LITORALPRESS

Fecha: 22-05-2026
Medio: Publimetro
Supl. : Publimetro
Tipo: Noticia general
Título: Bajo asedio digital: Por qué Latinoamérica sufre más ataques por semana

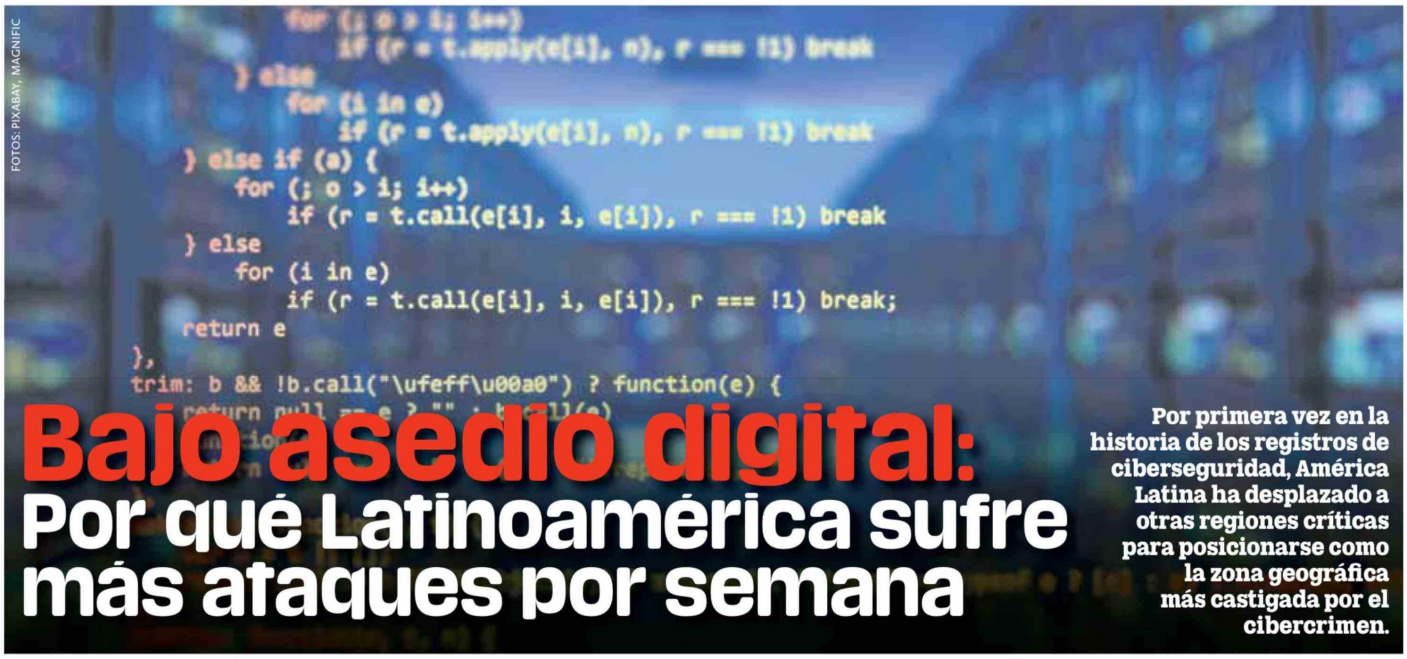
Pág. : 11
Cm2: 710,5
VPE: $ 4.527.513

Tiraje: 84.334
Lectoría: 382.227
Favorabilidad: No Definida

fayerwayer FW

3 factores críticos que han convertido a Latinoamérica en una zona de sacrificio digital:

1. **Obsolescencia Tecnológica:** Muchas instituciones operan con sistemas operativos sin soporte o sin parches de seguridad actualizados (la famosa *deuda técnica*).
2. **Falta de Legislación:** Los marcos legales en la mayoría de los países de la región son lentos para procesar crímenes transnacionales, lo que reduce el riesgo para los atacantes.
3. **El Factor Humano:** El 85% de los ataques exitosos comienzan con un error humano (ingeniería social). La falta de programas de concienciación en ciberseguridad es el mayor agujero en la muralla.



FOTOS: PIXABAY, MAGNIFIC

Bajo asedio digital: Por qué Latinoamérica sufre más ataques por semana

Por primera vez en la historia de los registros de ciberseguridad, América Latina ha desplazado a otras regiones críticas para posicionarse como la zona geográfica más castigada por el cibercrimen.

Natalia Gálvez
Fayerwayer

Las cifras no mienten y son escalofriantes. Según datos de Check Point Research y analistas regionales, una organización promedio en Latinoamérica sufre hoy más de 3,000 intentos de ataque cada semana.

Este incremento representa un salto del 20% respecto al año anterior, superando con creces la media global. La vulnerabilidad de nuestra infraestructura digital ha creado un ecosistema ideal para que bandas internacionales de ransomware y phishing operen con una impunidad alarmante.

LOS DATOS DEL ASEDIO: ¿QUIÉNES SON LOS MÁS GOLPEADOS?

El informe destaca que el ataque no es indiscriminado; los criminales buscan sectores donde el flujo de caja es alto y la tolerancia al tiempo de inactividad es baja.

Sectores más atacados en 2026:

- **Educación e Investigación:** El blanco número uno, con un promedio de 3,300 ataques semanales. La digitalización forzada y la falta de protocolos robustos en universidades las han vuelto vulnerables.
- **Gobierno y Militar:** Los ataques aquí no solo buscan dinero, sino desestabilización y robo de datos de inteligencia.
- **Salud:** El sector más crítico por el riesgo de pérdida de vidas humanas ante el bloqueo de sistemas hospitalarios.

MAPA DEL
CIBERCRIMEN EN LATINOAMÉRICA

EL IMPACTO DE LA IA EN LOS ATAQUES DE 2026

No podemos ignorar que los atacantes ahora utilizan Inteligencia Artificial Generativa para crear correos de phishing perfectos, sin errores gramaticales y con un tono de voz que imita perfectamente a jefes o entidades bancarias.

Esto ha hecho que la detección por parte de usuarios comunes sea casi imposible sin herramientas de defensa automatizadas.

HAY QUE ACTUAR

Ser el líder mundial en ciberataques no es un título que Latinoamérica deba portar con resignación. Las cifras presentadas este mayo de 2026 son una llamada de auxilio para los gobiernos y el sector privado. La ciberseguridad ha dejado de ser un gasto opcional para convertirse en el seguro de vida de cualquier operación moderna.

La tecnología, que tanto nos facilita la vida, está siendo utilizada como arma. Si las organizaciones regionales no aumentan sus presupuestos en defensa digital y educación ciudadana, los 3,000 ataques semanales de hoy parecerán una cifra pequeña en comparación con lo que vendrá. La guerra es digital, y Latinoamérica está perdiendo demasiadas batallas por puro descuido.

Preguntas frecuentes sobre la crisis de ciberseguridad

1 ¿Qué es lo que más buscan los atacantes?
—Principalmente dinero a través del secuestro de datos (ransomware), pero también hay un mercado creciente para la venta de identidades digitales y credenciales de acceso a redes corporativas.

2 ¿Cómo puedo proteger mi empresa o mis datos personales?
—La regla de oro en 2026 es el Zero Trust (Confianza Cero). Nunca asumas que un correo o mensaje es legítimo. Implementa autenticación de múltiples factores (MFA) física y mantén tus sistemas actualizados al día.

3 ¿Por qué hay tantos ataques en educación?
—Las redes universitarias tienen miles de puntos de acceso (estudiantes y profesores) con dispositivos personales que suelen tener poca seguridad, lo que ofrece una puerta de entrada fácil a servidores centrales.