Marzo 2026

CiberPulso

Boletín del Comité de Ciberseguridad

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

2026: La resiliencia dejó de ser opcional en Iberoamérica

Ana Cecilia Pérez

Líder del Comité de Ciberseguridad ALETI

El primer trimestre de 2026 confirma que América Latina enfrenta un entorno de riesgo estructural creciente.

El Global Cybersecurity Outlook 2026 del Foro Económico Mundial señala que **69 % de las organizaciones en la región reporta brechas críticas de talento**, y solo **13 % expresa alta confianza en la capacidad nacional para responder a un ataque significativo contra infraestructura crítica.**

A esto se suma la profesionalización del ransomware, la automatización del fraude mediante IA y el aumento de ataques a cadenas de suministro.

El desafío regional ya no es exclusivamente técnico. Es institucional.
La resiliencia depende de gobernanza, coordinación y capacidad real de respuesta.

2026 debe consolidarse como el año de la madurez operativa en Iberoamérica.

Panorama del mes

Cinco señales que marcan el inicio de 2026

- **Ransomware profesionalizado:** Modelos RaaS continúan facilitando ataques de alto impacto.
- **Identidad como vector dominante:** El abuso de credenciales y accesos privilegiados supera a la explotación puramente técnica.
- **IA aplicada al fraude:** Phishing hiperpersonalizado y automatización ofensiva reducen barreras de entrada para atacantes.
- **Superficie ampliada por terceros:** El riesgo ya no termina en el perímetro organizacional.

El riesgo evoluciona estructuralmente, no de forma lineal.

Latinoamérica en foco

Señales regionales clave

Brecha de resiliencia confirmada
Los datos 2026 muestran niveles de confianza institucional inferiores al promedio global en preparación ante ataques críticos.

Cooperación en consolidación
Se observa mayor énfasis en interoperabilidad entre equipos de respuesta (CERTs) y fortalecimiento de capacidades a nivel regional.

Regulación a distintas velocidades
La heterogeneidad normativa en Iberoamérica genera desafíos para empresas que operan en múltiples jurisdicciones.

Amenaza del mes

- **Cadena de suministro digital: el nuevo perímetro de riesgo**

Los ataques a proveedores tecnológicos se consolidan como uno de los vectores más críticos en 2026.

Los adversarios priorizan terceros con menor madurez para acceder indirectamente a múltiples organizaciones.

Factores que amplifican el riesgo en la región:

- Dependencia creciente de SaaS e integradores.
- Accesos privilegiados persistentes.
- Evaluaciones contractuales insuficientes.
- Supervisión limitada de terceros.

Preguntas estratégicas para este mes:

- ¿Tenemos visibilidad real de accesos de proveedores críticos?
- ¿Existen controles verificables más allá del cumplimiento documental?
- ¿Podemos responder a un incidente originado en un tercero?

La cadena de suministro es una extensión directa del perímetro digital.

- **Tu nueva caricatura con IA: ¿un avatar profesional o un regalo para los hackers?**

Por Carlos Enrique Ungo

En las últimas semanas, mis redes sociales se han llenado de caricaturas hechas con IA generativa. Ilustraciones bien logradas de colegas rodeados de sus certificaciones, experiencia profesional, el logo de sus empresas, referencias a sus hobbies y hasta retazos de su vida familiar.
Si bien es cierto estas caricaturas son llamativas, creativas y contagiosas, también pueden representar un enorme riesgo de seguridad.

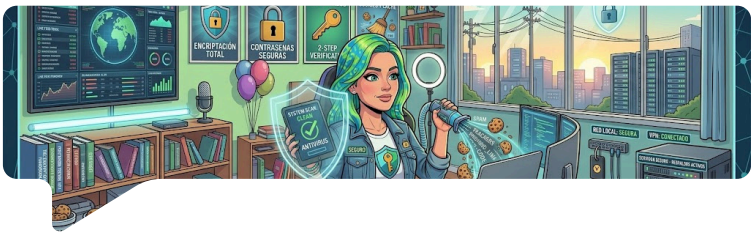
Como profesional de la tecnología y ciberseguridad, no puedo evitar mirar estas imágenes con otros ojos. Con el lente del OSINT (Open Source Intelligence), para ser exacto. Porque lo que muchos están viendo como una moda, tendencia o promoción de su marca personal, alguien con malas intenciones puede verlo como el paquete completo para un ataque de ingeniería social.

Para lograr esas imágenes, muchas veces estamos entregando a una plataforma de IA generativa información personal y profesional bastante detallada. Y aquí viene el punto clave: no importa tanto si esos datos entrenan o no modelos. El verdadero riesgo está en otra parte en el almacenamiento, la persistencia y la pérdida de control de toda esa información.

Veámoslo con algunos ejemplos sencillos:

- **Ingeniería social hiper personalizada:** Si tu caricatura deja claro que te encanta el senderismo o el jugar pádel, que tienes un perro llamado "Max" y que trabajas en banca, el atacante ya no necesita investigar. El phishing prácticamente se escribe solo. Y lo peor es que se siente legítimo.
- **Whaling o fraude del CEO:** Mostrar jerarquías, cargos ejecutivos o incluso herramientas específicas facilita estafas muy bien dirigidas. Precisas. Creíbles. De esas que no levantan sospechas a la primera.
- **Preguntas de seguridad comprometidas:** Mascotas, hobbies, ciudades favoritas, apodos; justo lo que muchos hackers y plataformas utilizan para recuperar cuentas. Publicarlo es como dejar las llaves puestas, pero en una versión artística.
- **Privacidad y control del dato:** Una vez que esa información sale de tus manos, puede quedar fuera de tu dominio y de los marcos de protección de datos que aplican en tu país.

No se trata de dejar de usar tecnología. Para nada. Se trata de usarla con un poco más de higiene digital:



- **Abstrae.** No todo lo que eres y haces tiene que estar en la imagen. Tu logo corporativo actual no define tu profesionalismo.
- **Menos, es más.** Evita nombres de familiares, mascotas o detalles internos de tu trabajo en los prompts. No aportan tanto y sí te exponen a ti y a tu empresa.
- **Piensa en tu huella digital.** Una vez que la imagen está en línea, ya no es solo tuya. Y eso conviene recordarlo.

La IAG es una herramienta poderosa para fortalecer tu marca personal, sin duda. Solo cuida que tu creatividad no termine convirtiéndose en la puerta de entrada a una vulnerabilidad innecesaria. Para ti o para tu organización.

- **El invitado invisible en tus reuniones** (**y por qué sí debería preocuparte**)

Por *Carlos Enrique Ungo*

Inicia la reunión. Saludos rápidos. Alguien comparte pantalla. Y aparece un "invitado silencioso": un bot que toma notas, resume acuerdos y promete eficiencia.

Suena bien. Y, en muchos casos, lo es. Pero también cambia las reglas del juego.

Mientras hablamos, el sistema no solo registra palabras. Captura contexto, intención, decisiones, prioridades. Lo que antes era una conversación entre cuatro paredes se convierte en un activo digital persistente.

La pregunta ya no es qué tan útil es el bot. La pregunta es ¿qué ocurre con esa información cuando la reunión termina?

Es importante recalcar que no todos los asistentes virtuales implican el mismo nivel de riesgo. Algunos entornos empresariales ofrecen controles sólidos de cifrado, retención y uso de datos. El problema no es la tecnología en sí.

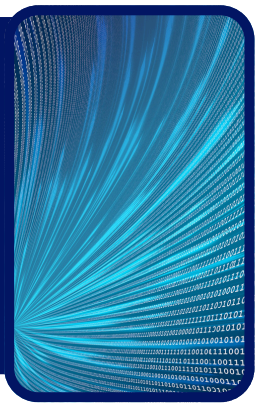
El problema es que, en muchas organizaciones, su adopción ocurre sin evaluación formal, sin clasificación de reuniones y sin validación de proveedores.

Y es precisamente ahí donde empiezan los riesgos reales.

Tres alertas que no deben ignorarse

Fuga silenciosa de información
En reuniones se discuten estrategias, negociaciones, datos de clientes, información regulada. Aunque no exista una "brecha" tradicional, puede haber pérdida de control sobre dónde se almacena la información, cuánto tiempo permanece y quién puede acceder a ella. En ciberseguridad, perder control ya es un incidente potencial.

El perímetro digital se expande
Agregar bots implica abrir integraciones vía APIs y extender el ecosistema tecnológico. No es que la plataforma base deje de ser segura; es que se introducen nuevas superficies de ataque y procesamiento que muchas veces TI no monitorea activamente o controla.



Riesgo regulatorio y reputacional
Normativas como GDPR y marcos regulatorios en LATAM exigen consentimiento informado, minimización y control sobre datos. ¿Se informa explícitamente que la conversación está siendo procesada por un tercero? ¿Se conoce la jurisdicción de almacenamiento? En muchos casos, no.

¡Bienvenidos al "Shadow AI"!

Así como ocurrió con el shadow IT, hoy enfrentamos shadow AI: herramientas útiles, adoptadas rápidamente, pero fuera del marco formal de gobierno corporativo.

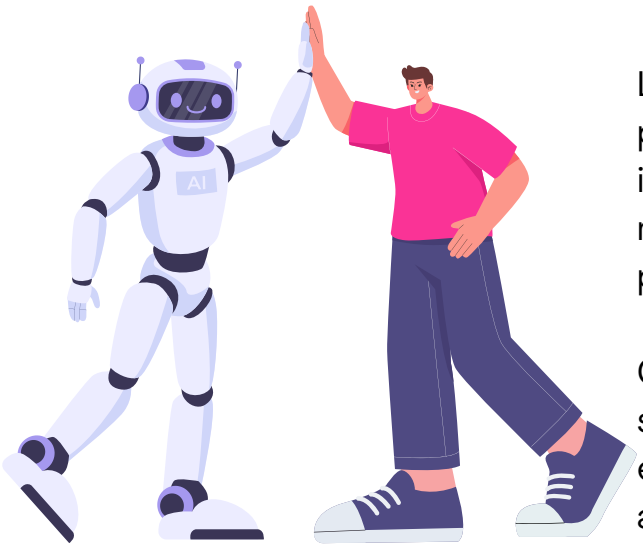
Y estas herramientas tienen acceso a uno de los activos más sensibles de la organización: sus conversaciones estratégicas.

¿Qué hacer?

Prohibir no es realista. Gobernar sí lo es.

Algunas medidas concretas:

- Clasificar reuniones según sensibilidad y definir dónde los bots están permitidos y dónde no.
- Controlar integraciones y validar proveedores (retención, residencia de datos, uso para entrenamiento).
- Establecer mecanismos claros de consentimiento y transparencia.
- Diseñar políticas que equilibren eficiencia y exposición.



La IA está transformando la productividad empresarial. Eso es irreversible. Pero también está redefiniendo los límites de la privacidad corporativa.

Cada reunión con un bot deja de ser solo una conversación. Se convierte en un registro. Y todo registro es un activo que debe gestionarse.

Porque en gestión de riesgos hay una regla constante: Lo que no se gobierna, tarde o temprano se expone.

Innovación y tecnología

Qué está marcando diferencia en 2026

- **Seguridad centrada en identidad.**
- **Zero Trust aplicado operativamente.**
- **Automatización defensiva con IA.**
- **Monitoreo continuo del riesgo de terceros.**

La diferencia regional no será qué tecnología se adquiere, sino cómo se integra en la gobernanza y gestión de riesgos.

Cultura y talento digital

La variable estructural

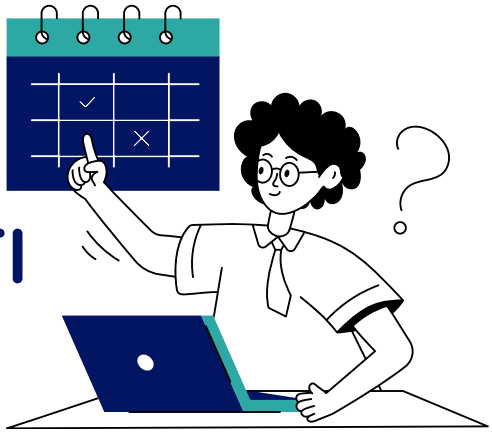
La brecha de talento sigue siendo uno de los principales factores de vulnerabilidad en América Latina.

Más allá de tecnología, persisten desafíos en:

- Integración de ciberseguridad en decisiones estratégicas.
- Formación ejecutiva en gestión de riesgo digital.
- Simulaciones institucionalizadas de crisis.

La resiliencia es una capacidad organizacional, no solo técnica.

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!