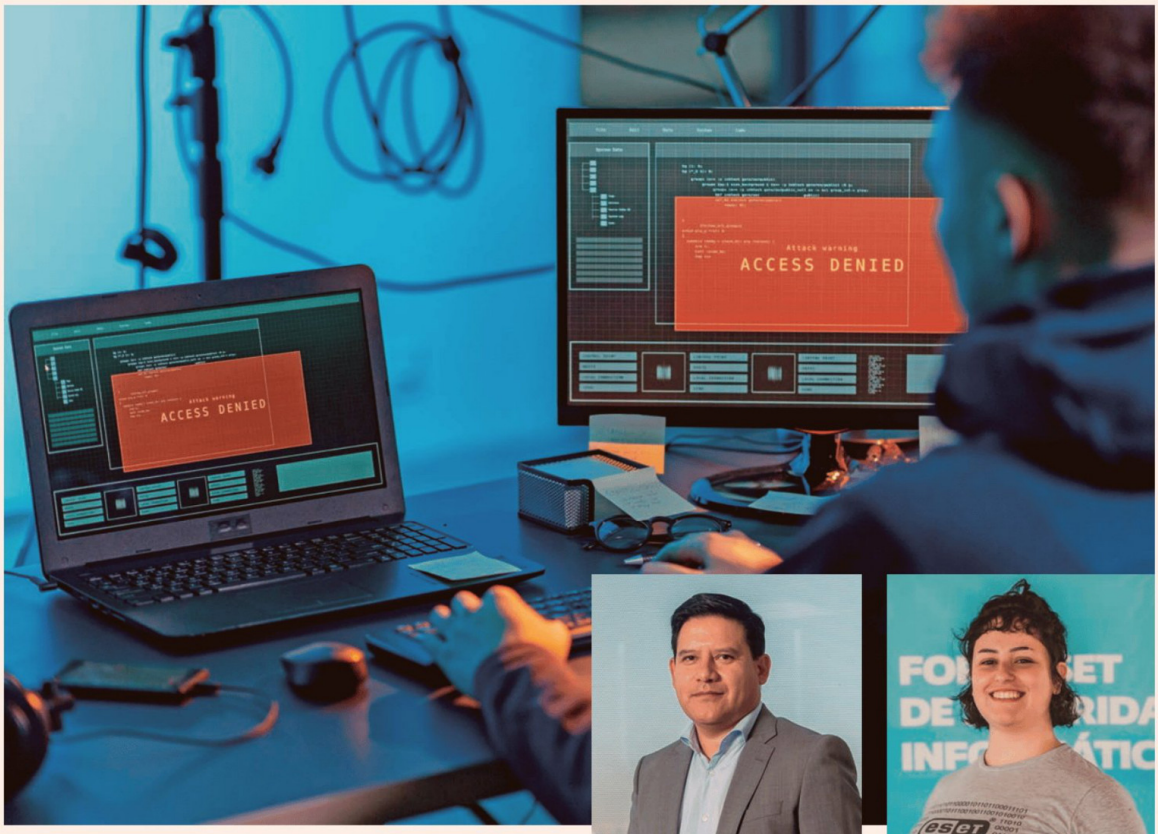
DIARIO FINANCIERO®

Fecha: 18/02/2026 Audiencia: 40.297 Sección: CIENCIA Y TECNOLOGIA
Vpe: $5.855.993 Tirada: 13.432 Frecuencia: 0
Vpe pág: $8.127.680 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 72,05%

Expertos proyectan los primeros ataques articulados completamente con IA, la clonación de tarjetas con tecnología inalámbrica y espionaje con computación cuántica.



Los nuevos métodos de ciberataques que llegarán a Latinoamérica en 2026

POR LAURA FLORES

Los nuevos métodos de ciberataque que se detectaron en el mundo en los últimos dos años llegarán a Latinoamérica a partir de 2026. Se trata de amenazas cada vez más sofisticadas que utilizan y se potencian con tecnologías como la inteligencia artificial (IA) y el *Near Field Communications* (NFC, su sigla en inglés), que permite la transmisión de datos en forma inalámbrica a corta distancia.

En 2025, según un informe de Entel Digital, se registró un alza de *ransomware* (secuestro de datos), ciberespionaje y filtración de datos en la región. Para este año expertos en ciberseguridad proyectaron la irrupción de nuevas amenazas, como la clonación de tarjetas sin contacto vía NFC, ciberespionaje con tecnología cuántica y ataques articulados completamente por agentes de IA, los cuales pueden afectar a una persona, organización o país.

La investigadora de Seguridad Informática de ESET Latinoamérica, Martina López, y el *country manager* de Fortinet Chile, Andrés Pérez, dijeron que estas tres modalidades podrían afectar a Latinoamérica a partir de 2026 y seguirán desarrollándose hasta 2030. Además, señalaron la importancia de que empresas y gobiernos que manejan información crítica tengan conocimiento de los nuevos métodos.

Espionaje con computación cuántica

La filtración de datos y espionaje en Latinoamérica aumentó 210%, según el último reporte de Entel Digital. Sin embargo, Pérez de Fortinet, señaló que este año continuará, pero con un cambio tecnológico: los grupos de *hackers* están accediendo a computadores cuánticos, lo que traerá a la región la amenaza potenciada con esta tecnología.

Explicó que la computación cuántica aumenta la capacidad de procesamiento de datos de forma exponencial, lo que permitirá desencriptar claves de acceso en segundos. "Se va a poder exponer un montón de información que antes tomaba años".

Dijo que antes los computadores cuánticos eran "muy difíciles de adquirir y tenían una cantidad de errores", en cambio ahora "son cada vez más comunes".

Según Pérez, el espionaje se da a nivel de Gobierno y empresas, ya que se ataca información crítica. Por ejemplo, un blanco podría ser el ejército: "Se puede saber dónde está, cuál es la comunicación que tiene, cómo está armado".

Y agregó que en el caso del Ejército de Chile "ya tomó medidas para protegerse con computación cuántica avanzada".

Amenazas completas hechas por agentes de IA

López de ESET señaló que los ataques generados en su totalidad por agentes de IA -aquellos que pueden ejecutar tareas en forma autónoma- "todavía siguen siendo pruebas de concepto o quizás cuestiones un poco más pequeñas", pero posiblemente empiecen a surgir desde este año en la región.

Señaló que hoy se pueden encontrar a "cientos de personas realizando acciones totalmente automatizadas", como programar un viaje completo, comprar pasajes y alojamiento, por lo tanto, no ve lejana la automatización de ataques hechos por agentes de IA.

Andrés Pérez, country manager de Fortinet Chile.

Martina López, investigadora de Seguridad Informática de ESET.

"Es una preocupación, no solo porque a un cibercriminal se le haría mucho más sencillo revisar con agente de IA la cadena de ataque completa, sino porque también lo que hace es democratizar el conocimiento técnico", dijo López.

En tanto Pérez enfatizó la importancia de que las organizaciones tengan un sistema de ciberseguridad con IA. "Va a ser imposible que se logre tomar medidas proactivas cuando tienes un software o agentes que están utilizando inteligencia artificial de última generación".

Ataques con tecnología inalámbrica (NFC)

Ambos expertos señalaron que la tecnología NFC se está usando para capturar datos de tarjetas de pago físicas y también conectadas a teléfonos celulares. Esta transferencia de datos se realiza a través del contacto directo con un dispositivo, pero también en forma inalámbrica a corta distancia.

Un ejemplo es el software malicioso -*malware*- NGate que está dirigido a sistemas Android y que -según López- es la primera evidencia de este tipo de ataques.

"Se descargaba una aplicación en un sitio no oficial de aplicaciones móviles, donde el atacante hacía una suplantación de la página de inicio de sesión de una entidad bancaria. Una vez que la persona entregaba sus credenciales bancarias, se le solicitaba que acercara su tarjeta para poder confirmar efectivamente la identidad", afirmó López.

Este *malware* incluye también una herramienta llamada NFCGate, la cual se utiliza para traspasar los datos desde un dispositivo Android a otro en forma inalámbrica a corta distancia.

Pérez señaló que a pesar de que "las tarjetas de crédito ya contienen bloqueadores NFC en billeteras y en sistemas, hoy podría ser vulnerable el uso de estas tarjetas conectadas a un teléfono móvil".

Además, advirtió que no solo puede haber transferencia de la información financiera, sino también del propio celular y un posible control sobre el dispositivo.

El ejecutivo señaló que el uso cotidiano de las tarjetas bancarias y la presencia de sistemas de clonación en "muchos lados" como internet o durante el pago con tarjeta, "dificulta la protección frente a este tipo de ataques".