimista respecto a que esto puede lograrse. Las empresas de ciberseguridad están incorporando la inteligencia artificial en sus flujos de trabajo y productos, pero el siguiente obstáculo es la implementación. Esto requiere una ejecución técnica, integración con las herramientas existentes, **capacitación del personal** y recursos presupuestarios para nuevos contratos. Todo ello representa una carga considerable para la mayoría de las organizaciones»

John Perrino
Senior Policy and Advocacy Expert
Internet Society (ISOC)
Estados Unidos

«Trabajo principalmente en ciberdefensa, más que en ciberdelincuencia. Por eso, mi enfoque está más orientado a los ataques que a la criminalidad. La diferencia es que los ataques suelen consistir principalmente en intrusiones o denegaciones de servicio, mientras que la criminalidad casi siempre implica algún tipo de extorsión financiera, apropiación indebida o fraude.

Combatir la ciberdelincuencia consiste, sobre todo, en dificultar que los delincuentes se hagan pasar por usuarios legítimos de Internet. Esto debe hacerse sin obstaculizar demasiado el trabajo legítimo de los usuarios, así que se trata de encontrar un equilibrio entre seguridad y usabilidad. Del mismo modo que las compañías de tarjetas de crédito asumen cierto nivel de fraude para no asustar a sus clientes, este mismo tipo de compromiso se da en la usabilidad de Internet. Las buenas defensas contra la ciberdelincuencia son aquellas que imponen barreras muy altas a los delincuentes, pero barreras imperceptibles para los usuarios legítimos. Existen otros equilibrios: los cortafuegos empresariales usan habitualmente certificados CA falsificados para realizar ataques de intermediario (man-in-the-middle) contra el tráfico cifrado, con el fin de analizar en profundidad los paquetes y detectar amenazas internas o usos no autorizados de la red corporativa… esto es, en esencia, indistinguible de los ataques criminales, por lo que los navegadores no advierten de estos ataques, ya que no pueden distinguir entre un intermediario "legítimo" y uno criminal, y no quieren "asustar" a los usuarios, debido a un desafortunado desajuste entre los incentivos del mercado y los objetivos de seguridad».

Entonces, ¿dónde nos deja esto?. No se puede esperar educar a todos los usuarios, por lo que las soluciones no deben requerir cambios en el comportamiento del usuario, ni una inteligencia o atención extraordinarias por su parte. Tampoco se puede esperar asegurar todos los puntos finales, así que las soluciones no pueden depender del software de los dispositivos finales. Eso nos deja con las defensas del lado del servidor y en la red. Las defensas en la red dependen de que el tráfico ilegítimo tenga metadatos observables diferentes al tráfico legítimo. El lado del servidor requiere que los servidores mantengan un gran volumen de información de estado. Ambas opciones son complejas, pero probablemente la del lado del servidor sea la más alcanzable de las dos».

Bill Woodcock
Secretary General
Packet Clearing House

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En conclusión, alcanzar una cultura de ciberseguridad sostenible implica comprender que la tecnología es solo una parte de la ecuación; el compromiso y la participación activa de las personas son esenciales para fortalecer cualquier estrategia de defensa. Solo integrando la seguridad en los valores y comportamientos cotidianos de todos los miembros de la organización, se podrá responder de manera efectiva a los desafíos cambiantes del entorno digital y proteger los activos críticos ante amenazas cada vez más sofisticadas.

2.1 CULTURA DE CIBERSEGURIDAD SOSTENIBLE[50]

La ciberseguridad no se trata solo de tecnología, se trata de personas. Aunque los sistemas de seguridad son clave, el factor decisivo suele estar en las decisiones individuales: hacer clic en enlaces sospechosos o reportar intentos de *phishing* marca la diferencia, o ¿pasa desapercibido? La cultura de ciberseguridad, es decir, los valores y comportamientos compartidos, se convierte así en una defensa crucial para cualquier organización. Las herramientas por sí solas no bastan; su eficacia real depende de la cultura que decide si pasa o no en la práctica del día a día.

En esencia, la cultura de ciberseguridad trata de lo que las personas hacen cuando nadie las observa. Es el instinto de cuestionar una solicitud sospechosa, la confianza para alzar la voz cuando algo parece incorrecto y la comprensión colectiva de que la seguridad es responsabilidad de todos.

2.1.1. ¿Cómo se construye cibercultura? La cultura no es simplemente un cartel en la pared. Se refleja en la forma en que los equipos interactúan y en los comportamientos que se reconocen y premian. Cada área de una organización debe asumir la seguridad digital como una responsabilidad fundamental propia. Esto significa formar y capacitar para tomar decisiones seguras y acertadas, fomentar un entorno en el que las personas se sientan cómodas al expresar cualquier sospecha o incidencia, y que todos los líderes de la organización sepan comunicar y colaborar eficazmente si sucede lo peor y se produce un incidente de seguridad.

Según la investigación académica[51], la cultura de ciberseguridad se entiende como el conjunto de valores, creencias y actitudes que motivan a los empleados a actuar para resguardar y defender a la organización ante posibles ciberataques. En la realidad, esta cultura puede observarse en tres niveles distintos:

- Nivel de liderazgo: donde se establecen las prioridades, las inversiones y el tono.
- Nivel de grupo: donde los equipos fijan normas y se ayudan mutuamente a incorporar prácticas seguras.
- Nivel individual: donde la concienciación personal, la confianza en uno mismo y las decisiones cotidianas refuerzan o debilitan la resiliencia.

[50] Cybersecurity Awareness Month 2025: Building a Cybersecurity Culture That Lasts. Disponible en: https://www.rapid7.com/blog/post/c-cybersecurity-awareness-month-2025-building-a-cybersecurity-culture-that-lasts/
[51] Cybersecurity Awareness Month 2025: Building a Cybersecurity Culture That Lasts. Disponible en: https://www.rapid7.com/blog/post/c-cybersecurity-awareness-month-2025-building-a-cybersecurity-culture-that-lasts/

El establecimiento de una cultura de seguridad resulta fundamental y su mantenimiento demanda dedicación, pues afianzar cambios sostenibles y modificar conductas implica tiempo. Las siguientes prácticas permiten fortalecer una cibercultura sólida:

2.1.1.1. Escasez de competencias y brechas de fuera laboral[52]**.** Las compañías necesitan dedicar tiempo y recursos financieros al desarrollo de talento humano para combatir la ciberdelincuencia, ya que aún se enfrentan desafíos debido a la escasez de especialistas y competencias en ciberseguridad.

Para estos efectos, las empresas elaboran presupuestos para contratación y capacitación, evalúan tecnologías como la inteligencia artificial generativa para suplir la falta de talento o ya la usan para reducir la brecha de competencias.

2.1.1.2. Liderazgo y gestión: Desempeñan un papel fundamental en la formación de una cultura de resiliencia cibernética. Cuando los líderes adoptan y muestran comportamientos de seguridad ejemplares, como el uso de contraseñas robustas, la notificación de intentos de *phishing* y el cumplimiento de los protocolos de protección de datos, transmiten el mensaje que la ciberseguridad es responsabilidad de todos y se trata como un riesgo empresarial estratégico, no solo como un problema técnico.

2.1.1.3. Comunicación y preparación: Los líderes de todos los departamentos deben comprender claramente sus funciones y responsabilidades. Es fundamental que sepan cómo comunicarse de manera efectiva entre ellos y con los equipos de seguridad si ocurre un incidente. Cuanto más se practique y se ponga a prueba las respuestas ante distintos escenarios, más preparados y seguros estarán las organizaciones.

2.1.1.4. Comunicación abierta: Animar a los empleados a informar sobre riesgos, errores o actividades sospechosas. Esta apertura garantiza que las amenazas potenciales se detecten pronto y se aborden con rapidez. Los nuevos empleados deben conocer las políticas y directrices de ciberseguridad desde el primer día, comprendiendo así de inmediato su importancia y los comportamientos esperados.

2.1.1.5. Seguridad y empoderamiento: Los errores se tratan como oportunidades de aprendizaje y se debe sentir que es seguro y alentador levantar la mano cuando detectan algo que no parece correcto. Al tener una cultura del aprendizaje, las organizaciones empoderan a los empleados para que se expresen, compartan ideas, mejoren continuamente y tomen decisiones seguras en su trabajo diario.

La seguridad no debe ser solo una política, sino una práctica integrada en el día a día que fomenta la resiliencia y la agilidad frente a amenazas en constante evolución. Es clave guiar a los equipos hacia nuevos enfoques y fomentar debates sobre casos prácticos, evitando limitarse a cursos online tradicionales.

[52] Cybersecurity Stats and Facts for 2025. Disponible en: https://www.vikingcloud.com/blog/cybersecurity-statistics#spending

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.1.1.6. Responsabilidad compartida: La ciberseguridad se percibe como responsabilidad de todos, no solo del departamento de informática. Desde el departamento legal hasta operaciones, pasando por finanzas y recursos humanos, cada parte de la organización debe reconocer e interiorizar que la seguridad también es su responsabilidad. Cuando los empleados comprenden cómo sus acciones afectan a la seguridad de la organización, son más sensibles a adoptar comportamientos seguros y a apoyarse mutuamente en este objetivo.

2.1.1.7. Operaciones complejas: Una de las principales cargas que pesa sobre los equipos de seguridad en las organizaciones es la complejidad. Cuanto más complejos sean los sistemas, mayor será la probabilidad de que se produzca un error. Las configuraciones incorrectas representan un riesgo significativo que los atacantes aprovechan. Es fundamental que los equipos validen la eficacia de las configuraciones y la implementación de controles para garantizar que el error humano no genere una vulnerabilidad.

2.1.1.8. Políticas de ciberseguridad claras y comprensibles: Asegura que las directrices no sean solo teóricas; explican el «cómo» y el «por qué», para hacerlas realmente prácticas. Las políticas deben ser accesibles y revisadas anualmente para reflejar nuevas amenazas y cambios tecnológicos.

2.1.1.9. Demostrar el retorno de la inversión: Para la dirección financiera, el gasto en seguridad suele verse como difícil de medir. Se invierte dinero, pero el beneficio en reducción de riesgos no es claro. Los SOC deben justificar sus inversiones, ya que a menudo son considerados solo un centro de costos sin impacto evidente en la rentabilidad del negocio.

En la actualidad, la seguridad cibernética debe probar su impacto en el rendimiento financiero mediante la prevención de brechas, reducción de falsos positivos, automatización, respuesta rápida y actualizaciones constantes para reducir riesgos y optimizar recursos.

2.1.1.10. Medir el desarrollo: No se puede mejorar lo que no se mide, pero limitarse a los índices de finalización de la formación no muestra cambios reales. Es necesario utilizar indicadores más relevantes que reflejen si hay modificación de comportamiento, como:

- Tasas de reporte de *phishing*: no solo quién hace clic, sino quién lo comunica
- Rapidez en la aplicación de parches: que tan rápido se instalan las actualizaciones críticas
- Higiene de contraseñas: uso de autenticación multifactor (MFA), fortaleza de las contraseñas y patrones de reutilización
- Actividad en la notificación de incidentes: frecuencia y calidad de los reportes

La inteligencia artificial analiza datos para generar puntuaciones de riesgo humano, identificar tendencias y señalar áreas de intervención. Esto permite a los líderes tomar decisiones basadas en datos y mostrar avances ante directivos y reguladores.

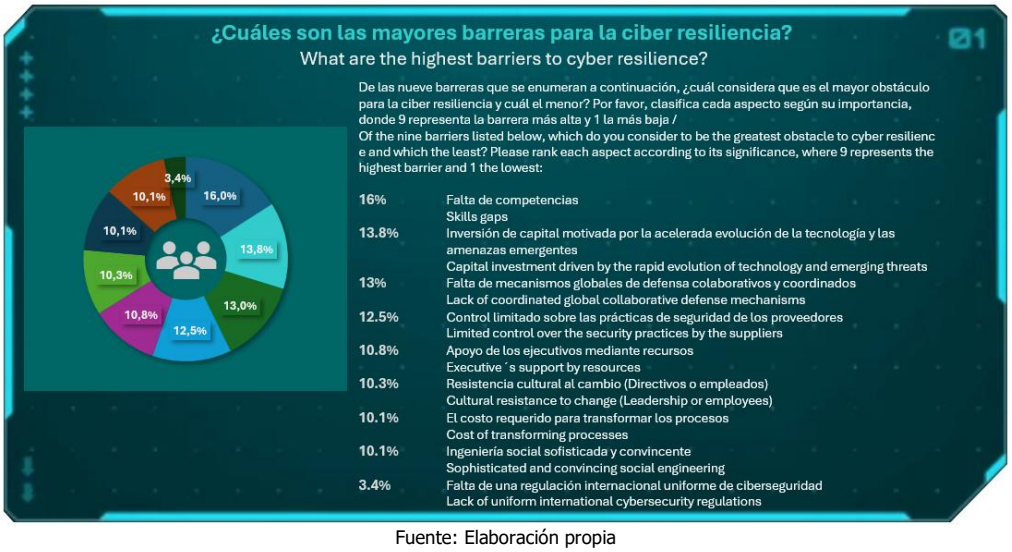
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.1.2. Cibercultura resiliente. Incorporar la mentalidad de ciberseguridad requiere más que módulos de formación anual e ir más allá del tradicional «cumplir el trámite». Una de las maneras más eficaces de fortalecer esta cultura es a través de simulacros de crisis y ejercicios de escritorio (tabletop). Estas simulaciones no solo ponen a prueba las respuestas técnicas, sino también la toma de decisiones, la comunicación y la coordinación entre equipos, convirtiendo la teoría en práctica y exponiendo posibles carencias antes de que surjan amenazas reales.

Otra práctica para normalizar estos comportamientos es reconocer y recompensar el buen comportamiento en ciberseguridad. Celebrar a quienes demuestran una buena higiene digital como aplicar prácticas seguras de manejo de datos, participar en iniciativas de capacitación y opinar sobre lo que funciona, lo que no está claro y dónde se pueden mejorar los procesos ayuda a construir una cultura de vigilancia y mejora continua. Se pueden incluir encuestas anónimas, evaluaciones tras formación, buzones de sugerencias o foros durante las reuniones de equipo, lo importante es actuar sobre el *feedback*, mostrando que los aportes se traducen en cambios reales. El reconocimiento puede ir desde menciones en reuniones de equipo y boletines internos hasta premios formales o incentivos.

La siguiente pregunta, formulada por la CRC a diversos actores que guardan algún tipo de relación con el sector de ciberseguridad y ciberdefensa, tiene por objetivo identificar y priorizar los principales obstáculos que enfrentan las organizaciones en el camino hacia una ciber resiliencia efectiva. Comprender cuáles son las barreras más significativas resulta esencial para orientar esfuerzos, recursos y políticas que permitan fortalecer las capacidades de respuesta y recuperación ante incidentes de ciberseguridad. Se solicita a los participantes que valoren nueve posibles barreras, clasificándolas según su impacto, para así obtener una visión integral de los desafíos más apremiantes y aquellos que presentan menor incidencia:

Gráfico 2.3 Consulta al sector



Fuente: Elaboración propia

Los resultados de la consulta realizada a actores que guardan algún tipo de relación con el sector de ciberseguridad y ciberdefensa permiten identificar cuáles son los principales obstáculos en el camino hacia la ciber resiliencia. La barrera más significativa, señalada con un 16%, es la falta de competencias, lo que evidencia una necesidad urgente de fortalecer las capacidades y habilidades en materia de ciberseguridad dentro de las organizaciones. En segundo lugar, con un 13,8%, se destaca la presión que genera la acelerada evolución tecnológica y la aparición constante de nuevas amenazas, que obliga a incrementar la inversión de capital para mantener la protección adecuada. Otros obstáculos relevantes son la ausencia de mecanismos globales de defensa colaborativos y coordinados (13%), el control limitado sobre las prácticas de seguridad de los proveedores (12,5%) y el insuficiente apoyo ejecutivo en términos de recursos (10,8%).

También sobresalen la resistencia cultural al cambio tanto de directivos como de empleados (10,3%), el costo requerido para transformar los procesos (10,1%) y la sofisticación de las técnicas de ingeniería social (10,1%). Por último, la menor barrera identificada, con apenas el 3,4%, es la falta de una regulación internacional uniforme de ciberseguridad, lo que sugiere que, aunque relevante, este aspecto es percibido como menos crítico en comparación con los desafíos internos y operativos que enfrentan las organizaciones actualmente.

2.1.3 El papel del liderazgo. El liderazgo dentro de una empresa ejerce una influencia profunda y de gran alcance en la forma en que las personas de esa organización se comportan, desde hacer lo correcto, pasando por priorizar la sostenibilidad o favorecer la producción en masa y el consumismo. Las empresas suelen expresar lo que significa el liderazgo para ellas a través de un conjunto de competencias que esperan que sus líderes encarnen.

Como señala Edgar Schein[53], los líderes son los arquitectos principales de la cultura organizacional, no solo sus influenciadores. La cultura se desarrolla a partir de las prácticas de liderazgo al definir lo que es importante, lo que hace que la gestión consciente y deliberada de la cultura sea una de las funciones más críticas del liderazgo.

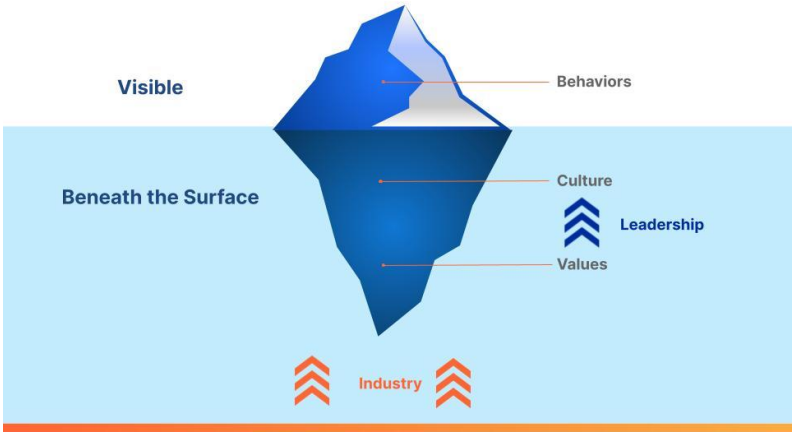
Schein define la cultura organizacional como «un patrón de pensamiento que un grupo ha aprendido mientras resolvía problemas y que luego enseña a los nuevos miembros del grupo como la forma correcta de percibir, pensar y sentir sobre esos problemas». Estos patrones de pensamiento conducen a ciertos comportamientos que, a su vez, se refuerzan cuando otros miembros del grupo exhiben dichos comportamientos.

El siguiente gráfico muestra cómo lo que es visible para los demás (los comportamientos) tiene raíces y significados mucho más profundos para una empresa que el mero comportamiento en sí:

[53] Cultura Organizacional y Liderazgo por Edgar H.Schein. Disponible en: https://wind4change.com/organizational-culture-leadership-framework-edgar-schein/
[53] What Do Coaches Need to Know About Edgar Schein?. Disponible en: https://www.executivecoachcollege.com/research-and-publications/what-coaches-need-to-know-about-edgar-schein.php#:~:text=%22The%20only%20thing%20of%20real,D

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 2.4 Raíces del comportamiento



Fuente: 2025 Data Breach Investigations Report

Los líderes[54] pueden facilitar o complicar la creación de una cultura cibersegura. Si no mantienen conductas seguras o no refuerzan el mensaje, la tarea se dificulta mucho. Conseguir que los líderes aprovechen cada oportunidad para hablar sobre ciberseguridad tendrá efectos exponenciales en la eficacia de las políticas.

Además, conviene evaluar el conocimiento en ciberseguridad durante la selección de personal. Incorporar líderes con alta conciencia de riesgos fortalece las buenas prácticas en sus equipos.

2.2 PROMOCION DE LA CIBERCULTURA[55]

Sin la ciberseguridad todos estaríamos expuestos y por esa razón es una prioridad para los gobiernos y empresas de todo el mundo, donde varios países organizan campañas para **promover la importancia de la ciberseguridad para toda la sociedad**, desde gobiernos, empresas hasta toda la ciudadanía. La promoción de la cibercultura «Mes de la promoción de la ciberseguridad» es un esfuerzo global para crear un entorno digital más seguro a través de la **educación, la prevención y la colaboración** ante el auge del cibercrimen y se ha convertido en una necesidad más que exigencia de la actualidad.

Los diferentes escenarios buscan **visibilizar amenazas invisibles** (alertar sobre tácticas de ciberdelincuentes, riesgos, vulnerabilidades en IT/OT), **impulsar acciones concretas** (Disparador para que empresas y personas revisen sus controles de seguridad, actualicen políticas y se formen en

[54] TheNET, Unlocking cyber resilience. Disponible en: https://www.cloudflare.com/the-net/unlocking-cyber-resilience/
[54] The role of leadership in shaping organizational culture. Disponible en: https://www.cloudflare.com/the-net/unlocking-cyber-resilience/
[55] Octubre, mes de concientización en Ciberseguridad. Disponible en: https://gblogs.cisco.com/la/ciberseguridad1-jreynabr-octubre-mes-de-la-concientizacion-sobre-la-ciberseguridad/

buenas prácticas) y **empoderar a la sociedad** (Que todos tengan los recursos para estar más seguros en línea, no solo expertos, sino ciudadanos comunes, pequeñas empresas y organizaciones.

Surgió en EEUU en 2004 y se declaró oficialmente el mes de octubre como el *National Cyber Security Awareness Month*[56] y este año cumplió 21 años de celebración con la intención de promover la ciberseguridad entre los ciudadanos y las organizaciones, con el objetivo de proporcionar información actualizada sobre ciberseguridad a través de la sensibilización y el intercambio de buenas prácticas. A su vez, Europa adopto esta buena práctica en el 2012, iniciativa organizada por la *Agencia Europea de Seguridad de las Redes y de la Información* (ENISA), declarándose así el *Mes Europeo de la Ciberseguridad* y desde el 2018, Chile se convirtió en el primer país latinoamericano en celebrar este mes, en un esfuerzo por promoverla y realizar ejercicios nacionales en esta área.

En este contexto de iniciativas internacionales y esfuerzos coordinados para fomentar la cibercultura y la seguridad digital, destaca también la conmemoración de fechas clave que buscan sensibilizar a la sociedad sobre los riesgos y la importancia de proteger la información. El Día Internacional (30 de Noviembre): Se estableció tras el Gusano Morris de 1988, el primer malware de propagación masiva en internet, para recordar la necesidad de proteger los datos digitales.

En definitiva, todas estas iniciativas y estrategias reflejan un esfuerzo global por sensibilizar y empoderar a las personas en materia de ciberseguridad, reconociendo que los individuos son el activo más valioso en el entorno digital. Por ello, la protección y la formación de las personas se han convertido en el eje central de las campañas internacionales, ya que solo una sociedad informada y consciente puede contribuir eficazmente a la construcción de un **ciberespacio más seguro** y resiliente.

[56] Conectados' Octubre, mes de la ciberseguridad. Disponible en: https://www.ui1.es/blog-ui1/octubre-celebrando-el-mes-de-la-ciberseguridad#:~:text=Reconocer%20y%20reportar%20phishing.,es%20para%20toda%20la%20sociedad.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

3. SEGURIDAD DIGITAL EN CIFRAS

La expansión de las redes de telecomunicaciones, impulsada por tendencias como la virtualización, la proliferación de dispositivos conectados y el despliegue de infraestructuras cada vez más amplias, está redefiniendo la manera en que circula la información. De acuerdo con la Unión Internacional de Telecomunicaciones (UIT), para el año 2024, alrededor del 68% de la población mundial utilizaba Internet, lo que equivale a alrededor de 5,5 mil millones de personas conectadas (UIT, 2024[57]). Asimismo, se estima que para 2028 habrá cerca de 35 mil millones de dispositivos IoT en funcionamiento, frente a los aproximadamente 16 mil millones registrados en 2023 (UNCTAD, 2024)[58]. Este crecimiento no solo acelera la digitalización y abre espacio para nuevos modelos de negocio y formas de interacciones sociales, sino que también incrementa los riesgos y vulnerabilidades de un mundo cada vez más interconectado.

El rápido avance y la adopción de las tecnologías digitales, si bien han generado enormes beneficios y se han convertido en un componente esencial para personas, empresas y gobiernos, también expone a la sociedad ante nuevas amenazas. La realidad actual evidencia que el mundo está cada vez más interconectado y, al mismo tiempo, más vulnerable, lo que hace imprescindible fortalecer la seguridad y la confiabilidad de los entornos digitales para aprovechar plenamente sus oportunidades sin aumentar los riesgos.

La ciberseguridad enfrenta una evolución acelerada de las amenazas. Lo que antes eran ataques puntuales ejecutados por actores individuales, desde entornos reducidos y con vectores simples, hoy se

[57] Cifras tomadas de uso del internet. Disponible en: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/
[58] UNCTAD (United Nations Conference on Trade and Development). (2024). *Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future.* Ginebra: Naciones Unidas. Disponible en: https://unctad.org/publication/digital-economy-report-2024

ha transformado en operaciones sostenidas por grupos organizados, con infraestructura global, múltiples vectores y capacidades potenciadas por inteligencia artificial. De acuerdo con el informe Global de Fortinet, «Panorama de Amenazas 2025 de Fortinet», los atacantes actúan con mayor rapidez, automatizan el reconocimiento de vulnerabilidades, reducen el tiempo entre su descubrimiento y explotación, y amplían sus operaciones mediante la industrialización del cibercrimen, erosionando así las ventajas defensivas tradicionales. (Fortinet, 2025[59]).

3.1 CADENA DE ATAQUE Y CICLO DE MATERIALIZACIÓN

Un ciberataque no se desarrolla de forma inmediata ni de manera aislada, sino que responde a una cadena de eventos secuenciales que permiten al atacante pasar del reconocimiento inicial al compromiso efectivo de los sistemas. Este proceso involucra múltiples actores y distintos niveles de especialización, que van desde grupos encargados del escaneo automatizado y la detección de vulnerabilidades, hasta redes dedicadas a la explotación, venta y uso de credenciales comprometidas en mercados clandestinos de la *dark web*.

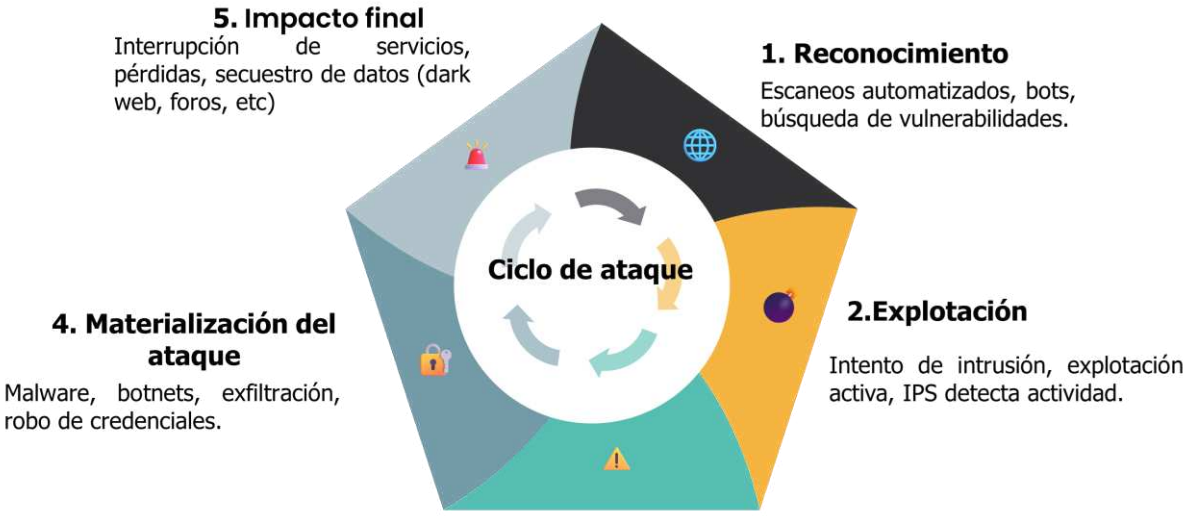
En las etapas iniciales predominan los escaneos y sondas automáticas, realizados por *bots* o *scripts* que rastrean la red en busca de fallas conocidas, seguidos por intentos de explotación activa detectados por los sistemas de prevención de intrusiones (IPS). Posteriormente, los ataques se trasladan a los puntos finales (*endpoint*), donde se concentran esfuerzos más sofisticados para comprometer equipos, manipular software o sustraer información sensible.

Finalmente, en la fase de materialización, los actores más especializados ejecutan acciones concretas como la distribución de *malware*, la activación de *botnets*, el robo de credenciales y la exfiltración de datos. Esta última etapa es donde el ataque produce los efectos tangibles: interrupción de servicios, pérdidas económicas, o acceso no autorizado a información crítica.

En conjunto, la cadena de ataque refleja la organización del cibercrimen, en la que las funciones se fragmentan, los actores se especializan y la colaboración entre ellos a través de foros, redes clandestinas o servicios de «ciberataque como servicio» (*Cybercrime-as-a-Service*), permite escalar las operaciones y reducir los tiempos entre el descubrimiento y la explotación de vulnerabilidades.

[59] Conectados. Disponible en: https://documents1.worldbank.org/curated/en/099041024190032046/pdf/P1812111db279e0141a72015f27c232cced.pdf

Gráfico 3.1 Ciclo de materialización del ataque

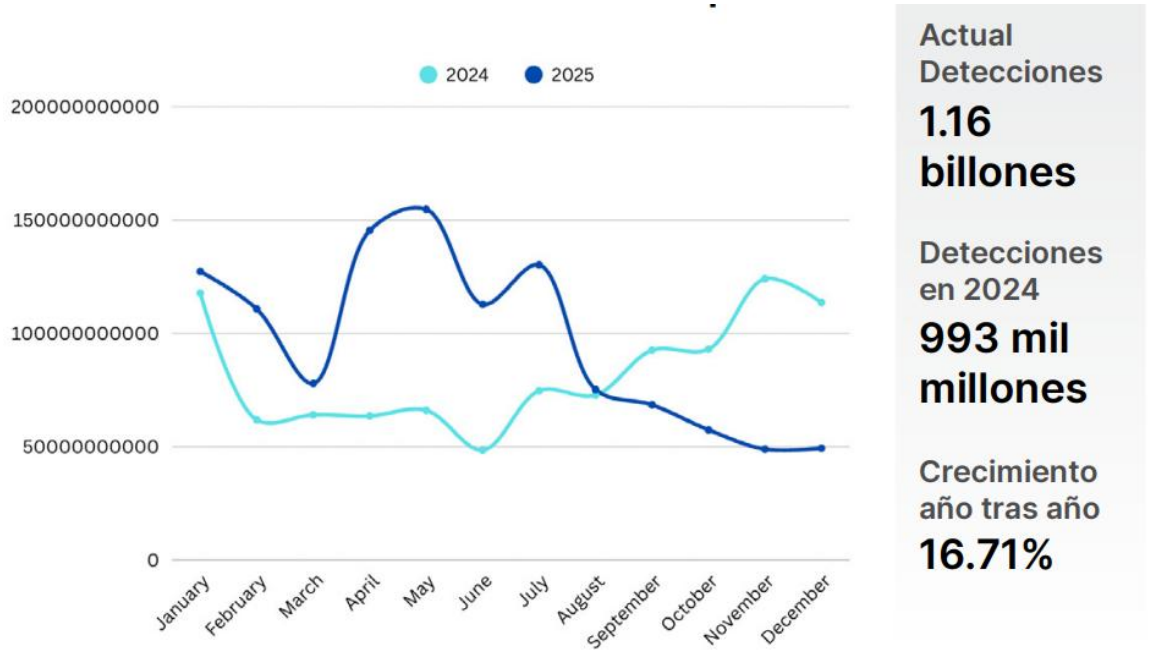


Fuente: Elaboración propia

3.1.1. Reconocimiento: Escaneo automático. El escaneo automatizado se ha consolidado como una de las tácticas más utilizadas para preparar ataques a gran escala. A través de herramientas de reconocimiento automáticas, los actores maliciosos rastrean redes y dispositivos en busca de puertos abiertos, configuraciones inseguras o vulnerabilidades recién divulgadas. De acuerdo con *FortiGuard Labs* (Fortinet, 2025[60]), esta práctica alcanzó picos históricos durante 2024, con un incremento global del 16,7% respecto a 2023. El volumen de esta actividad llegó a cerca de mil millones de escaneos mensuales, equivalentes a 36.000 por segundo. Ver Gráfico 3.2.

[60]Fortinet. (2025). FortiGuard Labs Global Threat Landscape Report 2025. Sunnyvale, CA: Fortinet, Inc. Disponible en: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

Gráfico 3.2 Número de escaneos mensuales



Fuente: Gráfico tomado del informe global del panorama de amenazas de Fortinet 2025

En este contexto, los atacantes concentran sus esfuerzos hacia protocolos ampliamente utilizados en sectores críticos como telecomunicaciones, industria, y servicios financieros. En 2024, casi la mitad de los escaneos activos (49%) se dirigieron a SIP (VoIP) y otros servicios de señalización y comunicaciones. La explotación de teléfonos IP, *gateways* y decodificadores no solo facilita fraudes e interceptación de llamadas, sino que además habilita movimientos laterales hacia redes corporativas. Mediante el uso de credenciales legítimas y dispositivos IoT comprometidos, los atacantes logran acceso inicial, y exfiltran información, transformando la infraestructura de telecomunicaciones en un vector estratégico de alto valor para el espionaje, el crimen organizado y operaciones patrocinadas por Estados.

3.1.2. Explotación: Intentos de vulneración de sistemas. Los sistemas de prevención de intrusiones (IPS, por sus siglas en inglés) monitorean de manera continua el tráfico de red para detectar, bloquear y registrar intentos de explotación de vulnerabilidades antes de que comprometan los sistemas internos.

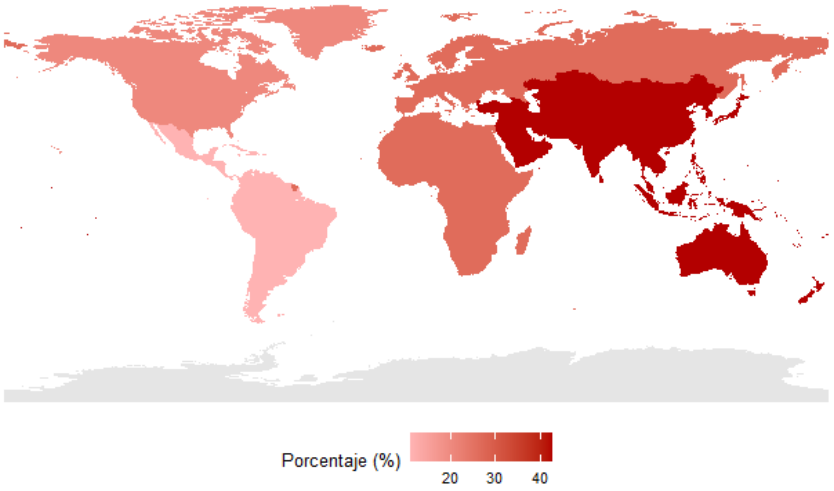
En este escenario de creciente sofisticación, el informe *Global Threat Landscape 2025 de Fortinet*[61] reporta que, durante el año 2024, el volumen de intentos de explotación detectados alcanzó más de 97

[61] Fortinet. (2025). FortiGuard Labs Global Threat Landscape Report 2025. Sunnyvale, CA: Fortinet, Inc. Disponible en: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

mil millones a nivel global, lo que refleja la magnitud del riesgo y la capacidad de los atacantes para operar de forma masiva. Aunque todas las regiones enfrentan amenazas significativas, el impacto no es homogéneo.

El mismo informe señala que, como se observa en el Gráfico 3.3, la región de Asia Pacífico (APAC) concentra el 42% de los intentos de explotación, lo que la convierte en el principal blanco de los cibercriminales. Europa, Medio Oriente y África (EMEA) representan el 26%, seguida por América del Norte con el 20%. En contraste, América Latina registra el 11%, una participación menor en el total global, aunque en crecimiento debido al avance de la digitalización y la exposición de infraestructuras críticas en la región.

Gráfico 3.3 Participación de los IPS por continente



Fuente: Elaboración propia a partir de datos del informe global del panorama de amenazas de Fortinet 2025 (Fortinet, 2025)

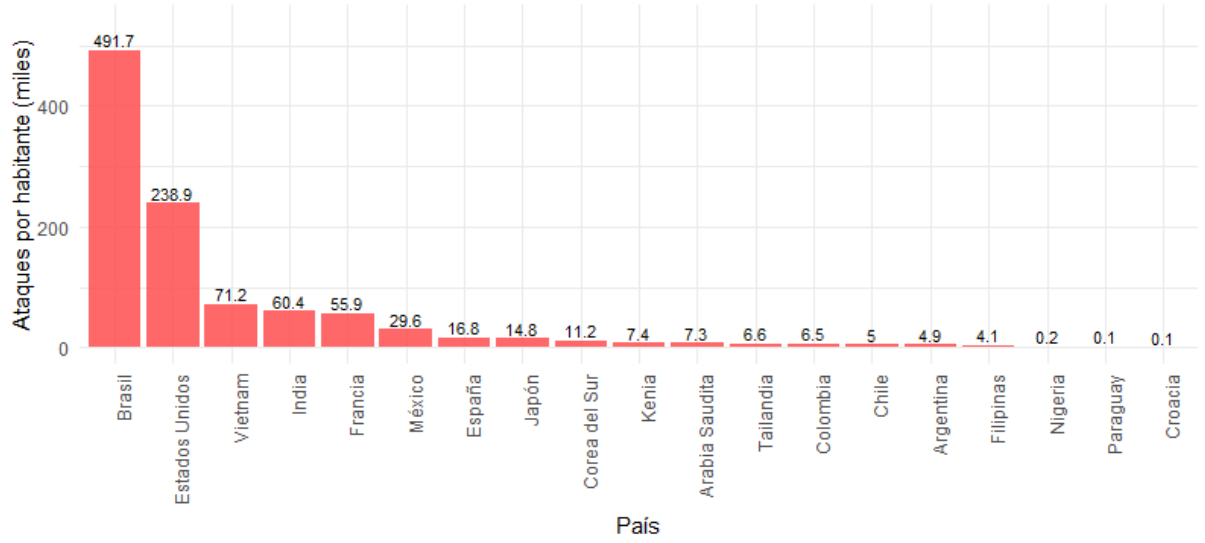
En línea con esta distribución regional, se presenta un análisis de los intentos de explotación detectados por sistemas IPS, expresados en ataques por habitante por mes, a partir de los datos de *FortiGuard Labs* correspondientes al periodo agosto-octubre de 2025. Para este ejercicio, se seleccionó una muestra de países con el propósito de reflejar tanto a las principales economías del mundo (como Estados Unidos, Japón y Alemania) como a economías emergentes de América Latina y Asia (entre ellas Brasil, México, Chile y Vietnam).

Los resultados del indicador mensual de ataques IPS cibernéticos por habitante (miles), presentados en el Gráfico 3.4, muestran una marcada concentración en Brasil (491,7 mil) y Estados Unidos (239,7 mil). Ambos países se consolidan como las principales economías del continente americano, lo que explica en parte su mayor exposición a actividades maliciosas y la intensidad relativa del riesgo cibernético que

enfrentan. En contraste, otros países latinoamericanos como México (29,6, mil), Colombia (6,5 mil), Chile (5 mil) y Argentina (4,9, mil) registran niveles considerablemente menores, reflejando una menor presión de intentos de explotación.

A escala global, naciones asiáticas como Vietnam (71,2 mil) e India (60,4 mil) presentan valores intermedios, mientras que varios países europeos (como Francia, España y Japón) exhiben tasas más bajas, probablemente asociadas con mayores estándares de actualización, segmentación de red y madurez en ciberseguridad.

Gráfico 3.4 Número de IPS promedio por mes por habitante, por país

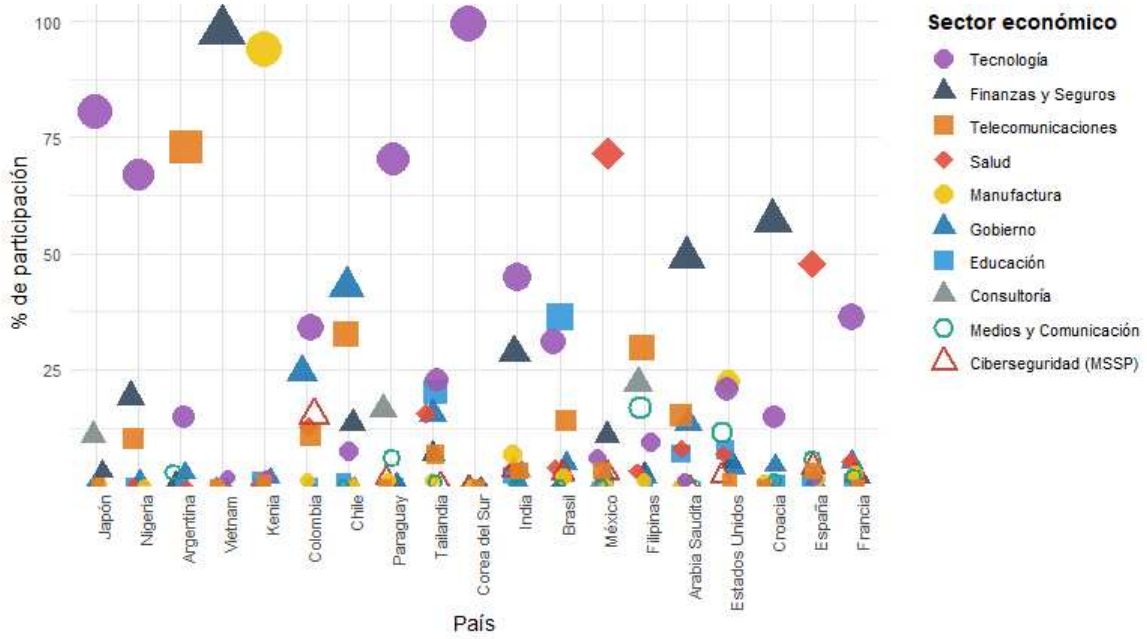


Fuente: Elaboración propia a partir de datos de FortiGuard Labs. https://www.fortiguard.com/threatintel-search

Al observar la distribución sectorial de los intentos de explotación detectados por los sistemas IPS en la muestra de países, se identifican patrones asociados al nivel de desarrollo tecnológico y económico. En países con alto desarrollo tecnología como Japón, Corea del Sur, Francia y Estados Unidos, los ataques se concentran principalmente en el sector tecnológico, reflejando su mayor nivel de digitalización y el valor estratégico de sus activos informáticos. Por otro lado, en economías emergentes o de menor tamaño, como Argentina, Colombia, Nigeria y Filipinas, los intentos de explotación con mayor frecuencia están dirigidos hacia los sectores de telecomunicaciones y gobierno, que suelen ser pilares de la infraestructura nacional y más expuestos a vulnerabilidades de red. Ver Gráfico 3.5.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 3.5 Participación de los ataques detectados por sistemas IPS, según principales sectores y países

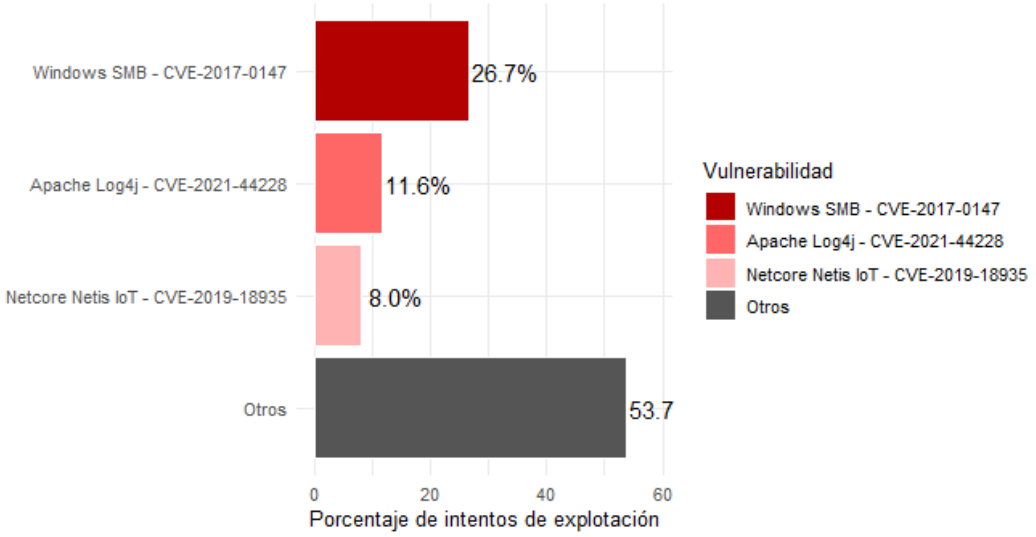


Fuente: Elaboración propia a partir de datos de FortiGuard Labs. https://www.fortiguard.com/threatintel-search

Los vectores de ataque más antiguos y conocidos siguen siendo los más explotados por los atacantes porque muchas organizaciones aún no mantienen una adecuada higiene digital. Los retrasos en la aplicación de parches, las configuraciones incorrectas y la falta de segmentación en las redes crean un entorno perfecto para que las vulnerabilidades, aprovechadas mediante la automatización, continúen siendo efectivas.

Como muestra el Gráfico 3.6, la vulnerabilidad de Windows SMB (CVE-2017-0147) representa el 26,7% de los intentos de explotación. Esta falla afecta al sistema de intercambio de archivos de Windows y puede permitir que un atacante acceda a información interna o se mueva dentro de la red de la empresa. En el caso de Apache Log4j (CVE-2021-44228), que concentra el 11,6% de los intentos, el problema está en una herramienta muy usada en aplicaciones Java: si no está actualizada, un atacante puede hacer que ejecute comandos de manera remota y tomar control del sistema. Por su parte, la vulnerabilidad en dispositivos *Netcore Netis* IoT (CVE-2019-18935), con un 8 %, se relaciona con contraseñas fijas que vienen programadas de fábrica; los atacantes las conocen y pueden entrar fácilmente a *routers* u otros aparatos conectados.

Gráfico 3.6 Principales puntos de entrada de intentos de explotación



Fuente: Elaboración propia a partir de datos del informe global del panorama de amenazas de Fortinet 2025

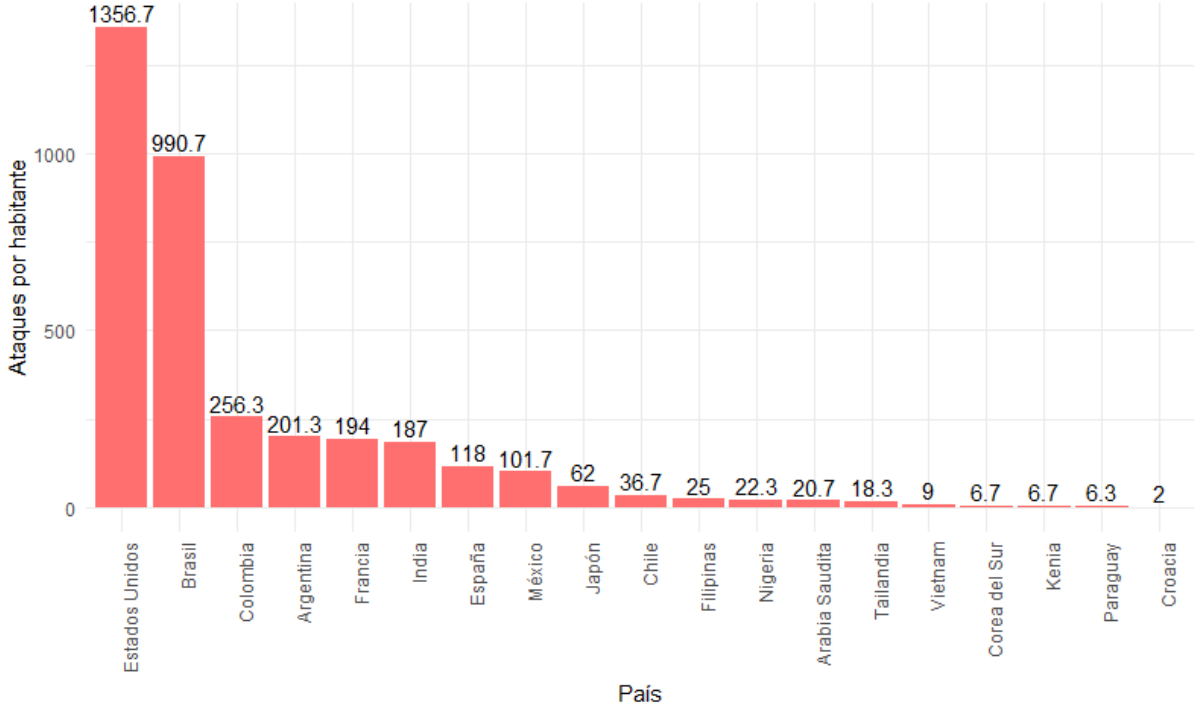
3.1.3. Endpoint. El indicador «detección de vulnerabilidades en *endpoint* por habitante por mes» refleja la cantidad de alertas generadas por las soluciones de seguridad instaladas directamente en los equipos finales, como antivirus, EDR (*Endpoint Detection and Response*) o agentes de monitoreo, que identifican comportamientos sospechosos, intentos de ejecución de *malware* o vulnerabilidades explotables en los dispositivos de los usuarios finales.

De acuerdo con los datos de Fortinet, de manera similar al comportamiento observado en los sistemas de prevención de intrusiones (IPS), Estados Unidos y Brasil presentan el mayor número de alertas en dispositivos finales, con 1.358 y 991 detecciones por mes por habitante, respectivamente. Colombia se ubica a continuación, con un promedio diario de 256 detecciones, lo que evidencia una exposición significativa a amenazas que operan directamente sobre los equipos de los usuarios. Aunque el país no presenta los niveles más altos en las fases iniciales del ataque, como el escaneo o la explotación de red (Ver Gráfico 3.7) sí enfrenta una mayor actividad de *malware* y explotación local en los dispositivos.

Este comportamiento podría estar relacionado no solo con una mayor exposición a campañas masivas orientadas al robo de información o credenciales, sino también con factores estructurales y cultura digital en el país. En particular, la rápida adopción de servicios digitales y financieros, combinada con hábitos de confianza en la interacción en línea y menor atención a las prácticas de ciberseguridad, puede hacer que los usuarios colombianos sean más susceptibles a técnicas de ingeniería social empleadas en campañas de *phishing* o *malware*. En conjunto, estos elementos contribuyen a que Colombia sea un objetivo recurrente para los actores maliciosos que buscan vulnerar los equipos finales de los usuarios.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 3.7 Vulnerabilidades *Endpoint* mes por habitante, según país



Fuente: Elaboración propia a partir de datos de FortiGuard Labs. https://www.fortiguard.com/threatintel-search

3.1.4. Materialización de los ataques

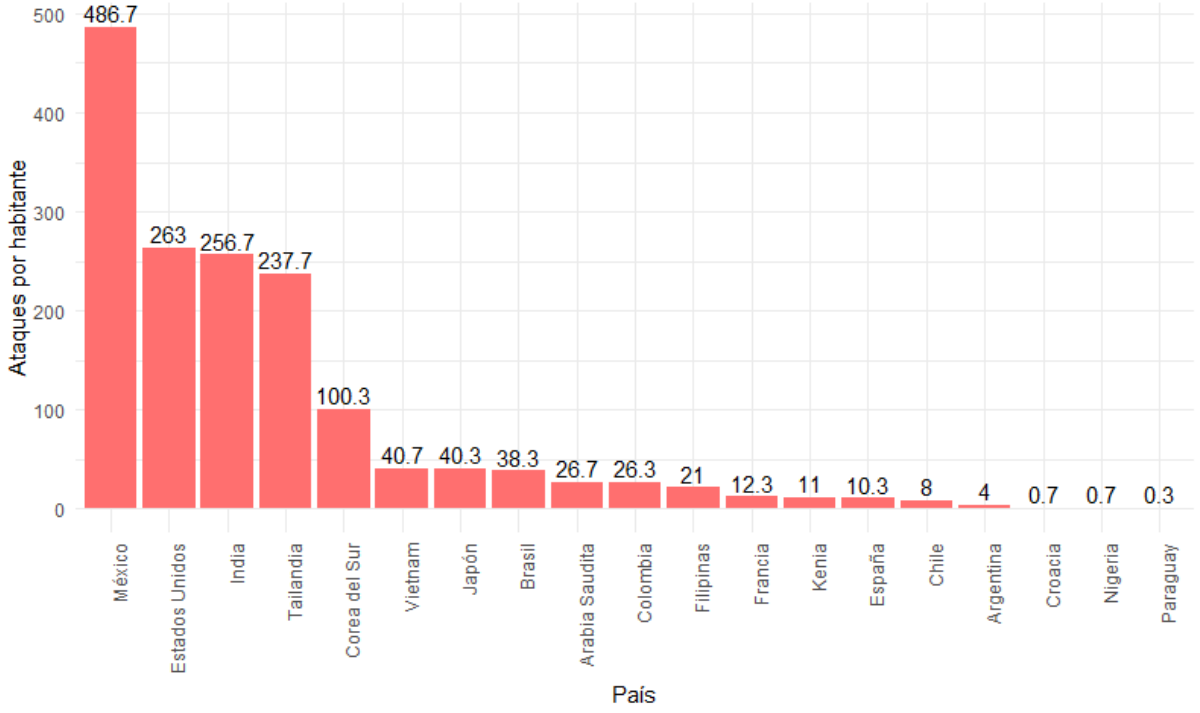
3.1.4.1. Botnet: El indicador de «ataques *botnet* mes por habitante» mide la cantidad de ataques que se materializan en la infección de dispositivos conectados dentro de un país, estandarizados por habitante para facilitar comparaciones internacionales. Las *botnets* son redes de computadores, teléfonos, *routers* o dispositivos IoT previamente comprometidos que ejecutan acciones maliciosas bajo el control de un atacante.

Los resultados muestran que la actividad *botnet* no se distribuye de manera homogénea entre los países y está fuertemente influenciada por la cantidad de dispositivos vulnerables, la exposición de la infraestructura digital y las capacidades de detección disponibles. México presenta el valor más alto del gráfico (487 ataques por habitante), lo que sugiere un nivel de actividad significativamente mayor que en otros países de la muestra. Este patrón puede estar asociado a la combinación de un amplio número y diversidad de dispositivos conectados, incluyendo *routers* domésticos, cámaras IP y equipos IoT de

bajo costo, que a menudo operan con software desactualizado, configuraciones débiles o credenciales por defecto, facilitando la explotación de vulnerabilidades conocidas. Ver Gráfico 3.8.

El resto de los países sigue una distribución escalonada: Estados Unidos (263), India (257) y Tailandia (238) conforman el segundo grupo con niveles altos asociados a ecosistemas digitales amplios y altamente expuestos. Corea del Sur (101), Vietnam (40,7), Japón (40,3) y Brasil (38,3) presentan valores intermedios. Colombia (26,3) se ubica por encima de otras economías latinoamericanas como Chile (8) y Argentina (4), y más digitalizadas como Francia, España y Filipinas.

Gráfico 3.8 Vulnerabilidades Bonet mes por habitante, según país



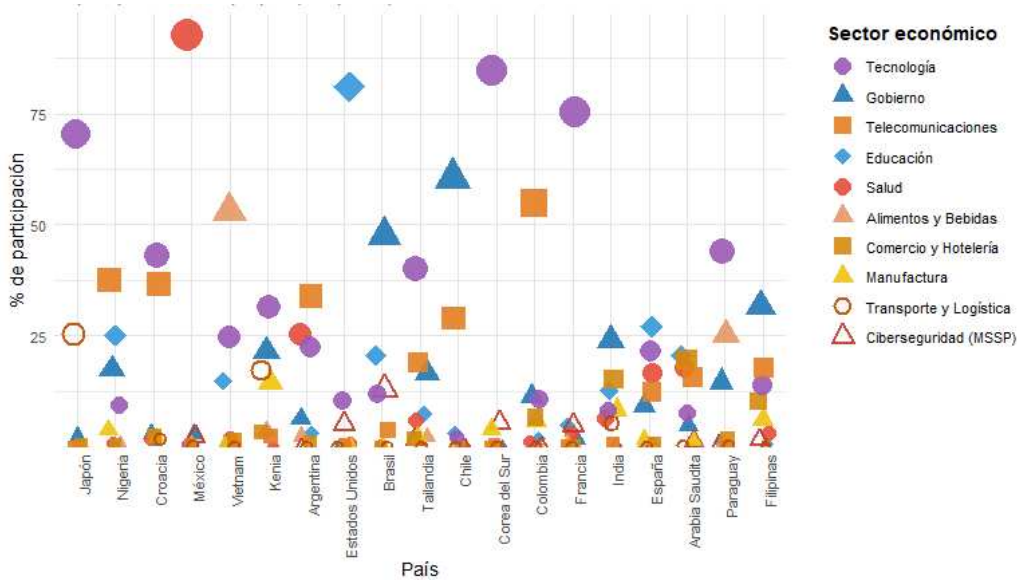
Fuente: Elaboración propia a partir de datos de FortiGuard Labs. https://www.fortiguard.com/threatintel-search

Al analizar la participación de dispositivos por sector económico, se observa que los sectores de Tecnología, Gobierno y Telecomunicaciones concentran la mayor proporción de dispositivos conectados en casi todos los países, destacando especialmente Tecnología en países como Corea del Sur, Estados Unidos y Japón. El sector de Educación presenta niveles intermedios de participación, mientras que Salud, Alimentos y Bebidas, Comercio y Hotelería, Manufactura, Transporte y Logística, y Ciberseguridad (MSSP) muestran una participación más baja y heterogénea entre los países. Este patrón sugiere que la exposición a dispositivos conectados y, en consecuencia, la vulnerabilidad a ataques *botnet* se

concentra principalmente en los sectores tecnológicos y de infraestructura crítica, donde la densidad de equipos conectados y la conectividad son mayores. Ver Gráfico 3.9.

En países como Nigeria, Colombia y Chile, el sector de Telecomunicaciones presenta diversas infraestructuras en rápida expansión, lo que incrementa la superficie de exposición y la probabilidad de observar incidentes asociados a *botnets*. La magnitud del despliegue, la variedad de tecnologías empleadas y la complejidad operativa necesaria para administrarlas se consolidan como factores que explican los mayores niveles de actividad maliciosa detectada en estos mercados. En este escenario, el sector de Telecomunicaciones se convierte en un punto particularmente sensible, donde cualquier vulnerabilidad puede amplificarse y generar efectos transversales en el ecosistema digital nacional.

Gráfico 3.9 Participación de los ataques Bonet, según principales sectores y países



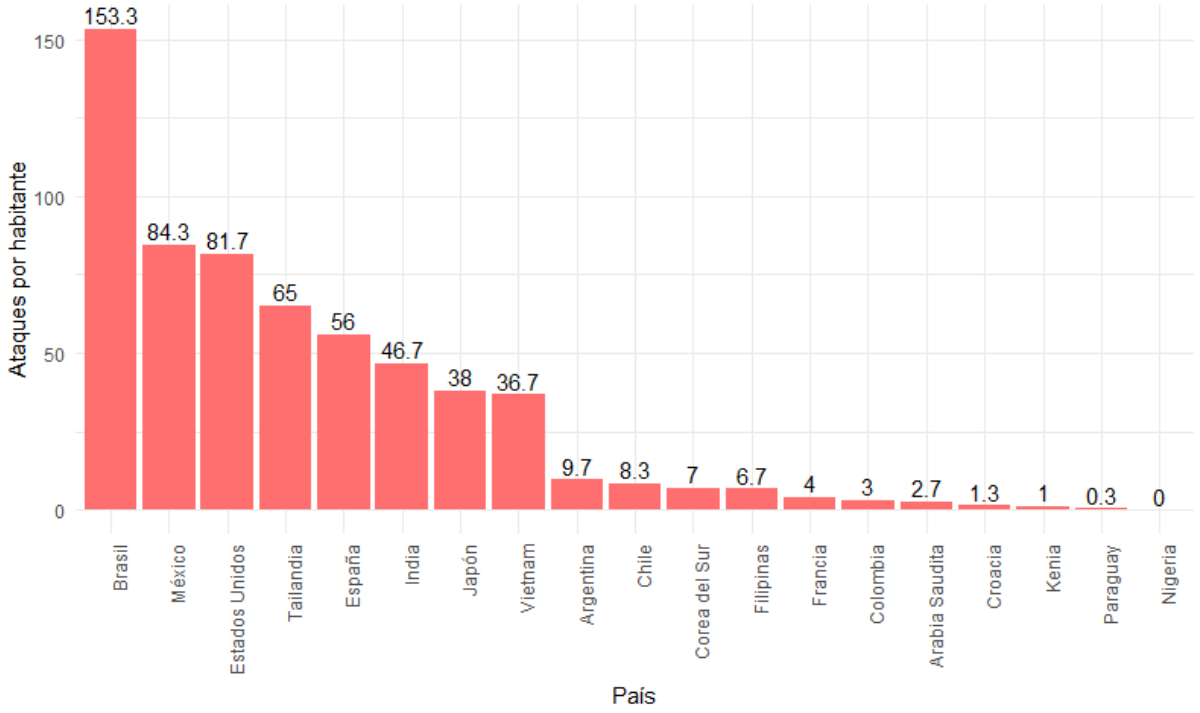
Fuente: Elaboración propia a partir de datos de FortiGuard Labs. https://www.fortiguard.com/threatintel-search

3.1.4.2. Virus: Los intentos de distribución de virus son la materialización de los ataques cibernéticos en los dispositivos finales. Este tipo de actividad se manifiesta cuando los actores maliciosos logran insertar o propagar archivos o códigos maliciosos con el objetivo de comprometer sistemas, robar información o habilitar accesos no autorizados.

De acuerdo con las cifras de Fortinet, los países analizados con mayor desarrollo digital y económico presentan también un mayor número de virus detectados por mes por habitante. Brasil, una de las principales economías de América Latina, es el país con el nivel más alto de detecciones, con alrededor de 153 por habitante al mes, muy por encima del resto de los países analizados. Le siguen México,

también entre las economías más grandes de la región, y Estados Unidos, con cerca de 250 detecciones por mes por habitante. En un nivel intermedio se ubican Tailandia, España, India, Japón y Vietnam, con valores entre 30 y 80 detecciones, mientras que países con economías más pequeñas como Chile, Argentina, Corea del Sur, Filipinas y Egipto registran menos de 10 ataques mes por habitante. Ver Gráfico 3.10.

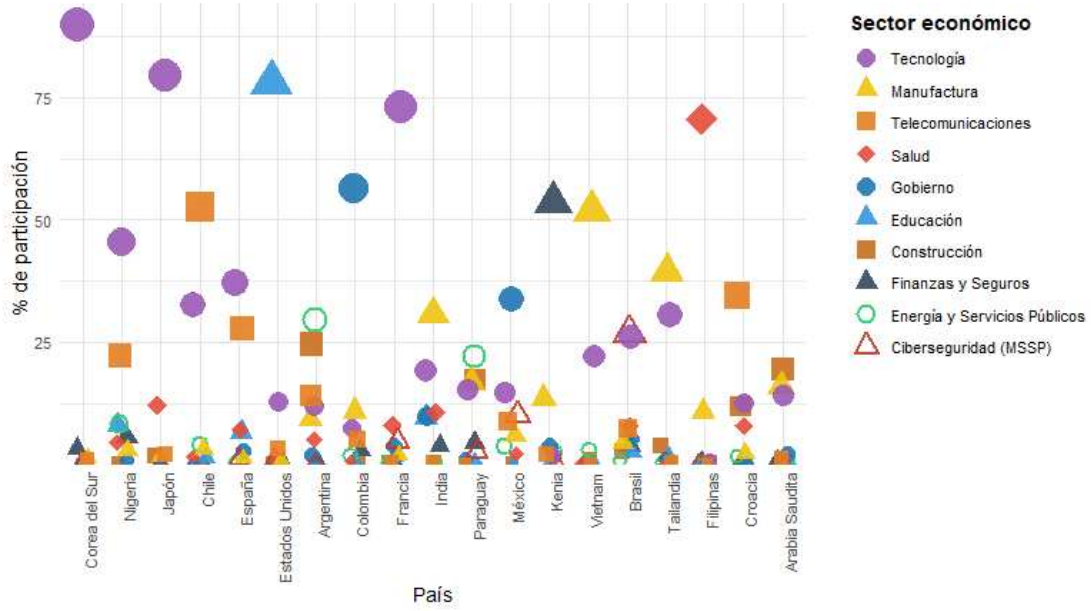
Gráfico 3.10 Intentos de distribución de virus mes por habitante, según país



Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (agosto-octubre de 2025).

Al analizar la distribución de ataques tipo **virus** por sector, se observa una brecha marcada entre países desarrollados y emergentes. En las economías avanzadas, como Estados Unidos, Japón o Corea del Sur, estos ataques se concentran en sectores de **Tecnología** y **Manufactura**, donde los actores maliciosos utilizan *malware* sofisticado para comprometer activos tecnológicos de alto valor y ejecutar campañas estratégicas. En contraste, en países emergentes como México, Colombia o Nigeria, los ataques virales se orientan principalmente a **Telecomunicaciones** y **Gobierno**, generando interrupciones operativas, fraude digital y *ransomware*. Ver Gráfico 3.11.

Gráfico 3.11 Participación de los ataques tipo virus, según principales sectores y países



Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (agosto-octubre de 2025).

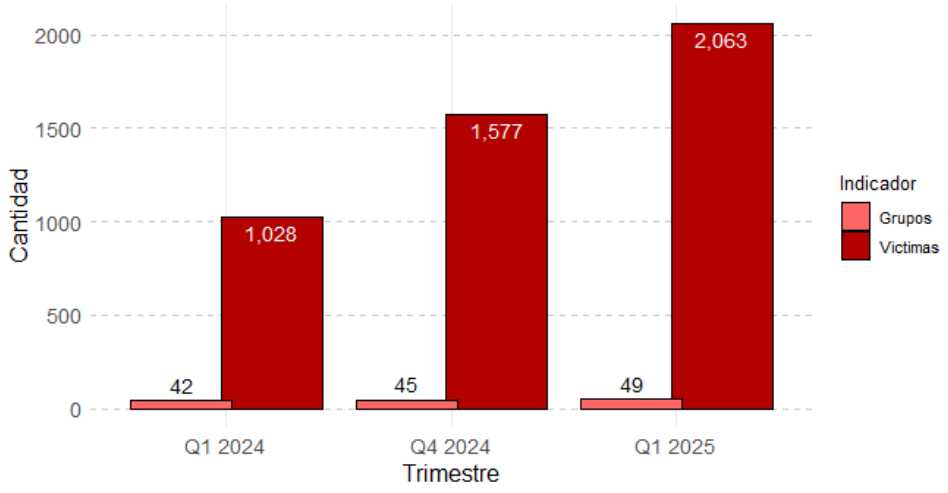
3.1.4.3. Ransomware: De acuerdo con el informe *Ransomware & Cyber Threat Report* de GRIT[62], elaborado a partir de registros públicos de víctimas publicados por los propios atacantes[63], a nivel global se observa un crecimiento histórico en los incidentes de *ransomware* a organizaciones. El primer trimestre de 2025 registró un nivel sin precedentes en dichos ataques, con un total de 2.063 organizaciones víctimas publicadas. Este valor supera ampliamente los 1.577 casos de Q4 2024 y duplica los 1.028 casos de Q1 2024 (Ver Gráfico 3.12).

El promedio diario de víctimas también evidenció un aumentó sostenida, pasando de 11,2 víctimas por día en Q1 2024, a 17,1 en Q4 2024, hasta alcanzar 22,9 en Q1 2025. Este comportamiento evidencia un crecimiento tanto en el volumen como en la frecuencia de los incidentes divulgados por los atacantes.

Este incremento está estrechamente relacionado con la expansión de criminales dedicados a proliferar *ransomware* y que alcanzó un récord trimestral de 70 grupos activos en el Q1 20225, frente a 60 en Q4 2024 y 45 en Q1 2024, lo que representa variaciones del 16,6% y 55,5%, respectivamente.

[62] GuidePoint Security Research and Intelligence Team (GRIT). (2025). GRIT 2025 Q1 Ransomware & Cyber Threat Report. GuidePoint Security. Disponible en: https://www.guidepointsecurity.com/wp-content/uploads/2025/04/GRIT-2025-Q1-Ransomware-Cyber-Threat-Report.pdf
[63] Las "víctimas publicadas" corresponden únicamente a organizaciones cuyos nombres o datos robados son divulgados en los sitios de filtración mantenido por los grupos de ransomware,

Gráfico 3.12 Número de víctimas y grupos criminales de *ransomware* activos, por trimestre



Fuente: Elaboración CRC. Datos tomados del *informe Ransomware & Cyber Threat Report* de GRIT

También en el mismo informe revela que, en el primer trimestre de 2025, Estados Unidos se consolidó como el país más afectado por el *ransomware*, concentrando el 58,8% de las víctimas a nivel global, el porcentaje más alto registrado desde 2022. Junto con Canadá, Alemania, Reino Unido y Francia, lo cual reafirma el predominio de las economías occidentales entre los principales objetivos de los grupos criminales. También destacan economías emergentes como Brasil e India, que continúan registrando un número considerable de víctimas.

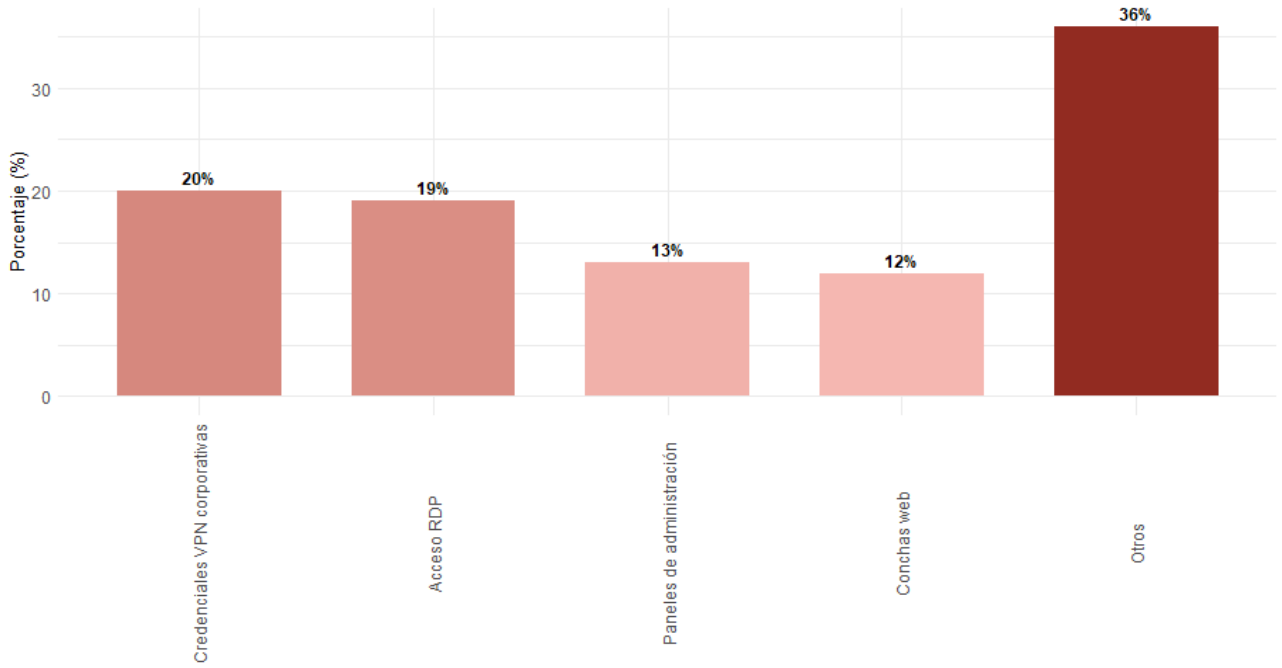
En 2025, el 63% de las víctimas de *ransomware* se negó a pagar un rescate, frente al 59% en 2024. Sin embargo, el coste medio de un incidente de extorsión o *ransomware* sigue siendo elevado, especialmente cuando lo comete un atacante (5,08 millones de dólares). Al mismo tiempo, menos víctimas de *ransomware* informaron haber involucrado a las fuerzas de seguridad: el 40% de las organizaciones este año frente al 53% del año pasado.

3.1.4.4. Robo de credenciales: Paralelamente, el ecosistema del cibercrimen ha evolucionado hacia un ecosistema organizado, donde distintos actores se especializan en etapas concretas de los ataques. Uno de los fenómenos más preocupantes es el auge de los *brokers* de acceso inicial (IAB), intermediarios que se encargan de comprometer sistemas corporativos y luego vender ese acceso en la *dark web*. Este modelo permite que grupos de ransomware, ladrones de datos o espías digitales eviten la fase más compleja de intrusión y se concentren directamente en ejecutar sus ataques.

De acuerdo con las cifras de *FortiGuard Labs*, en 2024 la economía de acceso directo en la *dark web* muestra una marcada preferencia por la comercialización de accesos a infraestructuras previamente comprometidas. (Ver Gráfico 3.13). Las credenciales VPN corporativas (20%) y el acceso mediante RDP

(Remote Desktop Protocol, por sus siglas en inglés) con un 19%, son los activos individuales más comercializados en la *dark web*, debido a que permiten a los atacantes realizar movimiento lateral y obtener acceso directo a redes internas sin necesidad de explotar vulnerabilidades adicionales. Asimismo, los paneles de administración (13%) y las conchas web (12%) también constituyen porciones significativas del mercado.

Gráfico 3.13 Porcentaje de activos comercializados en la dark web



Fuente: Elaboración CRC. Datos tomados del informe global del panorama de amenazas de Fortinet 2025

El informe también resalta que las credenciales se consolidaron como la moneda de cambio del cibercrimen. En 2024 se compartieron más de 100.000 millones de registros comprometidos en la *dark web*, un 42% más que el año anterior. El auge de las listas combinadas, que integran nombres de usuario, contraseñas y correos electrónicos, facilitó ataques automatizados de robo de credenciales, impulsando el fraude financiero y el espionaje corporativo.

Los entornos de nube se han convertido en el nuevo campo de batalla de la ciberseguridad. Su adopción masiva responde a las bondades que ofrece en términos de agilidad, escalabilidad y eficiencia operativa. No obstante, esta misma apertura expone las organizaciones a una superficie de ataque mucho más amplia y dinámica. Los adversarios aprovechan configuraciones incorrectas, identidades comprometidas y APIs inseguras para lanzar ataques cada vez más sofisticados y automatizados.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

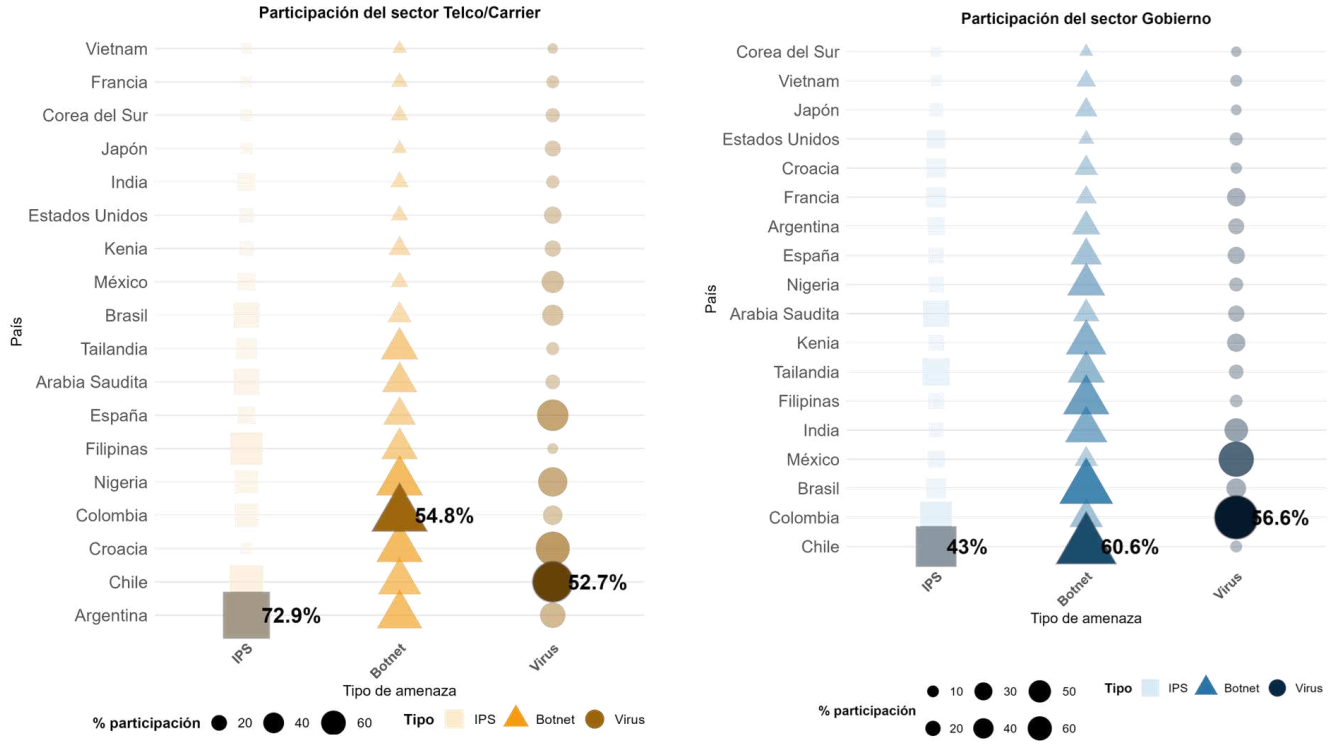
3.2 ANÁLISIS DE SECTORES ESENCIALES

A partir de los datos de Fortinet, se realizó un análisis comparativo de la participación de los sectores esenciales (gobierno, telecomunicaciones, energía y educación) en los distintos tipos de ciberataques detectados en la muestra de países analizadas. El objetivo es identificar qué proporción representan estos sectores dentro del total de vulnerabilidades reportadas y evaluar su exposición frente a amenazas que pueden comprometer infraestructuras críticas nacionales. En particular, se analizó la actividad asociada a tres tipos de detecciones: IPS, que reflejan intentos de explotación de vulnerabilidades; *Botnet*, que evidencian dispositivos comprometidos o redes controladas de forma remota; y Virus, que representan infecciones activas en equipos, redes o servicios institucionales.

De forma general, los países con mayor volumen en IPS y *Botnet son* los que muestran mayor exposición a ataques avanzados o dirigidos, especialmente en sectores esenciales como gobierno, telecomunicaciones, energía y educación. En el conjunto de la muestra, se destaca que los países latinoamericanos, Chile, Colombia y Brasil, junto con Nigeria, presentan una participación significativa en estos tipos de amenaza, lo cual amplía la superficie de ataque e incrementa la probabilidad de compromiso de infraestructuras críticas y de explotación efectiva de vulnerabilidades. La materialización de este tipo de riesgos puede ocasionar interrupciones operativas prolongadas, impacto en la disponibilidad de servicios esenciales y exposición de información sensible, afectando la resiliencia del ecosistema digital.

En el caso de Chile, se observa una actividad muy alta en las tres categorías (IPS, *Botnet* y Virus), lo que refleja una amplia superficie de ataque digital y una posible exposición a vulnerabilidades explotables en plataformas públicas y sistemas interconectados. En Colombia, la mayor participación se observa en *Botnet* dentro del sector de telecomunicaciones y en Virus en el sector gobierno, lo que revela posibles brechas de actualización y segmentación en redes institucionales. Brasil presenta altos niveles en IPS y *Botnet*, lo que denota una infraestructura digital compleja y altamente expuesta, susceptible a ataques avanzados tanto en telecomunicaciones como en sectores industriales y financieros. Ver Gráfico 3.14

Gráfico 3.14 Participación de los sectores esenciales de Telecomunicaciones y gobierno en las vulnerabilidades detectadas por país.



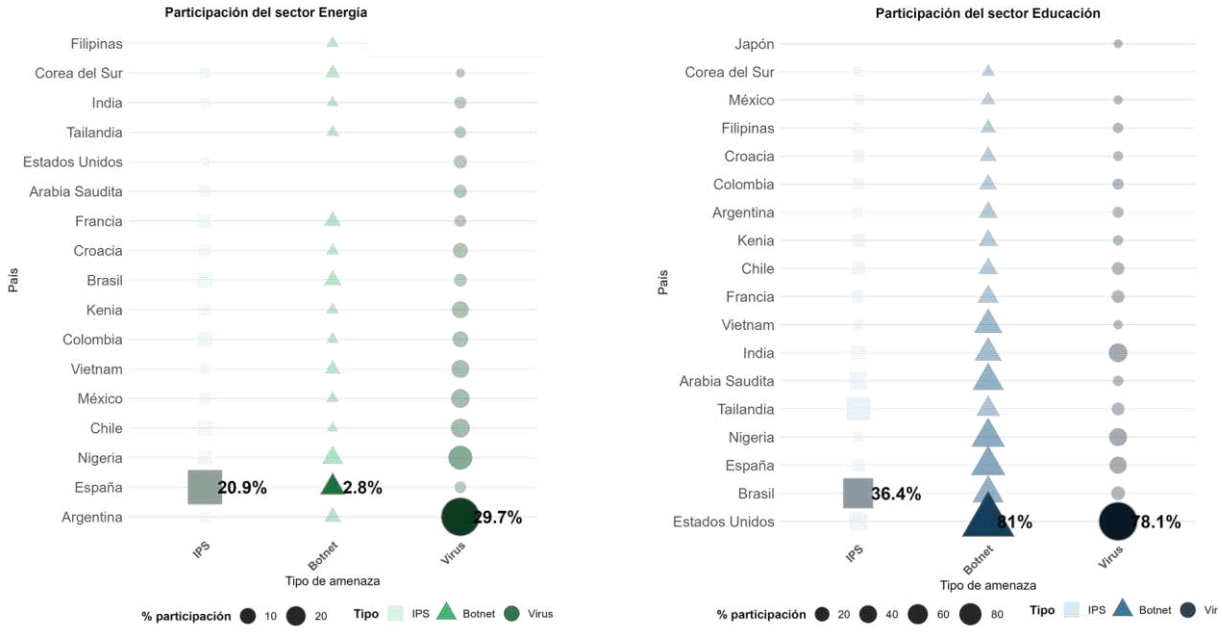
Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (agosto-octubre de 2025).

Por otra parte, España se destaca por una alta concentración de vulnerabilidades IPS en el sector energético, lo que sugiere que su red de energía está siendo objeto de intentos frecuentes de intrusión y monitoreo constante por parte de sistemas de defensa.

En el sector educativo, Estados Unidos, España y Brasil destacan por su alta exposición a amenazas cibernéticas, coherente con su amplio número de instituciones conectadas, redes de investigación y bases de datos académicas extensas. La concentración de amenazas en estos países se relaciona con la masificación de plataformas digitales y el alto intercambio de información académica, factores que incrementan los riesgos de infecciones tipo Virus, redes *Botnet* y otras amenazas cibernéticas. Ver Gráfico 3.15.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 3.15 Participación de los sectores esenciales de energía y educación en las vulnerabilidades detectadas por país.



Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (agosto-octubre de 2025).

3.3 CONTEXTO COLOMBIANO

Colombia, como una de las economías digitales de mayor crecimiento en América Latina, enfrenta un panorama de ciberseguridad cada vez más complejo. La expansión del uso de internet y el uso de un mayor número de dispositivos ha incrementado los puntos de vulnerabilidad y, con ello, la superficie de ataque disponible para los ciberdelincuentes.

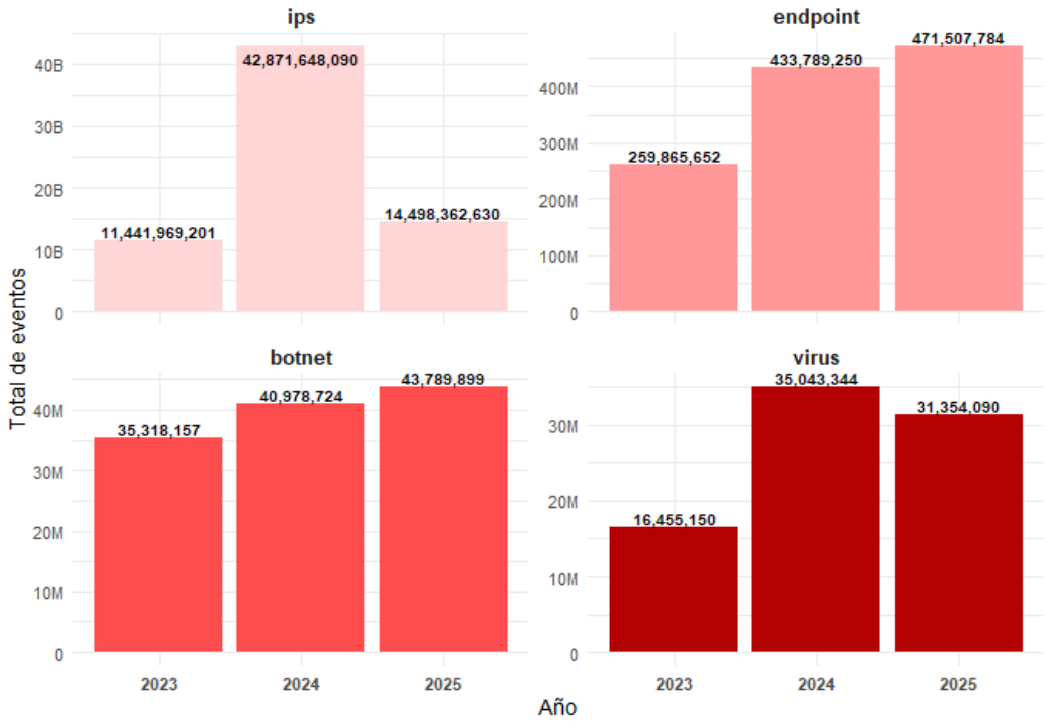
Al analizar los datos del periodo 2023–2025 (Ver Gráfico 3.16), se observa que los ataques dirigidos a *endpoints* concentran la mayor actividad maliciosa y representan la principal puerta de entrada para los actores de amenaza. En 2025, *FortiGuard Labs* registró 471,5 millones de eventos asociados a *endpoints*, lo que equivale a un promedio cercano a 1,3 millones de intentos por día.

Los ataques basados en *botnets* también muestran una tendencia creciente, pasando de 35,3 millones en 2023 a 43,8 millones en 2025, lo que representa alrededor de 120 mil intentos diarios en el último

año. Por su parte, los ataques tipo virus mantienen niveles relevantes: en 2025 se detectaron 31,3 millones de eventos, equivalentes a aproximadamente 85 mil intentos al día.

Finalmente, los sistemas de prevención de intrusiones (IPS) registraron un comportamiento fluctuante, alcanzando un pico de 42,8 mil millones de eventos en 2024, seguido de una reducción a 14,5 mil millones en 2025.

Gráfico 3.16 Ataques en Colombia, según tipo de ataque



Fuente: Elaboración propia con base en datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (enero-octubre de 2025).

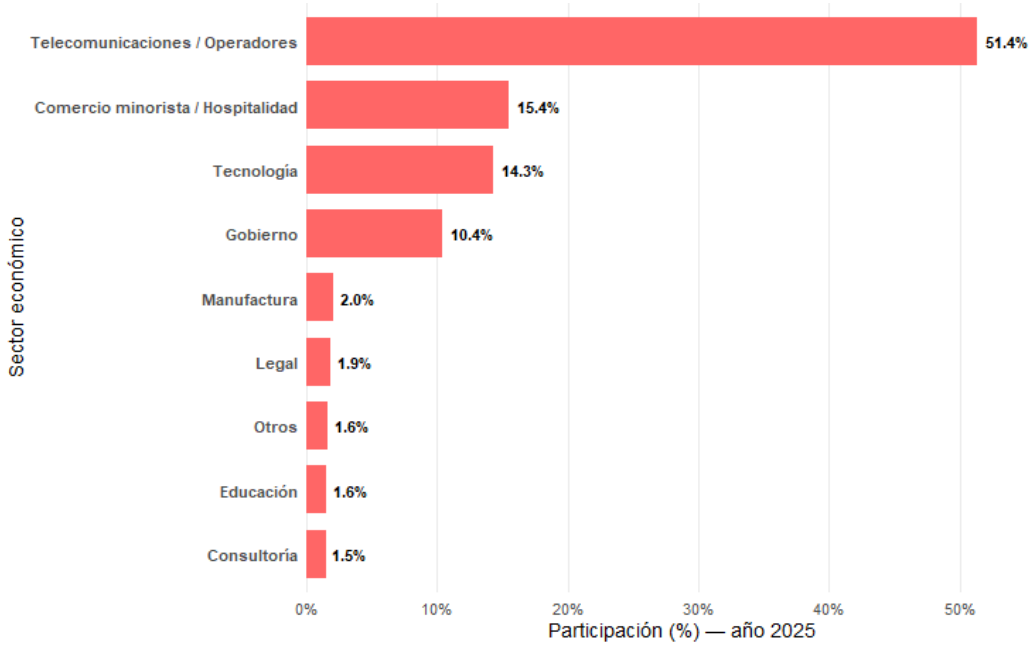
El Gobierno y el sector de Telecomunicaciones aparecen de manera recurrente entre los más afectados por ciberataques, lo que evidencia su relevancia estratégica y crítica para el país. Los intentos maliciosos no se concentran en un único frente, sino que afectan de forma transversal a múltiples sectores de la economía, empleando distintos vectores como virus, intrusiones IPS o ataques *botnets*.

Como se puede observar en el Gráfico 3.17, los ataques asociados a *botnets* se concentran en Telecomunicaciones/Operadores, que representan más del 51% del total. Le siguen a distancia

Comercio minorista y Hospitalidad[64] (15,4%) y el sector Tecnológico (14,3%), mientras que Gobierno ocupa el cuarto lugar con 10,4%. Los demás sectores, Manufactura, Legal, Educación, Otros y Consultoría, registran participaciones inferiores al 2%, reflejando una distribución altamente concentrada en el sector Telecomunicaciones.

La fuerte exposición de dicho sector responde a que los operadores administran millones de dispositivos de usuario final, como *routers*, decodificadores, módems, cámaras IP y equipos IoT, que suelen convertirse en objetivos prioritarios para la formación de redes de *bots*. Esto es consistente con alertas recientes de COLCERT que han documentado campañas de propagación de variantes tipo *Mirai*[65], utilizadas para comprometer grandes volúmenes de dispositivos conectados y posteriormente ejecutar ataques DDoS de alto impacto.

Gráfico 3.17 Participación de vulnerabilidades Botnet por sector económico en Colombia



Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (enero-octubre de 2025).

En el caso de los ataques tipo virus (Ver Gráfico 3.18), la distribución sectorial en 2025 evidencia un patrón de concentración muy marcado: el sector de Telecomunicaciones tiene el 84,7% de los incidentes detectados, seguido por Gobierno (7,2%), Manufactura (4,1%), Otros (2,8%) y Tecnología (1,2%). Esta prevalencia se explica por la amplia superficie de exposición del ecosistema de telecomunicaciones,

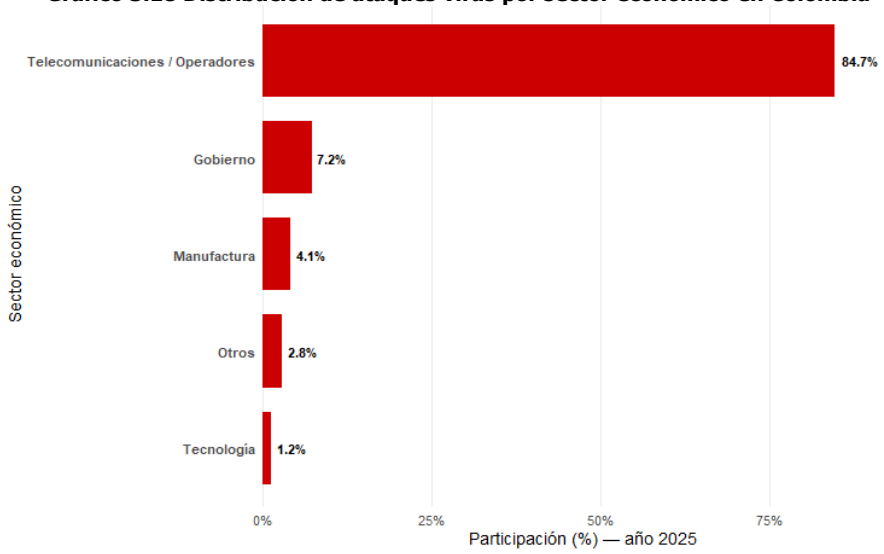
[64] Hoteles, bares y restaurantes que ofrecen a las personas comida, bebida o un lugar para dormir.
[65] Ataques a dispositivos domésticos conectados como cámaras, sistemas de alarma y routers personales.

donde intervienen tanto los dispositivos del usuario final (*routers*, CPE, ONT/ONU, *gateways* residenciales y equipos IoT) como los equipos propios de la infraestructura del operador, incluyendo nodos de acceso, equipos ópticos, switches de agregación y plataformas de administración remota. La masividad, heterogeneidad tecnológica y ciclos de actualización desalineados facilitan la propagación de *malware* y su aprovechamiento como infraestructura para campañas de mayor escala.

En Colombia, *FortiGuard Labs* ha reportado la presencia recurrente en el sector Telecomunicaciones de variantes como *MSI/Formbook.DXN!tr*, *W32/AI.PALLAS.SUSPICIOUS* y *Riskware/PassView*, utilizadas para capturar credenciales, ejecutar módulos adicionales y comprometer tanto equipos de borde como sistemas de gestión expuestos. Estas detecciones muestran que los operadores no solo enfrentan riesgos por la cantidad de dispositivos existentes en campo, sino también por la criticidad y complejidad de su infraestructura de red.

Este comportamiento confirma que el sector telecomunicaciones es uno punto de ataque para la distribución y amplificación de infecciones basadas en *malware* en Colombia, impulsado por la combinación de volumen, diversidad tecnológica y alta conectividad entre sus componentes.

Gráfico 3.18 Distribución de ataques virus por sector económico en Colombia

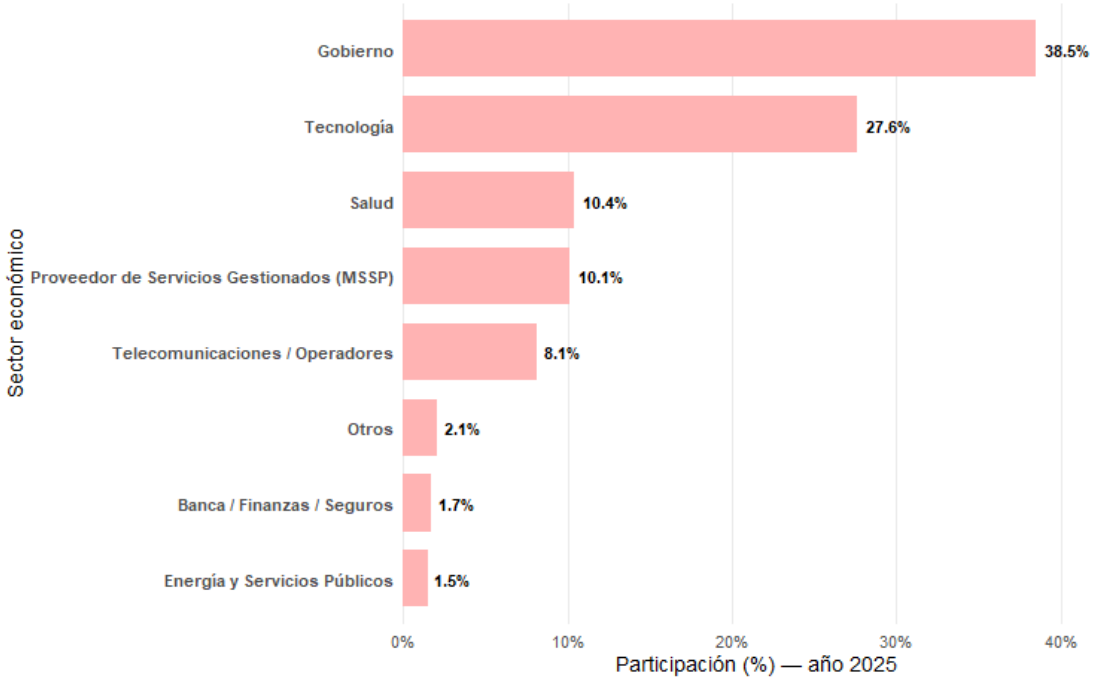


Fuente: Elaboración propia con base en datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (enero-octubre de 2025).

Finalmente, los ataques identificados por los sistemas de Prevención de Intrusiones (IPS) se concentran de manera significativa en los sectores de Gobierno, Tecnología y Salud, que en conjunto representan cerca del 75% del total registrado. (Ver Gráfico 3.19) El sector Gobierno lidera con un 38,5%, seguido

por Tecnología (27,6%) y Salud (10,4%), mientras que los Proveedores de Servicios Gestionados (MSSP) aportan un 10,1%, y el sector de Telecomunicaciones/Operadores registra un 8,1% del total. Esta tendencia refleja que los ciberdelincuentes buscan explotar vulnerabilidades en servicios críticos de conectividad y plataformas tecnológicas ya sea para interrumpir la operación mediante ataques de denegación de servicio (DDoS) o para obtener acceso no autorizado que facilite el robo de datos y el control de infraestructuras.

Gráfico 3.19 Distribución de IPS por sector económico



Fuente: Elaboración propia a partir de datos de Fortinet. Corresponde al total de vulnerabilidades detectadas por Fortinet durante el periodo de análisis (Enero-octubre de 2025).

Este panorama muestra que la amenaza no es homogénea, sino que se adapta a la naturaleza de cada sector y a la superficie de ataque que ofrece. En particular, los sectores con alta conectividad y grandes volúmenes de usuarios, como Telecomunicaciones, Salud y Tecnología, resultan especialmente atractivos para los atacantes, ya que comprometer su infraestructura puede tener un efecto multiplicador: interrumpir servicios críticos, acceder a datos masivos o utilizarlos como plataformas para escalar ataques hacia otros objetivos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4. VECTORES DE ATAQUE

En la última década, el ecosistema digital ha experimentado una transformación profunda impulsada por la convergencia de redes físicas y virtuales, el crecimiento exponencial de dispositivos conectados y la incorporación de tecnologías como el 5G, la computación en la nube, el Internet de las Cosas (IoT), las arquitecturas abiertas y la IA. Estos avances han traído consigo nuevos beneficios para los usuarios, pero también han ampliado de manera significativa la superficie de ataque, es decir, el conjunto de puntos potenciales que un actor malicioso puede aprovechar para comprometer la seguridad de los sistemas.

En este contexto, los vectores de ataque (mecanismos, rutas o métodos utilizados para explotar vulnerabilidades) se han diversificado y sofisticado, afectando no solo a las infraestructuras tradicionales de telecomunicaciones, sino también a nuevas capas lógicas y virtualizadas de la red. De acuerdo con el informe de ENISA sobre el panorama de amenazas 2023, los ataques más relevantes para el sector de telecomunicaciones incluyen el *ransomware*, los ataques a la cadena de suministro, la explotación de configuraciones inseguras en entornos de nube y las amenazas internas[66].

Esta sección ofrece una mirada estructurada a los principales vectores de ataque que amenazan la seguridad del ecosistema digital, así como a las tendencias emergentes que podrían afectar la estabilidad y confiabilidad de las redes de telecomunicaciones.

[66] ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4.1 PRINCIPALES VECTORES DE ATAQUE IDENTIFICADOS

El creciente dinamismo del ecosistema digital ha traído consigo una diversificación de los vectores de ataque que afectan a los distintos componentes de las redes de telecomunicaciones. Estos vectores representan las rutas, técnicas o mecanismos que utilizan los atacantes para vulnerar la seguridad de los sistemas, explotar brechas o interferir con la prestación de servicios críticos.

A continuación, se presentan los principales vectores de ataque identificados en el sector, agrupados según su ámbito de acción:

4.1.1. Vectores basados en infraestructura física y lógica de red. Los elementos tradicionales de red, como *routers, switches, gateways* y estaciones base, continúan siendo blanco de ataques de denegación de servicio (DoS/DDoS), manipulación de configuraciones y explotación de vulnerabilidades conocidas. Los ataques DDoS aumentaron en volumen y sofisticación durante 2024, afectando especialmente servicios de DNS, redes móviles y enlaces internacionales[67].

En este punto es importante mencionar que el modelo de negocio del cibercrimen se ha industrializado y adoptado esquemas similares a los del software comercial, dando lugar al fenómeno conocido como *Cybercrime-as-a-Service* (CaaS). Este modelo incluye variantes como el *Ransomware-as-a-Service* (RaaS), el *Phishing-as-a-Service* (PhaaS) y el *Access Broker-as-a-Service* que permiten que actores sin conocimientos técnicos avanzados puedan lanzar ataques sofisticados mediante la compra de servicios ilícitos en el mercado negro digital. Esto ha generado un aumento en la frecuencia y gravedad de los ataques dirigidos a infraestructuras de red, incluyendo operadores de telecomunicaciones.

Ejemplo: Ataques volumétricos DDoS dirigidos a operadores móviles, afectando el acceso a servicios OTT o portales gubernamentales[68].

4.1.2. Vectores asociados a virtualización y entornos en la nube. La virtualización de funciones de red (NFV) y la adopción de plataformas en la nube exponen nuevas superficies lógicas de ataque, especialmente a través de APIs mal configuradas, entornos *multitenant* sin aislamiento suficiente y acceso no controlado a contenedores o máquinas virtuales[69].

En este contexto, los ataques en la nube se han consolidado como la nueva frontera del riesgo cibernético. La escala global de actividad maliciosa evidencia la magnitud del desafío: las herramientas de inteligencia sobre amenazas de AWS identifican y detienen más de 7 mil millones de intentos diarios de escaneo externo no autorizado sobre sus servicios y detectan alrededor de 124.000 dominios

[67] INCIBE-CERT. (2025). DDoS attacks: techniques and mitigation in business infrastructures. Disponible en: https://www.incibe.es/en/incibe-cert/blog/ataques-ddos-tecnicas-y-mitigacion-en-infraestructuras-empresariales
[68] StormWall. (s.f.). 2024 in Review: DDoS Attacks Report by StormWall. Disponible en: https://stormwall.network/resources/blog/ddos-attack-statistics-2024
[69] Qiu, Q., Xu, S., Liu, S., Xu, T., & Zhao, B. (2024). Network virtualization security: Threats, measures, and use cases. 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K). Disponible en: https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/P.2Network_Virtualiazation_Security_Threats_Measures_and_Us.pdf

maliciosos cada día[70], mientras que servicios como DNSFilter identifican cerca de 200 millones de peticiones DNS maliciosas cada jornada. Estas cifras demuestran que el *phishing*, el *malware*, la explotación de vulnerabilidades y la manipulación de infraestructura DNS ya no son incidentes aislados, sino elementos permanentes de un ecosistema automatizado y en expansión[71].

De otra parte, análisis como los del reporte global de amenazas de *CrowdStrike* de 2025, que utilizan la taxonomía MITRE ATT&CK[72], revelan que el 35% de todos los incidentes en la nube involucraron el abuso de cuentas válidas (identidades legítimas comprometidas), el 79% de las intrusiones detectadas fueron libres de *malware* (*malware-free*), lo que significa que los atacantes usaron credenciales legítimas y herramientas nativas de la nube en lugar de virus tradicionales[73]

Un ejemplo de este escenario es la exposición de datos sensibles por fallos de autenticación en entornos de nube híbrida, o por errores de configuración en contenedores.

4.1.3. Vectores en redes abiertas y desagregadas. El despliegue de arquitecturas abiertas, promovidas para fomentar la interoperabilidad y reducir dependencia de proveedores únicos, introduce nuevos desafíos en materia de ciberseguridad sino se acompaña de controles robustos. La apertura de interfaces como A1, E2, O1 u O-RU aumenta el número de puntos de entrada para atacantes si no se implementan adecuadamente mecanismos de autenticación, cifrado y monitoreo[74].

En este sentido, informes de organismos como 5G Americas señalan que interfaces abiertas como A1, E2, O1, O2 y el *fronthaul* abierto amplían el número de puntos en los que un atacante puede interactuar con la RAN, lo que obliga a reforzar autenticación, cifrado y segregación de dominio de confianza[75].

Así mismo, artículos de seguridad han demostrado que una xApp con privilegios suficientes puede manipular suscripciones E2, generar tráfico anómalo o explotar fallos de implementación para provocar caídas de componentes del RIC o denegación de servicio en elementos E2, afectando directamente las decisiones de control de la red[76]

---

[70] Amazon Web Services. (s.f.). Global network. Amazon Web Services. Disponible en: https://aws.amazon.com/es/about-aws/global-infrastructure/global-network/

[71] DNSFilter. (2025). 2025 Annual Security Report. DNSFilter. Disponible en: https://www.dnsfilter.com/hubfs/Resources/2025-annual-security-report.pdf

[72] Base de conocimiento global, basada en observaciones reales, que clasifica las tácticas, técnicas y procedimientos usados por los atacantes en el ciclo completo de una intrusión cibernética. Organiza esta información en matrices (por ejemplo, Enterprise, Cloud, Mobile) que permiten a organizaciones de defensa mapear amenazas, evaluar riesgos, priorizar controles, fortalecer detecciones y mejorar la respuesta ante incidentes

[73] CrowdStrike. (2025). 2025 Global Threat Report. CrowdStrike, Inc. Disponible en: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

[74] Bundesamt für Sicherheit in der Informationstechnik. (2022). Open RAN risk analysis. Disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=5

[75] 5G Americas. (2023). Open RAN update. 5G Americas. Disponible en: https://www.5gamericas.org/wp-content/uploads/2023/11/Open-RAN-Update-Id.pdf

[76] Trend Micro. (2024). Open RAN: Attack of the xApps. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/open-ran-attack-of-the-xapps

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4.1.4. Vectores en dispositivos finales y terminales (usuarios y IoT). Los terminales (smartphones, módems, cámaras, sensores, *wearables*, etc.) son objetivos constantes de *malware*, troyanos, *ransomware*, y técnicas de *phishing* o *smishing*. En el caso del Internet de las Cosas (IoT), muchos dispositivos carecen de actualizaciones de seguridad, cifrado de datos o autenticación robusta[77].

La expansión de dispositivos IoT mal asegurados y la incorporación de nodos de *edge computing* sin control de seguridad estandarizado están creando nuevos puntos de entrada para atacantes. El bajo poder de cómputo y la fragmentación de estándares dificultan la aplicación de parches o el monitoreo de amenazas[78].

En este escenario, los dispositivos IoT destacan como uno de los blancos prioritarios para los actores maliciosos. A diferencia de los activos tradicionales de TI, muchos de estos equipos no cuentan con monitoreo continuo ni políticas de endurecimiento de seguridad. La ausencia de parches, la persistencia de contraseñas predeterminadas y las configuraciones abiertas permiten que los atacantes los utilicen como puntos de entrada inicial o como nodos silenciosos para espionaje, exfiltración de datos y conformación de *botnets* a gran escala.

Los datos más recientes respaldan esta tendencia. Según *FortiGuard Labs*, para 2024 los enrutadores y las cámaras de vigilancia lideran la lista de dispositivos IoT más atacados, debido a su exposición directa a internet y la alta frecuencia de configuraciones débiles o *firmware* desactualizado. Los atacantes suelen automatizar la explotación de nuevas vulnerabilidades apenas son divulgadas, incorporando estos equipos a *botnets* o utilizándolos como pivotes para infiltrarse en redes internas y robar información sensible.

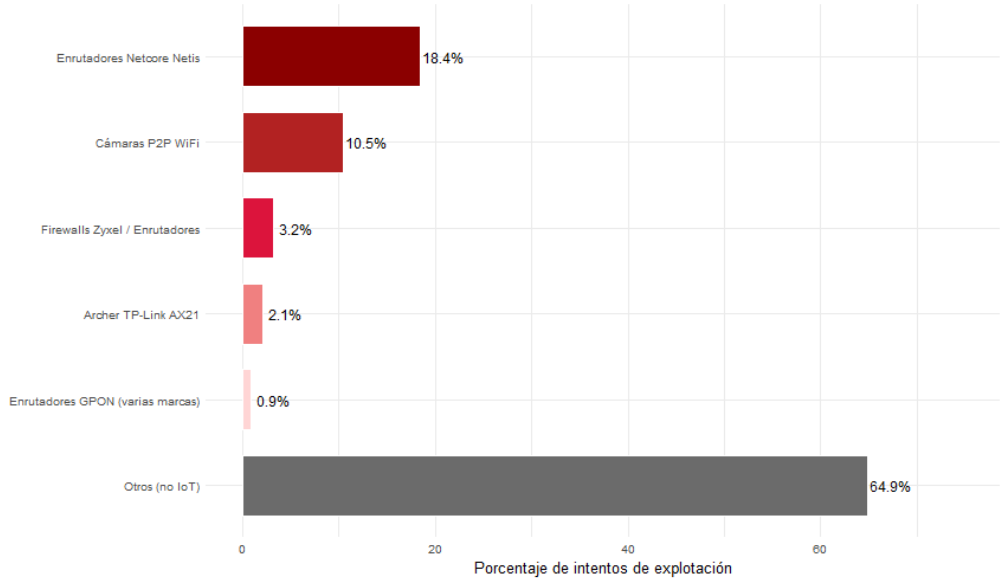
Como se observa en el Gráfico 4.1, los enrutadores *Netcore Netis* (18,4%) lideran los intentos de explotación debido a una vulnerabilidad crítica (CVE-2019-18935) que permite el control remoto del dispositivo, facilitando su reclutamiento en redes de ataque distribuidas. En segundo lugar, las cámaras P2P WiFi (10,5%) son altamente vulnerables por la CVE-2017-18377, que abre la puerta al espionaje y la exfiltración de información sensible.

En un nivel menor, los firewalls y enrutadores *Zyxel* (3,2%) presentan fallas que permiten manipular configuraciones internas de seguridad, mientras que los enrutadores *TP-Link Archer AX21* (2,1 %) son explotados mediante la CVE-2023-1389, que habilita el secuestro de tráfico y el robo de credenciales. Finalmente, los enrutadores GPON (0,9%), afectados por la CVE-2018-10561, ofrecen accesos persistentes que los atacantes aprovechan para lanzar ataques DDoS y reforzar sus *botnets*.

[77] Instituto Federal de Telecomunicaciones (IFT). (2020). Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las Cosas (IoT). Disponible en: https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf
[78] Siraparapu, S. R., & Azad, S. M. A. K. (2024). Securing the IoT landscape: A comprehensive review of secure systems in the digital era. e-Prime - Advances in Electrical Engineering, Electronics and Energy, 10, 100798. Disponible en: https://doi.org/10.1016/j.prime.2024.100798

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 4.1 Dispositivos IOT más atacados.



Fuente: Elaboración propia a partir de datos del informe global del panorama de amenazas de Fortinet 2025[79].

Un ejemplo del escenario que se ha presentado en este ámbito son los *botnets* basadas en dispositivos IoT comprometidos (como Mirai), utilizadas para lanzar ataques masivos a infraestructuras de telecomunicaciones[80].

4.1.5. Vectores en la cadena de suministro. Los atacantes han incrementado el uso de ataques indirectos a través de terceros proveedores, desarrolladores o fabricantes de componentes. Esta amenaza es crítica en el sector de telecomunicaciones, donde los equipos y software provienen de múltiples actores y geografías[81]. En este contexto, un compromiso en cualquier eslabón puede tener efectos amplificados sobre toda la operación. Ejemplo de ello son los ataques tipo *SolarWinds*, donde la inserción de código malicioso en una actualización legítima permitió comprometer a cientos de organizaciones sin necesidad de atacar directamente a cada una.

La cadena de suministro se ha consolidado como uno de los puntos de exposición más sensibles para las organizaciones. El *Global Cybersecurity Outlook* 2025[82] evidencia esta preocupación: el 54% de las

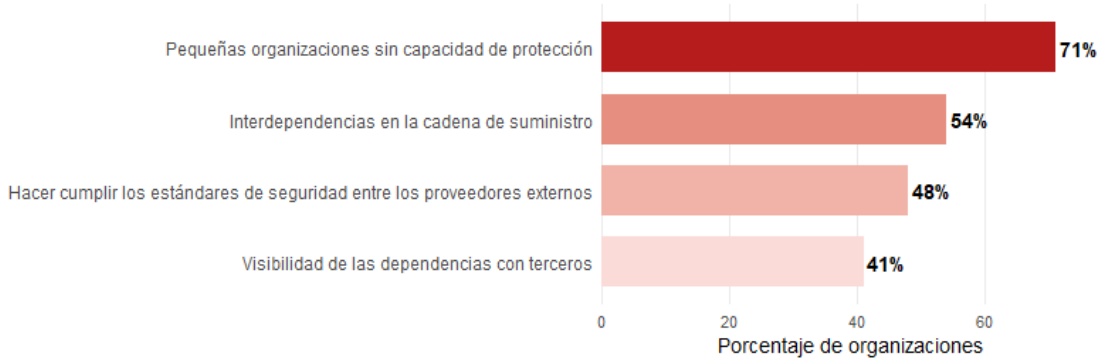
[79] Fortinet. (2025). Informe global del panorama de amenazas de 2025. Disponible en: https://www.fortinet.com/lat/resources/reports/threat-landscape-report https://www.fortinet.com/lat/resources/reports/threat-landscape-report
[80] Palo Alto Networks. (s.f.). IoT Under Siege: The Mirai Campaign. Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet
[81] Cybersecurity and Infrastructure Security Agency (CISA). (2021). Defending against software supply chain attacks. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[82] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Disponible en:

grandes empresas considera que las interdependencias con terceros constituyen la principal barrera para una gestión segura del riesgo digital. A esto se suma que el 48% de los directores de seguridad de la información (CISOs) identifica como su mayor reto garantizar que los proveedores cumplan con los estándares de seguridad exigidos por la regulación y las mejores prácticas del sector.

A su vez, el 41% de los líderes en ciberseguridad considera que mejorar la visibilidad de las dependencias de terceros debe ser la principal prioridad para fortalecer la resiliencia de la cadena. (Ver Gráfico 4.2). Esta falta de control sobre los proveedores, sumada a la alta concentración de servicios en pocos actores estratégicos, incrementa el riesgo sistémico: un solo incidente, como el ocurrido en 2024 con la falla de *CrowdStrike*[83], puede desencadenar impactos globales y paralizar sectores enteros.

Paralelamente, el *Data Breach Investigations Report* (DBIR, 2024) confirma la magnitud del riesgo. Más del 50% de los incidentes de *ransomware* se originan en fallas de terceros —incluyendo actualizaciones comprometidas, integraciones de software con validación insuficiente o accesos remotos inseguros—, lo que subraya que las brechas modernas no siempre comienzan dentro de la organización afectada. Además, el informe reporta que el 15% de todas las violaciones analizadas involucraron actores externos en la cadena de suministro, y un 32% de las organizaciones afectadas enfrentó impactos operativos significativos derivados de vulnerabilidades indirectas, tales como software manipulado, servicios gestionados vulnerados o configuraciones inseguras heredadas de proveedores.

Gráfico 4.2 Principales preocupaciones para las organizaciones en ciberseguridad sobre la cadena de suministro



Fuente: Elaboración propia a partir de los datos del informe Global Cybersecurity Outlook 2025[84].

https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[83] Incidente informático global que ocurrió el 19 de julio de 2024, causado por una actualización defectuosa del software de ciberseguridad de CrowdStrike Falcon, el cual interrumpió los sistemas de muchas empresas y organizaciones que usan Microsoft Windows

[84] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Disponible en: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Este comportamiento también se reflejó en las entrevistas realizadas en el marco del estudio. Los operadores consultados señalaron que la seguridad de sus redes está directamente condicionada por la seguridad de los proveedores y fabricantes de los equipos que utilizan, así como por el grado de control que estos mantienen sobre la operación y actualización de sus productos. En consecuencia, la ciberseguridad del sector Telecomunicaciones no depende únicamente de sus propias capacidades, sino de la solidez integral de su cadena de suministro.

Un ejemplo de este vector es la inserción de código malicioso en una actualización de software distribuida por un proveedor confiable (ataques tipo SolarWinds[85]).

4.1.6. Vectores emergentes impulsados por Inteligencia Artificial. La creciente disponibilidad de herramientas de IA generativa también está siendo aprovechada por actores maliciosos para generar contenido fraudulento, automatizar ataques de ingeniería social, generar *deepfakes* o incluso crear *malware* polimórfico que evade los sistemas tradicionales de detección[86].

Ejemplo de estas actividades es la automatización de campañas de *spear phishing* personalizadas usando modelos de lenguaje que imitan conversaciones previas o generan documentos falsificados[87].

Estos vectores no actúan de manera aislada, sino que suelen combinarse en campañas avanzadas, orquestadas por grupos criminales organizados o actores estatales. Por ello, es esencial adoptar un enfoque de defensa en profundidad que abarque todo el ecosistema, desde la infraestructura física hasta el plano lógico y de gestión, incorporando monitoreo continuo, segmentación, autenticación multifactor y análisis de comportamiento.

De acuerdo con el *Global Cybersecurity Outlook 2025* publicado por el Foro Económico Mundial[88] (WEF, 2025) la rápida adopción de la inteligencia artificial generativa (IA Gen) está reconfigurando el panorama de la ciberseguridad global. Las organizaciones reconocen que esta tecnología, aunque ofrece oportunidades significativas en automatización y eficiencia, también amplifica los riesgos existentes y crea nuevas vulnerabilidades que desafían las capacidades tradicionales de protección digital.

El informe revela que la IA generativa está transformando la naturaleza y la dinámica de las amenazas digitales, al ampliar la escala, personalización y sofisticación de los ciberataques. El 42% de las organizaciones reportó haber sufrido ataques exitosos de ingeniería social durante el último año, una

[85] El ataque SolarWinds fue un ciberataque que tuvo como objetivo varias agencias gubernamentales y corporaciones en los Estados Unidos en 2020. Fue llevado a cabo por un grupo de amenaza persistente avanzada (APT) que se cree que opera en nombre del gobierno ruso. El ataque implicó el uso de una actualización de software malicioso para la plataforma de gestión de red SolarWinds Orion, ampliamente utilizada por agencias gubernamentales y grandes empresas. La actualización contenía una puerta trasera que permitía a los atacantes acceder a las redes de las organizaciones que la instalaron.

[86] Schmitt, M., & Flechais, I. (2024). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. arXiv. https://arxiv.org/pdf/2310.13715

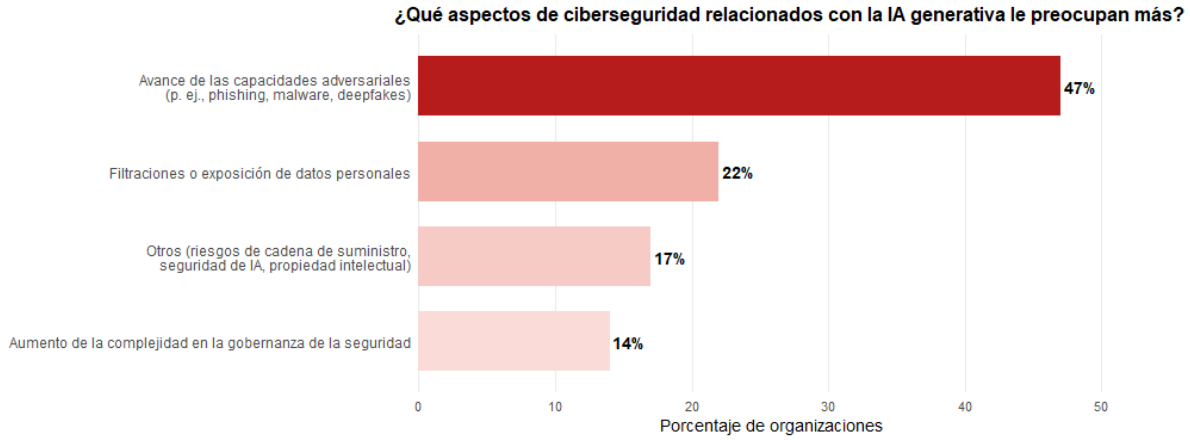
[87] World Economic Forum. (2023). What cybersecurity threats does generative AI expose us to?. Disponible en: https://www.weforum.org/stories/2023/06/what-cybersecurity-threats-are-posed-by-generative-ai/

[88] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Disponible en: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

tendencia que continúa en aumento debido al uso malicioso de la IA para crear contenidos sintéticos, comunicaciones persuasivas y *deepfakes* cada vez más difíciles de detectar.

Asimismo, los resultados muestran que la IA generativa no solo introduce nuevas amenazas, sino que multiplica la velocidad y alcance de las ya existentes. El 47% de las organizaciones considera que el mayor riesgo proviene del avance de las capacidades adversariales, es decir, del uso de IA por parte de atacantes para automatizar, personalizar y escalar campañas de *phishing*, *malware* y *deepfakes*. Un 22% identifica como amenaza prioritaria las filtraciones o exposición de datos personales, mientras que un 14% advierte que la rápida adopción de la IA está aumentando la complejidad de la gobernanza y la gestión ética de la seguridad, al requerir nuevos marcos de control, transparencia y responsabilidad corporativa. Ver Gráfico 4.3.

Gráfico 4.3 Preocupaciones de los empresarios sobre la IA en ciberseguridad



Fuente: Elaboración propia a partir de los datos del informe Global Cybersecurity Outlook 2025[89].

Además, el mismo informe advierte que la IA generativa permite replicar voces, videos, imágenes y estilos de escritura de líderes empresariales, incrementando el riesgo de fraudes basados en *deepfakes* y manipulación contextual. Entre 2023 y 2024 se observó un aumento del 223% en el comercio de herramientas de *deepfake* en la *dark web*, y el 55% de los CISOs considera estas técnicas como la principal amenaza para sus organizaciones.

[89] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Disponible en: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

En conclusión, la IA generativa representa una disrupción estructural en la gestión de la ciberseguridad: amplifica las amenazas existentes, reduce las barreras de entrada para actores maliciosos y expone nuevas vulnerabilidades en los sistemas de información. Frente a este escenario, las organizaciones deben reforzar sus capacidades de detección y respuesta basadas en IA confiable, así como fortalecer la gobernanza, la trazabilidad y los mecanismos éticos que aseguren un uso responsable y seguro de las tecnologías generativas.

4.2. IMPACTO PARA EL ECOSISTEMA DIGITAL

La evolución y diversificación de los vectores de ataque, junto con las tendencias emergentes en ciber amenazas, tienen implicaciones profundas sobre la integridad, disponibilidad, confidencialidad y confiabilidad de las redes de telecomunicaciones. Dado que estas redes constituyen la columna vertebral de los servicios digitales en todos los sectores productivos y sociales, el impacto de los ciberataques trasciende lo técnico y adquiere dimensiones regulatorias, económicas y sociales.

4.2.1. Expansión de la superficie de ataque en el ecosistema digital. La transformación del ecosistema digital ha traído consigo una ampliación sin precedentes de la superficie de ataque, entendida como el conjunto de puntos accesibles a actores maliciosos para comprometer la confidencialidad, integridad o disponibilidad de los sistemas de información. Esta expansión es el resultado directo de la creciente interconexión de dispositivos, la virtualización de funciones de red, la adopción de arquitecturas abiertas y el uso masivo de servicios en la nube.

De acuerdo con el informe de ENISA (2023)[90], la superficie de ataque se ha incrementado no solo en términos de volumen, sino también en complejidad, al incorporar componentes que operan fuera del perímetro tradicional de seguridad, tales como terminales IoT, redes de acceso desagregado, sistemas de *edge computing* y plataformas *multi-cloud*. Esta fragmentación del entorno operativo dificulta la visibilidad integral de las amenazas, genera nuevas interdependencias técnicas y expone a los actores del ecosistema a múltiples vectores de ataque simultáneos.

El concepto tradicional de perímetro de red ha perdido relevancia en un entorno caracterizado por la hiperconectividad, donde usuarios, dispositivos, aplicaciones y servicios interactúan desde múltiples ubicaciones y dominios de confianza. Esta situación ha obligado a adoptar enfoques como *Zero Trust Architecture* (ZTA), que parte del principio de que ningún elemento de la red debe ser considerado automáticamente confiable, incluso si opera dentro del perímetro organizacional[91].

Entre los elementos que han contribuido a la expansión de la superficie de ataque destacan:

[90] ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[91] National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. Disponible en: https://doi.org/10.6028/NIST.SP.800-207

- La virtualización de funciones de red (NFV) y la adopción de arquitecturas nativas en la nube (cloud-native), que han incrementado los puntos de exposición lógicos a través de interfaces API y contenedores inseguros[92].
- El despliegue de redes 5G, que habilita nuevos casos de uso, pero también multiplica los dominios que deben ser asegurados: núcleo, acceso, transporte y aplicaciones[93].
- La proliferación de dispositivos IoT, muchos de ellos con escasas capacidades de seguridad embebida, que actúan como puertas de entrada para ataques dirigidos o masivos.
- La apertura de interfaces y la desagregación funcional, que, si bien promueve la interoperabilidad, también introduce desafíos adicionales de coordinación y blindaje frente a vulnerabilidades de múltiples proveedores[94].

Esta expansión no es únicamente técnica, sino también organizacional y geoestratégica. Los ciberatacantes pueden aprovechar debilidades en terceros proveedores, errores humanos o malas prácticas de configuración para infiltrarse en las redes.

Como resultado, la protección de las redes de telecomunicaciones ya no puede limitarse al aseguramiento de elementos físicos o dispositivos finales. Se requiere una visión integral de la superficie de ataque, que considere todo el ciclo de vida de los activos digitales, la interdependencia entre proveedores y el uso de herramientas avanzadas de monitoreo, inteligencia de amenazas y respuesta coordinada ante incidentes[95].

4.2.2. Riesgos para la prestación continua de servicios críticos. Los operadores de redes están enfrentando una presión creciente para garantizar la disponibilidad ininterrumpida de servicios en contextos altamente hostiles. Las interrupciones causadas por ataques DDoS, *ransomware* o sabotajes en la cadena de suministro pueden afectar directamente servicios esenciales como salud, educación, gobierno electrónico, banca o transporte. En algunos casos, estos ataques no solo causan pérdida de conectividad, sino también de confianza en los prestadores[96].

4.2.3. Aumento de los costos de cumplimiento y operación. El cumplimiento de nuevas obligaciones regulatorias y normativas internacionales en ciberseguridad (como NIS2 en Europa, las directivas de CISA en EE. UU., o leyes nacionales de protección de infraestructuras críticas) exige a los operadores inversiones significativas en capacidades de monitoreo, auditoría, detección, respuesta y recuperación. Muchas organizaciones subestiman estos costos porque no consideran los gastos ocultos relacionados con integración de sistemas legados, capacitación, cambios organizacionales y consultoría

[92] Qiu, Q., Xu, S., Liu, S., Xu, T., & Zhao, B. (2024). Network virtualization security: Threats, measures, and use cases. 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K).
[93] 3GPP. (2024). TS 33.501: Security architecture and procedures for 5G System. 3rd Generation Partnership Project. Disponible en: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/
[94] ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
[95] ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[96] Gupta, A. (2025). Telecom Sector – Cyber Risk. KPMG India. Disponible en: https://kpmg.com/in/en/blogs/2025/02/telecom-sector-cyber-risk.html

especializada[97]. En la práctica, muchas entidades anticipan un aumento permanente en el presupuesto de ciberseguridad para cumplir con NIS2, y un porcentaje notable de pymes puede no lograr obtener los recursos financieros pertinentes para esa adaptación[98].

En el caso estadounidense, las directivas de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) que obliga a nuevas adquisiciones de tecnología, monitoreo continuo y escaneo automatizado también generan presión sobre la estructura operativa y de recursos humanos de los prestadores de servicios de comunicaciones[99].

Este aumento de costos plantea un desafío de sostenibilidad especialmente para los operadores de tamaño mediano y pequeño, que pueden no disponer de economías de escala o márgenes financieros suficientes para absorber esos incrementos sin comprometer su competitividad o calidad de servicio.

4.2.4. Reputación, confianza y relación con el usuario. Las brechas de seguridad que impactan a usuarios finales, por ejemplo, SIM *swap*, accesos no autorizados a datos personales o suplantación de identidad pueden erosionar seriamente la confianza de los ciudadanos en el ecosistema digital. La experiencia negativa del usuario cuando siente que su integridad digital ha sido vulnerada se traduce muchas veces en rechazo, migración hacia otros proveedores o desconfianza persistente.

Se proyecta un aumento en los ataques que buscan erosionar la confianza de los usuarios en la infraestructura digital, mediante interrupciones prolongadas, manipulación de datos, suplantación de identidad y campañas de desinformación que explotan canales digitales legítimos[100].

Si la gestión de incidentes es deficiente por demoras en la comunicación, falta de transparencia o respuestas inadecuadas el operador se expone a pérdidas reputacionales significativas, sanciones legales y, en última instancia, al deterioro de la percepción de seguridad por parte de la población. Las brechas no solo implican pérdidas económicas inmediatas: también comprometen la lealtad de los usuarios, el prestigio institucional y la posición en el mercado[101].

En suma, la reputación y la confianza son activos críticos para los operadores del ecosistema de telecomunicaciones: una falla de seguridad mal gestionada puede desencadenar un círculo negativo donde la desconfianza debilita la posición competitiva, el daño institucional y las sanciones reguladoras obligan a medidas costosas, y la recuperación exige recursos adicionales para reconstruir credibilidad.

---

[97] Barbour, D. (2025). How much does NIS2 compliance really cost? Complete budget guide. Kiteworks. Disponible en: https://www.kiteworks.com/blog/security-and-compliance/nis2-compliance-cost-budget-guide/

[98] European Union Agency for Cybersecurity (ENISA). (2024,). Navigating cybersecurity investments in the time of NIS 2. Disponible en: https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

[99] Ribeiro, A. (2022, October 6). CISA directive likely to drive investment costs, raise need for more staff, update technology and processes. Industrial Cyber. Disponible en: https://industrialcyber.co/cisa/cisa-directive-likely-to-drive-investment-costs-raise-need-for-more-staff-update-technology-and-processes/

[100] Alvisi, L., Bianchi, J., Tibidò, S., & Zucca, M. V. (2024). Weaponizing disinformation against critical infrastructures. arXiv. Disponible en: https://doi.org/10.48550/arXiv.2406.08963

[101] F5, Inc. (2025). What are security breaches? F5. Disponible en: https://www.f5.com/glossary/security-breaches

4.2.5. Desigualdades y vulnerabilidades regulatorias. El ecosistema de telecomunicaciones engloba operadores de diferentes escalas, infraestructura y grado de madurez en ciberseguridad. Esta heterogeneidad implica que ciertos prestadores, sobre todo los ubicados en zonas rurales o con estructuras limitadas, enfrenten mayores dificultades para adoptar medidas de prevención y respuesta frente a amenazas. Por ejemplo, los operadores rurales a menudo carecen de los recursos financieros y de personal para dedicar tiempo sustancial a planificación prospectiva, análisis de riesgos y capacitación especializada en ciberseguridad.

En zonas rurales hay evidentes brechas de seguridad derivadas de menor inversión en defensa digital: si bien se destinan recursos para extender la conectividad, frecuentemente no se asigna suficiente para fortalecer la infraestructura frente a amenazas emergentes.

Desde el punto de vista del regulador, es clave reconocer esta diversidad: los reguladores de tecnologías de la información y las comunicaciones deben adoptar enfoques escalables y proporcionales, en lugar de normativas uniformes que puedan imposibilitar el cumplimiento a operadores con menor capacidad técnica o financiera[102].

Si estas desigualdades no se abordan, los puntos débiles de algunos operadores podrían convertirse en vectores de propagación para ataques que comprometan no solo redes aisladas sino el sistema en su conjunto.

4.2.6. Tensión entre innovación, apertura y seguridad. La adopción de arquitecturas abiertas, la virtualización y el uso de software libre o componentes provenientes de múltiples proveedores plantean el desafío de equilibrar innovación y aseguramiento de componentes críticos. La apertura y desagregación de la red implica que funciones que antes eran cerradas y uniformes ahora estén distribuidas en múltiples nodos, interfaces e implementaciones heterogéneas, lo que puede incrementar la superficie de ataque si no se gestionan correctamente[103].

En el contexto de Open RAN, la desagregación obliga a que distintos proveedores dividan las funciones más allá de la Unidad de Radio (RU) en Unidades Distribuidas (DUs), Unidades Centralizadas (CU) y controladores (RICs) que deben interoperar de forma segura, lo cual exige que cada interfaz abierta (por ejemplo, *fronthaul*) preserve confidencialidad, integridad y disponibilidad[104].

[102] International Telecommunication Union & World Bank. (2024, febrero 5). Guiding principles for ICT regulators to enhance cyber resilience. Digital Regulation Platform. Disponible en: https://digitalregulation.org/guiding-principles-for-ict-regulators-to-enhance-cyber-resilience/
[103] Azariah, W., Bimo, F. A., Lin, C. W., Cheng, R. G., Nikaein, N., & Jana, R. (2024). A survey on open radio access networks: Challenges, research directions, and open source approaches. Sensors, 24(3), 1038. Disponible en: https://doi.org/10.3390/s24031038
[104] Zwarico, A., & Jeux, S., junto con otros colaboradores. (2025). The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components. O-RAN ALLIANCE. Disponible en: https://www.o-ran.org/blog/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Los mecanismos de *security-by-design* deben ser parte integral desde la fase de arquitectura: esto implica modelado de amenazas temprano, privilegios mínimos, separación de dominios de confianza, defensa en profundidad, auditoría continua y revisión sistemática de vulnerabilidades[105].

En entornos virtualizados (VMs, contenedores, microservicios), los riesgos comunes como fallas del hipervisor, mal configuración en entornos compartidos, escalamiento lateral no deseado o vulnerabilidades en interfaces virtuales se vuelven relevantes en redes de telecomunicaciones[106].

Por ello, cualquier decisión de arquitectura ya sea para incorporar Open RAN, contenedorización o software de múltiples orígenes debe contemplar criterios de seguridad desde el diseño (*security-by-design*), interoperabilidad segura, mecanismos de aislamiento, cadena de suministro segura y evaluación permanente de vulnerabilidades.

En conclusión, el impacto de las amenazas cibernéticas no se limita a aspectos técnicos o financieros, sino que afecta directamente la sostenibilidad, confiabilidad y legitimidad del ecosistema digital. Fortalecer la resiliencia digital de las redes requiere de un enfoque sistémico, colaborativo y adaptativo, con la participación de todos los actores: operadores, desarrolladores, certificadores, usuarios, academia y autoridades.

[105] Cesarano, C., Foggia, A., Roscigno, G., Andreani, L., & Natella, R. (2025). Security-by-design at the telco edge with OSS: Challenges and lessons learned. arXiv. Disponible en: https://arxiv.org/abs/2505.00111
[106] National Cyber Security Centre. (2019). Virtualisation security design principles. NCSC. Disponible en: https://www.ncsc.gov.uk/collection/cyber-security-design-principles/virtualisation-security-design-principles

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5. INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas son aquellos sistemas, servicios, redes o activos cuya interrupción o deterioro tendría un impacto grave en la seguridad nacional, la economía, la salud pública o el bienestar de la población. Incluyen sectores esenciales como la energía, el transporte, el agua, las finanzas, la salud y las telecomunicaciones, los cuales dependen crecientemente de sistemas digitales interconectados.

En este contexto, las infraestructuras críticas cibernéticas comprenden el conjunto de componentes tecnológicos, plataformas y servicios digitales que sustentan el funcionamiento seguro y continuo de dichas infraestructuras. Su protección frente a incidentes o ataques cibernéticos se ha convertido en una prioridad estratégica de los Estados, dada su relación directa con la continuidad de los servicios esenciales y la estabilidad nacional.

En esta sección se revisa el estado de la gestión y la gobernanza de las infraestructuras críticas cibernéticas en diferentes países y regiones, incluyendo Estados Unidos, Canadá, México, Brasil, Chile, Argentina, la Unión Europea y por supuesto en Colombia. Finalmente, se presenta una recopilación de planes y programas de referencia para la protección de infraestructuras críticas cibernéticas.

5.1 REFERENCIAS INTERNACIONALES

5.1.1. Unión Europea. Desarrolló uno de los marcos regulatorios más robustos del mundo para la protección de infraestructuras críticas cibernéticas, estableciendo un modelo de gobernanza multinivel que combina regulación vinculante, coordinación supranacional y cooperación entre Estados miembros. Este enfoque busca crear un espacio digital europeo resiliente, seguro y confiable frente a amenazas cibernéticas cada vez más sofisticadas y de alcance transfronterizo.

A continuación, se presentan cuatro pilares fundamentales en europea para la ciberseguridad de las infraestructuras críticas:

5.1.1.1. Directiva NIS2 (*Red and Information Systems Security* 2) - Directiva (UE) 2022/2555: Adoptada en diciembre de 2022 con plazo de transposición hasta octubre de 2024. NIS2 amplía dramáticamente el alcance respecto a NIS1, cubriendo 18 sectores críticos organizados en dos categorías:

- Entidades Esenciales (máxima prioridad): Energía (electricidad, gas, petróleo, hidrógeno, calefacción), transporte (aéreo, ferroviario, acuático, carretero), banca, infraestructura de mercados financieros, salud, agua potable, aguas residuales, infraestructura digital (DNS, dominios TLD, computación en nube, centros de datos, CDN), gestión de servicios TIC, administración pública central y sector espacial.
- Entidades Importantes: Servicios postales, gestión de residuos, productos químicos, alimentos, fabricación de productos críticos (dispositivos médicos, equipos informáticos, vehículos), proveedores de servicios digitales (mercados en línea, buscadores, redes sociales) e investigación.

La directiva aplica principalmente a empresas medianas y grandes, aunque ciertos proveedores de infraestructura digital están sujetos independientemente del tamaño. Las entidades esenciales e importantes deben adoptar medidas técnicas, operacionales y organizacionales apropiadas y proporcionales basadas en enfoque «*all-hazards*» (todas las amenazas).

Las medidas mínimas obligatorias incluyen:

- Políticas de análisis de riesgos y seguridad de sistemas de información
- Gestión de incidentes y crisis
- Continuidad de negocio (gestión de copias de seguridad, recuperación ante desastres)
- Seguridad de cadena de suministro (evaluación de terceros y proveedores)
- Seguridad en adquisición, desarrollo y mantenimiento de sistemas
- Ciberhigiene y capacitación en ciberseguridad
- Criptografía y cifrado de datos
- Seguridad de recursos humanos y control de acceso
- Autenticación multifactor (MFA) o autenticación continua
- Comunicaciones seguras (voz, video, texto) incluyendo emergencias

Reporte de Incidentes: Notificación sin demora indebida y, en cualquier caso, dentro de 24 horas (alerta temprana), 72 horas (notificación formal), y un mes (informe final). Un incidente significativo causa perturbación operacional grave de servicios o pérdidas financieras considerables[107].

[107] European Commision. NIS2 Directive: securing network and information systems. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Aplicaciones y sanciones. La NIS2 otorga a las autoridades nacionales amplias facultades de supervisión, que incluyen auditorías periódicas, inspecciones de seguridad, emisión de instrucciones vinculantes y, de manera destacada, la imposición de multas administrativas. La responsabilidad se extiende directamente a los órganos de gestión: los miembros de la junta directiva pueden ser considerados personalmente responsables del cumplimiento, y fallos graves de gobernanza pueden derivar en sanciones como prohibiciones temporales o inhabilitación para ejercer funciones de liderazgo. Con NIS2, la ciberseguridad deja de ser un asunto exclusivamente técnico y se consolida como una responsabilidad estratégica del máximo nivel, integrada en la gestión del riesgo operacional[108].

5.1.1.2. Directiva CER (*Critical Entities Resilience*) - Directiva (UE) 2022/2557: Complementa NIS2 enfocándose en resiliencia física y operacional de 11 sectores críticos (energía, transporte, banca, infraestructura financiera, salud, agua, aguas residuales, infraestructura digital, administración pública, espacio y alimentos). Mientras NIS2 aborda riesgos cibernéticos, CER cubre amenazas físicas, desastres naturales y disrupciones de cadena de suministro[109].

5.1.1.3. *Digital Operational Resilience Act* (DORA) - Reglamento (UE) 2022/2554: En vigor desde enero de 2025, específicamente para el sector financiero (más de 22.000 entidades incluyendo bancos, aseguradoras, proveedores TIC financieros). DORA armoniza gestión de riesgo TIC, gestión de incidentes, continuidad de negocio, pruebas de resiliencia (incluyendo pruebas de penetración basadas en amenazas para entidades significativas) y gestión de riesgo de terceros TIC[110].

5.1.1.4. *Cyber Resilience Act* (CRA) - Reglamento (UE) 2024/2847: Aplicable 36 meses después de su publicación a todos los productos con elementos digitales comercializados en la UE. El CRA requiere que fabricantes implementen seguridad por diseño y por defecto, establezcan procesos de gestión de vulnerabilidades, proporcionen actualizaciones de seguridad oportunas y mantengan comunicación transparente sobre riesgos[111].

Así mismo, la Unión Europea cuenta con varias instituciones de Coordinación:

5.1.1.5. Agencia de la Unión Europea para la Ciberseguridad (ENISA): Fue creada en 2004 y fortalecida por el *Cybersecurity Act* de 2019. Sus responsabilidades incluyen asesorar a la Comisión y Estados miembros en materia de seguridad de la información, recopilar y analizar datos sobre incidentes

[108] Radlanski, P., & Rudt, J. (2025). EU NIS 2 Directive: Expanded cybersecurity obligations for key sectors. Greenberg Traurig LLP. Disponible en: https://www.gtlaw.com/en/insights/2025/8/eu-nis-2-directive-expanded-cybersecurity-obligations-for-key-sectors
[109] European Parliament & Council of the European Union. (2022, December 14). Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 164–198. Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[110] European Insurance and Occupational Pensions Authority (EIOPA). Digital Operational Resilience Act (DORA). Disponible en: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[111] European Commission. Cyber Resilience Act. Shaping Europe's digital future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

de seguridad en Europa, promover métodos de evaluación y gestión de riesgos, y fomentar la cooperación entre diferentes actores mediante asociaciones público-privadas[112].

ENISA desempeña un papel estratégico en la implementación de la Directiva NIS[113], proporcionando orientación y apoyo operacional a los Estados miembros, facilitando el intercambio de información entre autoridades nacionales y empresas privadas, y desarrollando estándares técnicos. La agencia organiza regularmente ejercicios de ciberseguridad a nivel de la Unión (*Cyber Europe Exercises*) para mejorar capacidades de respuesta y coordina la Red de CSIRTs (*Computer Security Incident Response Teams*) que conecta los equipos nacionales de respuesta a incidentes.

5.1.1.6. Red de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs Network): Establecida bajo la Directiva NIS, esta red facilita la cooperación operacional entre los equipos nacionales de respuesta a incidentes, permitiendo el intercambio rápido de información sobre amenazas, alertas tempranas y coordinación de respuestas. Cada Estado miembro debe designar uno o más CSIRTs nacionales con capacidades técnicas y operacionales para manejar incidentes y riesgos cibernéticos[114].

5.1.1.7. Organización Europea de Enlace para Crisis Cibernéticas (EU-CyCLONe): Creada bajo NIS2, EU-CyCLONe gestiona a nivel operacional incidentes cibernéticos a gran escala y crisis que afecten múltiples Estados miembros o sectores críticos. Sus funciones principales incluyen desarrollar conciencia situacional compartida, evaluar consecuencias e impactos de incidentes relevantes, coordinar la gestión de crisis cibernéticas a gran escala, apoyar la toma de decisiones políticas, e incrementar el nivel de preparación mediante ejercicios y planificación conjunta. También coopera estrechamente con la Red de CSIRTs en aspectos técnicos[115].

5.1.1.8. Unidad Cibernética Conjunta (Joint Cyber Unit - JCU): Propuesta por la Comisión en junio 2021, la JCU constituye una plataforma de cooperación virtual y física que reúne recursos y experiencia disponibles en la UE y Estados miembros para prevenir, disuadir y responder efectivamente a incidentes cibernéticos masivos y crisis. La JCU busca crear solidaridad y asistencia europea coordinada contra ciberataques a gran escala, conectando comunidades civiles, de aplicación de la ley, diplomáticas y de ciberdefensa que tradicionalmente operaban separadamente[116].

5.1.1.9. Esquema de Certificación Europeo (EUCC): El Esquema Europeo de Certificación de Ciberseguridad sobre Criterios Comunes (EUCC), en vigor desde febrero de 2025, proporciona

[112] Rupp, C. (2025). ENISA: Fit for Purpose? Reviewing the EU Cybersecurity Agency's Role in an Evolving Policy Ecosystem. Interface. Disponible en: https://www.interface-eu.org/publications/enisa-fit-for-purpose
[113] European Commision. NIS2 Directive: securing network and information systems. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[114] CSIRTs Network. Disponible en: https://csirtsnetwork.eu/
[115] European Union Agency for Cybersecurity (ENISA). EU CyCLONe. Disponible en:https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone
[116] European Commission. (2021). Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents. Press corner. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

certificación armonizada voluntaria de productos TIC a través de la UE, basada en estándar internacional *Common Criteria* (ISO/IEC 15408). El EUCC reemplaza esquemas nacionales SOGIS (transición hasta enero 2026) y propone dos niveles de aseguramiento: «sustancial» y «alto», con certificados válidos por cinco años[117].

5.1.2. Estados Unidos. Cuenta con el marco más desarrollado y consolidado para la protección de infraestructuras críticas cibernéticas de las américas. *La Cybersecurity and Infrastructure Security Agency* (CISA)[118], creada en 2018, lidera los esfuerzos nacionales para comprender, gestionar y reducir riesgos en la infraestructura crítica del país. El país ha identificado 16 sectores críticos que incluyen energía, transporte, servicios financieros, salud, telecomunicaciones, agua, agricultura, manufactura crítica, servicios de emergencia, sector químico, instalaciones gubernamentales, tecnologías de la información, sector nuclear, represas, instalaciones comerciales y defensa industrial[119].

El modelo estadounidense se distingue por un enfoque de colaboración público-privada, sustentado en el reconocimiento de que la mayor parte del porcentaje de la infraestructura crítica pertenece y es operada por el sector privado. En este esquema, CISA actúa como entidad articuladora, trabajando con las *Sector-Specific Agencies* (SSAs), responsables de cada sector crítico, y con el *National Risk Management Center* (NRMC) para identificar, priorizar y gestionar los riesgos más significativos[120].

A continuación, algunos de los elementos en los que se fundamenta la arquitectura regulatoria:

5.1.2.1. *Presidential Policy Directive* 21 (PPD-21) de 2013: Establece la política nacional sobre seguridad y resiliencia de infraestructuras críticas, definiendo roles federales y promoviendo la colaboración entre entidades gubernamentales y operadores privados. Esta directiva refina las relaciones funcionales en el gobierno federal y busca habilitar el intercambio efectivo de información[121].

5.1.2.2. *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) de 2022: Marca un avance decisivo en materia de reporte obligatorio de incidentes. Una vez entren en vigor las regulaciones finales, actualmente programadas para mayo de 2026, las entidades cubiertas deberán notificar a CISA los incidentes cibernéticos sustanciales en un plazo máximo de 72 horas, y los pagos relacionados con *ransomware* dentro de 24 horas. Se estima que la obligación aplicará a más de 300.000 entidades pertenecientes a los 16 sectores de infraestructura crítica[122].

---

[117] Thales Group. (2025). Introducing EUCC: A new certificate to boost cybersecurity in Europe. Disponible en: https://www.thalesgroup.com/en/news-centre/insights/public-security/national-security/introducing-eucc-new-certificate-boost
[118] Cybersecurity and Infrastructure Security Agency (CISA). About CISA. Disponible en: https://www.cisa.gov/about
[119] Nevada Office of Emergency Management. Critical Infrastructure. Disponible en: https://www.oem.nv.gov/homeland-security/critical-infrastructure/
[120] Brooks, M., Fixler, A., & Montgomery, M. (2023, June 7). Revising public-private collaboration to protect U.S. critical infrastructure. Cyberspace Solarium Commission 2.0. Disponible en: https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/
[121] The White House. (2013). Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21). Disponible en: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[122] Nozomi Networks. (2024). Get ready for CIRCIA and NIS2 cyber incident reporting. Disponible en: https://www.nozominetworks.com/blog/get-ready-for-circia-and-nis2-cyber-incident-reporting

5.1.2.3. NIST *Cybersecurity Framework* (CSF): Actualizado a la versión 2.0, establece un enfoque voluntario, flexible y basado en riesgos que integra estándares y mejores prácticas de la industria. El marco se organiza en seis funciones principales: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar, incorporando la función «Gobernar» como el elemento más reciente para reforzar la alineación estratégica entre la gestión de la ciberseguridad y los objetivos organizacionales[123].

Para sectores específicos existen regulaciones adicionales. Tras el ataque a Colonial Pipeline en 2021, la ***Transportation Security Administration* (TSA)** emitió directivas de seguridad de carácter obligatorio para los operadores de oleoductos y gasoductos, exigiendo la implementación de medidas de mitigación, la elaboración de planes de contingencia cibernética y la realización de evaluaciones de arquitectura de seguridad[124].

5.1.2.4. SEC[125] **-** Norma de gestión de riesgos, estrategia, gobernanza e incidentes de ciberseguridad. En el ámbito de los mercados de valores, la *Securities and Exchange Commission* (SEC) de Estados Unidos adoptó una regulación específica que refuerza la transparencia y la responsabilidad de las empresas frente a los riesgos de ciberseguridad. La norma exige que los emisores informen a la SEC sobre incidentes de ciberseguridad materiales en un plazo máximo de cuatro días hábiles desde que se determina su materialidad, describiendo la naturaleza, el alcance y el momento del incidente, así como su impacto actual o potencial en la situación financiera y la estrategia corporativa, sin requerir la divulgación de detalles técnicos o vulnerabilidades concretas.

Adicionalmente, las compañías deben explicar cómo gestionan los riesgos materiales de ciberseguridad: sus procesos de evaluación e identificación de riesgos, la forma en que estos se integran en el sistema general de gestión de riesgos, el rol de terceros (como consultores o auditores) y la supervisión de riesgos asociados a proveedores y otros actores de la cadena de suministro. La norma también obliga a describir la gobernanza de la ciberseguridad, incluyendo la manera en que el consejo de administración y sus comités supervisan estos riesgos, los canales de reporte y el papel de la alta dirección, detallando los cargos responsables y su experiencia relevante.

Finalmente, la SEC subraya la importancia de contar con controles internos y de divulgación sólidos que aseguren reportes completos, precisos y oportunos. El director ejecutivo (*Chief Executive Officer*, CEO) y el director financiero (*Chief Financial Officer*, CFO) deben certificar la veracidad de los informes anuales y la eficacia de dichos controles, lo que implica documentar y actualizar los procesos, roles y responsabilidades, así como revisar periódicamente los incidentes y los controles a la luz de marcos de referencia como ERM, NIST o ISO 27001. Esto contribuye a integrar la ciberseguridad en el corazón de la estrategia empresarial y de la rendición de cuentas frente a los inversionistas.

---

[123] Koba, J. (2025). Cybersecurity standards for critical infrastructure. Kogifi. Disponible en: https://www.kogifi.com/articles/cybersecurity-standards-for-critical-infrastructure

[124] Industrial Cyber. (2025). Strengthening pipeline security: A guide for OT professionals on TSA pipeline security directives and the 2024 notice of proposed rules. Disponible en: https://industrialcyber.co/regulation-standards-and-compliance/strengthening-pipeline-security-a-guide-for-ot-professionals-on-tsa-pipeline-security-directives-and-the-2024-notice-of-proposed-rules/

[125] The SEC Finalizes Rule on Cybersecurity Disclosures. Disponible en: https://www.cpajournal.com/2025/08/27/the-sec-finalizes-rule-on-cybersecurity-disclosures

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5.1.3. Canadá. Fortaleció de manera significativa su postura en ciberseguridad de infraestructuras críticas con la presentación del Bill C-8 en junio de 2025, que de ser aprobado se convertiría en la primera legislación federal vinculante y de alcance intersectorial dirigida a los proveedores de infraestructura esencial. El enfoque canadiense parte del reconocimiento de que los sistemas vitales del país están expuestos no solo a actores cibernéticos hostiles, sino también a desastres naturales y fenómenos climáticos extremos[126].

En este contexto también es importante citar el centro de seguridad de las comunicaciones de Canadá, el *Communications Security Establishment* (CSE). Su función principal es proteger los sistemas y la información del Estado frente a amenazas cibernéticas, proporcionando asesoría, servicios de seguridad y capacidades técnicas avanzadas. Además, el CSE detecta y analiza actividades cibernéticas maliciosas en el exterior y, cuando la ley lo autoriza, puede realizar operaciones cibernéticas defensivas y ofensivas para impedir o interrumpir acciones de actores hostiles. También opera el *Canadian Centre for Cyber Security* (*Cyber Centre*), que coordina la respuesta nacional a incidentes cibernéticos y comparte información de amenazas con instituciones públicas, operadores de infraestructura crítica y socios internacionales. En síntesis, el CSE es el centro nacional de inteligencia y operaciones cibernéticas de Canadá, encargado de proteger al Estado y apoyar la resiliencia del país frente a riesgos digitales[127].

El Bill C-8 se compone de dos elementos principales[128]:

- Enmiendas a la *Telecommunications Act*, que otorgan nuevas facultades para reforzar la seguridad del sistema de telecomunicaciones canadiense y adoptar medidas frente a proveedores de alto riesgo; y
- La *Critical Cyber Systems Protection Act* (CCSPA), que establece un régimen regulatorio para fortalecer la ciberseguridad de servicios y sistemas esenciales en sectores como telecomunicaciones, oleoductos y líneas eléctricas interprovinciales, energía nuclear, transporte, banca y sistemas de compensación y liquidación.

5.1.4. México. Mediante Decreto del 28 de noviembre de 2024, se creó la Agencia de Transformación Digital y Telecomunicaciones (ATDT), que integra dentro de su estructura a la Dirección General de Ciberseguridad (DGCiber), bajo la Coordinación Nacional de Infraestructura Digital. La DGCiber[129], adscrita a la Coordinación Nacional de Infraestructura Digital y constituida como el centro operativo de la estrategia de ciberseguridad de la Administración Pública Federal (APF), cuenta con 14 atribuciones estratégicas, de gestión de riesgos, auditoría, coordinación, respuesta a incidentes y colaboración, y

[126] Parliament of Canada. (2025). Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. Disponible en: https://www.parl.ca/DocumentViewer/en/45-1/bill/C-8/first-reading
[127] Government of Canada. (2025). Communications Security Establishment Canada. Disponible en: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/welcome-package-minister-national-defence/communications-security-establishment-canada.html
[128] Darktrace. (2024). Understanding the Canadian Critical Cyber Systems Protection Act. Disponible en: https://www.darktrace.com/blog/understanding-the-canadian-critical-cyber-systems-protection-act
[129] Diario Oficial de la Federación (DOF). (2025). Acuerdo por el que se establecen disposiciones en materia de telecomunicaciones y radiodifusión. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5747756&fecha=24/01/2025#gsc.tab=0

tiene el mandato de establecer y fortalecer la postura de ciberseguridad de la Administración Pública Federal (APF), así como promover mecanismos de cooperación con otras entidades gubernamentales, el sector privado y organismos internacionales, posicionándose como un actor central del ecosistema nacional de ciberseguridad.

Adicionalmente, mediante reforma publicada en el Diario Oficial de la Federación (DOF) el 30 de septiembre de 2024, la Guardia Nacional, que tiene a su cargo el Centro de Respuesta a Incidentes Cibernéticos (CERT-MX), fue transferida a la Secretaría de la Defensa Nacional (SEDENA).

En diciembre de 2025, la ATDT expidió el Plan Nacional Ciberseguridad[130] con una visión a largo plazo que define un grupo de proyectos a desarrollar de 2025 a 2030, cada uno con su objetivo, su alcance y metas definidas. A nivel general, los proyectos están distribuidos en 6 fases.

Fase 1 – Fundamento (2025). Establecimiento del marco federal de ciberseguridad y políticas.
Fase 2 – Expansión (2026). Implementación de Administración Pública Federal cibersegura, Centro Nacional de Operaciones en Ciberseguridad – SOC (CSOC), CSIRT Nacional APF (CSIRT-APF) y estrategias nacionales.
Fase 3 – Consolidación (2027). Integración de gestión de riesgos y *Cyber Range National*.
Fase 4 – Maduración (2028). Adopción de IA para ciberdefensa y Centro Regional LATAM de Respuestas.
Fase 5 – Liderazgo (2029). Estrategia de exportación de servicios, Ventanilla Única de Información de Ciberseguridad (VUIC) y observatorio APF de ciberseguridad.
Fase 6 – Transformación y proyección (2030). Certificación nacional para el cumplimiento de los lineamientos y protocolos de ciberseguridad de la APF y Next-Gen SecOps (IA avanzada y tecnologías emergentes).

5.1.5. Brasil. Desarrolló un marco institucional robusto para la protección de infraestructuras críticas, articulado a través de tres instrumentos normativos principales. La Política Nacional de Seguridad de Infraestructuras Críticas (PNSIC) de 2018 (Decreto nº 9.573/2018) que establece los fundamentos conceptuales, definiendo infraestructuras críticas como «instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, total o parcial, provoque serio impacto social, ambiental, económico, político, internacional o a la seguridad del Estado y de la sociedad»[131].

La *Estratégia Nacional de Segurança de Infraestruturas Críticas* (ENSIC) de 2020 (Decreto nº 10.569) identifica los principales desafíos para la seguridad de las infraestructuras críticas y define ejes estratégicos para su abordaje[132].

[130] Gobierno de México. (2025). Plan Nacional de Ciberseguridad. Disponible en: https://www.gob.mx/atdt/planes_nacionales/ciberseguridad/Plan_Nacional_de_Ciberseguridad.pdf
[131] Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (2025). Segurança de Infraestruturas Críticas. Disponible en: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas/seguranca-de-infraestruturas-criticas-sic
[132] Instituto Igarapé. (2025). National Strategy for Critical Infrastructures Security (ENSIC). Portal Brasileiro da Cibersegurança. Disponible en: https://cibersegurança.igarape.org.br/en/national-strategy-for-critical-infrastructures-security-ensic/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Así mismo, el *Plano Nacional de Segurança de Infraestruturas Críticas* (PLANSIC) de 2022 (Decreto nº 11.200/2022) pone en operación estas políticas, estableciendo orientaciones generales, responsabilidades sectoriales, metas, plazos y promoviendo la elaboración de planes sectoriales[133].

La gobernanza está coordinada desde el *Gabinete de Segurança Institucional da Presidência da República* (GSI/PR), que preside la política de infraestructuras críticas y articula la implementación del marco. En 2024 se instituyó el *Comitê Nacional de Segurança de Infraestruturas Críticas* (CNSIC) mediante la *Portaria Interministerial* nº 4, integrando 15 ministerios, como órgano colegiado para monitorear la implementación de la PNSIC y del PLANSIC[134].

Brasil ha identificado varias áreas prioritarias, entre las que figuran agua, energía, transportes, comunicaciones/telecomunicaciones y finanzas, para la aplicación del marco de infraestructuras críticas. Para cada uno de esos sectores se promueve la elaboración de planes específicos, con énfasis en la gestión de riesgos y el análisis de interdependencias entre sistemas.

En relación con la ciberseguridad, Brasil cuenta con una nueva estrategia nacional (E-Ciber, Decreto nº 12.573/2025)[135] que aborda la protección del ciberespacio e infraestructuras digitales. La cual está conformada por 4 ejes: Eje 1 – protección y concientización del ciudadano y la sociedad, Eje 2 – seguridad y resiliencia de los servicios esenciales y las infraestructuras críticas, Eje 3 - cooperación e integración público-privada y cooperación internacional, Eje 4 – soberanía nacional y gobernanza.

5.1.6. Chile. En los últimos años ha desarrollado un marco institucional y normativo robusto para la protección de su infraestructura crítica, abordando tanto los aspectos físicos como cibernéticos de los sistemas esenciales del país. Este marco se articula a través de reformas constitucionales, leyes específicas y políticas públicas que establecen responsabilidades compartidas entre el Estado y el sector privado.

El elemento fundamental de la gobernanza de infraestructura crítica en Chile es la Ley 21.542 de 2023, que modificó la Constitución para permitir que las Fuerzas Armadas protejan la infraestructura crítica cuando exista peligro grave o inminente. Esta reforma constitucional define la infraestructura crítica como aquella indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de servicios básicos como energía, gas, agua, telecomunicaciones, conexión vial, aérea, terrestre, marítima, portuaria, ferroviaria, y servicios de utilidad pública como sistemas sanitarios o de salud[136]. Complementariamente, el Boletín 16.143 tramita actualmente en el Congreso un proyecto de ley que establece criterios específicos para determinar la infraestructura crítica, crea instrumentos de

[133] Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (2025). Segurança de Infraestruturas Críticas. Disponible en: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas/seguranca-de-infraestruturas-criticas-sic
[134] Agência Gov. (2024, noviembre). Governo Federal institui Comitê Nacional de Segurança de Infraestruturas Críticas. Disponible en: https://agenciagov.ebc.com.br/noticias/202411/governo-federal-institui-comite-nacional-de-seguranca-de-infraestruturas-criticas
[135] Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (2025). Estratégia Nacional de Cibersegurança (E-Ciber). Disponible en: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber
[136] Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.883. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1188583

planificación y gestión para su protección, impone obligaciones a los operadores públicos y privados, y confiere facultades a los organismos del Estado responsables de su resguardo[137].

En el ámbito cibernético, la Ley 21.663 (Ley Marco de Ciberseguridad), promulgada en abril de 2024, constituye el marco regulatorio para la protección de infraestructuras críticas de la información. Esta ley creó la Agencia Nacional de Ciberseguridad (ANCI), organismo autónomo con facultades de fiscalización, regulación y sanción que comenzó a operar el 2 de enero de 2025. La ANCI tiene entre sus funciones calificar a los servicios esenciales y operadores de importancia vital, establecer estándares de ciberseguridad, administrar el Registro Nacional de Incidentes de Ciberseguridad, y coordinar con el CSIRT Nacional (Equipo de Respuesta a Incidentes de Seguridad Informática)[138].

Chile ha adoptado un modelo de gobernanza que enfatiza la alianza público-privada y el trabajo entre agencias. La Política Nacional de Ciberseguridad 2023-2028, aprobada mediante Decreto Supremo 164 de 2023[139], establece cinco objetivos: infraestructura resiliente, derechos de las personas, cultura de ciberseguridad, coordinación nacional e internacional, y fomento de la industria y la investigación científica. Esta política es implementada por el Comité Interministerial sobre Ciberseguridad, que aprobó un plan de acción con 15 medidas estratégicas para fortalecer la resiliencia digital del país[140].

La coordinación entre ministerios es fundamental en este esquema. El Ministerio del Interior y Seguridad Pública lidera la protección física de la infraestructura crítica, mientras que diversos ministerios sectoriales (Energía, Obras Públicas, Transporte y Telecomunicaciones, Hacienda, Defensa) tienen responsabilidades específicas sobre la infraestructura de sus respectivos ámbitos. La ANCI coordina las acciones de ciberseguridad entre organismos del Estado y entre éstos y los particulares, supervisando el cumplimiento de estándares mínimos por parte de los operadores de servicios esenciales.

5.1.7. Argentina. La Resolución 1523/2019 define formalmente las infraestructuras críticas como aquellas indispensables para servicios esenciales (salud, seguridad, economía, defensa), identificando sectores como energía, agua, transporte, telecomunicaciones, finanzas y salud. La Dirección Nacional de Ciberseguridad ejerce la responsabilidad primaria en ciberseguridad, apoyada operativamente por el CERT.ar para la respuesta ante incidentes informáticos[141].

[137] Senado de la República de Chile. (2025, julio 18). Protección de la infraestructura crítica: Comisión de Defensa perfecciona definiciones de conceptos claves. Disponible en: https://www.senado.cl/comunicaciones/noticias/proteccion-de-la-infraestructura-critica-comision-de-defensa-perfecciona
[138] Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.663. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1202434
[139] Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.738. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1198702
[140] Biblioteca del Congreso Nacional de Chile (BCN). (2025, julio 11). Resolución N° 28 Exenta. Disponible en: https://bcn.cl/b4YIYf
[141] Secretaría de Innovación Pública. (2025). Objetivos de la Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros, República Argentina. Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/objetivos-de-la-direccion

Argentina aprobó su primera Estrategia Nacional de Ciberseguridad en 2019 y actualizó con una segunda versión en 2023, reconociendo la dependencia crítica de las redes informáticas en servicios esenciales y promoviendo colaboración público-privada[142].

5.2. COLOMBIA

En Colombia, las infraestructuras críticas cibernéticas y los servicios esenciales corresponden con aquellos activos, servicios y sistemas cuya interrupción, degradación o destrucción puede generar una afectación significativa a la seguridad nacional, la economía, el bienestar social o la prestación de funciones estatales esenciales. El Decreto 338 de 2022 adopta un modelo de gobernanza de seguridad digital, ordena identificar y mantener el inventario de infraestructuras críticas públicas y definir servicios esenciales (metodología definida por el MinTIC), y fija lineamientos de gestión de riesgos y coordinación de respuesta a incidentes como ejes prioritarios de protección[143].

La protección de infraestructuras críticas cibernéticas y servicios esenciales se ha venido consolidando a través de una trayectoria de política pública que va desde los Lineamientos de Ciberseguridad y Ciberdefensa (CONPES 3701 de 2011)[144], pasando por la Política Nacional de Seguridad Digital (CONPES 3854 de 2016)[145] y la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020)[146], hasta la Estrategia Nacional de Seguridad Digital 2025-2027[147] liderada por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que actualiza la visión país en gobernanza, resiliencia, promueve la cooperación multisectorial y alinea las acciones nacionales con estándares y buenas prácticas internacionales. Estos instrumentos subrayan la seguridad digital como condición habilitante para la competitividad y la confianza, con enfoque en gestión de riesgos y participación de múltiples partes interesadas.

En cuanto al CONPES 4144 de 2025[148] (Política de IA), su relación con infraestructuras críticas cibernéticas es transversal: aborda gobernanza, infraestructura tecnológica y gestión de riesgos de IA como habilitadores del ecosistema digital, pero no sustituye las políticas específicas de seguridad digital.

---

[142] Secretaría de Innovación Pública. (2023). Se aprobó la segunda Estrategia Nacional de Ciberseguridad. Gobierno de la República Argentina. Disponible en: https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad

[143] Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2022). Decreto 338 de 2022: Por el cual se adiciona el Título 21 al Decreto Único 1078 de 2015 en materia de seguridad digital. Disponible en: https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0338_2022.htm

[144] Departamento Nacional de Planeación (DNP). CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

[145] Departamento Nacional de Planeación (DNP). CONPES 3854 de 2016: Política Nacional de Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf

[146] Departamento Nacional de Planeación (DNP). CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[147] Presidencia de la República (2025). Estrategia Nacional de Seguridad Digital 2025-2027. Disponible en: https://mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

[148] Departamento Nacional de Planeación (DNP). (2025). CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

La protección de infraestructuras críticas no solo es un asunto técnico, sino también estratégico y multisectorial. Por ello, se promueve la colaboración entre las múltiples partes interesadas, en la interpretación y aplicación de los lineamientos normativos que permita establecer condiciones para el desarrollo eficiente de alianzas que favorecen la seguridad digital del país y sus habitantes, aumentando la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital[149]. Asimismo, la cooperación internacional con organismos como la OEA, la OCDE y la UIT refuerza la capacidad nacional para responder a amenazas transnacionales que impactan directamente a las infraestructuras críticas digitales.

En este escenario, el reto para Colombia radica en avanzar hacia un modelo integral de protección y resiliencia de infraestructuras críticas digitales, que no solo contemple la gestión de incidentes, sino también la anticipación de riesgos, la interoperabilidad entre sectores y la construcción de confianza en el ecosistema digital.

5.2.1. **Marco normativo colombiano**. El abordaje normativo de las infraestructuras críticas cibernéticas en Colombia se ha desarrollado en el marco de una evolución gradual de las políticas de seguridad digital, a partir de los desafíos generados por la transformación digital del Estado, la dependencia tecnológica de sectores estratégicos y la necesidad de fortalecer la resiliencia nacional frente a amenazas cibernéticas.

A continuación, se presentan los principales instrumentos normativos y de política pública que han definido el marco de acción nacional:

5.2.1.1. Documento CONPES 3701 de 2011[150]: Lineamientos de Política para la Ciberseguridad y Ciberdefensa:

- Fue el primer instrumento de política pública que propuso lineamientos para la ciberseguridad y la ciberdefensa a nivel nacional.
- Introdujo la necesidad de articular esfuerzos civiles y militares para la protección del ciberespacio.
- Implementa instancias encargadas de prevenir, coordinar, atender, controlar, recomendar y regular los incidentes o emergencias cibernéticas.
- Presentó como uno de sus objetivos específicos conformar organismos con capacidad técnica y operativa para la defensa y seguridad en materia de seguridad digital.
- Propuso la creación de un equipo de respuesta a incidentes y la articulación de una red nacional de respuesta.

[149] Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2022). Decreto 338 de 2022: Por el cual se adiciona el Título 21 al Decreto Único 1078 de 2015 en materia de seguridad digital. Disponible en: https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0338_2022.htm

[150] Departamento Nacional de Planeación (DNP). CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5.2.1.2. Documento CONPES 3854 de 2016[151]: Política Nacional de Seguridad Digital

- Establece la Política Nacional de Seguridad Digital, creando condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital y se genere confianza en el entorno digital.
- Propone un cambio de paradigma respecto a la política anterior de ciberseguridad y ciberdefensa (CONPES 3701 de 2011), que se centraba en la defensa nacional y la lucha contra el cibercrimen. Este nuevo documento incorpora la gestión de riesgos como eje central, reconociendo que el entorno digital afecta no solo al Estado, sino también a ciudadanos, empresas y organizaciones. Se busca que todos los actores involucrados (múltiples partes interesadas) participen activamente en la identificación, tratamiento y mitigación de riesgos digitales.
- Describe cuatro principios fundamentales y cinco dimensiones estratégicas. Los principios son: salvaguardar los derechos humanos y los valores fundamentales, adoptar un enfoque incluyente y colaborativo, asegurar una responsabilidad compartida entre las múltiples partes interesadas y adoptar un enfoque basado en la gestión de riesgos. Las dimensiones estratégicas son: gobernanza de la seguridad digital, marco legal y regulatorio, gestión sistémica y cíclica del riesgo, cultura ciudadana para la seguridad digital y fortalecer capacidades para la gestión del riesgo.
- Define mecanismos estratégicos para impulsar cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional.
- Propone fortalecer las capacidades institucionales (como las del COLCERT) y promueve el desarrollo de marcos sectoriales.
- Marca el inicio formal de la identificación de activos críticos del Estado, sentando las bases para la definición de infraestructuras críticas cibernéticas.

5.2.1.3. Documento CONPES 3995 de 2020[152]: Política Nacional de Confianza y Seguridad Digital

- Define la Política Nacional de Confianza y Seguridad Digital, orientada a establecer medidas para desarrollar la confianza digital mediante la mejora de la seguridad digital en el país.
- Plantea como objetivo que Colombia sea una sociedad incluyente y competitiva en el futuro digital, a través del fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital.
- Fortalece el enfoque en gestión de riesgos, resiliencia y cooperación público-privada.
- Reconoce la necesidad de articular al sector productivo en la protección de activos esenciales.
- Introduce el concepto de «confianza digital», en el que las infraestructuras críticas desempeñan un papel central para la estabilidad económica y social.

[151] Departamento Nacional de Planeación (DNP). CONPES 3854 de 2016: Política Nacional de Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf
[152] Departamento Nacional de Planeación (DNP). (2020) CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Promueve la adopción de modelos con énfasis en nuevas tecnologías para mejorar la seguridad y confianza digital.

5.2.1.4. Documento CONPES 4144 de 2025[153]: Política Nacional para el Desarrollo y Uso de la Inteligencia Artificial

- Aunque su enfoque principal es la IA, identifica riesgos asociados al uso indebido de esta tecnología sobre sistemas críticos.

- Establece principios de seguridad y robustez técnica que pueden impactar directamente en la protección de infraestructuras críticas cibernéticas en sectores automatizados.

5.2.1.5. Decreto 338 de 2022: Es un instrumento fundamental para la gestión de infraestructuras críticas cibernéticas en el país, a continuación, se presentan los puntos más importantes:

- Objeto y alcance general

  El Decreto 338 de 2022 adiciona el Título 21 al Decreto 1078 de 2015 para establecer los lineamientos generales de: gobernanza de la seguridad digital, identificación de infraestructuras críticas cibernéticas (ICC) y servicios esenciales, gestión de riesgos y respuesta a incidentes de seguridad digital.

  Sus disposiciones son obligatorias para las entidades de la Administración Pública y para particulares que ejercen funciones públicas; los privados que gestionan ICC o servicios esenciales pueden acogerse de manera voluntaria siempre que no contraríen su régimen propio.

- Definiciones básicas del régimen colombiano de ICC

  Define infraestructura crítica cibernética como sistemas y activos (físicos o virtuales) soportados por TIC cuya afectación significativa tendría un impacto grave en el bienestar social o económico, o en el funcionamiento efectivo del gobierno o la economía.

  Define servicio esencial como aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país que depende de las TIC y cuya afectación puede generar daños significativos y paralizar dichas actividades.
  Introduce formalmente la gobernanza de la seguridad digital, el Modelo de Gobernanza de Seguridad Digital y el concepto de múltiples partes interesadas.

- Principios rectores para la protección de ICC y servicios esenciales

[153] Departamento Nacional de Planeación (DNP). (2025). CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Establece principios específicos como: confianza, coordinación, colaboración entre múltiples partes interesadas, cooperación, enfoque basado en riesgos, gradualidad, inclusión, proporcionalidad, salvaguarda de derechos humanos y uso eficiente de la infraestructura y recursos para la protección de ICC y servicios esenciales.

- Modelo de gobernanza de seguridad digital

  Obliga a las autoridades a adoptar el Modelo de Gobernanza de la Seguridad Digital, con el objetivo de fortalecer la seguridad digital, la protección de redes, ICC, servicios esenciales y sistemas de información.

  El modelo se estructura en tres niveles: estratégico (políticas y prioridades), táctico (planes, procesos, coordinación) y operacional (implementación de actividades y tareas rutinarias de seguridad digital). Ver Gráficos 5.1 y 5.2.

Gráfico 5.1 Decreto 338 de 2022. Niveles del Modelo de Gobernanza de la Seguridad Digital.

Fuente: Elaboración propia.

Gráfico 5.2 Decreto 338 de 2022. Instancias de decisión del Modelo de Gobernanza de la Seguridad Digital.

Fuente: Elaboración propia.

- Instancias institucionales de gobernanza

  Crea e institucionaliza cinco instancias: Coordinación Nacional de Seguridad Digital, Comité Nacional de Seguridad Digital, Grupos de Trabajo de Seguridad Digital, Mesas de Trabajo de Seguridad Digital y Puestos de Mando Unificado (PMU) de Seguridad Digital. Ver Gráfico 5.2.

  El Coordinador Nacional de Seguridad Digital, designado por el Presidente, es responsable de coordinar la agenda de seguridad digital del Gobierno Nacional y de articular prioridades e iniciativas.

  El Comité Nacional de Seguridad Digital es la instancia de coordinación interinstitucional de alto nivel para impulsar la política de seguridad digital, proteger ICC y servicios esenciales y articular la respuesta ante incidentes graves.

- Identificación e inventario de ICC y servicios esenciales

  Establece tres criterios acumulativos para determinar si una actividad o servicio es esencial: (1) la actividad es fundamental para el mantenimiento de actividades sociales o económicas o se basa en información estratégica; (2) la prestación depende de TIC y redes/sistemas de información; y (3) un incidente tendría efectos significativos en su prestación.

Ordena al MinTIC, dentro de los 12 meses siguientes a la expedición del decreto, definir la metodología de levantamiento del inventario de ICC y servicios esenciales a cargo de las autoridades, incorporando mejores prácticas y un mecanismo para seleccionar a los representantes sectoriales ante el Comité Nacional.

Las autoridades identificadas como titulares de ICC o prestadoras de servicios esenciales deben vincularse formalmente ante COLCERT, siguiendo lineamientos y estándares que el MinTIC defina.

- Gestión de incidentes y CSIRT

  Crea y regula el CSIRT-GOBIERNO, encargado de apoyar a todas las autoridades en las fases de prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje frente a incidentes de seguridad digital.

  Prevé la conformación y acompañamiento de CSIRT sectoriales y CSIRT de sectores críticos, y ordena la adopción de un protocolo nacional de cooperación y coordinación entre CSIRT, con roles, responsabilidades, canales de comunicación y tiempos de respuesta definidos.

  Encarga al MinTIC la definición del Modelo Nacional de Atención y Gestión de incidentes de seguridad digital, alineado con la política de Gobierno Digital.

- Plataforma Nacional de Notificación y Seguimiento de Incidentes

  Ordena que el MinTIC, a través de COLCERT, ponga en marcha una Plataforma Nacional de Notificación y Seguimiento de Incidentes de Seguridad Digital, disponible para prestadores de servicios esenciales, titulares de ICC, autoridades y CSIRT sectoriales.

  La plataforma debe garantizar disponibilidad, autenticidad, integridad y confidencialidad de la información, soportar el intercambio de información sobre incidentes y ciberamenazas, análisis de muestras, registro de vulnerabilidades, comunicaciones seguras, intercambio masivo de datos y generación de estadísticas e informes agregados.

- Responsabilidades generales de las autoridades

  Obliga a las autoridades a adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos, la identificación y reporte de ICC y servicios esenciales, y la gestión y respuesta a incidentes.

  Pide expresamente que los reguladores y supervisores evalúen la necesidad de normas e instrucciones sectoriales específicas para protección de ICC y servicios esenciales, reforzando la dimensión sectorial del esquema.

5.2.1.6. Estrategia Nacional de Seguridad Digital 2025–2027. Documento que se presenta como una respuesta integral y proactiva del Coordinador Nacional de Seguridad Digital colombiano para enfrentar los crecientes desafíos en materia de ciberseguridad. Se construye sobre los cimientos de políticas públicas previas, como los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020, y tiene como objetivo fortalecer y consolidar un entorno digital seguro, confiable y resiliente. Los puntos principales, a continuación:

- Propósito y objetivo general:

  Busca «fortalecer y consolidar un entorno digital seguro, confiable y resiliente en Colombia» que apoye el desarrollo económico, la inclusión social y la innovación tecnológica, con énfasis explícito en la protección de infraestructuras críticas cibernéticas y servicios esenciales y en la garantía de la privacidad, integridad, disponibilidad y seguridad de la información.

  Establece acciones dirigidas a todos los sectores de la economía y la sociedad (administración pública, industria, ciudadanía) para alcanzar el objetivo general y los objetivos específicos.

- Principios orientadores

  Enfoque multisectorial y colaborativo: La estrategia se rige por principios como coordinación, colaboración y cooperación multisectorial, promoviendo la interacción entre sector público, privado, academia y sociedad civil, a nivel nacional e internacional, para compartir información, recursos y buenas prácticas.

  Resiliencia basada en gestión de riesgos: Introduce la resiliencia como capacidad de anticipar, resistir, recuperarse y adaptarse a las amenazas cibernéticas, con un enfoque explícito de gestión de riesgos para proteger infraestructuras críticas cibernéticas y servicios esenciales.

  Innovación, talento y transparencia: Promueve la innovación tecnológica, la formación continua en seguridad digital y la investigación en soluciones avanzadas, junto con principios de transparencia y confianza digital, rendición de cuentas y participación ciudadana en la formulación y evaluación de políticas.

- Ejes estratégicos y objetivos específicos. La Estrategia se estructura en cuatro grandes áreas que responden a las principales brechas identificadas en Colombia.

  Consolidar la gobernanza de seguridad digital. Propone fortalecer la gobernanza nacional mediante:
  - Creación de una entidad nacional especializada para planificar, coordinar y hacer seguimiento a la seguridad digital.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Revisión y adecuación del Modelo de Gobernanza de Seguridad Digital del Decreto 338 de 2022, incorporando principios de igualdad de género y enfoque diferencial, y ajustándolo al nuevo contexto nacional e internacional.

Mejorar la ciberresiliencia nacional. Aborda de manera directa la vulnerabilidad ante amenazas cibernéticas sofisticadas, buscando fortalecer capacidades técnicas, procesos de prevención, detección, respuesta y recuperación en todo el ecosistema digital (con foco en ICC y servicios esenciales).

Desarrollar una fuerza laboral robusta en seguridad digital. Plantea acciones para enfrentar la escasez de talento especializado, promoviendo formación, certificación, diversidad e inclusión en perfiles de seguridad digital.

Adaptar y adecuar el marco normativo cibernético. Propone actualizar el marco legal para responder a amenazas emergentes, mejorar la persecución del cibercrimen y alinear la regulación de privacidad y protección de datos con estándares internacionales.

- Protección de infraestructuras críticas cibernéticas

ICC y servicios esenciales como foco explícito. La Estrategia reconoce de forma expresa que la protección de infraestructuras críticas cibernéticas y servicios esenciales es un componente central de un entorno digital seguro y confiable.

Articulación con el modelo de gobernanza del Decreto 338 de 2022. Ordena revisar el Modelo de Gobernanza de Seguridad Digital del Decreto 338 de 2022 para adaptarlo al contexto actual de ciberseguridad, reforzando la protección de ICC y servicios esenciales y alineando la gobernanza con principios de equidad de género y enfoque diferencial.

Articulación con planes sectoriales. Prevé acciones para mejorar la coordinación con planes y estrategias sectoriales, de manera que la gestión de riesgos sobre ICC y servicios esenciales quede incorporada de forma coherente en los sectores críticos.

- Dimensión normativa y actualización legal

Revisión del marco legal de seguridad digital y ciberdelito. Incluye una Línea de Acción 4.1–4.2 dedicada a actualizar y fortalecer el marco legal en materia de seguridad digital, cumplir con el Convenio de Budapest y robustecer la persecución del cibercrimen, así como adaptar el marco sustantivo y procesal frente a nuevas amenazas.

Protección de datos y privacidad en tecnologías emergentes. Prevé regulaciones específicas para la protección de datos y privacidad en tecnologías como IA y aprendizaje automático,

incluyendo mitigación de sesgos y discriminación algorítmica, y nuevas reglas de responsabilidad ejecutiva en seguridad digital.

Cloud y nube pública gubernamental. Ordena actualizar el marco de seguridad para la adopción de tecnologías *cloud* en el sector público, con énfasis en la nube pública gubernamental, lo que impacta directamente la gestión segura de activos y servicios críticos digitalizados

- Implementación

  Plan de acción con indicadores y responsables. La Estrategia se implementa a través de un plan de acción que asocia cada línea de acción con: número de acción, indicador de producto, método de medición, clasificación, plazo y entidad responsable, lo que permite seguimiento y rendición de cuentas.

  Compromiso de recursos y cultura de seguridad. El documento enfatiza que Colombia reconoce las amenazas como una realidad presente y no un riesgo futuro, y se compromete a asignar recursos gubernamentales, establecer alianzas y promover una cultura de seguridad digital en el sector público.

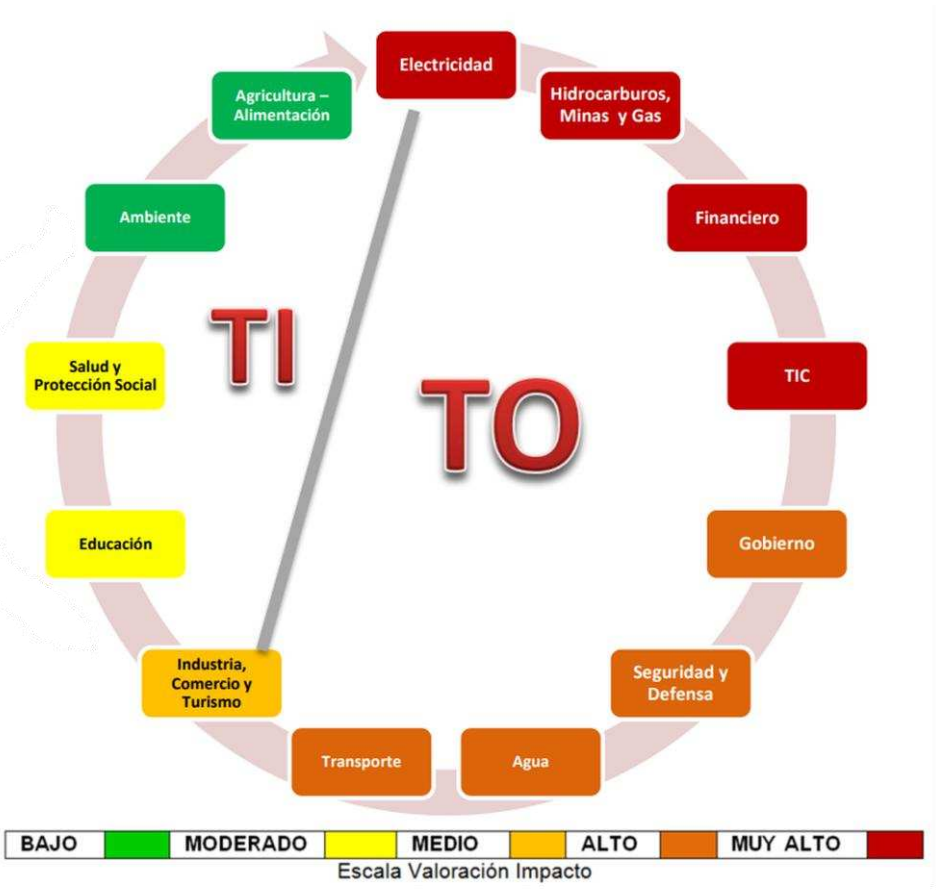
5.2.1.7. Lineamientos para la identificación de infraestructuras críticas cibernéticas (ICC)[154]. Los Lineamientos para la identificación de infraestructuras críticas cibernéticas se emiten en desarrollo del Decreto 338 de 2022 y del Modelo de Seguridad y Privacidad de la Información (MSPI). Su propósito es unificar criterios para que las entidades públicas (y, como referente, las privadas) identifiquen, clasifiquen y reporten sus infraestructuras críticas cibernéticas y los servicios esenciales que soportan, facilitando la construcción del inventario nacional y el diseño de medidas de resiliencia. Los puntos clave, a continuación:

- Objetivo y alcance. Establecen criterios mínimos de reporte y una metodología práctica para que propietarios y operadores identifiquen ICC, evalúen los riesgos asociados y definan acciones de mejora en resiliencia, tanto en entidades públicas como privadas.

- Se basa en sectores críticos y catálogo previo. Retoman el trabajo del Catálogo de Infraestructura Crítica Cibernética y organizan el análisis en 13 sectores críticos (alimentación y agricultura, agua, comercio–industria–turismo, defensa, educación, electricidad, financiero, gobierno/Estado, recursos naturales–medio ambiente, recursos minero-energéticos, salud y protección social, TIC y transporte), resaltando la interdependencia entre ellos. Ver Gráfico 5.3.

[154] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Lineamientos para la identificación de las infraestructuras críticas cibernéticas. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401778_recurso_1.pdf

Gráfico 5.3 Infraestructuras Críticas Cibernéticas en Colombia.



Fuente: Comando Conjunto Cibernético[155]

- Metodología «paso a paso». Proponen un ciclo estructurado que incluye: identificar funciones y servicios esenciales; mapear los activos TIC que los soportan; recopilar y analizar información; evaluar impacto y criticidad; y documentar y reportar las ICC para su incorporación en el inventario nacional.

[155] Giraldo Gallo, J. F. (2016). Infraestructuras críticas cibernéticas en Colombia [Diapositivas de PowerPoint]. Comando Conjunto Cibernético (CCOC). Disponible en: https://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticas-ciber-en-colombia.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Escala de criticidad y clasificación. Introducen una escala de criticidad que distingue entre: Infraestructura crítica cibernética (ICC), servicios esenciales, servicios importantes y activos secundarios, en función del impacto y del tiempo de indisponibilidad, para orientar la priorización de controles y recursos.

- Actualización metodológica y alineación con el MSPI. Incorporan mejoras como el etiquetado explícito de ICC, la actualización de la clasificación de activos, la identificación de operadores y redes de operación, el análisis de interdependencias entre sectores, y la armonización con la gestión inventario clasificación de activos de infraestructura crítica cibernética del MSPI.

- Enfoque de derechos y resiliencia. Vinculan la protección de ICC con la garantía de derechos fundamentales (información, seguridad, igualdad y no discriminación) y subrayan que la identificación de ICC debe conducir a medidas proactivas de resiliencia, manteniendo un equilibrio adecuado entre ciberseguridad y libertades.

Este marco normativo demuestra un proceso progresivo de maduración institucional en Colombia hacia la protección de las infraestructuras críticas cibernéticas. Sin embargo, aún persisten desafíos relacionados con la coordinación multisectorial, y la implementación efectiva de mecanismos de evaluación y respuesta ante riesgos cibernéticos complejos.

5.2.1.8. Normas complementarias de carácter sectorial y transversal:

- Ley 1341 de 2009 (modificada por la Ley 1978 de 2019): reconoce a las telecomunicaciones como un servicio público esencial y promueve su continuidad, resiliencia y libre elección del proveedor.
- Ley 1621 de 2013: define disposiciones sobre inteligencia y contrainteligencia, enfocadas en la protección de la seguridad nacional, incluyendo infraestructura crítica.
- Decreto 1083 de 2015 y Decreto 1499 de 2017 (MIPG): establecen el marco de referencia para la gestión y el desempeño institucional de las entidades públicas, incluyendo la obligación de gestionar riesgos que afectan la continuidad de los servicios a cargo del Estado, lo cual es relevante para servicios esenciales soportados en TIC.
- Lineamientos de la Superintendencia Financiera y del sector energético: establecen normas técnicas y operativas para la continuidad y protección de sistemas considerados críticos (p. ej., circular externa 007 de 2018 en el sector financiero).

5.3. PLANES Y PROGRAMAS DE REFERENCIA

Para cerrar este capítulo es importante mencionar que, la protección de las infraestructuras críticas cibernéticas no descansa en un único estándar, sino en un ecosistema de normas, marcos de gestión y *playbooks* operativos que se complementan entre sí. La Tabla 5.1 resume los principales referentes internacionales utilizados por operadores, autoridades competentes y organismos reguladores para gestionar el riesgo, garantizar la continuidad de los servicios esenciales y responder a incidentes y crisis

que afecten a las infraestructuras críticas cibernéticas. Los estándares se organizan por tipo de plan o programa, ofreciendo una visión integrada que permite identificar qué marco resulta más pertinente según el objetivo de gestión y el nivel (estratégico, táctico u operativo) en el que se interviene.

Tabla 5.1. Planes y programas para la protección de infraestructuras criticas cibernéticas.

TIPO DE PLAN / PROGRAMA	ALCANCE	FRAMEWORKS / PLAYBOOKS PRINCIPALES
Programa de Ciberseguridad / Sistema de Gestión de Seguridad de la Información SGSI (ISMS)	Gobierno integral de la ciberseguridad y gestión de riesgos en toda la organización, incluyendo activos e infraestructuras críticas.	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 31000, NIST Cybersecurity Framework (CSF), NIST SP 800-53, COBIT.
Business Continuity Plan (BCP)	Operaciones transversales y continuidad de servicios esenciales ante interrupciones graves (incluyendo ICC).	ISO 22301, ISO 22313, ISO/IEC 27031, NFPA 1600/1660, NIST CSF (función Recover).
Disaster Recovery Plan (DRP)	Recuperación de infraestructura y servicios TI que soportan procesos críticos e ICC (*data centers*, redes, plataformas críticas).	ISO/IEC 27031, NIST SP 800-34, ISO 22301, guías de proveedores *cloud* alineadas con estos marcos.
Incident Response Plan (IRP)	Respuesta operativa a incidentes de ciberseguridad (detección, análisis, contención, erradicación, lecciones aprendidas).	ISO/IEC 27035, NIST SP 800-61, CISA Cybersecurity Incident & Vulnerability Response Playbooks, SANS Incident Handler's Handbook.
Crisis Management Plan (CMP)	Coordinación ejecutiva y estratégica de crisis que afectan infraestructuras críticas y servicios esenciales.	ISO 22361, buenas prácticas ENISA para gestión de crisis y ejercicios de respuesta, Directiva NIS2 (requisitos de gestión de incidentes y coordinación).
Cyber Crisis Mgmt Playbook	Operación táctica de la crisis de ciberseguridad (SOC, CSIRT, equipos de continuidad) cuando el incidente escala a crisis.	Playbooks de ENISA y CISA, NIST CSF (Detect / Respond / Recover), playbooks SOC propietarios.
Ransomware BCP/DRP u otros planes específicos de amenaza	Respuesta y recuperación frente a amenazas prioritarias (*ransomware*, DDoS, sabotaje de ICS, etc.) con foco en mantener operativas las ICC.	Guías de CISA y NCSC UK sobre *ransomware*, buenas prácticas sectoriales basadas en ISO 22301, ENISA Threat

TIPO DE PLAN / PROGRAMA	ALCANCE	FRAMEWORKS / PLAYBOOKS PRINCIPALES
		Landscape & sectoral good practices.
Emergency Communication Plan	Comunicación interna y externa durante incidentes y crisis (autoridades, CERT/CSIRT nacional, reguladores, ciudadanía, medios).	ISO 22301 (comunicación en continuidad), ISO 22361 (comunicación en crisis), guías nacionales de comunicación de emergencias, orientaciones ENISA/NIS2 sobre notificación de incidentes.
Programa de Ciberseguridad OT/ICS	Protección de sistemas de control industrial (SCADA, PLC, IACS) que operan infraestructuras críticas (energía, agua, transporte, manufactura crítica, etc.).	IEC 62443 (serie completa), NIST SP 800-82, ISO/IEC 27019 (sector eléctrico y utilities), NERC CIP.
Programa de Seguridad en Telecom y Servicios TIC Críticos	Operación segura de redes de telecomunicaciones y servicios *cloud* que soportan servicios esenciales (p. ej. servicios públicos, financiero, salud).	ISO/IEC 27011 (operadores de telecom), ISO/IEC 27017 y 27018 (seguridad y protección de datos en la nube), ISO/IEC 20000-1, ITIL.
Gestión de amenazas y pruebas de seguridad	Modelado de amenazas, *threat hunting*, validación de coberturas de control, ejercicios de *red-teaming* sobre ICC.	MITRE ATT&CK, MITRE D3FEND, ENISA Threat Landscape, marcos de red-teaming y purple-teaming.
Marco regulatorio de infraestructuras críticas cibernéticas	Identificación de ICC/servicios esenciales, requisitos mínimos de seguridad y resiliencia, supervisión y reporte de incidentes.	Directiva NIS2, Directiva CER, Reglamento DORA (financiero), National Infrastructure Protection Plan (NIPP, EE. UU.), estrategias y marcos nacionales equivalentes.

Fuente: Elaboración propia.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6. CIBERDEFENSA INTELIGENTE

La asimetría entre la velocidad de ejecución de los ataques y los tiempos de respuesta defensiva se evidencia en las métricas operativas. Los grupos criminales, con estructuras aproximadas de 50 integrantes, son capaces de materializar una fuga de información en cerca de 48 minutos. En contraste, los equipos defensivos, habitualmente integrados por entre 12 y 20 analistas SOC, requieren en promedio 21 días para detectar un compromiso y entre 6 y 12 horas adicionales para contener y erradicar la intrusión.

Esta brecha, donde los atacantes avanzan en minutos mientras las defensas responden en días o semanas, refleja tanto la creciente sofisticación de las amenazas como las limitaciones de las capacidades de monitoreo tradicionales. Por ello, resulta imprescindible adoptar herramientas inteligentes de defensa para fortalecer las capacidades de anticipación y respuesta.

En este marco de la ciberdefensa, tres componentes emergen como pilares esenciales: las redes colaborativas, que permiten compartir información y alertas de manera oportuna; la inteligencia de amenazas, que permite estructurar y acelerar el intercambio de información accionable; y el papel estratégico de la inteligencia artificial, que aporta analítica avanzada y automatización. Estos componentes, desarrollados a continuación, constituyen la base de una defensa inteligente capaz de responder con mayor eficacia al ritmo del adversario.

Gráfico 6.1 Métricas Globales en Ataques y Defensa Cibernética

Fuente: Elaboración propia a partir de datos de CrowdStrike Global Threat Report 2024. https://www.crowdstrike.com

6.1 REDES COLABORATIVAS

En un contexto de creciente sofisticación y diversificación de las amenazas, las redes colaborativas de ciberseguridad son elementos esenciales para fortalecer la resiliencia y la defensa, al permitir que múltiples actores coordinen capacidades, articulen respuestas y anticipen escenarios de ataque. El intercambio sistemático de información crítica, como indicadores de compromiso, alertas tempranas, tácticas emergentes y análisis de incidentes, permite que una amenaza identificada por un miembro de la comunidad sea rápidamente evaluada, contextualizada y comunicada al resto, reduciendo la posibilidad de propagación y acelerando la contención.

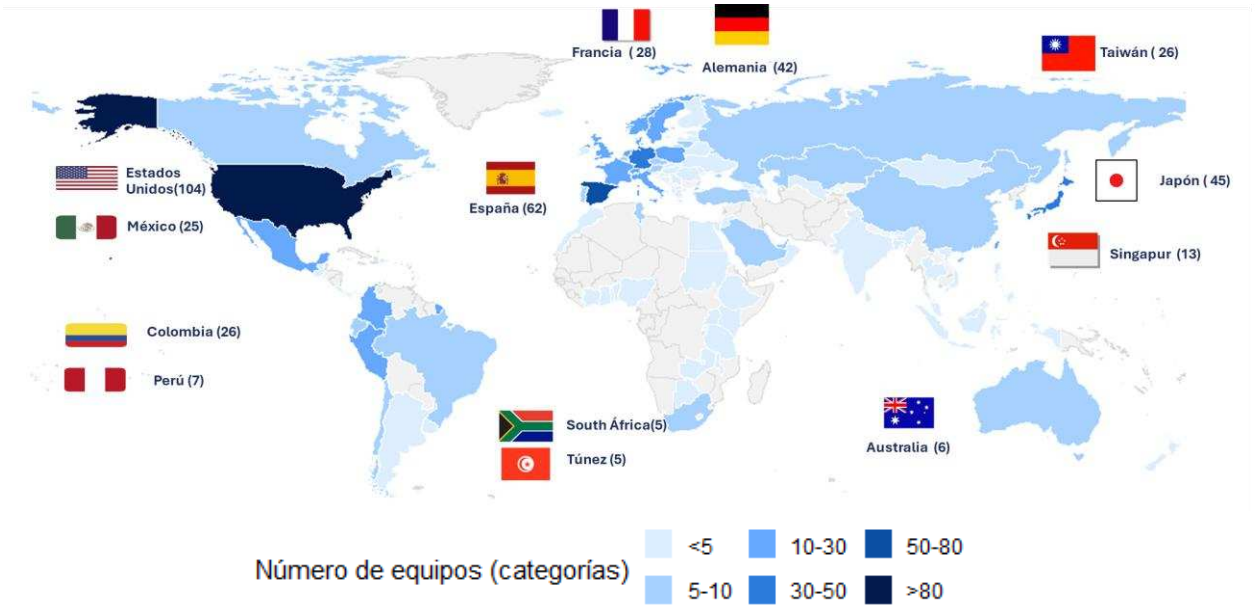
En este ecosistema, los CSIRT y Centros de Operaciones de Seguridad (SOC) o grupos ciberseguridad de las organizaciones actúan como nodos operativos clave, responsables de procesar, correlacionar y transformar la información proveniente de redes y plataformas colaborativas en acciones tácticas de detección, análisis y respuesta. La integración con estas plataformas les permite reforzar sus capacidades de monitoreo con indicadores validados, contextualizar eventos locales dentro de patrones globales de amenaza, identificar campañas distribuidas en fases tempranas y ajustar sus criterios de correlación y priorización de acciones, orientando los esfuerzos hacia bloqueos, contenciones o erradicaciones según el nivel de riesgo y el impacto potencial.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Este conjunto de redes globales, regionales y sectoriales proporciona la infraestructura colaborativa que permite a los SOC anticipar ataques, mejorar su capacidad analítica y fortalecer la defensa colectiva. A continuación, se presentan el Gráfico 6.2 correspondientes a FIRST uno de los ecosistemas de colaboración más representativos dentro de este modelo.

A escala global, FIRST (*Forum of Incident Response and Security Teams*) se constituye como una de las comunidades de mayor cobertura internacional, con 818 equipos distribuidos en 113 países, integrando CSIRT y SOC de sectores públicos, privados y académicos. El siguiente mapa muestra la distribución geográfica de los equipos miembros, evidenciando distintos niveles de madurez y capacidad de respuesta entre regiones. América del Norte, liderada por Estados Unidos, concentra el mayor número de equipos a nivel mundial. Europa conforma el bloque más equilibrado, con España, Alemania y Francia entre los países más activos dentro de la red. En Asia-Pacífico, se destacan países con capacidades avanzadas en ciberdefensa como Japón, Taiwán, Singapur. En América Latina, la participación continúa en expansión, destacándose Colombia y México, aunque aún con menos presencia en comparación con los otros continentes.

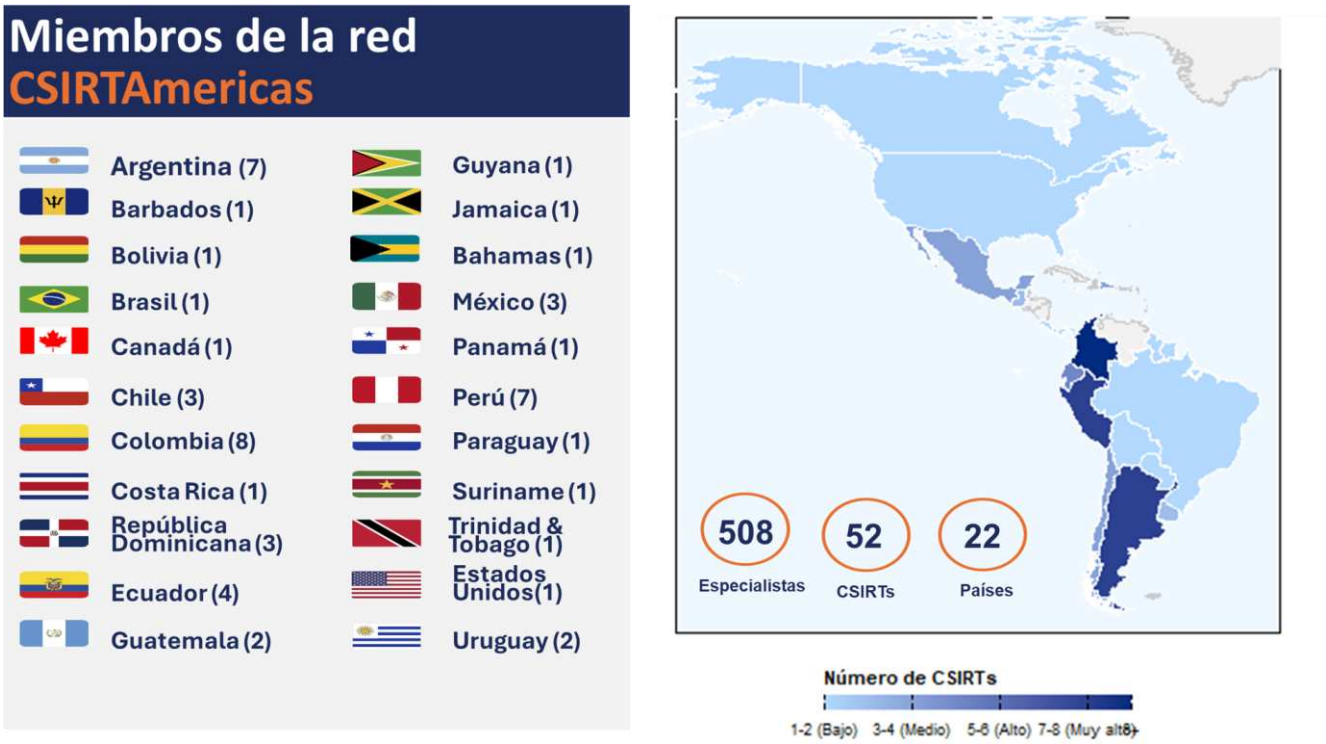
Gráfico 6.2 Distribución global de los equipos de respuesta a incidentes participantes en FIRST



Fuente: Elaboración propia a partir de datos de FIRST. https://www.first.org/members/map

En el plano regional, se destaca la Red gubernamental de CSIRT Américas[156], administrada y coordinada por la OEA, la cual reúne a más de 20 países para articular respuestas conjuntas frente a amenazas que afectan infraestructuras estratégicas del hemisferio. La red está integrada exclusivamente por CSIRTs oficiales del sector gubernamental de los Estados Miembros de la OEA que cuentan con un mandato formal para gestionar incidentes cibernéticos. En este contexto, Colombia cuenta actualmente con ocho[157] CSIRTs oficiales registrados en la Red CSIRT Américas, lo que evidencia un avance significativo en la organización institucional y el fortalecimiento gubernamental de sus capacidades de respuesta ante incidentes cibernéticos.

Gráfico 6.3 Número de miembros de CSIRTAmericas



Fuente. Elaboración propia a partir de datos de CSIRTAmericas. https://csirtamericas.org/es

[156] Disponible en: https://csirtamericas.org/es
[157] Los CSIRT incluidos son: COCIB;CSIRT Aeronáutico; CSIRT-CCOCI, CSIRT-Defensa Colombia; CSIRT-EJC; CSIRT-PONAL;CSIRT-PRESIDENCIA;ColCERT

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En el sector de telecomunicaciones destacan redes de cooperación diseñadas para reforzar la ciberseguridad. La principal es GSMA T-ISAC[158], el centro global donde los operadores móviles comparten inteligencia sobre amenazas. A través de esta plataforma, se reciben y distribuyen alertas tempranas, se analizan campañas dirigidas y se coordina la respuesta ante incidentes que afectan redes y servicios móviles, como redes 4G/5G, IMS, Core y servicios de *roaming*, permitiendo anticipar riesgos y fortalecer la defensa colectiva del sector.

6.1.1. Inteligencia de amenazas. Ciclo de vida y mecanismos técnicos para intercambio de información. En el ecosistema de ciberseguridad, el intercambio de información solo es posible gracias a un conjunto de actividades, estándares y plataformas técnicas que permiten estructurar, clasificar y automatizar los flujos de información de inteligencia de inteligencia de amenazas entre organizaciones. El ciclo de vida de la inteligencia de amenazas es un proceso utilizado en ciberseguridad para la recopilación, el procesamiento, el análisis y la aplicación de información sobre amenazas potenciales y activas[159].

De acuerdo con IBM Security (2024)[160], este ciclo comprende seis fases:

6.1.1.1. Planificación y dirección: En esta fase, los operadores móviles o sus SOC definen los objetivos y necesidades de inteligencia. Esto incluye priorizar amenazas relevantes, como ataques a la infraestructura Core 5G, campañas dirigidas contra infraestructuras críticas o actividades maliciosas relacionadas con señalización y redes móviles.

6.1.1.2. Recolección: En esta fase se obtienen datos relevantes de fuentes internas y externas. Entre las principales fuentes se incluyen:

- Redes colaborativas de intercambio de información: CSIRT nacionales, sectoriales o internacionales.
- Telemetría interna: registros provenientes de SIEM, XDR/EDR, logs de red y sondas de monitoreo para 4G/5G.
- Boletines técnicos de proveedores especializados y agencias de ciberseguridad.
  Para habilitar el intercambio estructurado y automatizado de datos, se emplean estándares ampliamente adoptados en ciberseguridad:
  - STIX (*Structured Threat Information Expression*): formato estándar para representar indicadores de compromiso (IoC), tácticas, técnicas, actores de amenaza y campañas.
  - TAXII (Trusted Automated eXchange of Intelligence Information): protocolo para transportar de manera segura información expresada en STIX.

6.1.1.3. Procesamiento: Esta fase se encarga de depurar, normalizar y clasificar los datos para que puedan ser utilizados en el análisis. Esto incluye eliminar duplicados, filtrar falsos positivos y estructurar los elementos relevantes. Para contextualizar adecuadamente la información procesada, se utilizan

[158] Disponible en: https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/
[159] Methods and Methodology: The Intelligence Lifecycle. Disponible en: https://www.first.org/global/sigs/cti/curriculum/methods-methodology
[160] What is threat intelligence?. Disponible en: ttps://www.ibm.com/think/topics/threat-intelligence

marcos de referencia como MITRE ATT&CK[161], que permiten mapear tácticas, técnicas y procedimientos de amenazas conocidas.

6.1.1.4. Análisis: En esta fase, la información procesada se convierte en inteligencia accionable mediante correlación, contextualización y evaluación del riesgo. Las plataformas de análisis y los motores de correlación —incluidos los SIEM y sistemas de inteligencia— integran fuentes diversas para identificar patrones, priorizar amenazas y generar alertas o recomendaciones útiles para la toma de decisiones.

6.1.1.5. Difusión: Los productos de inteligencia se distribuyen a los equipos responsables según su sensibilidad, utilizando esquemas como TLP (*Traffic Light Protocol*)[162] para controlar su divulgación. La inteligencia generada puede integrarse con herramientas de automatización y respuesta (como SOAR o XDR), que utilizan esta información para generar alertas, priorizar riesgos o ejecutar acciones automáticas de mitigación.

En conjunto, estos estándares y plataformas constituyen la infraestructura técnica que hace posible la cooperación entre redes como FIRST, CSIRT Américas y GSMA T-ISAC, y permiten que los equipos SOC no solo accedan a inteligencia global en tiempo real, sino que también la integren, analicen y usen de forma eficiente para fortalecer la resiliencia de sus redes.

En este mismo contexto de cooperación, el *Mobile Cybersecurity Knowledge Base* (MCKB)[163] de la GSMA se convierte en un complemento estratégico para los operadores móviles. Mientras las redes colaborativas permiten compartir inteligencia, alertas y análisis en tiempo real, el MCKB ofrece el marco técnico y operativo para que cada operador pueda evaluar, estandarizar y madurar sus procesos internos de seguridad en redes móviles. El MCKB guía la adopción de controles FS.31, la implementación de prácticas *End-to-End* en RAN y Core, y el desarrollo de capacidades de gestión de vulnerabilidades, configuración y protección operacional.

6.2 EL PAPEL ESTRATEGICO DE LA IA EN CIBERDEFENSA

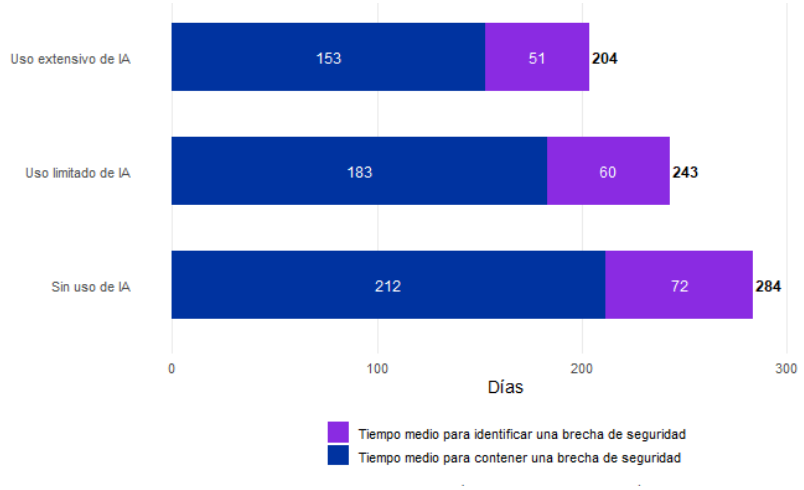
El uso de la inteligencia artificial (IA) ha transformado la capacidad para identificar y contener vulnerabilidades, así como responder de manera más efectiva ante ataques. Según el Informe sobre el costo de una violación de datos de IBM[164], las organizaciones que implementan esta tecnología mejoran su resiliencia operativa, reducen los costos asociados a los incidentes de seguridad y acortan

[161] ITRE ATT&CK (MITRE ATT&CK. Disponible en: https://www.ibm.com/think/topics/mitre-attack
[162] TRAFFIC LIGHT PROTOCOL (TLP). Disponible en: https://www.first.org/tlp/
[163] Cybersecurity document library. Disponible en: https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/cybersecurity-document-library/
[164] IBM & Ponemon Institute (2025). Cost of a Data Breach Report 2025. IBM. Disponible en: https://www.ibm.com/reports/data-breach

significativamente los tiempos de respuesta, fortaleciendo así su posición frente a un entorno de amenazas cada vez más complejo.

De acuerdo con el citado informe, para el año 2025 las organizaciones que no emplean IA tardan en promedio 212 días en identificar una brecha y 72 días adicionales en contenerla, lo que representa un total de 284 días. Por el contrario, aquellas que utilizan la IA y la automatización reducen estos tiempos a 153 días para identificar y 51 días para contener, sumando 204 días en total. Esto implica que la IA reduce el tiempo total de gestión de una brecha en 80 días, es decir, casi un 30% menos que las organizaciones sin IA.

Gráfico 6.4 Tiempo promedio para identificar y contener una brecha de seguridad, según el nivel de uso

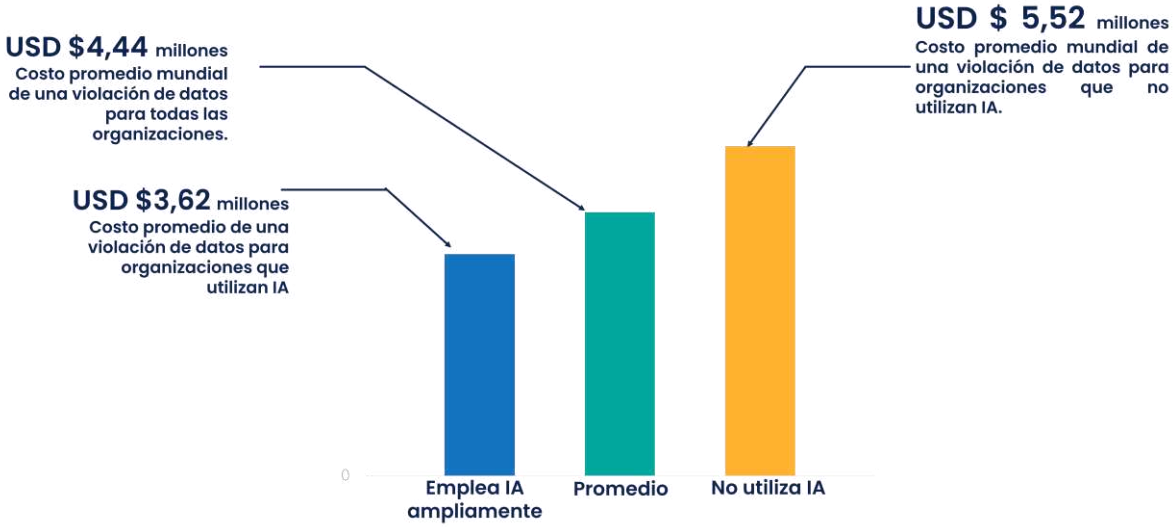


Fuente: Elaboración propia a partir de datos de Cost of a Data Breach Report 2025

Además, la adopción de IA no solo acelera la detección, sino que disminuye significativamente los costos asociados a una violación de datos. El costo promedio de una brecha asciende a 5,52 millones de dólares para las organizaciones que no usan IA, mientras que aquellas que la implementan de manera amplia reportan un costo promedio de 3,62 millones de dólares, lo que equivale a un ahorro de 1,9 millones de dólares.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Gráfico 6.5 Costo Promedio de una Brecha de Datos, según el Uso de IA



Fuente: Elaboración propia a partir de datos de Cost of a Data Breach Report 2025.

La IA se consolida como un componente esencial en la detección, defensa, recuperación y respuesta ante incidentes. La IA redefine la ciberseguridad, pasando de un enfoque reactivo a uno predictivo y adaptativo. La capacidad de identificar y contener brechas con mayor rapidez se traduce en una reducción tangible de pérdidas financieras, una mitigación más efectiva de los riesgos y un fortalecimiento de la resiliencia cibernética.

El informe del foro global de ciberseguridad «*Intelligent Defense: The Strategic Role of AI in Telecom Cybersecurity*»[165] propone un marco estratégico de cuatro pilares que orienta la integración efectiva de la IA en la gestión de la ciberseguridad y la ciberdefensa dentro del sector de telecomunicaciones. Este enfoque busca garantizar la protección de redes, infraestructuras críticas y servicios digitales en un entorno en el que las amenazas aumentan en complejidad y escala. Los cuatro pilares que analiza son:

6.2.1. Detección proactiva de amenazas. La IA permite analizar de forma continua grandes volúmenes de tráfico y señales de red, identificando patrones anómalos que podrían indicar intrusiones, intentos de denegación de servicio (DDoS) o accesos no autorizados en las diferentes capas funcionales en las redes de telecomunicaciones. Se pueden emplear modelos predictivos que distinguen comportamientos legítimos de uso de red o maliciosas, anticipando así ataques antes de que afecten la operación.

[165] Global Cybersecurity Forum (GCF) (2025). Intelligent Defense: The Strategic Role of AI in Telecom Cybersecurity. Disponible en: https://api.gcforum.org/api/files/public/upload/b79bbb2a-550f-4dd9-ab57-3cd0b6e49925_v-Intelligent-Defense-The-Strategic-Role.pdf

A través de modelos de aprendizaje de máquina, los operadores pueden identificar el funcionamiento de torres falsas (*rogue cell tower*), reconocer anomalías de señalización y detectar desviaciones en los flujos y parámetros del núcleo de red (*Core Network*). La IA también ha demostrado alta efectividad en la detección temprana de ataques DDoS, monitoreando en tiempo real el tráfico en redes regionales y troncales para identificar picos artificiales o comportamientos coordinados que indiquen un ataque en curso, habilitando medidas de mitigación preventiva.

En el ámbito móvil, la IA se ha consolidado como herramienta clave en la detección de fraude por intercambio de SIM (SIM *swap*). Mediante el análisis automatizado de solicitudes de cambio de tarjeta SIM, patrones de consumo, perfiles de usuario y señales externas, los sistemas identifican intentos sospechosos en tiempo real y bloquean la suplantación antes de que se materialice. De acuerdo con el informe, estas soluciones han mitigado hasta el 80% de los intentos de SIM *swap* en mercados como el Reino Unido, fortaleciendo la seguridad del usuario y la resiliencia operativa de los operadores.

6.2.2. Defensa. Mediante la IA los operadores pueden activar mecanismos de contención en tiempo real, aumentando la resiliencia de la infraestructura de red frente a ataques cibernéticos. La IA puede ejecutar un bloqueo dinámico de tráfico malicioso, identificando un aumento anómalo de solicitudes hacia un puerto específico y bloqueando automáticamente las IP de origen asociadas al ataque antes de que saturen la red. Asimismo, el sistema puede detectar actividad irregular en un nodo crítico del *core*, aislando temporalmente dicho segmento para evitar la propagación de la intrusión y preservando la integridad del resto de la red.

En escenarios más complejos, como ataques DDoS o intentos de explotación de vulnerabilidades, la IA puede ajustar en tiempo real las reglas del firewall, endureciendo los filtros y priorizando la inspección de paquetes sospechosos sin necesidad de intervención manual. Además, mediante el análisis continuo de patrones históricos de intrusión, el sistema puede anticipar amenazas recurrentes y activar políticas de mitigación preconfiguradas, como la limitación de conexiones por usuario o la segmentación dinámica de subredes, garantizando así una defensa proactiva y adaptativa frente a ataques sofisticados.

6.2.3. Gobernanza y cumplimiento inteligente. La IA también cumple un rol estratégico en la gestión del riesgo y el aseguramiento del cumplimiento normativo. A través de sistemas de monitoreo continuo, los operadores pueden verificar automáticamente la adherencia a regulaciones sectoriales, políticas internas y estándares internacionales de seguridad. Estos modelos analizan configuraciones, flujos de tráfico y eventos críticos en busca de desviaciones que puedan comprometer la integridad o disponibilidad de la red. Además, las capacidades de automatización permiten generar reportes y auditorías en tiempo real, facilitando la trazabilidad y reduciendo la carga administrativa de los equipos de cumplimiento.

6.2.4. Optimización continua y aprendizaje adaptativo. Este pilar reconoce el carácter evolutivo de la ciberseguridad y la necesidad de que los sistemas aprendan de cada incidente. A través de modelos

de aprendizaje adaptativo, la IA ajusta umbrales, perfiles de comportamiento y reglas de detección conforme emergen nuevas tácticas, técnicas y procedimientos utilizados por actores maliciosos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7. CONCLUSIONES

La ciberseguridad constituye un elemento fundamental para individuos, empresas y gobiernos en la protección de infraestructuras críticas. Aunque se aplican diversas estrategias para mitigar amenazas, la constante evolución de actores y técnicas de ataque exige una actualización continua y eficiente de las políticas y controles de seguridad. Es imprescindible **robustecer la cultura organizacional** enfocada en la seguridad digital y anticiparse a los efectos disruptivos de tecnologías emergentes, como la computación cuántica, que representa una amenaza potencial para los sistemas actuales de cifrado. En el caso de Colombia, el país ha superado la etapa conceptual y cuenta con una Estrategia Nacional de Seguridad Digital 2025 – 2027 y un marco normativo para infraestructuras críticas cibernéticas, equiparable en enfoque, aunque no necesariamente en grado de madurez a lo observado en otras naciones de la región.

La velocidad y la evolución de los ciberataques serán factores clave durante la próxima década. Las organizaciones que implementen una gobernanza sólida y fomenten el **compromiso de la alta dirección**, integrando una **cibercultura** como fundamento para el desarrollo de buenas prácticas eficaces y naturales, estarán mejor posicionadas. El **aprovechamiento del conocimiento de las personas como elemento multiplicador de la defensa**, junto con el uso de la inteligencia artificial y la automatización en sistemas de respuesta unificados, permitirá consolidar **estrategias resilientes** y proyectadas al futuro.

Para el año 2026, se proyecta que el cibercrimen será la tercera economía más grande a nivel mundial, impulsado principalmente por los avances en *inteligencia artificial* y *computación cuántica*. Estos progresos facilitan la ejecución de ataques autónomos y la generación de audio y vídeo manipulados a través de *deepfakes* y contenido sintético, permitiendo a los atacantes suplantar identidades confiables y acceder a sistemas protegidos.

Además, aumentarán las intrusiones que se adaptan en tiempo real a las defensas, como el *malware* polimórfico, capaz de reescribirse para evitar su detección, impulsando un modelo delictivo completamente autónomo. Y los ciberataques se enfocarán especialmente en entornos *cloud* híbridos, cadenas de suministro de software, paquetes de código abierto maliciosos y manipulación de infraestructuras de IA mediante datos corruptos.

En la actualidad, los operadores de *ransomware* muestran patrones organizacionales similares a los de empresas legítimas. Estos actores utilizan infraestructuras en la nube, contratan servicios informáticos y establecen entidades comerciales ficticias para encubrir sus actividades. La constante reidentificación de estas organizaciones, impulsada por acciones policiales y sanciones, les permite eludir la atribución, mejorar su posicionamiento y atraer nuevos colaboradores. Esta flexibilidad exige que los profesionales de la ciberseguridad enfoquen sus esfuerzos en identificar tácticas, técnicas y procedimientos recurrentes, en lugar de centrarse únicamente en grupos específicos. Se estima que, para 2027, el cibercrimen alcanzará una escala equiparable a la de industrias legítimas.

El ecosistema digital enfrenta un panorama de amenazas cada vez más complejo, marcado por ataques interdependientes, una creciente automatización criminal y la irrupción de tecnologías disruptivas. En este contexto, la seguridad ya no puede sostenerse mediante controles tradicionales ni acciones aisladas: las organizaciones deben adoptar estrategias capaces de anticipar riesgos, asegurar la continuidad operativa y fortalecer la confianza de los usuarios.

Para ello, es indispensable abandonar un enfoque reactivo y avanzar hacia una resiliencia verdaderamente proactiva. Esto implica integrar la seguridad desde el diseño en todas las capas tecnológicas servicios en la nube, hardware y cadena de suministro, asegurando visibilidad de extremo a extremo, **automatización con validación humana**, supervisión continua de vulnerabilidades y procesos robustos de actualización, pruebas de reversión y respuesta.

La resiliencia del ecosistema digital también depende de la colaboración. Debido a que los vectores de ataque afectan simultáneamente a operadores, proveedores, usuarios y autoridades, la respuesta no puede ser individual ni uniforme. Se requieren redes colaborativas que compartan inteligencia de amenazas en tiempo real, coordinen respuestas frente a incidentes de alto impacto e identifiquen tácticas persistentes que trascienden a grupos criminales específicos. Esto exige mecanismos de *Threat Intelligence* con gobernanza formal, procesos estandarizados y plataformas seguras que gestionen el ciclo integral de inteligencia. En un entorno donde el cibercrimen podría convertirse en una de las mayores economías globales para 2026, la colaboración deja de ser una recomendación y se convierte en un pilar indispensable para la sostenibilidad del ecosistema digital.

El sector de telecomunicaciones es unos de los sectores relevantes dentro de la política de ciberseguridad en Colombia. El análisis de sectores estratégicos muestra que este sector se encuentra entre los más expuestos y vulnerables del país, en gran medida debido a la masiva cantidad de dispositivos finales que administra, su alto grado de interconectividad y su rol como infraestructura crítica que soporta servicios gubernamentales, financieros, industriales y ciudadanos.

Los datos analizados refuerzan esta conclusión: el 56% de la actividad *Botnet* detectada en Colombia durante 2025 tuvo como objetivo el sector de telecomunicaciones. Esta proporción es sustancialmente mayor que la registrada en la mayoría de los países de la muestra, superando ampliamente a economías como México, Brasil, India, Japón, Estados Unidos y España. La materialización de estos riesgos puede generar interrupciones operativas prolongadas, impactos en la disponibilidad de servicios esenciales y exposición de información sensible, afectando directamente la resiliencia del ecosistema digital.

La expansión de la superficie de ataque es estructural y permanente. La convergencia entre 5G, *cloud*, IoT, arquitecturas abiertas y *edge computing* ha desdibujado el perímetro tradicional de seguridad. Esto obliga a adoptar enfoques como *Zero Trust* y defensa en profundidad, donde ningún elemento se considera confiable por defecto y la seguridad se integra en todo el ciclo de vida de los activos.

Los vectores de ataque se han diversificado en todas las capas de la red. Hoy coexisten ataques sobre infraestructura física y lógica (DDoS, explotación de vulnerabilidades), entornos virtualizados y nube

(APIs, identidades, contenedores), redes abiertas y desagregadas, dispositivos finales/IoT, cadena de suministro y campañas impulsadas por IA generativa. La seguridad ya no puede centrarse en un solo ámbito, sino abarcar de forma integrada infraestructuras, plataformas, aplicaciones y usuarios.

La cadena de suministro se ha consolidado como uno de los principales riesgos estructurales para la ciberseguridad, especialmente en el sector de telecomunicaciones, donde convergen múltiples proveedores de hardware, software, firmware, servicios en la nube, data centers y plataformas de gestión. Esta interdependencia crea un ecosistema altamente vulnerable: un solo componente comprometido, por ejemplo, una actualización de software, un servicio gestionado o un equipo de red, puede escalar a incidentes masivos que afecten de forma simultánea a varios operadores.

De manera complementaria, la gestión de identidades y credenciales (tanto humanas como de máquina) se ha convertido en un vector de riesgo dominante en entornos *cloud* y redes modernas. La explotación de cuentas con privilegios excesivos, configuraciones débiles de control de acceso o credenciales comprometidas permite a los atacantes obtener acceso inicial, persistencia y movimiento lateral dentro de los sistemas, amplificando el impacto de cualquier brecha y, en muchos casos, pasando desapercibidos al camuflarse como usuarios o servicios legítimos.

La computación cuántica ofrece importantes oportunidades económicas y científicas al desbloquear una potencia de cálculo sin precedentes y aunque sigue siendo incierto el plazo para alcanzar el máximo potencial de la computación cuántica, los riesgos asociados a la seguridad cuántica ya están presentes.

Es por esto que para prepararse frente a la era cuántica y antes de que sea demasiado tarde, **en 2026 la prioridad será desarrollar una cultura de ciberseguridad** a través de la capacitación del recurso humano; la identificación de vulnerabilidades como la obsolescencia de estándares actuales de cifrado utilizados para proteger redes móviles e infraestructura heredada diseñada para la computación clásica y dispositivos IoT; la migración a cifrados resistentes a la computación cuántica; la transformación de las arquitecturas de red y un enfoque con visión para gestionar redes que operan sobre tecnologías emergente (red cuántica); así como la adaptación de los modelos de negocio, pues en tanto que la industria trabaja hace una década en la interconexión de ordenadores cuánticos, también los delincuentes conocidos como «Cosechar ahora, descifrar después» *Harvest Now, Decrypt Later,* (HNDL) están interceptando y almacenando datos cifrados hoy en día, preparándose para el momento en que la tecnología cuántica permita descifrarlos, transportarlos y explotarlos.

La tecnología cuántica posee el potencial de transformar las redes de telecomunicaciones soportadas en el cifrado, la transmisión de datos y la seguridad de la infraestructura, al posibilitar nuevas eficiencias en la optimización de redes, la gestión del espectro y el procesamiento ultrarrápido de datos. No obstante, también puede representar una amenaza significativa para la seguridad de las redes 5G, debido a su capacidad para vulnerar los sistemas de cifrado que actualmente protegen estos entornos.

La inteligencia artificial está alcanzando un nivel de integración en nuestra vida diaria comparable a hitos históricos como la llegada de la mecánica, la electricidad o las telecomunicaciones. Esto implica

que, cada vez más, pasará desapercibida, convirtiéndose en una tecnología de fondo que dejará de ser resaltada. Para las nuevas generaciones, especialmente los niños nacidos en la última década, interactuar de manera natural y fluida con dispositivos y máquinas será algo habitual; ya no lo percibirán como una innovación destacable, sino como la manera normal en que opera el mundo que les rodea.

Los agentes autónomos de IA son la nueva primera línea en el cibercrimen que multiplicará las amenaza y permitirá censar defensas para encontrar vulnerabilidades y lanzar intentos de ingeniería social cada vez más engañosos (Se prevé que surjan otras tácticas de presión reputacional, como divulgar información manipulada o crear escándalos para forzar los pagos) y los *bots* de extorsión impulsados por IA se involucrarán directamente con las víctimas en las negociaciones de rescate. Sin embargo, los agentes autónomos también ofrecen a los defensores nuevas opciones para detectar y responder de forma autónoma.

El impacto trasciende lo técnico y genera retos económicos, sociales y regulatorios. Los ciberataques afectan la continuidad de servicios críticos, incrementan de forma permanente los costos de cumplimiento y operación, erosionan la confianza de los usuarios y agravan desigualdades entre operadores grandes y pequeños. Además, la tensión entre innovación (arquitecturas abiertas, multi-vendor) y seguridad exige marcos regulatorios proporcionales, basados en riesgo y con énfasis en seguridad desde el diseño y gestión de la cadena de suministro.

Por otro lado, Colombia presenta una de las mayores tasas de exposición a vulnerabilidades en dispositivos finales (*endpoint*) dentro de la región, incluso comparada con países que tienen economías más grandes, mayor digitalización y un ecosistema tecnológico más desarrollado. Esta situación resulta relevante, dado que los *endpoints*, *routers*, *módems*, *smartphones*, dispositivos IoT, computadores y terminales de usuario, constituyen el primer punto de acceso para una amplia gama de ataques, desde *botnets* hasta r*ansomware* y robo de credenciales.

Para 2026, se prevé que los grupos de *ransomware* adoptarán la IA agéntica para automatizar gran parte del ciclo de vida del ataque, minimizando la intervención humana. Esta automatización, combinada con el uso de *deepfakes* para manipular la percepción y facilitar el fraude, marca un salto significativo en la sofisticación de las amenazas.

El auge de estos ataques, facilitado por el modelo de *Ransomware-as-a-Service* (RaaS), obliga a las organizaciones a replantear urgentemente sus estrategias de resiliencia. En este nuevo panorama, la inmutabilidad y la segmentación de las copias de seguridad se consolidan como defensas críticas e ineludibles. En Europa, esta transformación es ya una realidad: normativas como NIS2 y DORA elevan la gestión de las copias de seguridad de una simple buena práctica de TI a un requisito legal cuyo incumplimiento conlleva sanciones económicas.

Las campañas de *ransomware* evolucionarán para ser más imperceptibles, agresivas y selectivas. Los atacantes explotarán activamente la complejidad de las cadenas de suministro y los ecosistemas digitales de las empresas. Las dependencias de componentes de código abierto, los servicios de terceros

y los flujos de trabajo integrados con IA se convertirán en las principales vías de acceso. Esto permitirá al *ransomware* infiltrarse en sistemas de confianza, mimetizándose con la actividad operativa normal de la organización.

El uso intensivo de análisis de datos permitirá a los ciberdelincuentes identificar con precisión las vulnerabilidades críticas y priorizar objetivos. Esto culminará en estrategias de coacción diseñadas a medida, enfocadas en un menor número de víctimas, pero con un valor de extorsión significativamente mayor.

Los marcos de *zero trust* fortalecen la seguridad ante amenazas como el *ransomware*, pero requieren medidas adicionales. Es clave formar a las personas regularmente contra la ingeniería social avanzada (que incluye el uso de IA) y usar plataformas de inteligencia de amenazas para rastrear y diseñar defensas eficaces que involucren análisis de impacto, manuales probados de recuperación y flujos de contingencia, indispensables para garantizar la continuidad de la operación.

La transformación digital ha eliminado la tradicional desconexión física (*air-gapping*) entre los sistemas de Tecnologías de la Información (IT) y las Tecnologías Operativas (OT), impulsada por la necesidad de datos en tiempo real. Esta convergencia, aunque aumenta la eficiencia, ha convertido la ciberseguridad de la OT en un componente central de la fabricación moderna y en un nuevo punto de explotación para los atacantes.

El cambio más significativo para 2026 será la gobernanza unificada de los dominios IT y OT. Es necesario superar la gestión aislada (tradicionalmente ISO 27001 para IT y IEC 62443 para OT) para adoptar un enfoque holístico, como lo exigen marcos como el CAF 4.0 (Ciberseguridad y Resiliencia). Esto implica unificar los Sistemas de Gestión de Seguridad de la Información (ISMS) y los Sistemas de Gestión de Seguridad Cibernética (CSMS) para una gestión estratégica de consecuencias que vaya más allá del mero cumplimiento.

En el contexto actual de digitalización acelerada y avance tecnológico, la seguridad en el sector energético se convierte en un aspecto fundamental para preservar la estabilidad y la soberanía digital de los países. El crecimiento exponencial de los centros de datos destinados para el entrenamiento de la inteligencia artificial está redefiniendo la independencia tecnológica y energética de las naciones, así como la necesidad de garantizar la protección de sistemas críticos frente a amenazas externas.

Para 2026, un elemento central del discurso en torno a la protección de datos y la IA, será mejorar la eficiencia de los sistemas que alimentan y enfrían millones de computadores que procesan enormes volúmenes de datos. Así como también buscar métodos innovadores para generar energía

El país ha avanzado más en infraestructuras críticas cibernéticas digitales que en un régimen integral de «infraestructuras críticas» (físicas más cibernéticas) como lo tienen, por ejemplo, la Unión Europea o Brasil. En la práctica, la protección de infraestructuras críticas cibernéticas es más exigente y

estructurada en algunos sectores (financiero, eléctrico) que en otros, lo que genera brechas de resiliencia entre sectores críticos.

Hoy existe por primera vez una metodología oficial unificada para infraestructuras críticas cibernéticas, pero su implementación práctica (inventario completo, criterios homogéneos, uso sistemático por todos los sectores) todavía está en construcción.

Conceptualmente, Colombia tiene un puente bien diseñado entre gestión de seguridad de la información (MSPI) e infraestructuras críticas cibernéticas, pero en la práctica no todas las entidades tienen el MSPI maduro, y la capacidad técnica es muy desigual (entidades nacionales frente a entidades territoriales, sectores regulados frente a sectores no regulados). El propio diagnóstico oficial admite que, aunque el marco existe, la gobernanza real de las infraestructuras críticas cibernéticas (quién manda, quién coordina, con qué recursos y con qué herramientas) todavía es frágil.

La ciberseguridad debe ser medible y demostrable en tiempo real. Esto implicará que los gobiernos exijan pruebas continuas de resiliencia y que las organizaciones demuestran controles preventivos, planes de respuesta y políticas de protección de datos de forma ininterrumpida.

La convergencia de normas para la seguridad IT/OT es tanto una exigencia regulatoria como una necesidad estratégica. Esta doble responsabilidad implica evolucionar del cumplimiento al manejo de consecuencias, y orientar la ingeniería de la resiliencia como una capacidad vivida y real, no solo como una aspiración.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8. ANÁLISIS Y ACCIONES ESTRATÉGICAS

Como resultado del análisis desarrollado en el presente documento y de las conclusiones expuestas, la CRC identifica un conjunto de acciones estratégicas orientadas a fortalecer la seguridad y resiliencia del ecosistema digital colombiano. Estas acciones responden a los desafíos evidenciados en relación con la vulnerabilidad de varios sectores incluido telecomunicaciones, y la necesidad de consolidar redes colaborativas de intercambio de inteligencia, elementos esenciales para mejorar la capacidad de anticipación y mitigación de incidentes.

8.1 ACCIONES A SER EJECUTADAS POR LA CRC

8.1.1. Marco normativo.

En atención a lo previsto en el parágrafo 3 del artículo 2.2.21.1.1.2 del Decreto 1078 de 2015, la CRC reconoce la importancia de que, en el marco de la política sectorial que defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) como cabeza del sector, se evalúe la necesidad de realizar ajustes o precisiones a las disposiciones vigentes en materia de gestión de seguridad de la información en redes de telecomunicaciones. En este contexto, la CRC estará atenta a acompañar técnicamente, en el ámbito de sus competencias, los análisis que se consideren pertinentes respecto del artículo 5.1.2.3 del Régimen Integral de Calidad de la Resolución 5050 de 2016, particularmente en lo relacionado con gestión de riesgos, continuidad del servicio y reporte de incidentes, buscando su adecuada articulación con el Modelo Nacional de Atención y Gestión de Incidentes y la Plataforma Nacional de Notificación y Seguimiento de Incidentes de Seguridad Digital.

8.1.2. Networking.

8.1.2.1. El simposio «Ciberseguridad como motor de confianza en las telecomunicaciones», organizado recientemente por la CRC, subrayó la relevancia de convocar a actores estratégicos de diferentes sectores para facilitar el análisis de tendencias, el intercambio de información crítica y la identificación de desafíos comunes a lo largo de toda la cadena digital. En su calidad de articulador del sector de telecomunicaciones, la CRC continuará promoviendo espacios permanentes de diálogo y colaboración, integrando no solo a los sujetos regulados, sino también a todas las partes que conforman este ecosistema: entidades gubernamentales, academia, centros de investigación, fabricantes, desarrolladores tecnológicos, proveedores de infraestructura, sectores estratégicos, como financiero y energético , organizaciones de la sociedad civil y expertos independientes.

8.2 RECOMENDACIONES: ACCIONES QUE OTRAS ENTIDADES PODRÍAN IMPLEMENTAR

La evolución constante del entorno digital y el auge de tecnologías disruptivas como la inteligencia artificial y la computación cuántica han redefinido los desafíos de la ciberseguridad en todos los sectores.

Resulta esencial que las organizaciones adopten un enfoque proactivo y adaptativo, integrando la protección de datos y la resiliencia operativa en cada fase de su desarrollo tecnológico y empresarial. En este contexto, las siguientes recomendaciones están orientadas a anticipar riesgos, fortalecer defensas y fomentar una cultura colaborativa que permita a los distintos sectores afrontar con éxito las amenazas emergentes y consolidar una postura robusta frente a la transformación digital.

8.2.1. Estado.

En concordancia con las mejores prácticas internacionales, tales como la creación de una unidad especializada en seguridad digital y la implementación de estrategias integrales, coordinadas y colaborativas para la protección de infraestructuras críticas y la asignación de responsabilidad formal sobre el inventario nacional que sustenten la seguridad digital, así como la gestión de incidentes de gran escala, el establecimiento de redes de intercambio de inteligencia y la coordinación de CSIRT sectoriales, el Estado podrá evaluar qué medidas resultan convenientes para Colombia con el fin de fortalecer su arquitectura institucional de gobernanza digital.

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

8.2.2.1. Resulta necesario consolidar el marco jurídico de las infraestructuras críticas cibernéticas. Aunque el Decreto 338 de 2022 y los lineamientos técnicos constituyen una base importante, se recomienda avanzar hacia una norma de rango legal que recoja y actualice sus elementos centrales, reconozca expresamente los sectores críticos, defina con mayor precisión las obligaciones de los operadores privados de servicios esenciales e incorpore un régimen claro de reporte de incidentes significativos. Esta norma debería armonizar las definiciones de infraestructura crítica, infraestructura crítica cibernética, servicio esencial e información estratégica, evitando solapamientos o contradicciones en el ordenamiento. Se estima que las entidades que tienen competencias para poner en práctica esta recomendación son el MinTIC y Ministerio de Justicia, como redactores y promotores del proyecto de ley, así como el Departamento Nacional de Planeación (DNP), como articulador de política pública, asegurando coherencia con el CONPES y el Plan Nacional de Desarrollo. Y por supuesto, el Congreso de la República para el trámite del proyecto legislativo.

8.2.2.2. Es necesario completar y aprovechar de manera efectiva el inventario de infraestructuras críticas cibernéticas. Para ello, se sugiere fijar metas y plazos para que las entidades líderes de cada sector crítico identifiquen sus servicios esenciales, mapeen los activos TIC que los soportan e informen sus infraestructuras críticas cibernéticas a MinTIC, siguiendo los lineamientos metodológicos e integrando, cuando aplique, el inventario de activos del MSPI. El inventario consolidado por MinTIC podría enlazarse con la Plataforma Nacional de Notificación y Seguimiento de Incidentes de Seguridad Digital y generar información agregada y anonimizada sobre la exposición del país, con MinTIC como responsable del inventario nacional y de la plataforma, y las entidades cabeza de cada sector crítico como articuladoras del reporte en su ámbito.

8.2.2.3. Es clave reforzar la cooperación internacional y establecer un esquema de evaluación continua. Colombia puede aprovechar de forma más sistemática los espacios multilaterales y regionales para alinear su enfoque de infraestructuras críticas cibernéticas con estándares y buenas prácticas internacionales y, en paralelo, definir un conjunto acotado de indicadores nacionales sobre protección de infraestructuras críticas cibernéticas (por ejemplo, avance en inventarios, análisis de riesgos, tiempos de reporte e intensidad de ejercicios intersectoriales). Estos indicadores permitirían medir de manera objetiva si la maduración institucional reflejada en las políticas y en el Decreto 338 de 2022 se traduce en mejoras reales en la resiliencia y la gobernanza de las infraestructuras críticas digitales del país. En este escenario, se recomienda que el Coordinador Nacional de Seguridad Digital y el MinTIC, lideren el diseño y el seguimiento de los indicadores y su articulación con el modelo de gobernanza, mientras que la Cancillería podría estar a cargo del liderazgo en la inserción de Colombia en los espacios de cooperación y diálogo internacional en seguridad digital e infraestructuras críticas cibernéticas.

8.2.3. Todos los sectores.

8.2.3.1. Conviene profundizar la regulación sectorial y cerrar brechas de capacidad. Se recomienda que los reguladores y supervisores revisen su normativa para incorporar obligaciones específicas de gestión de riesgos, seguridad digital, continuidad del servicio y reporte de incidentes, vinculadas explícitamente a infraestructuras críticas cibernéticas y servicios esenciales, priorizando sectores de alta criticidad como el financiero, el eléctrico, las telecomunicaciones, la salud y el agua. Este esfuerzo normativo debería ir acompañado de programas de fortalecimiento de capacidades para entidades públicas y operadores privados, simulacros conjuntos de cibercrisis y acciones de sensibilización dirigidas a la alta dirección de los operadores de infraestructuras críticas. En este escenario, las comisiones de regulación y las superintendencias competentes (SIC, Superintendencia Financiera y Superintendencia de Servicios Públicos) podrían liderar la actualización normativa en sus respectivos sectores y el diseño de los programas de capacidades y simulacros con los operadores de infraestructuras críticas cibernéticas y prestadores de servicios esenciales.

8.2.4. Sector minero energético.

8.2.4.1. Ante la posible antigüedad de sistemas esenciales en los procesos de generación y distribución de energía, resulta prioritario que las organizaciones del sector energético estudien el desarrollo de un plan integral de modernización tecnológica. Este plan debe contemplar la sustitución progresiva de infraestructuras y tecnologías heredadas por soluciones avanzadas y seguras, así como la adopción de prácticas de gestión de riesgos proactiva. Igualmente, se recomienda realizar auditorías periódicas de vulnerabilidades, invertir en la formación continua del personal en ciberseguridad y establecer mecanismos de respuesta rápida ante incidentes. Solo mediante la actualización constante y la protección reforzada de sus infraestructuras críticas, el sector podrá reducir su exposición a amenazas cibernéticas cada vez más sofisticadas y garantizar la continuidad y resiliencia de los servicios energéticos.

8.2.4.2. La creciente adopción de inteligencia artificial, computación cuántica y otras tecnologías avanzadas está generando una presión significativa sobre la infraestructura energética, por ello, se recomienda al sector energético proyectar y planificar sus operaciones considerando:

- La inversión en infraestructuras propias y resilientes que garanticen la independencia nacional en la gestión energética, evitando la dependencia de recursos externos.
- El desarrollo de centros de datos energéticamente eficientes, utilizando fuentes renovables y sistemas de optimización que minimicen el impacto ambiental y los costes operativos.
- La implementación de mecanismos de monitorización y predicción de la demanda energética, integrando tecnologías de automatización y análisis de datos para anticipar picos de consumo derivados de la actividad tecnológica.
- El refuerzo de la ciberseguridad en infraestructuras críticas, asegurando que el incremento en la capacidad energética no exponga a los sistemas a riesgos adicionales.
- La colaboración intersectorial para compartir buenas prácticas, innovaciones y estrategias de adaptación frente al crecimiento acelerado de la demanda energética por el uso de tecnologías emergentes.

De este modo, el sector energético podrá anticiparse y adaptarse al nuevo escenario, garantizando la continuidad operativa, la soberanía tecnológica y la protección de infraestructuras clave frente a los retos que plantea la transformación digital.

8.2.5 Sector de telecomunicaciones.

8.2.5.1. Para que las redes colaborativas de intercambio de inteligencia operen de manera efectiva, es indispensable que los operadores cuenten con una infraestructura tecnológica y organizacional capaz de integrarse plenamente a los flujos sectoriales de información. Esto incluye la implementación de un ciclo completo de inteligencia dentro de sus SOC, que abarque recolección, análisis, validación, priorización y difusión, así como herramientas que automaticen el procesamiento de datos. Al mismo tiempo, se requiere la existencia de mecanismos operativos que permitan transformar dicha inteligencia en decisiones y acciones concretas de seguridad.

8.2.5.2. No basta con proteger únicamente la infraestructura propia del operador; es esencial implementar una gestión integral de la ciberseguridad que abarque toda la cadena de suministro. Se recomienda a los operadores establecer controles verificables y mecanismos obligatorios que aseguren la trazabilidad, supervisión y evaluación continua de todos los componentes, dispositivos y servicios que se incorporan a la red.

Para fortalecer esta estrategia, los operadores podrían:

- Realizar auditorías periódicas y evaluaciones de riesgos a proveedores y terceros involucrados en el ciclo de vida de la red.
- Exigir el cumplimiento de estándares internacionales de seguridad y la adopción de buenas prácticas en ciberseguridad por parte de todos los proveedores.

- Implantar mecanismos de reporte y respuesta ante incidentes que incluyan a los proveedores, garantizando una comunicación fluida y una reacción coordinada ante amenazas o vulnerabilidades detectadas.
- Integrar cláusulas de cripto-agilidad y actualización tecnológica (parches que aseguren el mantenimiento del firmware y software de extremo a extremo) en los contratos, para facilitar la adaptación a nuevas amenazas y la modernización continua de los sistemas.
- Campañas de ciber higiene digital masivas, dirigidas a hogares y pymes, enfocadas en contraseñas, autenticación, actualizaciones y configuración segura.

8.2.5.3. Para avanzar eficazmente en la migración hacia la criptografía post-cuántica, es imprescindible establecer mecanismos sólidos de colaboración sectorial. Se recomienda crear foros y grupos de trabajo conjuntos entre operadores, proveedores tecnológicos y organismos reguladores, con el objetivo de definir estándares comunes, intercambiar buenas prácticas y coordinar la integración de nuevos algoritmos de criptografía post-cuántica en los productos y servicios. Además, resulta fundamental exigir a los proveedores la inclusión de actualizaciones periódicas y mecanismos de modernización en sus ciclos de desarrollo, garantizando así la resiliencia y seguridad de todo el ecosistema digital frente a amenazas emergentes. Esta colaboración debe estar alineada con las directrices regulatorias y los avances internacionales en la materia, asegurando una transición ordenada, eficiente y segura.

8.2.5.4. Debido a que cada red posee particularidades operativas propias, es esencial que la transformación hacia la criptografía post-cuántica se adapte específicamente a las necesidades y características de cada ecosistema. Para lograr un equilibrio adecuado entre seguridad y rendimiento, se recomienda implementar pruebas de los nuevos algoritmos de criptografía post-cuántica en las redes existentes e identificar problemas ocultos que, en el futuro, podrían impedir completar la migración a la criptografía post-cuántica.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9. BIBLIOGRAFÍA

3GPP. (2024). TS 33.501: Security architecture and procedures for 5G System. 3rd Generation Partnership Project. Recuperado de https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/

5G Americas. (2023). Open RAN update. 5G Americas. Recuperado de https://www.5gamericas.org/wp-content/uploads/2023/11/Open-RAN-Update-Id.pdf

Agência Gov. (2024). Governo Federal institui Comitê Nacional de Segurança de Infraestruturas Críticas. Recuperado de https://agenciagov.ebc.com.br/noticias/202411/governo-federal-institui-comite-nacional-de-seguranca-de-infraestruturas-criticas

Amazon Web Services. (s.f.). Global network. Amazon Web Services. Recuperado de https://aws.amazon.com/es/about-aws/global-infrastructure/global-network/

America´s Cyber Defense Agency. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptograph. Recuperado de https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Alvisi, L., Bianchi, J., Tibidò, S., & Zucca, M. V. (2024). Weaponizing disinformation against critical infrastructures. arXiv. Recuperado de https://doi.org/10.48550/arXiv.2406.08963

Azariah, W., Bimo, F. A., Lin, C. W., Cheng, R. G., Nikaein, N., & Jana, R. (2024). A survey on open radio access networks: Challenges, research directions, and open source approaches. Sensors, 24(3), 1038. Recuperado de https://doi.org/10.3390/s24031038

Banco Mundial. (2023). Conectados: Tecnologías digitales para la inclusión y el crecimiento. Informe Económico — América Latina y el Caribe. Washington, DC: Banco Mundial. Recuperado de https://documents1.worldbank.org/curated/en/099041024190032046/pdf/P1812111db279e0141a72015f27c232cced.pdf

Barbosa, D. C. (2022). Ransomware como servicio (RaaS): qué es y cómo funciona este modelo. ESET – WeLiveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2022/02/23/ransomware-as-a-service-raas-que-es-como-funciona/

Barbour, D. (2025). How much does NIS2 compliance really cost? Complete budget guide. Kiteworks. Recuperado de https://www.kiteworks.com/regulatory-compliance/nis2-compliance-costs/

Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.663. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1202434

Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.738. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1198702

Biblioteca del Congreso Nacional de Chile (BCN). (2025). Ley N° 21.883. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1188583

Biblioteca del Congreso Nacional de Chile (BCN). (2025, julio 11). Resolución N° 28 Exenta. Recuperado de https://bcn.cl/b4YIYf

Bleeping computer. (2025). LameHug malware uses AI LLM to craft Windows data-theft commands in real-time. Recuperado de https://www.bleepingcomputer.com/news/security/lamehug-malware-uses-ai-llm-to-craft-windows-data-theft-commands-in-real-time/

Braking News. Biden signs ambitious order to bolster energy resources for AI data centers. Recuperado de https://apnews.com/article/biden-white-house-ai-artificial-intelligence-7458d9d1bb537929c5dcfb5192695223

Brooks, M., Fixler, A., & Montgomery, M. (2023, June 7). Revising public-private collaboration to protect U.S. critical infrastructure. Cyberspace Solarium Commission 2.0. Recuperado de https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/

Bundesamt für Sicherheit in der Informationstechnik. (2022). Open RAN risk analysis. Recuperado de https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI). (2025). Propuesta de Lineamientos para una Estrategia Nacional de Ciberseguridad para México. Recuperado de https://canieti.org/storage/PageBuilderFiles/U8qtgYwLbQbxIuNSDAgwmKmlqtp32e-metaU21DKyAtIENhbmlldGkgLSBFc3RyYXRlZ2lhIENpYmVyc2VndXJpZGFkIC0gMjAyNTExIC0gdjEuMC5wZGY%3D-.pdf

Cargoson. (2025). Recuperado de https://www.cargoson.com/es/blog/numero-de-centros-de-datos-por-pais

Cesarano, C., Foggia, A., Roscigno, G., Andreani, L., & Natella, R. (2025). Security-by-design at the telco edge with OSS: Challenges and lessons learned. arXiv. Recuperado de https://arxiv.org/abs/2505.00111

CISA. (2020). Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise. Cybersecurity and Infrastructure Security Agency. Recuperado de https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

Cisco. (2022). Octubre, mes de concientización en Ciberseguridad. Recuperado de https://gblogs.cisco.com/la/ciberseguridad1-jreynabr-octubre-mes-de-la-concientizacion-sobre-la-ciberseguridad/

Cloudflare. TheNET, Unlocking cyber resilience. Recuperado de https://www.cloudflare.com/the-net/unlocking-cyber-resilience/

Cloudflare. The role of leadership in shaping organizational culture. Recuperado de https://www.cloudflare.com/the-net/unlocking-cyber-resilience/

Cloudflare. Your first line of defense in cybersecurity. Recuperado de https://www.cloudflare.com/the-net/security-first-culture

Comisión Económica para América Latina y el Caribe (CEPAL). (2018). Tecnologías digitales para un nuevo futuro. Santiago de Chile: CEPAL. Recuperado de https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

CrowdStrike. (2025). 2025 Global Threat Report. CrowdStrike, Inc. Recuperado de https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

Cyberfort. Building a Cyber Resilient Culture – Why people matter most. Recuperado de https://cyberfortgroup.com/building-a-cyber-resilient-culture-why-people-matter-most/#:~:text=Culture%20and%20Behaviour,another%20in%20doing%20the%20same.

Cybersecurity and Infrastructure Security Agency (CISA). (2021). Defending against software supply chain attacks. Recuperado de https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (s.f.). About CISA. Recuperado de https://www.cisa.gov/about

Cyber Press. (2025). Ransomware Trends 2026. Recuperado de: https://cyberpress.org/ransomware-trends-2026-how-businesses-can-build-resilience/#:~:text=Ransomware%20in%202026%20is%20driven,the%20decisive%20line%20of%20defense

Cyber Press. (2025). GLOBAL GROUP's Golang Ransomware Expands Attacks Across Major Operating Systems. Recuperado de https://cyberpress.org/global-groups-golang-ransomware-expands-attacks/

CSIRTs Network. (s.f.). CSIRTs Network. Recuperado de https://csirtsnetwork.eu/
Darktrace. (2024). Understanding the Canadian Critical Cyber Systems Protection Act. Recuperado de https://www.darktrace.com/blog/understanding-the-canadian-critical-cyber-systems-protection-act

Departamento Nacional de Planeación (DNP). (2011). CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación (DNP). (2016). CONPES 3854 de 2016: Política Nacional de Seguridad Digital. Recuperado de https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación (DNP). (2020). CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación (DNP). (2025). CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

Diario Oficial de la Federación (DOF). (2025). Acuerdo por el que se establecen disposiciones en materia de telecomunicaciones y radiodifusión. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5747756&fecha=24/01/2025

DNSFilter. (2025). Annual Security Report. DNSFilter . Recuperado de https://www.dnsfilter.com/hubfs/Resources/2025-annual-security-report.pdf

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

European Commission. (2021). Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents. Press corner. Recuperado de https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

European Commission. (s.f.). Cyber Resilience Act. Shaping Europe's digital future. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (s.f.). NIS2 Directive: Securing network and information systems. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Insurance and Occupational Pensions Authority (EIOPA). (s.f.). Digital Operational Resilience Act (DORA). Recuperado de https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 164–198. Recuperado de https://eur-lex.europa.eu/eli/dir/2022/2557/oj

European Union Agency for Cybersecurity (ENISA). (s.f.). EU CyCLONe. Recuperado de https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone

European Union Agency for Cybersecurity (ENISA). (2024). Navigating cybersecurity investments in the time of NIS 2. Recuperado de https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

College of Executive Coaching. (2023). What Do Coaches Need to Know About Edgar Schein?. Recuperado de https://www.executivecoachcollege.com/research-and-publications/what-coaches-need-to-know-about-edgar-schein.php#:~:text=%22The%20only%20thing%20of%20real,D

F5, Inc. (2025). What are security breaches? F5. Recuperado de https://www.f5.com/glossary/security-breaches

Forbes. (2025). Las ocho tendencias de IA más importantes para 2026 que todos deben afrontar. Recuperado de https://forbes.es/tecnologia/801213/las-ocho-tendencias-de-ia-mas-importantes-para-2026-que-todos-deben-afrontar/

Fortinet. (2025). FortiGuard Labs Global Threat Landscape Report 2025. Sunnyvale, CA: Fortinet, Inc. Recuperado de https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

Fortinet. (2025). 2025 State of Operational Technology and Cybersecurity. Recuperado de https://www.fortinet.com/resources/reports/state-ot-cybersecurity

Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (2025). Estratégia Nacional de Cibersegurança (E-Ciber). Recuperado de https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber

Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (2025). Segurança de Infraestruturas Críticas. Recuperado de https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas/seguranca-de-infraestruturas-criticas-sic

Giraldo Gallo, J. F. (2016). Infraestructuras críticas cibernéticas en Colombia [Diapositivas de PowerPoint]. Comando Conjunto Cibernético (CCOC). Recuperado de https://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticas-ciber-en-colombia.pdf

Global Cybersecurity Forum (GCF) & STC. (2025). Intelligent Defense: The Strategic Role of AI in Telecom Cybersecurity. Recuperado de https://api.gcforum.org/api/files/public/upload/b79bbb2a-550f-4dd9-ab57-3cd0b6e49925_v-Intelligent-Defense-The-Strategic-Role.pdf

Global Cybersecurity Forum (GCF). (2025). Securing the Future. Recuperado de https://api.gcforum.org/api/files/public/upload/ec47f543-2a80-45bb-8d43-b11b5df4b5e7_Future-of-Quantum.pdf

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. National Security Archive. Recuperado de https://nsarchive.gwu.edu/sites/default/files/documents/4333130/Government-of-Mexico-Estrategia-Nacional-de.pdf

Gobierno de México. (2025). Plan Nacional de Ciberseguridad. Recuperado de https://www.gob.mx/atdt/planes_nacionales/ciberseguridad/Plan_Nacional_de_Ciberseguridad.pdf

Gobierno de México. (s.f.). Guardia Nacional CERT-MX. Recuperado de https://www.gob.mx/gncertmx
Government of Canada. (2025). Communications Security Establishment Canada. Recuperado de https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/welcome-package-minister-national-defence/communications-security-establishment-canada.html

Greenberg Traurig, LLP. (2025). EU NIS 2 Directive: Expanded Cybersecurity Obligations for Key Sectors. Recuperado de https://www.gtlaw.com/en/insights/2025/8/eu-nis-2-directive-expanded-cybersecurity-obligations-for-key-sectors

GSMA. (2023). Guidelines for Quantum Risk Management for Telco. Recuperado de https://www.gsma.com/get-involved/working-groups/gsma_resources/guidelines-for-quantum-risk-management-for-telco/

GuidePoint Security Research and Intelligence Team (GRIT). (2025). GRIT 2025 Q1 Ransomware & Cyber Threat Report. GuidePoint Security. Recuperado de https://www.guidepointsecurity.com/wp-content/uploads/2025/04/GRIT-2025-Q1-Ransomware-Cyber-Threat-Report.pdf

Gupta, A. (2025). Telecom Sector – Cyber Risk. KPMG India. Recuperado de https://kpmg.com/in/en/blogs/2025/02/telecom-sector-cyber-risk.html

IBM. Introducción a Qiskit y IBM Quantum. Recuperado de https://quantum.cloud.ibm.com/docs/es/guides

IBM & Ponemon Institute (2025). Cost of a Data Breach Report 2025. IBM. Recuperado de https://www.ibm.com/reports/data-breach

IBM. Riesgo humano en ciberseguridad. Recuperado de https://www.ibm.com/es-es/think/insights/cisos-list-human-error-top-cybersecurity-risk

IEEE. (2025). Homomorphic Encryption in Quantum Computing. Recuperado de https://ieeexplore.ieee.org/document/11012553/authors#authors

INCIBE-CERT. (2025). DDoS attacks: Techniques and mitigation in business infrastructures. Recuperado de https://www.incibe.es/en/incibe-cert/blog/ataques-ddos-tecnicas-y-mitigacion-en-infraestructuras-empresariales

Industrial Cyber. (2025). Strengthening pipeline security: A guide for OT professionals on TSA pipeline security directives and the 2024 notice of proposed rules. Recuperado de https://industrialcyber.co/regulation-standards-and-compliance/strengthening-pipeline-security-a-guide-for-ot-professionals-on-tsa-pipeline-security-directives-and-the-2024-notice-of-proposed-rules/

Instituto Federal de Telecomunicaciones (IFT). (2018). Plan de acciones en materia de ciberseguridad. Unidad de Política Regulatoria, Dirección General de Regulación Técnica. Recuperado de https://ciberseguridad.ift.org.mx/files/guias_y_estudios/5_upr_planaccionesciberseguridad.pdf

Instituto Federal de Telecomunicaciones (IFT). (2020). Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las Cosas (IoT). Recuperado de https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

Instituto Federal de Telecomunicaciones (IFT). (2021). Marco Nacional de Regulación sobre Ciberseguridad: Recomendaciones. Comité Técnico en materia de despliegue de 5G en México, Mesa 5 Ciberseguridad. Recuperado de https://comite5g.ift.org.mx/vendor/descarga_archivo.php?id_archivo=22632

Instituto Igarapé. (2025). National Strategy for Critical Infrastructures Security (ENSIC). Portal Brasileiro da Cibersegurança. Recuperado de https://ciberseguranca.igarape.org.br/en/national-strategy-for-critical-infrastructures-security-ensic/

International Telecommunication Union & World Bank. (2024). Guiding principles for ICT regulators to enhance cyber resilience. Digital Regulation Platform. Recuperado de https://digitalregulation.org/guiding-principles-for-ict-regulators-to-enhance-cyber-resilience/

Katz, R., Callorda, F., Iglesias, E., Gabarró, P. P., Dalio, M., & Zaballos, A. G. (2023). Impacto del uso compartido de infraestructura en la adopción de tecnologías digitales. Banco Interamericano de Desarrollo. Recuperado de https://publications.iadb.org/es/impacto-del-uso-compartido-de-infraestructura-en-la-adopcion-de-tecnologias-digitales

Keepnet. (2025) Security Awareness Training Statistics. Recuperado de https://keepnetlabs.com/blog/security-awareness-training-statistics

Koba, J. (2025). Cybersecurity standards for critical infrastructure. Kogifi. Recuperado de https://www.kogifi.com/articles/cybersecurity-standards-for-critical-infrastructure

KPMG. (2025). Novedades en ciberseguridad post-cuántica: del aviso al plan de acción. Recuperado de https://www.tendencias.kpmg.es/2025/06/novedades-ciberseguridad-post-cuantica-aviso-plan-accion/

Llamas Covarrubias, J. (2024). Ciberseguridad en México: nueve años de debate legislativo y propuestas de ley (2015-2024). Foro Jurídico. Recuperado de https://forojuridico.mx/ciberseguridad-en-mexico-nueve-anos-de-debate-legislativo-y-propuestas-de-ley-2015-2024/

MeriTalk. (2025). NIST, OMB Outline Challenges in Post-Quantum Migration. Recuperado de https://www.meritalk.com/articles/nist-omb-outline-challenges-in-post-quantum-migration/

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2022). Decreto 338 de 2022: Por el cual se adiciona el Título 21 al Decreto Único 1078 de 2015 en materia de seguridad digital. Recuperado de https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0338_2022.htm

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Lineamientos para la identificación de las infraestructuras críticas cibernéticas. Recuperado de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401778_recurso_1.pdf

National Cyber Security Centre. (2019). Virtualisation security design principles. NCSC. Recuperado de https://www.ncsc.gov.uk/collection/cyber-security-design-principles/virtualisation-security-design-principles

National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Nevada Office of Emergency Management. (s.f.). Critical Infrastructure. Recuperado de https://www.oem.nv.gov/homeland-security/critical-infrastructure/

Nozomi Networks. (2024). Get ready for CIRCIA and NIS2 cyber incident reporting. Recuperado de https://www.nozominetworks.com/blog/get-ready-for-circia-and-nis2-cyber-incident-reporting

Palo Alto Networks. (s.f.). IoT Under Siege: The Mirai Campaign. Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

Palo Alto Networks. Why Culture Is the First Line of Defense in the Age of Agentic AI. Recuperado de https://www.paloaltonetworks.com/perspectives/why-culture-is-the-first-line-of-defense-in-the-age-of-agentic-ai/#:~:text=It%20(%20a%20deeply%20ingrained%20security%20culture,formidable%20part%20of%20our%20collective%20security%20solution

Parliament of Canada. (2025). Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. Recuperado de https://www.parl.ca/DocumentViewer/en/45-1/bill/C-8/first-reading

PMK. (2025). El tsunami tecnológico de 2026. Recuperado de https://www.puromarketing.com/12/216477/tsunami-tecnologico-2026-colision-entre-cuantica

Presidencia de la República. (2025). Estrategia Nacional de Seguridad Digital 2025-2027. Recuperado de https://mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

Post-Quantum Cryptography Coalition. (2025). Post-Quantum Cryptography (PQC) Migration Roadmap. Recuperado de https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf

Proofpoint. (2024). Voice of the CISO 2024. Recuperado de https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2024-voice-ciso-report-reveals-three-quarters-cisos-identify

Proofpoint. (2025). Voice of the CISO 2025. Recuperado de https://www.proofpoint.com/sites/default/files/white-papers/pfpt-es-wp-voice-of-the-CISO-report.pdf

QuTech. (2021). Dutch researchers establish the first entanglement-based quantum network. Recuperado de: https://qutech.nl/2021/04/15/dutch-researchers-establish-the-first-entanglement-based-quantum-network/

Qiu, Q., Xu, S., Liu, S., Xu, T., & Zhao, B. (2024). Network virtualization security: Threats, measures, and use cases. En 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K). Recuperado de https://www.itu.int/en/ITU-T/academia/kaleidoscope/2024/Documents/P.2Network_Virtualiazation_Security_Threats_Measures_and_Us.pdf

Rapid7. (2025). Cybersecurity Awareness Month 2025: Building a Cybersecurity Culture That Lasts. Recuperado de https://www.rapid7.com/blog/post/c-cybersecurity-awareness-month-2025-building-a-cybersecurity-culture-that-lasts/

Radlanski, P., & Rudt, J. (2025). EU NIS 2 Directive: Expanded cybersecurity obligations for key sectors. Greenberg Traurig LLP. Recuperado de https://www.gtlaw.com/en/insights/2025/8/eu-nis-2-directive-expanded-cybersecurity-obligations-for-key-sectors

Red Seguridad (2025). Telefónica Tech e IBM colaboran en el desarrollo de tecnología de seguridad cuántica. Recuperado de https://www.redseguridad.com/actualidad/telefonica-tech-e-ibm-colaboran-en-el-desarrollo-de-la-tecnologia-de-seguridad-cuantica_20250203.html

Ribeiro, A. (2022). CISA directive likely to drive investment costs, raise need for more staff, update technology and processes. Industrial Cyber. Recuperado de https://industrialcyber.co/cisa/cisa-directive-likely-to-drive-investment-costs-raise-need-for-more-staff-update-technology-and-processes/

Rupp, C. (2025). ENISA: Fit for Purpose? Reviewing the EU Cybersecurity Agency's Role in an Evolving Policy Ecosystem. Interface. Recuperado de https://www.interface-eu.org/publications/enisa-fit-for-purpose

Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. Heliyon, 9(7), e17156. Recuperado de https://doi.org/10.1016/j.heliyon.2023.e17156

Schmitt, M., & Flechais, I. (2024). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. arXiv. Recuperado de https://arxiv.org/pdf/2310.13715

Secretaría de Innovación Pública. (2023). Se aprobó la segunda Estrategia Nacional de Ciberseguridad. Gobierno de la República Argentina. Recuperado de https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad

Secretaría de Innovación Pública. (2025). Objetivos de la Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros, República Argentina. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/objetivos-de-la-direccion

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Senado de la República de Chile. (2025). Protección de la infraestructura crítica: Comisión de Defensa perfecciona definiciones de conceptos claves. Recuperado de https://www.senado.cl/comunicaciones/noticias/proteccion-de-la-infraestructura-critica-comision-de-defensa-perfecciona

Siraparapu, S. R., & Azad, S. M. A. K. (2024). Securing the IoT landscape: A comprehensive review of secure systems in the digital era. e-Prime – Advances in Electrical Engineering, Electronics and Energy, 10, 100798. Recuperado de https://doi.org/10.1016/j.prime.2024.100798

StormWall. (s.f.). 2024 in Review: DDoS Attacks Report by StormWall. Recuperado de https://stormwall.network/resources/blog/ddos-attack-statistics-2024

Thales Group. (2025). Introducing EUCC: A new certificate to boost cybersecurity in Europe. Recuperado de https://www.thalesgroup.com/en/news-centre/insights/public-security/national-security/introducing-eucc-new-certificate-boost

The CPA Journal. (2025). The SEC Finalizes Rule on Cybersecurity Disclosures. Recuperado de https://www.cpajournal.com/2025/08/27/the-sec-finalizes-rule-on-cybersecurity-disclosures

The Hacker News. (2025). AI-Driven Ransomware FunkSec Targets 85 Victims Using Double Extortion Tactics. Recuperado de https://thehackernews.com/2025/01/ai-driven-ransomware-funksec-targets-85.html

The NET. Your first line of defense in cybersecurity. Recuperado de https://www.cloudflare.com/the-net/security-first-culture/

The SEC Finalizes Rule on Cybersecurity Disclosures. Recuperado de https://www.cpajournal.com/2025/08/27/the-sec-finalizes-rule-on-cybersecurity-disclosures

The White House. (2013). Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21). Recuperado de https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Trend Micro. (2024). Open RAN: Attack of the xApps. Recuperado de https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/open-ran-attack-of-the-xapps

Trend Micro. (2025). Qué es el SIM swapping y cómo evitarlo. Trend Micro. Recuperado de https://www.trendmicro.com/es_es/what-is/cyber-attack/types-of-cyber-attacks/sim-swapping-scams.html

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Trend Micro. (2025). SECURITY PREDICTIONS FOR 2026. Recuperado de https://documents.trendmicro.com/assets/research-reports/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026.pdf?_gl=1*dxiz24*_gcl_au*MTQwMTEwNTA2OC4xNzY0NzI3NDEz*_ga*MTk4ODk0NzI4Ni4xNzY0NzI3NDEz*_ga_PCCSVH5M9H*czE3NjQ3Mjc0NTgkbzEkZzEkdDE3NjQ3Mjc1NTUkajQ3JGwwJGgxNDYyNTUxOTM1

Universidad Isabel I (UI1), España. (2023). Conectados' Octubre, mes de la ciberseguridad. Recuperado de https://www.ui1.es/blog-ui1/octubre-celebrando-el-mes-de-la-ciberseguridad#:~:text=Reconocer%20y%20reportar%20phishing.,es%20para%20toda%20la%20sociedad.

UNCTAD (United Nations Conference on Trade and Development). (2024). Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future. Ginebra: Naciones Unidas. Recuperado de https://unctad.org/publication/digital-economy-report-2024

Verizon Business. (2025). 2025 Data Breach Investigations Report (DBIR). Nueva York: Verizon. Recuperado de https://www.verizon.com/business/resources/reports/dbir/

Vikingcloud. (2025). Cybersecurity Stats and Facts for 2025. Recuperado de https://www.vikingcloud.com/blog/cybersecurity-statistics#spending

Wind4change. Cultura Organizacional y Liderazgo por Edgar H.Schein. Recuperado de https://wind4change.com/organizational-culture-leadership-framework-edgar-schein/

World Economic Forum. (2023). What cybersecurity threats does generative AI expose us to? Recuperado de https://www.weforum.org/stories/2023/06/what-cybersecurity-threats-are-posed-by-generative-ai/

World Economic Forum. (2025). Global Cybersecurity Outlook 2025. Ginebra: World Economic Forum. Recuperado de https://www.weforum.org/publications/global-cybersecurity-outlook-2025