Tendencias en Ciberseguridad y Criptografía para un Futuro Confiable 2026

Conecta
Mayo 2026

WP01

ÍNDICE

PRÓLOGO

En los últimos años, el sector tecnológico ha vivido un punto de inflexión: más digitalización, más datos, más automatización y también más riesgo. La ciberseguridad dejó de ser un tema reservado para especialistas; hoy es un eje que define la capacidad de un país, una empresa o una industria para innovar, competir y crecer.

En Conecta creemos que la confianza digital es el nuevo habilitador económico de América Latina. La región tiene talento, creatividad y una adopción tecnológica que avanza más rápido de lo que muestran las estadísticas tradicionales, pero también enfrenta desafíos históricos: desinformación, ataques a infraestructura crítica, sistemas fragmentados y brechas de protección de datos.

Este white paper nace con un propósito claro: ofrecer una visión regional y global sobre las tendencias de ciberseguridad y criptografía que marcarán el rumbo hacia 2026. Pero sobre todo, busca convertirse en una guía accesible para líderes tecnológicos, innovadores y responsables de diseñar el futuro digital de América Latina.

La confianza no se decreta; se construye. Y en Conecta estamos convencidos de que un ecosistema más seguro, interoperable y responsable es la base para acelerar la innovación que viene. Gracias por acompañarnos en este recorrido hacia un futuro donde la tecnología inspire certeza y no vulnerabilidad.

INTRODUCCIÓN

1.1 Propósito del documento

En Conecta estamos convencidos de algo que parece simple, pero que cambia por completo la forma en que entendemos el futuro digital: **la seguridad ya no es un requisito técnico, es una condición indispensable para operar.** En un entorno donde la tecnología avanza más rápido que las regulaciones y donde los riesgos evolucionan casi a diario, la ciberseguridad y la criptografía se han convertido en pilares que determinan quién puede innovar con confianza.

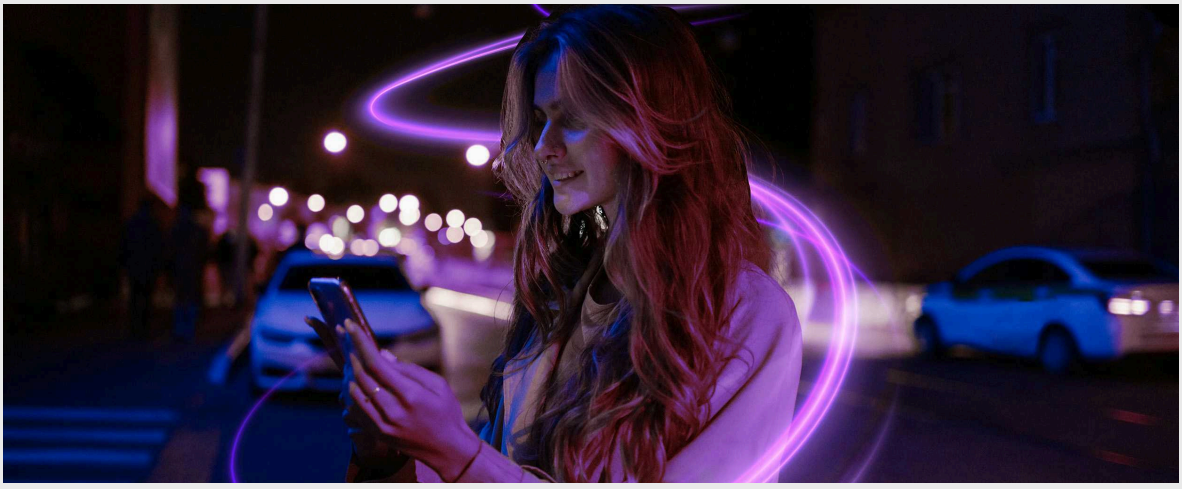
Este documento nace justamente de esa convicción. A lo largo del último año hemos analizado, contrastado y reinterpretado las tendencias más relevantes publicadas por organismos como la OCDE, Gartner, WEF, ENISA y la Unión Europea.

Pero más allá de reunir información global, nuestro trabajo ha sido traducirla al lenguaje, los retos y las oportunidades reales de México y América Latina. Conecta aporta aquí su mirada y, por ende, su criterio.

Este white paper busca dos cosas:

Ayudar a entender hacia dónde se mueve la seguridad digital mundial, qué tecnologías están cambiando las reglas del juego y qué riesgos emergen con mayor rapidez.

Ofrecer caminos de acción claros, realistas y adaptados a distintos niveles de madurez organizacional, para que la región pueda acelerar innovación sin perder estabilidad ni confianza.



Vemos este documento como una herramienta, pero también como una invitación a que líderes tecnológicos, reguladores, emprendedores y responsables de innovación se animen a mirar la seguridad no como un freno, sino como un habilitador.

Porque si algo hemos aprendido en Conecta es que la confianza digital no surge de la nada: se diseña, se construye y se sostiene con visión de largo plazo. Este es nuestro aporte a ese futuro. Y apenas es el comienzo.

1.2 Por qué la ciberseguridad será un acelerador crítico de competitividad en 2026

El entorno digital global evoluciona con velocidad; a medida de que las empresas, los gobiernos y los ciudadanos migran hacia lo digital, aumenta también la superficie de riesgo: datos, identidades, infraestructura, interdependencia de servicios.

En ese contexto, la ciberseguridad deja de ser un gasto, se convierte en un activo estratégico.

Gestionar adecuadamente el riesgo digital ya no es opcional: es una condición para la continuidad operativa, la atracción de inversiones, la innovación sostenible y la competitividad en mercados cada vez más exigentes. Para muchas organizaciones en México y América Latina, diseñar con seguridad no es solo una buena práctica: será una ventaja competitiva.

Estos datos reflejan una tendencia global clara: la inversión en seguridad ya no crece sólo por miedo a pérdidas, sino por necesidad de resiliencia, continuidad y confianza.

Indicador / Tendencia	Valor estimado / Cambio	Fuente / Reporte
Gasto mundial en seguridad informática (2025)	US$ 213.000 millones	Gartner (forecast 2025)
Crecimiento proyectado del gasto en 2026	**12.5 %** (hasta US$ 240. 000 millones)	Gartner 2025 forecast
Enfoque de la seguridad digital como factor económico/ social, no solo técnico	Conceptualización de riesgo digital como condición para prosperidad	OECD / Policy Framework on Digital Security / Digital Security Risk Management

Datos globales recientes (contexto 2024–2025)

Qué significa para México y América Latina

Para organizaciones en México y la región, esto implica una ventana importante de oportunidad.
Con un mercado global que incrementa su inversión en seguridad y con una transformación digital acelerada, asegurar operaciones, datos e infraestructuras digitales será clave para:

Cumplir con estándares internacionales, regulaciones y mejores prácticas globales.

Atraer inversiones extranjeras o de capital internacional, mostrando madurez en gobernanza digital.

Ofrecer servicios digitales confiables, lo que incrementa la confianza de usuarios y stakeholders.

Competir en mercados globales o regionales cuando la barrera de entrada sea la seguridad.

En otras palabras: la ciberseguridad dejará de ser un costo inevitable para convertirse en un requisito imprescindible para competir, crecer e innovar.

2. Panorama Global de Amenazas hacia 2026

La ciberseguridad a nivel global enfrenta una convergencia de factores que intensifican los riesgos estructurales en el entorno digital. La digitalización masiva de servicios críticos, combinada con la sofisticación de actores maliciosos y la introducción de inteligencia artificial en tácticas ofensivas, ha transformado las amenazas en un desafío sistémico con implicaciones macroeconómicas y de resiliencia operativa.

De hecho, el Global Cybersecurity Outlook 2025 del Foro Económico Mundial subraya que la complejidad del panorama se ve intensificada por tensiones geopolíticas, interdependencias de cadenas de suministro digital y la sofisticación del crimen cibernético organizado.

2.1. Evolución del riesgo en el entorno digital

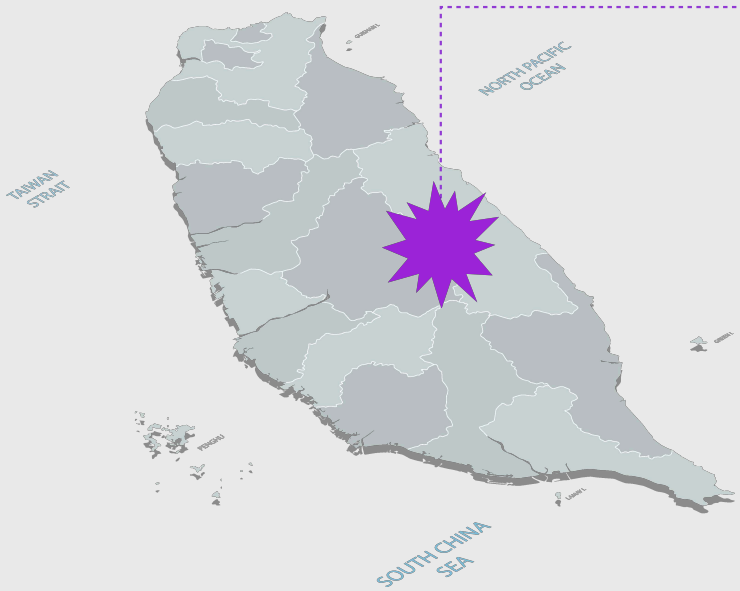
Diversos informes globales de amenaza muestran que el riesgo digital ya no es un fenómeno aislado. ***El Global Threat Landscape Report 2025 de FortiGuard Labs*** documenta un incremento notable en la automatización de ataques, robo de credenciales y explotación de vulnerabilidades conocidas, indicando que los adversarios están ampliando su superficie de ataque mediante prácticas más rápidas y escalables.

Este proceso de profesionalización y escalabilidad se refleja en cifras de incidentes que aumentan tanto en volumen como en sofisticación, generando un entorno donde la continuidad de servicios esenciales y la estabilidad operativa son vectores críticos a proteger.

2.2. Aumento de ataques a infraestructura crítica

Los ataques dirigidos a infraestructura crítica han crecido en frecuencia e impacto. Un artículo reciente de Reuters reporta que, en 2025, Taiwán enfrentó un promedio de 2.63 millones de ataques diarios contra infraestructura esencial, incluyendo hospitales, energía y bancos, lo que muestra la dimensión de este riesgo incluso en economías avanzadas.

Otras fuentes especializadas muestran que los ataques a la cadena de suministro y a plataformas operativas de terceros se han consolidado como vectores preferidos tanto por grupos criminales como por actores estatales, con repercusiones directas en disponibilidad y resiliencia operativa.



Un artículo reciente de Reuters reporta que, en 2025

2.63

millones de ataques diarios en Taiwan

2.3. Estado de la cibercriminalidad global y expansión de mercados ilícitos

La cibercriminalidad global opera con una lógica empresarial. El Global Threat Report 2025 de CrowdStrike destaca que los adversarios actúan con modelos organizados ,incluyendo automatización, IA y tácticas de ingeniería social, lo que los convierte en competidores más sofisticados de los defensores tradicionales.

Otros reportes de Cyble muestran un aumento sostenido de ransomware, explotación de vulnerabilidades de día cero y la aparición de nuevos grupos de amenazas en múltiples regiones, lo que subraya la expansión continua de mercados ilícitos que lucran con la interrupción, extorsión y explotación de datos.

2.4. Tendencias en ataques basado en IA generativa

Una variable clave hacia 2026 es el uso malicioso de IA generativa por parte de actores ofensivos.

El Global Cybersecurity Outlook 2025 ya señalaba que casi la mitad de las organizaciones a nivel global identifican el uso malicioso de IA generativa como una de sus principales preocupaciones cibernéticas.

Informes de tendencias de seguridad indican un crecimiento exponencial en ataques de phishing potenciados por IA y otras formas de explotación automatizada que reducen la barrera de entrada para atacantes menos especializados.

Además, noticias de organismos como Europol advierten sobre la incorporación de IA en operaciones del crimen organizado ,incluyendo deepfakes y técnicas de suplantación avanzadas, lo que realza la complejidad del panorama de amenazas.

3.Ciberseguridad impulsada por IA

La inteligencia artificial (IA) ya no es solo un componente emergente de las estrategias de seguridad: es un factor transformador que redefine radicalmente tanto las capacidades ofensivas de los cibercriminales como las defensivas de las organizaciones.

En 2026, la IA impulsará una verdadera "carrera armamentista" cibernética en la que la automatización, la adaptabilidad y la autonomía acelerarán tanto ataques como defensas.

3.1. IA ofensiva: automatización del hacking y explotación de vulnerabilidades

La IA ofensiva permite a los atacantes escalar operaciones que antes requerían equipos humanos completos. Modelos avanzados ahora automatizan tareas como:

- **Reconocimiento de superficies de ataque,**
- **Búsqueda de vulnerabilidades,**
- **Generación de exploits adaptativos,**
- **Ingeniería social altamente personalizada.**

Expertos han documentado casos recientes en los que campañas de hacking han sido dirigidas por IA con niveles mínimos de intervención humana, señalando un aumento tangible en la sofisticación y la rapidez de ejecución.

Diversos informes indican que la IA se utiliza para automatizar ataques complejos, desde phishing hiperrealista hasta malware polimórfico que evade detecciones tradicionales mediante modificaciones permanentes de su firma.

3.2. IA defensiva: detección anticipada, threat intelligence y respuesta autónoma

En el lado defensivo, la IA está redefiniendo la detección y respuesta:

La detección basada en patrones clásicos está siendo reemplazada por análisis de comportamiento y anomalías impulsados por IA, lo que reduce el tiempo de respuesta de días a minutos.

Plataformas integrales de Threat Intelligence anticipan vectores emergentes, correlacionan señales en tiempo real y ajustan defensas de forma automática.

La automatización de respuesta permite contener incidentes sin intervención humana directa, especialmente útil para ataques que se propagan a velocidades que superan la reacción tradicional.

Este enfoque ayuda a las organizaciones a escalar defensas de manera eficiente y a compensar la escasez de talento especializado en seguridad.

3.3. Security AI Fabric y Cyber-security Mesh hacia 2026

Hacia 2026 se proyecta una evolución arquitectural en seguridad:

- **Security AI Fabric** se refiere a la integración de capacidades de IA en todos los niveles de la pila de seguridad, desde sensores hasta respuesta automatizada. Este enfoque pretende asegurar que la IA no solo detecte amenazas, sino que participe como una capa transversal de resiliencia en redes, aplicaciones, identidades y cargas de trabajo.

- **Cybersecurity Mesh** adopta un enfoque descentralizado en el cual los controles de seguridad están distribuidos y adaptativos, lo que permite a entornos híbridos y multi-cloud responder con mayor agilidad ante amenazas.

Estos modelos responden a la complejidad creciente de los entornos empresariales y la necesidad de visibilidad y orquestación en tiempo real en un contexto de proliferación de activos digitales.

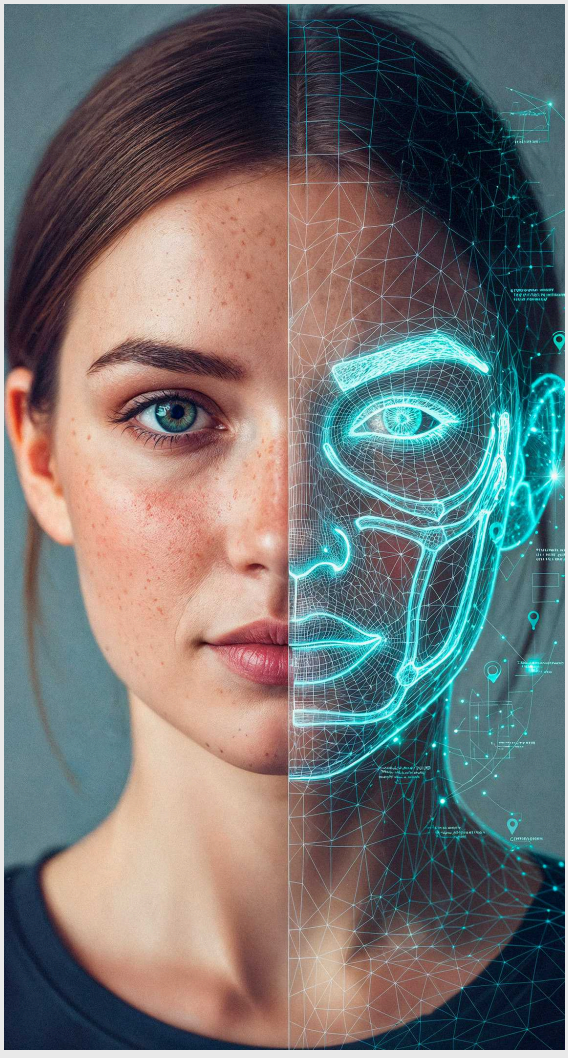
3.4. Riesgos de modelos fundacionales y deepfakes

- **Los modelos fundacionales** (como grandes modelos de lenguaje y generativos) introducen riesgos inherentes que se traducen en nuevas superficies de ataque: Deepfakes y contenidos sintéticos altamente verosímiles se usan para ingeniería social avanzada, fraude e intrusiones. En 2026 estos ya no son amenazas aisladas, sino parte del núcleo de los vectores de riesgo.

- **Los modelos pueden ser explotados** para prompt injection, jailbreaking o como portaaviones de código malicioso sofisticado.

- **El mal uso de modelos generativos** puede corroer la confianza digital y facilitar ataques dirigidos a personas clave (executive impersonation), extorsión y fraude de identidad.

Además, deepfakes no solo representan un riesgo de confianza, sino también un desafío de seguridad operativa que afecta desde canales de comunicación interna hasta procesos de autenticación y decisiones automatizadas.



4. Criptografía en la era post-cuántica

La criptografía de clave pública que sostiene Internet y los sistemas financieros modernos (p. ej., RSA y ECC) enfrenta un cambio estructural: computadoras cuánticas suficientemente capaces podrían romper estos esquemas, afectando confidencialidad, firmas digitales e integridad.

Aunque el "Q-Day" no tiene fecha cierta, el riesgo operativo ya es presente por dos razones: (1) la inercia de migración criptográfica es alta (años), y (2) existe el escenario "harvest now, decrypt later" (capturar hoy para descifrar después). La respuesta global está convergiendo en una transición hacia criptografía post-cuántica (PQC) y, sobre todo, hacia criptoagilidad como capacidad estratégica.

4.1. La amenaza cuántica y por qué está acelerando la migración

La amenaza cuántica se concentra en dos clases de activos:

- **Confidencialidad de largo plazo** (datos personales, financieros, secretos comerciales, expedientes médicos, información gubernamental) que deben permanecer protegidos por años.
- **Confianza transaccional** (firmas digitales, certificados, autenticación) que sostiene pagos, mensajería financiera, actualizaciones de software y no repudio.

Por eso, gobiernos y reguladores están empujando la planeación anticipada. La Comisión Europea emitió una Recomendación (EU) 2024/1101 para coordinar la transición a PQC en el sector público y promover una migración sincronizada. En paralelo, el BIS (enfocado en estabilidad financiera) publicó un marco de "quantum-readiness" para acelerar inventario criptográfico y transición en el sistema financiero.

4.2. Directrices para la transición post-cuántica

La transición hacia criptografía post-cuántica no es un ejercicio teórico ni un reemplazo inmediato de algoritmos, sino un proceso gradual de gestión de riesgo, continuidad operativa y cripto-agilidad. A nivel global, las recomendaciones más consistentes convergen en una ruta práctica que permite a las organizaciones prepararse sin interrumpir operaciones críticas, priorizando visibilidad, clasificación de riesgos y planes de migración por dominios tecnológicos. Estas directrices buscan habilitar una transición ordenada, compatible con ecosistemas complejos y dependencias externas.

Las guías más consistentes a nivel global convergen en una ruta práctica:

Inventario criptográfico (crypto inventory)

- Mapear dónde se usa criptografía (TLS, VPN, HSM, PKI, firmas, cifrado en reposo, mensajería, tokens, APIs, mobile, backups) y qué algoritmos/longitudes de clave están desplegados:

Clasificación por criticidad y vida útil del dato

- Priorizar sistemas con datos de largo plazo y funciones críticas (pagos, core, identidad, canales, interbancario, SWIFT, etc.).

Plan de migración por dominios

- Priorizar PKI/certificados, TLS, firmware/software signing, y canales críticos.
- Diseñar ventanas de transición y compatibilidad con terceros.

Pruebas de desempeño y compatibilidad

- PQC cambia tamaños de llaves/firmas y puede impactar latencia, CPU, MTU, appliances y sistemas legados; requiere pruebas en escenarios reales.

Gobernanza y procurement

- Exigir a proveedores soporte PQC/criptoagilidad (roadmap, validaciones, interoperabilidad), especialmente en servicios cloud, HSM, PKI, IAM, gateways y plataformas de pago.

4.3. Algoritmos post-cuánticos: estándares emergentes 2024–2026

El hito clave reciente es la formalización de estándares PQC por NIST en agosto de 2024:

- FIPS 203 (ML-KEM): mecanismo de encapsulación de claves (basado en CRYSTALS-Kyber renombrado).
- FIPS 204 (ML-DSA): firmas digitales (basado en CRYSTALS-Dilithium renombrado).
- FIPS 205 (SLH-DSA): firmas hash-based (SPHINCS+).

Esto marca la base para despliegues en sector público y referencia global para industria regulada. Adicionalmente, algunos marcos gubernamentales (por ejemplo NSA CNSA 2.0) establecen perfiles de algoritmos y cronogramas orientativos para sistemas de alta criticidad, empujando adopción temprana y validación de proveedores.

4.4. Criptoagilidad como requisito estratégico

En la práctica, el mayor riesgo no es solo "qué algoritmo elegir", sino cuán rápido puede una organización:

- rotar algoritmos,
- reemplazar bibliotecas criptográficas,
- reemitir certificados,
- migrar HSM/PKI,
- y asegurar interoperabilidad con terceros,

sin detener operaciones.

Por eso, la criptoagilidad debe tratarse como capacidad de resiliencia operativa: arquitectura modular, abstracción criptográfica, inventario siempre actualizado, automatización de rotación de llaves/certificados, y controles de configuración para evitar "cripto-deuda" (dependencias heredadas que frenan el cambio). ETSI, ENISA y BIS convergen en esta tesis: la preparación (inventario + agilidad) es tan importante como el algoritmo.

4.5. Casos de uso emergentes en finanzas, gobierno y salud

Finanzas

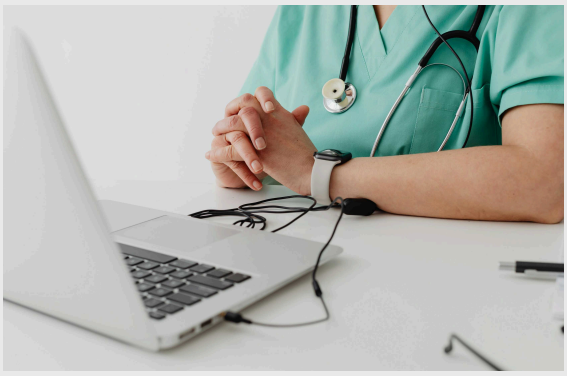
- *Sistemas de pagos y mensajería*: pilotos y experimentos de bancos centrales y socios (incluyendo SWIFT) muestran la complejidad real de sustituir firmas tradicionales por PQC en flujos operativos.
- PKI y canales (TLS): migración de certificados y autenticación en canales digitales, APIs y conexiones B2B.

Gobierno

- *Coordinación nacional y procurement*: la Recomendación de la Comisión Europea impulsa planes coordinados sincronizados, clave para inter-operabilidad en servicios públicos y proveedores.
- *Perfiles de seguridad de alta criticidad*: guías tipo CNSA 2.0 orientan adopción de algoritmos "quantum-resistant" en sistemas sensibles.

Salud

- *Protección de datos de largo plazo*: expedientes clínicos, genómica y datos sensibles requieren confidencialidad prolongada; el riesgo "harvest now, decrypt later" vuelve prioritaria la planeación y el cifrado robusto en reposo y tránsito.



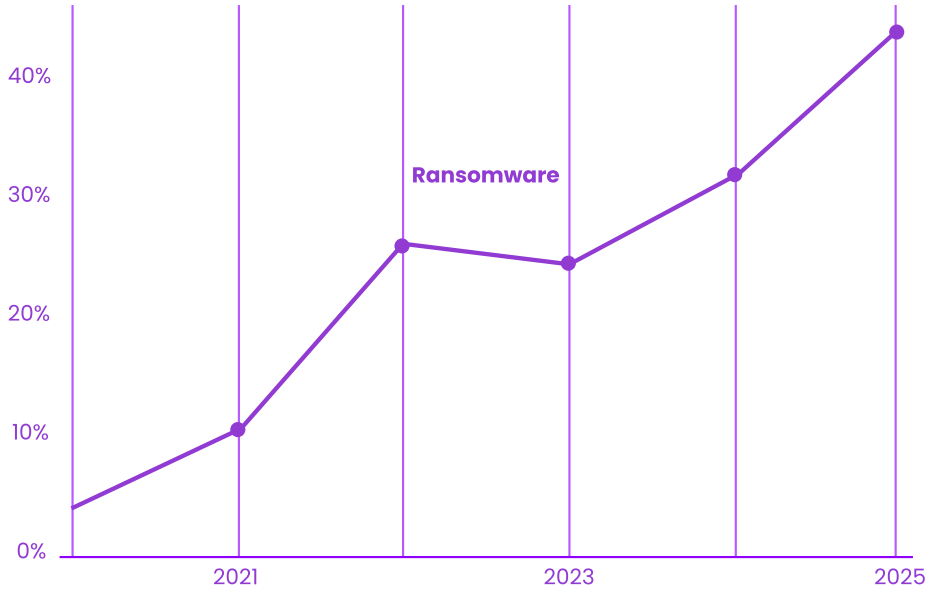
5. Ransomware

El ransomware es un riesgo de resiliencia operativa: afecta disponibilidad, integridad y, cada vez más, la confidencialidad (por exfiltración). En infraestructura financiera y de pagos, su criticidad aumenta por (i) alta dependencia de disponibilidad, (ii) interconexión con terceros y (iii) presión regulatoria ante interrupciones y fuga de datos.

En términos de tendencia, el ransomware ya no se limita a "cifrar y cobrar", sino que opera como intrusión persistente con extorsión múltiple y explotación de superficies híbridas (on-prem, cloud, SaaS y supply chain).

5.1. Evolución y amenazas actuales de ransomware

La evidencia reciente confirma que el ransomware es una técnica dominante dentro de incidentes de intrusión. Verizon reporta que el ransomware estuvo involucrado en el 44% de las brechas de seguridad evaluadas y que su presencia **creció un 37% desde el ultimo reporte.** Esto refuerza que el ransomware es un resultado frecuente de compromisos que comienzan con credenciales, vulnerabilidades o accesos remotos.



Fuente: www.verizon.com

En impacto económico, la presión sobre recuperación y continuidad es material: Sophos señala que "The average (mean) cost to recover… came in at **$1.53 million** (excluyendo el pago del rescate)", y que "53%" de las organizaciones se recuperaron en una semana. Complementariamente, IBM/Ponemon destaca el costo de disrupción y respuesta: "The global average cost of a data breach… reaching USD 4.88 million", impulsado en gran parte por business disruption.

A nivel macro de riesgo, ENISA coloca el ransomware como una de las amenazas prime del periodo y observa que, en su muestra de eventos, el sector finance representa 9% de los eventos objetivos (en su distribución sectorial). Implicación práctica: el ransomware debe modelarse como un escenario plausible de operación (no excepcional), con supuestos de intrusión previa, potencial exfiltración y necesidad de recuperación bajo presión de tiempo y de terceros.

5.2. Vectores de ataque y errores comunes

Vectores técnicos recurrentes:

1. **Credenciales comprometidas** (phishing, password reuse, infostealers) y abuso de sesiones legítimas.
2. **Exposición/compromiso de edge** (VPN, gateways, dispositivos perimetrales) y explotación de vulnerabilidades.
3. **Terceros y supply chain** (proveedores con acceso, integraciones, cuentas compartidas).
4. **Entornos híbridos:** credenciales/roles en cloud mal gobernados + movimientos laterales hacia activos on-prem.

Verizon aporta un dato relevante sobre la superficie perimetral: los dispositivos edge y las VPN representaron el 22% de los objetivos en la explotación de vulnerabilidades, y solo aproximadamente **el 54% de estas vulnerabilidades fueron completamente remediadas,** con un tiempo mediano de corrección de 32 días.

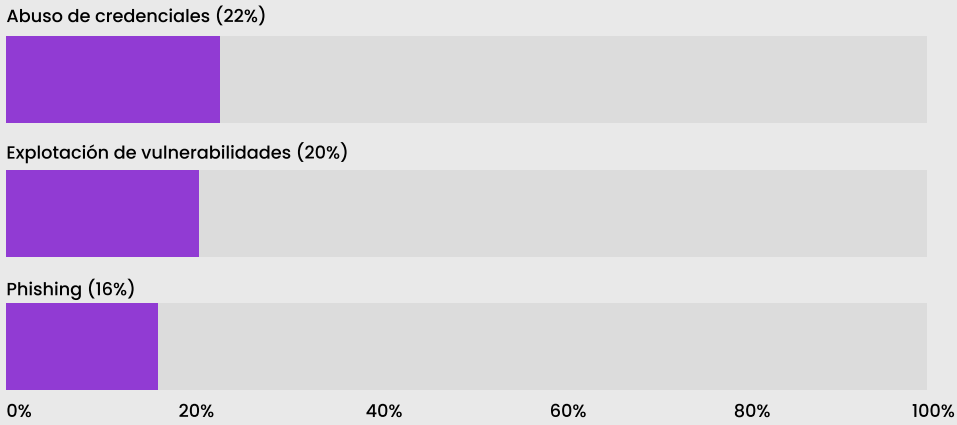
Errores operativos típicos

- *Privilegios excesivos* (ausencia de least privilege y separación de funciones).
- *Segmentación insuficiente* (capacidad del atacante de moverse a AD/PKI, backups, virtualización, sistemas de pago).
- *Backups* sin aislamiento/ inmutabilidad y sin pruebas periódicas de restauración.
  Telemetría incompleta (sin EDR/NDR eficaz, sin logging centralizado, sin correlación de identidades).

5.3 Impacto técnico, financiero y reputacional

Técnico
Cifrado + deshabilitación de herramientas defensivas, sabotaje de respaldos, compromiso de AD, hypervisors, repositorios y pipelines.

Afectación de servicios críticos (canales, conciliación, mensajería, onboarding/ identidad, operación interbancaria) por indisponibilidad o pérdida de integridad.



Vector de acceso inicial conocido en brechas de seguridad que no son de tipo Error ni Uso Indebido.(n 9,891)

Fuente: www.verizon.com

Financiero

Costos directos: respuesta a incidentes, forense, contención, reconstrucción, hardening, reemplazo de equipos y horas hombre.

Costos indirectos: pérdida de ingresos por downtime, penalizaciones contractuales, litigios y potenciales sanciones.

Referencias de magnitud: **Sophos reporta $1.53M** promedio de recuperación (sin rescate). **IBM reporta $4.88M** costo promedio global por brecha (con fuerte componente de disrupción).

SOPHOS

$1.53M

promedio de recuperación

IBM

$4.88M

promedio global por brecha

Reputacional y regulatorio

Notificación obligatoria/expectativas de supervisión, pérdida de confianza, deterioro de relaciones con partners y clientes, y mayor escrutinio de controles de continuidad y seguridad.

5.4 Estrategias de contención, mitigación y defensa

La defensa efectiva se basa en reducir probabilidad de intrusión exitosa, limitar propagación y asegurar recuperación.

Prevención y reducción de superficie

- MFA fuerte y controles anti-phishing; hardening de accesos remotos; PAM para privilegios; rotación y gestión de secretos.
- Gestión de vulnerabilidades con foco en edge y exposición externa (SLA de parchado y verificación).
- Control de identidades y permisos en cloud (least privilege + políticas de acceso condicional).

Resiliencia y recuperación

- Backups **inmutables/air-gapped** con pruebas regulares de restauración (RTO/RPO por dominio).
- "Golden images" y procedimientos de rebuild; recuperación priorizada de identidad (AD/IAM), redes, y plataformas transaccionales.
- Simulacros (table-top + técnicos) con participación de operaciones, seguridad, legal/compliance y negocio.

Gobernanza y terceros

- Exigir a proveedores controles verificables
- Métricas de resiliencia (tiempo de detección/contención, cobertura de logging, éxito de restauración, cumplimiento de parchado en edge).

Cyber Data Security

6. Seguridad en Infraestructura Crítica y Cloud Soberano

La seguridad de la infraestructura crítica se consolida como un eje estratégico de soberanía digital y resiliencia nacional. La convergencia IT/OT, la adopción de arquitecturas cloud distribuidas y el incremento de amenazas avanzadas amplían de forma significativa la superficie de ataque de sectores esenciales como energía, tele-comunicaciones, servicios financieros y gobierno.

De cara a 2025–2026, el desafío no radica únicamente en prevenir incidentes, sino en diseñar infraestructuras seguras por diseño, resilientes por defecto y alineadas con marcos regulatorios emergentes.

6.1 Seguridad en OT/ICS: tendencias hacia 2025–2026

Los entornos OT/ICS atraviesan una transformación estructural impulsada por su integración con plataformas digitales y cloud. Protocolos industriales heredados, originalmente aislados, operan ahora en ecosistemas interconectados, lo que incrementa la exposición a ataques dirigidos con impacto físico y operacional. Hacia 2025–2026, se consolida un enfoque de defensa en profundidad adaptado a OT, basado en visibilidad continua, segmentación industrial, detección de anomalías por comportamiento y control estricto de accesos privilegiados, priorizando la continuidad operativa sobre modelos tradicionales de patching.

6.2 Zero Trust aplicado a infraestructuras nacionales

Zero Trust evoluciona hacia un marco arquitectónico clave para la protección de infraestructuras nacionales altamente distribuidas. Su aplicación en entornos críticos implica verificación continua de identidades humanas y no humanas, segmentación lógica de activos esenciales y políticas de acceso dinámicas basadas en riesgo.

Más que una implementación tecnológica, Zero Trust representa un cambio estructural en los modelos de gobernanza de acceso, particularmente relevante para ecosistemas público-privados interconectados.

6.3 Transición hacia nubes soberanas

La transición hacia nubes soberanas responde a la necesidad de control jurisdiccional, gobernanza de datos críticos y reducción de dependencias estratégicas. El modelo dominante hacia 2025–2026 se orienta a arquitecturas híbridas y multicloud soberanas, que combinan capacidades de proveedores globales con control local de datos sensibles. Este enfoque habilita innovación controlada en sectores regulados, siempre que exista madurez en clasificación de datos, cifrado y auditoría continua.

6.4 Protección de datos sensibles y continuidad operativa

La protección de datos sensibles y la continuidad operativa convergen en un enfoque integral de ciberresiliencia. Los incidentes recientes evidencian que la indisponibilidad de servicios esenciales puede generar impactos sistémicos.

Por ello, las organizaciones líderes integran protección de datos, arquitecturas de alta disponibilidad, respaldos inmutables y planes de recuperación probados periódicamente. Hacia 2025–2026, la continuidad operativa se consolida como una capacidad estratégica más allá del cumplimiento normativo.

7. Marcos Regulatorios y Estándares Internacionales

El entorno regulatorio en ciberseguridad y tecnologías avanzadas ha entrado en una fase de endurecimiento estructural. A partir de 2025, los marcos normativos dejan de enfocarse únicamente en controles técnicos y comienzan a exigir capacidades organizacionales medibles: gobernanza, gestión de riesgos, resiliencia operativa y responsabilidad directa del liderazgo ejecutivo.

De acuerdo con el Global Cybersecurity Outlook 2025 del World Economic Forum, el 92% de los líderes globales considera que la fragmentación regulatoria incrementa de forma material el riesgo operativo y de cumplimiento, especialmente para organizaciones con presencia multinacional.

7.1 Regulaciones de ciberseguridad a nivel internacional

Las regulaciones internacionales convergen hacia enfoques basados en riesgo sistémico y continuidad operativa. Iniciativas como la Directiva NIS2 en Europa amplían de manera significativa el universo de organizaciones sujetas a obligaciones de ciberseguridad, elevando responsabilidades explícitas a nivel de consejo y alta dirección. La Comisión Europea estima que NIS2 multiplica por más de diez el número de entidades reguladas, reflejando un cambio claro: la ciberseguridad deja de ser una función técnica y pasa a ser un elemento de gobernanza corporativa.

7.2 Regulaciones emergentes sobre IA y seguridad

La inteligencia artificial entra en un ciclo de regulación estructural. Marcos como el AI Act europeo introducen una clasificación de riesgos que impacta directamente a sectores financieros, infraestructura crítica y servicios digitales esenciales. Estas regulaciones no solo buscan mitigar riesgos éticos, sino también reducir vulnerabilidades de seguridad, abuso de modelos y riesgos sistémicos derivados del uso de IA en procesos críticos. Para las organizaciones, esto implica rediseñar procesos de desarrollo y despliegue incorporando controles de seguridad, trazabilidad y supervisión desde el origen.

7.3 Principios de IA confiable y segura

Los principios de IA confiable: transparencia, explicabilidad, robustez, equidad y supervisión humana, se han consolidado como referencia transversal. Más allá del cumplimiento normativo, estos principios comienzan a integrarse en marcos de auditoría interna y gestión de riesgos tecnológicos. Su adopción se vuelve un requisito operativo para preservar confianza, especialmente en contextos donde decisiones automatizadas impactan directamente a clientes, ciudadanos o mercados.

7.4 Marcos de gobernanza y seguridad para modelos avanzados

El uso de modelos fundacionales y sistemas de IA avanzados introduce riesgos no triviales asociados a dependencia tecnológica, uso indebido y exposición de datos. Hacia 2026, los marcos de gobernanza más maduros priorizan el control del ciclo de vida del modelo, la evaluación continua de riesgos y la segregación clara de responsabilidades entre áreas técnicas, legales y de seguridad.

Este enfoque responde a una realidad creciente: los fallos en IA ya no son solo fallos técnicos, sino eventos con impacto reputacional, regulatorio y operativo.

7.5 Hacia un estándar latino-americano de ciberseguridad

En América Latina, la fragmentación regulatoria limita la cooperación regional y eleva costos de cumplimiento. Organismos multilaterales han señalado que la falta de estándares comunes dificulta la respuesta coordinada a incidentes y frena la inversión digital. Avanzar hacia un estándar latino-americano alineado con marcos internacionales, pero adaptado a realidades locales, representa una oportunidad estratégica para fortalecer resiliencia regional y competitividad.

8. Confianza Digital: Identidad, Datos y Privacidad

La confianza digital se ha convertido en un activo crítico para la economía digital. La gestión de identidad, datos y privacidad ya no puede abordarse como capas aisladas, sino como un sistema integrado que sostiene acceso, transacciones y decisiones automatizadas.

La pérdida de confianza se traduce rápidamente en impactos operativos y de negocio: estudios de la OECD indican que más del 60% de los usuarios abandonaría una organización tras un incidente grave de uso indebido de datos.

8.1 Identidad digital resistente a fraudes

La identidad digital se consolida como el nuevo perímetro de seguridad. Reportes recientes de Experian muestran un crecimiento interanual superior al 20% en fraude de identidad, impulsado por esquemas sintéticos y suplantación avanzada. Hacia 2026, las arquitecturas dominantes combinan autenticación multifactor adaptativa, identidades verificables y análisis de comportamiento en tiempo real para proteger no solo accesos, sino flujos completos de negocio.

8.2 Marcos de protección de datos

Los marcos de protección de datos evolucionan hacia enfoques de gobernanza integral del dato. Las organizaciones líderes integran clasificación, cifrado, control de acceso y trazabilidad como capacidades estructurales, particularmente relevantes en arquitecturas cloud y en el uso intensivo de analítica e inteligencia artificial. Este enfoque reduce fricción regulatoria y mitiga riesgos de exposición masiva de información sensible.

8.3 Privacidad diferencial y confidential computing

La privacidad diferencial y el confidential computing emergen como habilitadores clave para el uso avanzado de datos en entornos regulados. Estas tecnologías permiten procesar información sensible sin exponerla, incluso durante su uso, facilitando colaboración interinstitucional y adopción de IA sin comprometer cumplimiento ni confianza.

8.4 Secure Multi-Party Computation y Zero-Knowledge Proofs

Técnicas como Secure Multi-Party Computation y Zero-Knowledge Proofs avanzan como mecanismos prácticos para validar información sin revelar datos subyacentes. Su adopción en servicios financieros y procesos de cumplimiento refuerza modelos de confianza basados en verificación matemática, reduciendo dependencia de intermediarios y superficies de ataque asociadas al intercambio de datos.

9. Criptografía Aplicada e Innovación Descentralizada

La criptografía aplicada se ha convertido en infraestructura crítica de confianza.
Su relevancia se extiende más allá de blockchain hacia modelos de verificación, integridad y gobernanza en sistemas distribuidos y plataformas digitales complejas.

9.1 Tendencias de seguridad en blockchain hacia 2026

La seguridad en blockchain evoluciona desde la protección de smart contracts hacia la gestión de riesgos sistémicos. **El Crypto Crime Report de Chainalysis señala que más del 70% de los incidentes recientes se originaron en fallas de gobernanza,** custodia o infraestructura, no en el protocolo base. Esto refuerza la necesidad de estándares operativos comparables a los de infraestructuras financieras tradicionales.

9.2 Tokenización segura y riesgos de ciberinfraestructura

La tokenización habilita eficiencias significativas, pero introduce riesgos asociados a custodia, gestión de llaves e interoperabilidad. **Incidentes reportados por CertiK muestran pérdidas superiores a USD 2,000 millones** en un año por vulnerabilidades en infraestructura, subrayando que la seguridad subyacente es un prerrequisito para la adopción institucional.

9.3 Validity proofs y ZK-rollups como pilares de verificación

Las validity proofs y los ZK-rollups emergen como mecanismos fundamentales para escalar sistemas distribuidos sin sacrificar verificabilidad ni seguridad. Estas tecnologías permiten validar transacciones o estados sin revelar información subyacente, reforzando modelos de confianza matemática. Documentación técnica de la Ethereum Foundation y análisis de agencias europeas de ciberseguridad muestran que estos enfoques comienzan a extenderse más allá de blockchain, con aplicaciones potenciales en auditoría digital, validación de procesos y sistemas distribuidos de alta Integridad.

9.4 Criptografía homomórfica para análisis seguro de datos

La criptografía homomórfica representa una frontera avanzada en el análisis seguro de datos, permitiendo realizar operaciones sobre información cifrada sin necesidad de descifrarla.
El NIST reconoce esta tecnología como estratégica para sectores altamente regulados, aunque todavía limitada por costos computacionales y complejidad operativa. Hacia el mediano plazo, su relevancia crecerá en casos donde la confidencialidad de largo plazo sea prioritaria, como banca, salud y sector público.

10. Preparación Organizacional para 2026

La preparación organizacional frente a riesgos digitales se redefine como una capacidad ejecutiva. ***El Cost of a Data Breach Report 2024 de IBM indica que el 83% de las organizaciones experimentó al menos un incidente con impacto operativo en los últimos dos años,*** evidenciando que la pregunta ya no es si ocurrirá un incidente, sino cuán preparada está la organización para absorberlo.

10.1 Ciberresiliencia: métricas y capacidades recomendadas

La ciberresiliencia se consolida como el indicador clave de madurez en seguridad. Estudios del ***World Economic Forum y firmas globales*** de consultoría muestran que las organizaciones con capacidades maduras de detección, contención y recuperación reducen de forma significativa el impacto financiero y operativo de incidentes. En particular, programas robustos de resiliencia pueden reducir hasta en 45% el impacto económico, principalmente por menor tiempo de inactividad y recuperación más eficiente.

45%

en impacto económico

10.2 Gestión de riesgos y continuidad en ambientes híbridos

Los entornos híbridos como cloud, on-premise y terceros, amplifican dependencias y superficies de ataque. ***El Foro Económico Mundial*** identifica la falta de integración entre estos dominios como uno de los principales amplificadores de impacto en incidentes mayores. La gestión de riesgos debe, por tanto, diseñarse de forma transversal, incorporando escenarios de cibercrisis complejas, fallas en proveedores y recuperación coordinada de servicios críticos.

10.3 Cultura de seguridad: el factor humano como eje central

El factor humano continúa siendo uno de los principales vectores de riesgo. ***El Data Breach Investigations Report del Verizon*** muestra de forma consistente que el abuso de credenciales, el phishing y los errores humanos están presentes en una proporción significativa de los incidentes. Las organizaciones más maduras avanzan hacia modelos continuos de concientización, entrenamiento y responsabilidad compartida, integrados a la operación diaria.

10.4 Modelos de gobernanza y roles clave (CISO, DPO, AI Security Lead)

Roles como CISO, DPO y AI Security Lead se consolidan como funciones estratégicas. Su efectividad depende de autoridad real, acceso a la toma de decisiones y alineación con objetivos de negocio y cumplimiento.

10.5 Gestión y gobernanza avanzada de llaves

La gestión avanzada de llaves criptográficas se vuelve crítica ante la expansión de cifrado, tokenización y Zero Trust. La madurez en Key Management impacta directamente la resiliencia y la capacidad de recuperación ante incidentes severos.

11. Recomendaciones Estratégicas para Líderes Tecnológicos

De cara a 2025–2026, la ciberseguridad debe ser abordada por los líderes tecnológicos como una capacidad estratégica de negocio y no como un conjunto de controles aislados.

La convergencia de inteligencia artificial, infraestructuras híbridas, regulación más exigente y amenazas persistentes obliga a replantear prioridades de inversión, modelos operativos y estructuras de gobernanza. Las decisiones que se tomen en este periodo condicionarán la resiliencia, competitividad y credibilidad digital de las organizaciones en el mediano plazo.

En primer lugar, la priorización de inversiones debe orientarse a capacidades transversales que reduzcan riesgo sistémico. Identidad digital robusta, arquitecturas Zero Trust, protección avanzada de datos y resiliencia operativa deben considerarse prerrequisitos para cualquier iniciativa de transformación digital. Estudios de mercado indican que las organizaciones que invierten de manera consistente en estos ejes reducen hasta en 50% la probabilidad de incidentes severos, no por eliminar amenazas, sino por limitar su propagación e impacto.

Para organizaciones que se encuentran en etapas iniciales de madurez, el enfoque debe estar en establecer fundamentos sólidos: gobierno claro de ciberseguridad, visibilidad integral de activos, control efectivo de accesos y alineación con requerimientos regulatorios básicos. Intentar adoptar tecnologías avanzadas sin estos cimientos suele generar una falsa sensación de seguridad y aumenta la deuda técnica y organizacional.

En el caso de organizaciones maduras, el reto se desplaza hacia la optimización y anticipación. La automatización de detección y respuesta, la integración de métricas de ciberresiliencia en tableros ejecutivos, la gobernanza del uso de inteligencia artificial y la adopción de tecnologías de privacidad avanzada se convierten en diferenciadores competitivos. En este nivel, la seguridad no solo protege operaciones, sino que habilita velocidad, escalabilidad y confianza en entornos altamente regulados.

Para América Latina, este periodo representa una oportunidad estratégica singular. La región puede avanzar más rápido que otros mercados si logra combinar adopción tecnológica con convergencia regulatoria, desarrollo de talento especializado e interoperabilidad regional. Las organizaciones que lideren este proceso no solo reducirán riesgos, sino que podrán posicionarse como referentes de confianza digital en mercados locales e internacionales.

Desde la perspectiva de Conecta, el liderazgo tecnológico efectivo en este nuevo ciclo exige una visión integradora: comprender la ciberseguridad como un sistema que conecta tecnología, personas, regulación y mercado.

Aquellos líderes que logren traducir riesgos técnicos en decisiones estratégicas estarán mejor preparados para navegar un entorno digital donde la confianza es el activo más escaso y valioso.

12. Conclusiones: Ciberseguridad Infraestructura de Confianza del Próximo Ciclo Digital

El periodo 2025–2026 marca un punto de inflexión. La ciberseguridad deja de ser una función defensiva para convertirse en la infraestructura de confianza que sostiene la economía digital. ***El costo global del cibercrimen, proyectado en USD 10.5 billones anuales según Cybersecurity Ventures,*** ilustra la magnitud sistémica del riesgo.

Desde la perspectiva de Conecta, el desafío para los líderes no es adoptar más herramientas, sino construir capacidades estructurales: resiliencia operativa, gobernanza tecnológica y anticipación de riesgos emergentes. Las organizaciones que integren seguridad, regulación y arquitectura desde la estrategia estarán mejor posicionadas para innovar sin erosionar confianza. América Latina tiene la oportunidad de cerrar brechas históricas y emerger como un actor relevante en el nuevo ciclo tecnológico, siempre que la ciberseguridad sea tratada como un habilitador económico y no como un costo operativo.

13. Fuentes Internacionales Consultadas

- https://www.frontier-enterprise.com/the-2026-cybersecurity-predictions-bonanza
- https://www.gartner.com/en/newsroom/press releases/2025-07-29-gartner-forecasts-worldwide-end-user-spending-on-information-security-to-total-213-billion-us-dollars-in-2025
- https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf
- https://es.weforum.org/publications/global-cybersecurity-outlook-2025
- https://www.crowdstrike.com/es-es/global-threat-report
- https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf
- https://cyble.com/resources/research-reports/global-threat-landscape-report-may-2025
- https://es.weforum.org/stories/2025/05/el-72-de-los-lideres-en-ciberseguridad-ve-riesgos-crecientes-asi-responden-gobiernos-y-empresas
- https://www.reuters.com/world/china/chinese-cyberattacks-taiwan-infrastructure-averaged-26-million-day-2025-report-2026-01-05/
- https://northwave-cybersecurity.com/resources/global-threat-landscape-2025
- https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18

- https://globalcybersecuritynetwork.com/blog/ai-driven-cyber-threats-for-the-next-year/
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://latam.kaspersky.com/about/press-releases/la-ia-redefinira-la-ciberseguridad-empresarial-en-2026-anticipa-kaspersky
- https://esemanal.mx/2025/12/ia-y-desinformacion-los-desafios-de-la-ciberseguridad-para-2026
- https://www.bis.org/publ/bppdf/bispap158.htm
- https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
- https://www.bis.org/publ/bppdf/bispap158.htm
- https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
- https://csrc.nist.gov/pubs/fips/203/final
- https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- https://www.bis.org/publ/bppdf/bispap158.htm
- https://csrc.nist.gov/pubs/fips/203/final
- https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
- https://www.bis.org/publ/othp107.htm
- https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
- https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
- https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
- https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
- https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
- https://www.sophos.com/en-us/blog/the-state-of-ransomware-2025
- https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

- https://www.sophos.com/en-us/blog/the-state-of-ransomware-2025
- https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
- https://www.enisa.europa.eu/publications/threat-landscape-for-industrial-control-systems
- https://www.isa.org/products-and-publications/standards/iec-62443-series-of-standards
- https://www.iso.org/standard/75106.html
- https://www.worldbank.org/en/topic/digitaldevelopment/brief/cybersecurity
- https://www.nist.gov/publications/zero-trust-architecture
- https://www.weforum.org/reports/advancing-cyber-resilience
- https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
- https://www.oecd.org/digital/cloud-computing/
- https://www.gartner.com/en/documents/sovereign-cloud
- https://oecd.ai/en/ai-principles
- https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
- https://www.oas.org/wearesorry.htm
- https://z.cash/learn/what-are-zk-snarks/
- https://www.accenture.com/us-en/services/cybersecurity/cyber-resilience
- https://www.nist.gov/cryptography
- https://www.ibm.com/reports/data-breach
- https://www.verizon.com/business/resources/reports/dbir/