Resiliencia y Cumplimiento: Desafíos de Ciberseguridad 2026

LEY MARCO DE CIBERSEGURIDAD

Cumplimiento Normativo, Gestión de Riesgos y Gobernanza de la ANCI

Ahora es una obligación legal

Las empresas deben cumplir nuevas exigencias normativas y de protección.

Impacto directo en la operación

Impacta procesos, tecnología y capacitación interna.

Responsabilidad ante incidentes y posibles sanciones

Se exige reportar incidentes y cumplir estándares definidos por la autoridad.

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Graciela González
Gerente de Relaciones Públicas y comunicaciones

Problema Global de Gran Escala

América Latina fue la región más atacada del mundo en 2025

Superando a Europa, Asia-Pacífico y Norteamérica. LATAM lideró ataques globales en 2025 con +3,000 semanales por entidad (+17%). Colombia y México fueron los más golpeados. El auge se debe al uso de IA generativa por hackers y brechas de seguridad en educación, gobierno y salud.

70%

Vulneraciones Globales 2025

Se registraron 7,419 ataques de ransomware exitosos (un 32% más que en 2024). De estos, el 85% (6,292) fueron dirigidos específicamente a empresas.

$11.9
billonesUSD

Costo Global del Cibercrimen

Las proyecciones 2026 sugieren que la cifra subirá a un rango entre $11.9 y $12.5 billones de dólares.

1.600

Ciberataques por Segundo

1.600 registros en America Latina durante el 2025.

[1] Comparitech; Worldwide ransomware roundup: 2025 end-of-year report
[2] Aftra; Beyond the numbers: The economic impact of cybercrime in 2026
[3] Weforum; Global Cybersecurity Outlook 2025

Casos de Ciberataques

Caso PIX Brasil (2025)

Fue un golpe quirúrgico contra el sistema de pagos instantáneos más grande de la región. El ataque no se dirigió a los ciudadanos, sino que explotó una vulnerabilidad en un proveedor tecnológico interconectado (C&M Software), permitiendo a los atacantes infiltrarse en el núcleo del Banco Central para desviar fondos directamente desde las cuentas de reserva bancarias.

Caso Copec Chile (2025-2026)

Exfiltración de 6 TB de datos internos por el grupo de ransomware Anubis, que afectó información corporativa y de trabajadores tras un fallo en los controles de acceso perimetral.

Caso Clínica Dávila (2025)

Ataque de ransomware con doble extorsión que resultó en la exfiltración y posterior publicación en la dark web de 250 GB de datos sensibles, incluyendo fichas médicas y resultados de exámenes, tras vulnerar el acceso remoto (VPN) de la institución.

Nuevas **Amenazas**

IA Generativa

Se ha convertido en una "espada de doble filo", mejorando las defensas pero también sofisticando los ataques de Phishing y Ransomware.

Ataques de Terceros

Las vulnerabilidades en la cadena de suministro son hoy la principal puerta de entrada para incidentes a gran escala.

Ciberresiliencia

El enfoque ha migrado de "evitar el ataque" a "garantizar la continuidad del negocio" durante y después de la crisis.

Ecosistema de Ciberseguridad

Ley de delitos informáticos 21.459
(2022)

Ley marco de ciberseguridad 21.663
(2024)

Ley de protección datos 21.719
(2025)

Impacto de la **Ley Marco 21.663**

Nuevas Facultades

La ANCI ya no solo supervisa, sino que audita activamente el cumplimiento de los Sistemas de Gestión de Seguridad (SGSI).

Operadores de Importancia Vital (OIV)

Las vulnerabilidades en la cadena de suministro son hoy la principal puerta de entrada para incidentes a gran escala.

Responsabilidad del Directorio

La ley establece una responsabilidad directa de la alta gerencia en la gobernanza de ciberseguridad.

Ley Marco 21.663

Gestión de Incidentes y Reporte (3 Horas)

Detección Temprana

La prioridad es la notificación al CSIRT Nacional en menos de 3 horas para mitigar el efecto en cadena.

Transparencia

La ley exige ahora informar no solo a la autoridad, sino también a los usuarios finales si sus datos están comprometidos.

Informe Post-Mortem

Es obligatorio presentar un análisis técnico detallado tras cada incidente para mejorar la postura nacional.

Ley Marco 21.663

Obligación especial para provedores de Servicios de TI

Exigir A Provedores

Se requiere exigir a los proveedores de servicios de tecnología de la información compartan detalles sobre vulnerabilidades e incidentes que podrían afectar las redes y los sistemas informáticos del Estado.

Prohibición

Se prohíbe que los contratos contengan cláusulas que restrinjan la comunicación de información sobre amenazas.

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Manteniendo el Compromiso

ESTAMOS CERTIFICADOS CON LA NORMA INTERNACIONAL ISO/IEC 27001:2022 E ISO/IEC 27701:2019

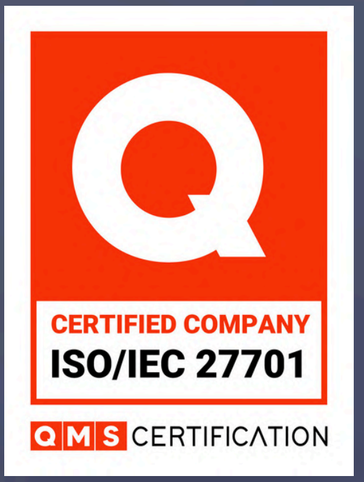
Segundo año de **Excelencia**

ISO/IEC 27001:2022 (Seguridad de la Información)

Aseguramos que la confidencialidad e integridad de los datos sean la base de todas nuestras operaciones y sistemas.

ISO/IEC 27701:2019 (Privacidad de la Información)

Como extensión de la anterior, gestionamos la privacidad con estándares globales, alineándonos con normativas exigentes como el RGPD.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet

Gracias!

13 AÑOS DE EXPERIENCIA EN CIBERSEGURIDAD

Nuestra trayectoria es un testimonio de Compromiso y Excelencia.

CERTIFIED COMPANY
ISO/IEC 27001
QMS CERTIFICATION

CERTIFIED COMPANY
ISO/IEC 27701
QMS CERTIFICATION