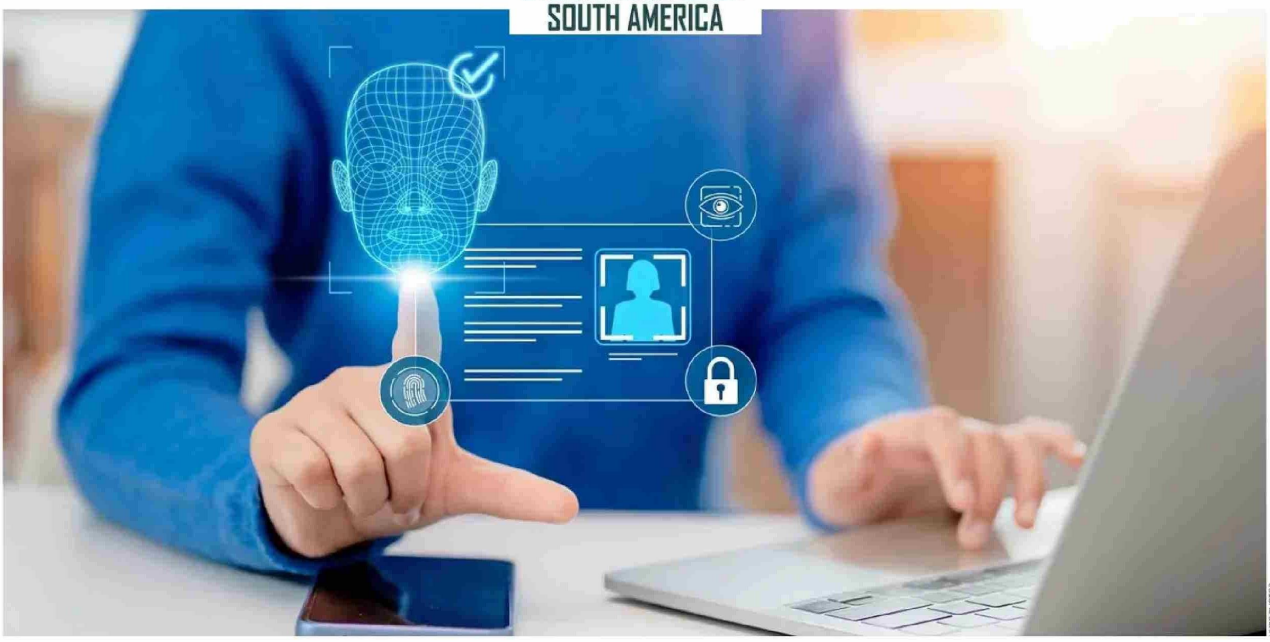
LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Del ransomware al robo de identidad: Los peligros del mundo conectado**

Pág. : 30
Cm2: 901,0

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CYBER & TECHNOLOGY
SOUTH AMERICA



QUE ACECHA A PERSONAS Y EMPRESAS

Del *ransomware* al robo de identidad: Los peligros del mundo conectado

En 2023, Chile se convirtió en el país más afectado por el secuestro y cifrado de datos en América Latina, con más de 1.300 incidentes semanales. David Nieto, *country manager* de Telefónica Tech, analiza cómo la IA, el *blockchain* y una nueva conciencia en ciberseguridad pueden frenar este fenómeno mundial que ya no solo roba datos, sino que también destruye reputaciones.

CRISTIÁN MÉNDEZ

Los ciberataques ya no son eventos aislados ni exclusivos de empresas gigantes. Hoy, basta con un clic en un correo engañoso para que una pyme pierda todo su sistema operativo o que una persona vea su identidad suplantada.

En este escenario, el *ransomware* —técnica de secuestro y cifrado de datos con fines extorsivos— y el robo de identidad digital se han convertido en las principales amenazas del mundo conectado. Lo que antes era una molestia ocasional, "hoy es un negocio multimillonario para grupos de ciberdelincuentes organizados", asegura David Nieto, *country manager* de Telefónica Tech.

Según datos de la empresa, durante 2023, Chile se convirtió en el país más atacado por *ransomware* en América Latina, con más de 1.300 incidentes semanales, lo que significa un alza de 17% en un año. Esta realidad "ha hecho sonar las alarmas en el ámbito público y privado, con sectores como transporte, manufactura, salud, energía e instituciones gubernamentales en el centro de los ataques", detalla Nieto.

La razón de este auge es muy clara: "Los ciberdelincuentes están usando inteligencia artificial generativa (GenIA) para personalizar ataques con un realismo que antes no existía", explica el ejecutivo.

Este tipo de incidentes son usados por los criminales para chantajear a las víctimas en lo que se denomina "doble extorsión", ya que no solo cifran los datos de una víctima y exigen un rescate para desbloquearlos, sino que también roban información sensible.

LA TRIPLE EXTORSIÓN

"Y ahora se suma la 'triple extorsión', donde amenazan con contactar a clientes o socios comerciales para dañar aún más la reputación de las víctimas", comenta el *country manager* de Telefónica Tech.

El tema, continúa, es que el *ransomware* "no solo roba datos, sino que paraliza completamente una operación". A diferencia del *phishing*, que engaña a los usuarios para obtener claves, o del *malware* bancario, que se enfoca en acceder a cuentas, el *ransomware* inutiliza los sistemas y exige un rescate monetario para restablecerlos. "Además, su impacto es más duradero, porque incluye la amenaza pública de divulgar datos sensibles", agrega.

Como dato: "en 2023 se identificaron 33 filtraciones de datos en foros clandestinos que incluían información robada a instituciones chilenas", destaca el experto.

En ese contexto, las pequeñas y medianas empresas (pymes) son especialmente vulnerables, pero muchas creen que no. "Las pymes suelen pensar que no serán objetivo porque no manejan millones de dólares, pero eso es justamente lo que las hace más atractivas: poca inversión en ciberseguridad y respuestas lentas ante incidentes", dice Nieto. El costo promedio de un rescate a nivel mundial ha pasado de "US$ 200.000 a más de US$ 400.000 en pocos años, sin contar el daño a la imagen corporativa", advierte.

Las formas o vectores de ataque también han evolucionado. Hoy no basta con evitar *links* sospechosos. "Tenemos desde correos con ingeniería social generada por IA, hasta ataques en la cadena de suministro de *software* confiable", comenta el ejecutivo. También están los *brokers* de acceso inicial, como los asociados a los Qakbot (un *malware* que comenzó como un troyano bancario en 2008, diseñado para robar credenciales de inicio de sesión en banca en línea), que usan llamadas telefónicas para obtener credenciales legítimas y usarlas. "El teléfono, ese canal que considerábamos seguro, ahora es una vía común para infiltrarse", enfatiza.

También están los *ransomware* autorreplicantes, como Virlock, que se expanden dentro de las redes corporativas en minutos. "La amenaza es tan rápida que, si no tienes medidas preventivas, no hay margen de reacción", asegura.

SER O NO SER

El robo de identidad se ha convertido en el complemento perfecto del *ransomware*. "Mientras el *ransomware* busca secuestrar, el robo de identidad busca suplantar", explica. Plataformas sociales como Facebook e Instagram se han convertido en catálogos abiertos para delincuentes. "Con ver una cuenta pública, ya puedes saber nombres, rutinas, colegio de los hijos, y usar esa información para diseñar un ataque", comenta Nieto.

La situación se agrava con la proliferación del Internet de las Cosas (IoT). "Una cámara de seguridad con contraseña débil es una puerta abierta para el atacante", advierte. Según la PDI, en 2023 hubo más de 3.000 denuncias por robo de identidad en Chile, con un alza de 15% en un año.

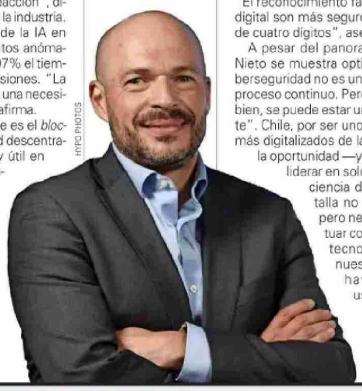
"Las víctimas suelen ser personas que comparten información personal en redes sociales o que utilizan dispositivos móviles sin medidas de seguridad adecuadas", destaca el ejecutivo.

QUÉ HACER

Para las empresas, la mejor defensa es una mezcla de prevención, detección y respuesta ágil. "El 85% de las compañías que incorporaron análisis predictivo mejoraron significativamente su capacidad de reacción", dice Nieto, citando cifras de la industria. Además, destaca el rol de la IA en identificar comportamientos anómalos y reducir hasta en un 97% el tiempo de detección de intrusiones. "La IA ya no es una opción, es una necesidad en ciberseguridad", afirma.

Otro camino emergente es el *blockchain*. "Ofrece seguridad descentralizada y trazabilidad, muy útil en sectores como salud y logística", indica Nieto. También subraya la colaboración público-privada como factor clave: "España invirtió más de mil millones de euros en desarrollar algoritmos propios y fortalecer su ciberdefensa pública. En Chile deberíamos mirar ese modelo".

EL IMPACTO DE *RANSOMWARE* ES MÁS DURADERO, porque además del robo y el pago incluye la amenaza pública de divulgar datos sensibles.



En cuanto a las personas, el ejecutivo entrega una batería de recomendaciones. La primera: olvidarse de contraseñas como "123456" o el nombre del perro. "Hay que usar gestores de contraseñas y autenticación de dos pasos siempre que se pueda", indica. También recomienda evitar redes wifi públicas para operaciones sensibles y cambiar las contraseñas predeterminadas de dispositivos IoT.

El rol de la familia también es clave. "Muchas veces, el eslabón más débil es el humano. Enseñar a niños y adultos mayores a identificar correos falsos es tan importante como tener un buen *firewall*".

Entre las tecnologías emergentes para usar, menciona la identidad autosoberana (SSI), que permite a los usuarios controlar su identidad digital sin intermediarios, y la biometría: "El reconocimiento facial o la huella digital son más seguros que un PIN de cuatro dígitos", asegura.

A pesar del panorama sombrío, Nieto se muestra optimista. "La ciberseguridad no es un estado, es un proceso continuo. Pero si se invierte bien, se puede estar un paso adelante". Chile, por ser uno de los países más digitalizados de la región, tiene la oportunidad —y el deber— de liderar en soluciones y conciencia digital. "La batalla no está perdida, pero necesitamos actuar con urgencia. La tecnología está de nuestro lado, solo hay que saber usarla".

REGLAS BÁSICAS PARA PROTEGER LA IDENTIDAD DIGITAL

- Configurar adecuadamente las opciones de privacidad en redes sociales, limitando la visibilidad de la información personal.
- Utilizar contraseñas fuertes y únicas para cada cuenta, y activar la autenticación de dos factores siempre que sea posible.
- Evitar conectarse a redes wifi públicas sin protección, especialmente al realizar transacciones sensibles.
- Actualizar regularmente los dispositivos IoT y cambiar las contraseñas predeterminadas por otras más seguras.
- Ser cautelosos al compartir información personal en línea y verificar la autenticidad de las solicitudes de datos.