Agosto 2025

CiberPulso

Boletín del Comité de Ciberseguridad

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

LÍDER COMITÉ DE CIBERSEGURIDAD

Ana Cecilia Pérez

Líder del Comité de Ciberseguridad ALETI

Iniciamos agosto con una convicción compartida: la ciberseguridad no es un reto individual, es una responsabilidad colectiva. Desde gobiernos hasta empresas, familias y escuelas, todos tenemos un rol que desempeñar en la construcción de un entorno digital más seguro. Por eso nos emociona anunciar que ya están disponibles las encuestas del estudio regional **'Visión Cibersegura de Iberoamérica'.**

Este es un esfuerzo sin precedentes que nos permitirá entender el verdadero estado de la ciberseguridad en nuestra región y diseñar soluciones que respondan a nuestras realidades. Este mes, más que nunca, tu participación importa.

Lanzamiento del estudio Visión Cibersegura de Iberoamérica

Ya puedes participar en la encuesta más importante del año para entender el nivel de madurez en ciberseguridad de organizaciones, gobiernos y hogares en Iberoamérica. Este estudio busca recopilar datos reales que permitan:

- Identificar brechas y prioridades en gestión de riesgos digitales.
- Fortalecer políticas públicas y marcos regulatorios.
- Promover una cultura digital sólida, tanto en entornos corporativos como familiares.

Participar toma menos de 10 minutos, no estamos solicitando datos personales y la información recabada nos permitirá tomar decisiones para un futuro mas seguro y preparado para todos.

Comparte con tu comunidad. Tu voz también transforma.

Participa en la encuesta aquí

Revive el lanzamiento aquí

Nota de prensa

Noticias clave en ciberseguridad en LATAM (julio-agosto 2025)

- **Explosiva alza de ataques digitales en la región:** Check Point reportó un aumento del **39%** en ataques semanales en América Latina, con un promedio de **2,716** incidentes por organización, muy por encima del promedio global.

- **Ransomware sigue creciendo en LATAM:** CrowdStrike identificó **291** víctimas corporativas en la región en lo que va del año, un incremento del **15%**. Brasil, México y Argentina lideran en número de ataques.

- **La banca regional bajo amenaza:** El reporte de Digi Americas y Duke University indica que solo **7 de 32** países tienen infraestructura robusta para proteger sus sistemas financieros ante incidentes cibernéticos.

Panorama crítico: Ransomware y las nuevas formas de extorsión

El ransomware ya no se limita a cifrar información. Hoy enfrentamos esquemas de doble y triple extorsión, donde los atacantes también roban datos y amenazan con filtrarlos, o incluso contactan a clientes y empleados para presionar aún más.

La pregunta clave ya no es si la información puede ser robada, sino qué tan controlada está incluso cuando sale de tu perímetro. Hoy existen soluciones que permiten revocar accesos, proteger archivos en tránsito y prevenir que datos sensibles sean compartidos o utilizados para entrenar IA sin consentimiento.

Estrategias recomendadas:

✅ Etiquetado de información y control persistente.
✅ Prevención de fugas con protección post-filtración.
✅ Concienciación y simulacros ante ataques.
✅ Evaluación de soluciones tecnológicas basadas en casos de uso reales.

Servicio destacado: Protección de Datos con ITsMine (por Capa 8)

¿La protección de datos ya no puede depender únicamente de firewalls y soluciones tradicionales. Con ITsMine, ahora puedes proteger tu información incluso cuando ya fue descargada, compartida por error o enviada fuera del entorno corporativo. Esta tecnología permite:

✅ Deshabilitar archivos robados (File-GPS™)
✅ Establecer tiempos de expiración automáticos (TimeBomb™)
✅ Prevenir que IA generativas absorban datos no autorizados.
✅ Detectar accesos indebidos a través de inteligencia contextual.

Todo esto, sin depender de agentes instalados ni clasificaciones complejas. Ideal para organizaciones que quieren anticiparse al ransomware y reducir su riesgo operativo.

Escríbenos para agendar una demo personalizada y ver cómo funcionaría con tus datos a **contacto@capa8.com**

Sexting con IA y sextorsión digital: una amenaza emergente en entornos familiares

Contexto y modus operandi

- Algunos agresores recopilan fotos reales de perfiles públicos en redes sociales (por ejemplo, adolescentes activos en TikTok o Instagram).

- Usan herramientas de IA generativa para crear imágenes íntimas falsas: desnudos o videos manipulados, que se presentan como reales.

- Luego, chantajean a la víctima o a su entorno familiar, exigiendo dinero o contenido más explícito, bajo amenaza de difundir el material si no se paga.

- En muchos casos no se trata de imágenes reales, pero los adolescentes o sus familias no lo saben, y sucede sin consentimiento ni primeros indicios visibles.

Consecuencias comprobadas

- El FBI reportó un caso reciente en EE.UU. donde un adolescente recibió amenazas —cobraban USD 3,000 por un video íntimo generado por IA— y terminó suicidándose tras sufrir sextorsión.

- Estudios de ONG en América Latina, como Aldeas Infantiles SOS en Perú, revelan que un 22 % de menores han escuchado casos de sextorsión con IA, y más del 33 % se sienten inseguros en línea.

Impacto emocional y social

- **Reparación casi imposible:** aunque se retire el contenido, el daño psicológico y reputacional persiste.

- **Vulnerabilidad exacerbada,** ya que muchas víctimas no reconocen la manipulación hasta que es demasiado tarde.

- **Criminalización digital** y presión emocional intensa: los menores se enfrentan a climas de miedo, culpa y desconfianza en su entorno familiar o escolar.

¿Por qué este tema es clave en la encuesta Visión Cibersegura de Iberoamérica?

La dimensión familiar del estudio adquiere relevancia frente a estos riesgos emergentes:

- Permite medir cómo están las familias latinoamericanas frente a fenómenos como el sexting con IA y sextorsión digital.
- Facilita identificar brechas concretas de protección, conocimiento y respuesta en hogares con adolescentes expuestos a estas amenazas.
- Sirve para definir mejores estrategias de educación digital, prevención y apoyo psicosocial desde instituciones y campañas públicas.

Tu participación en la encuesta familiar es fundamental. Con tu aporte podemos generar datos significativos que impulsen políticas públicas y programas que protejan a los menores frente a estas nuevas formas de violencia digital.

Encuesta de Ciberseguridad en hogares y escuelas

Acciones recomendadas para padres y responsables

- Habla abiertamente con adolescentes sobre riesgos digitales, sextorsión y sexting con IA.
- Supervisa y acompaña el uso de redes sociales, apps de mensajería y contenido que consumen.
- **Fomenta círculos de confianza:** que sepan a quién acudir si reciben mensajes sospechosos.
- Reporta y busca ayuda profesional ante amenazas o chantajes digitales.

Eventos

CTF Empresas 2025 – Ciber-ejercicio Iberoamérica

Prepárate para un reto real de ciberseguridad con enfoque empresarial.

Dirigido a: Equipos de ciberseguridad de empresas de Iberoamérica
📍 Online, en equipos, tipo Capture The Flag (CTF)
📅 3 al 5 de septiembre 2025

Certificado y visibilidad internacional

IFC 2025 – Congreso de Informática Forense y Ciberseguridad

Temas: Ciberseguridad, IA, ransomware, Zero Trust, privacidad, OT, entre otros.

📍 Punta Cana, República Dominicana
📅 23 al 26 de octubre de 2025
🌐 www.ifcforensic.com

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

En Ciberpulso, nos dedicamos a proporcionar a nuestra comunidad la información más relevante y actualizada sobre ciberseguridad. Esta edición está diseñada para equipar a profesionales y organizaciones con el conocimiento y las herramientas necesarias para enfrentar los desafíos de un mundo digital cada vez más complejo y conectado. Aproveche las oportunidades de aprendizaje y colaboración presentadas este mes y manténgase a la vanguardia en la protección de su entorno digital.

CONTÁCTANOS:

comunicaciones@aleti.org

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