

Enero 2026



CiberPulso

Boletín del Comité de Ciberseguridad



COMITÉ DE CIBERSEGURIDAD
PARA LA REGIÓN



aleti

impulsamos la transformación digital

Editorial | 2026: el año para convertir el riesgo digital en decisiones estratégicas



Ana Cecilia Pérez

Líder del Comité de
Ciberseguridad ALETI



Feliz inicio de año a la comunidad de ALETI. Arrancamos 2026 con un contexto claro: **la ciberseguridad dejó de ser un tema reactivo y se consolidó como un habilitador de confianza, inversión y continuidad operativa** para gobiernos, empresas y sociedad.

El cierre de 2025 confirmó dos realidades simultáneas. Por un lado, el crecimiento sostenido de **ransomware, fraude digital y suplantación de identidad**, cada vez más apoyados por inteligencia artificial. Por otro, **decisiones institucionales y regulatorias** que comienzan a elevar el estándar en distintos países de la región.

Este boletín inaugura el año con una convicción: **2026 no es un año para diagnósticos aislados**, sino para traducir evidencia en decisiones y colaboración en impacto regional.

Panorama del mes



Cinco señales que marcan el inicio de 2026

- **Ransomware** consolidado como modelo de negocio con doble y triple extorsión.
- **Fraude e identidad digital** acelerados por IA generativa (phishing, deepfakes, impersonación).
- **Sector público e infraestructura crítica** como objetivos prioritarios.
- **Regulación más exigible**, no solo declarativa.
- **Ciberseguridad como criterio para inversión y cooperación internacional**.

Estas señales explican por qué 2026 exigirá mayor velocidad de respuesta, gobernanza clara y cooperación regional.



Latinoamérica en foco

Decisiones concretas que cerraron 2025



Chile | Exigibilidad y supervisión

Implementó la **Ley Marco de Ciberseguridad (Ley 21.663)** y fortaleció la **Agencia Nacional de Ciberseguridad**, estableciendo obligaciones claras para operadores de servicios esenciales. Un referente regional por su enfoque institucional.



México | Hoja de ruta nacional

Presentó el **Plan Nacional de Ciberseguridad 2025–2030**, ordenando la agenda en gobernanza, infraestructura crítica y capacidades. El reto de 2026 será su implementación efectiva.



República Dominicana | Estándares mínimos claros

Publicó la **NORTIC A8:2025**, norma general de ciberseguridad para instituciones públicas, elevando el nivel base de protección del Estado.





Uruguay | Continuidad como ventaja

Avanzó con su **Estrategia Nacional de Ciberseguridad 2024–2030** y la actualización de su Marco de Ciberseguridad, destacando por consistencia institucional.



España (referencia iberoamericana)

Aplicó medidas operativas contra fraude en telecomunicaciones, con resultados medibles en bloqueo de llamadas y mensajes fraudulentos.



Amenaza del mes

Ransomware y fraude impulsados por IA: la convergencia crítica

En 2025 se consolidó una convergencia clave: **ransomware, robo de datos y fraude** operando juntos, apoyados por IA para acelerar reconocimiento, personalización y extorsión.

La amenaza ya no es solo técnica: **es operativa, financiera y reputacional**. Para 2026, a diferencia estará en **detectar antes, responder más rápido y comunicar mejor**.



Innovación y tecnología

Lo que sí está funcionando

- **IA defensiva** para detección de anomalías y reducción de falsos positivos.
- **Automatización de respuesta** para ganar velocidad frente a ataques a escala.
- **Secure by design** como requisito en proyectos digitales.
- **Protección de la información**, más allá del perímetro.
- **Métricas de impacto de negocio**, no solo técnicas.

La tecnología habilita; la diferencia está en cómo se integra y gobierna.



La ventaja sigue siendo humana

El cierre de 2025 reafirmó que la **cultura organizacional y el liderazgo** son determinantes.

Las organizaciones más resilientes fueron aquellas que:

- invirtieron en concienciación continua,
- involucraron a negocio, legal y comunicación,
- y prepararon a sus equipos para decidir bajo presión.

En 2026, **talento, liderazgo y corresponsabilidad** marcarán la diferencia.

Agenda y colaboraciones ALETI

¿Qué haremos en 2026?



El Comité de Ciberseguridad de ALETI impulsará una agenda basada en:

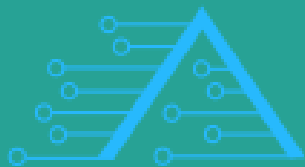
Estudio Visión Cibersegura Iberoamérica: análisis colaborativo y evidencia regional.

Webinars y paneles estratégicos con enfoque regional y ejecutivo.

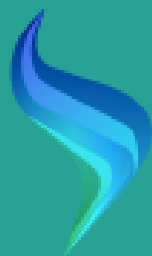
Cápsulas en video con voces del Comité sobre temas de actualidad.

Ciberpulso como boletín de referencia.

Cooperación internacional UE–ALC, incluyendo Global Gateway y EU–LAC Shield.



COMITÉ DE CIBERSEGURIDAD
PARA LA REGIÓN



aleti

impulsamos la transformación digital

Convocatoria 2026

Invitamos a la membresía a **sumarse activamente** al análisis del Estudio, a la generación de contenido y al diálogo regional.

La ciberseguridad de Iberoamérica se construye con evidencia, colaboración y liderazgo compartido.

 Si tienes algo que aportar, escríbenos.

 Y si este boletín te resultó útil, compártelo con tus colegas.

Gracias por ser parte activa de esta red que, con cada acción, colorea un mundo digital sin grises.

Nos leemos el próximo mes.

— Comité de Ciberseguridad ALETI

CONTÁCTANOS:



comunicaciones@aleti.org

¡Únete aquí al comité de trabajo que promueve la ciberseguridad en la región!

