

MES DE LA CIBERSEGURIDAD



Desde el año 2018, a partir de la entrada en vigencia de la Ley 21.113, cada octubre hay esfuerzos conjuntos en el país para promover la educación y concientización frente a los riesgos digitales. En un escenario de amenazas más sofisticadas y ataques crecientes, las nuevas tecnologías plantean también nuevas formas de fortalecer la protección.

**IA acelera
la carrera
entre
atacantes y
defensores**

PÁGS. 2 Y 3

**Las
transferencias
internacionales
se blindan ante el
fraude digital**

PÁG. 9

**Biometría:
una llave de
seguridad que
también necesita
protección**

PÁG. 11

LA IA ACELERA LA CARRERA ENTRE ATACANTES Y DEFENSORES

Mientras el uso de esta tecnología permite desplegar ataques en menor tiempo y a mayor escala, las empresas la incorporan para responder con mayor rapidez y efectividad.

POR ANDREA CAMPILLAY



La inteligencia artificial (IA) está transformando las capacidades de atacantes y defensores, aunque no al mismo ritmo. Por un lado, un correo fraudulento puede prepararse en minutos, adaptarse al lenguaje de

una organización y replicarse sobre miles de potenciales víctimas. A su vez, los equipos de ciberseguridad la utilizan para procesar grandes volúmenes de alertas y detectar comportamientos anómalos.

Bajo la mirada de la directora de

la Alianza Chilena de Ciberseguridad, Claudia Santa Ana, la balanza de quién está aprovechando mejor esta tecnología hoy se inclina hacia el lado de los atacantes. "No porque sean más inteligentes, sino porque no tienen comité, ni pre-

PUBLIRREPORTAJE

LUBILAY VARGAS, VICEPRESIDENTA LATAM DE NOVENTIQ, PARTNER GLOBAL DE MICROSOFT

“Tenemos que dejar de pensar en la ciberseguridad como un proyecto de tecnología, es un tema de negocios”



Con más de 2500 clientes a nivel regional y operaciones en todo el mundo, la compañía está pronta a inaugurar su nuevo SOC y planea llevar a sus clientes a Microsoft 365 E7, Frontier Suite que unifica productividad, seguridad e IA empresarial en un solo plan.

Para Lubilay Vargas, vicepresidenta Latam de Noventiq, el mercado está cambiando y la ciberseguridad es un punto clave que ya no se trata solo de un tema tecnológico, sino más bien de negocios. Así, un CEO hoy debe preguntarse ¿cuáles son mis activos más críticos? ¿Quién tiene acceso a esos activos? ¿Cómo tiene acceso? ¿Cuánto tiempo tardó en detectar que mi plataforma está comprometida y, por tanto, mi negocio también lo está? Y si mañana hay un ataque ¿cuánto tiempo necesito para volver a operar? ¿Cuánto dinero pierdo? ¿Cuántos días de trabajo? ¿Qué hago con mis colaboradores?

“Si las organizaciones, tanto en Chile como en Latinoamérica, no tienen hoy la capacidad de responder esas preguntas con claridad, probablemente todavía tienen una brecha de madurez y de seguridad”, afirma.

Y es que hoy las organizaciones enfrentan nuevos desafíos. El primero es la velocidad y superficie de ataque que está creciendo mucho más rápido que la capacidad de las empresas para protegerse.

“Hay un cambio en la manera en que se ataca, en cómo las compañías detectan el ataque y en su resiliencia. Ya no es suficiente tener buenas herramientas. Hay que preguntar cuánto tiempo se tarda en identificar una vulnerabilidad y, sobre todo, cuánto tiempo tarda corregirla. Ese es el punto de partida”, explica.

Un segundo desafío tiene que ver con la inteligencia artificial (IA). Aún hay empresas que no tienen resueltos algunos temas básicos, como el análisis de data, su organización e identificación y cómo se protege.

“Tenemos ahí una gran oportunidad para apoyar



“Podemos acompañar a las empresas en este viaje de transformación y seguridad”, afirma Lubilay Vargas, vicepresidenta Latam de Noventiq.

a nuestros clientes a acelerar su transformación tecnológica con la IA, pero de manera segura, ética, regulada y controlada. En ese punto surge Copilot, pues tiene embebidas dentro de su propio motor diferentes IAs. Entonces es una excelente alternativa para probar a nivel corporativo”, destaca.

Lo que viene

Sin duda, la ciberseguridad es uno de los principales motores de crecimiento de los servicios de Noventiq. “El mercado está evolucionando desde proyectos aislados hacia servicios continuos,

porque una empresa puede implementar una solución de seguridad hoy, pero mañana aparece una nueva vulnerabilidad. También puede cambiar su infraestructura, incorporar nuevas aplicaciones o introducir IA. Entonces ese proyecto aislado no es suficiente, debe abarcar 360”, sostiene.

En ese marco, la apuesta de Noventiq se consolida en

un SOC moderno, con base en Estados Unidos para atender a toda la región, que no solamente cuida las aplicaciones On-Premise, sino que combina capacidades locales con otras regionales y globales, en la nube.

“Otra proyección es la IA. Porque la conversación ya no va a ser cómo utilizamos la IA para automatizar, sino cómo la utilizamos para defendernos”, concluye.

<https://noventiqlatinoamerica.com/>

supuesto anual, ni deuda técnica: adoptan la herramienta el mismo día que aparece", precisa.

La velocidad ya se refleja en los ataques. Según Santa Ana, redactar un señuelo de phishing convincente pasó de tomar cerca de 16 horas a unos cinco minutos y "el 82,6% de los correos de phishing ya incluyen contenido generado con IA". A ello, añade que una de cada cuatro brechas maliciosas involucra IA del lado del atacante.

El chief information security officer

más rápido en capacidad operacional, trazable y escalable.

Sin embargo, este cambio no se refleja de igual manera en todas las dimensiones de un ciberataque. A nivel de costos, el CEO de Nivel4, Fernando Lagos, afirma que ejecutarlos ya era relativamente barato antes de la irrupción de la IA, con kits y servicios de phishing o ransomware disponibles incluso para personas sin conocimientos técnicos. Según plantea, lo que cambia es cuánto puede hacerse

bertrust, José Antonio Lagos, esta puede aumentar las capacidades de ciberdefensa en actividades repetitivas como clasificar alertas, recolectar información de incidentes o resumir vulnerabilidades, permitiendo que los especialistas puedan dedicar su tiempo a actividades que generen más valor y que requieren funciones humanas no sustituibles como el pensamiento crítico y la toma de decisiones complejas. No obstante, aclara que "a priori mayor automatización

idad esto significa que ya no están enfrentando únicamente a personas, sino a procesos automatizados que pueden operar las 24 horas del día, probar miles de variantes de ataque en muy poco tiempo y aprender de los resultados obtenidos", detalla. De esta manera, si antes una organización podía tener horas para reaccionar ante ciertas amenazas, ahora en muchos casos ese tiempo puede reducirse a minutos.

Nuevos riesgos

"La paradoja de esta etapa es que la herramienta que más productividad entrega es también la que más rápido está ampliando la superficie de ataque, y casi siempre sin que nadie lo decida formalmente", advierte Santa Ana. Entre los riesgos asociados a su uso, identifica el ingreso de información sensible en plataformas públicas de IA, el uso de aplicaciones sin control corporativo y la manipulación de modelos mediante instrucciones ocultas.

González suma el riesgo de los agentes conectados a correos, bases de datos y aplicaciones corporativas que podrían dar acceso indirecto a distintos recursos.

"Lo preocupante es que estos ataques no siempre explotan vulnerabilidades técnicas tradicionales; muchas veces buscan influir en la lógica de funcionamiento del propio sistema de IA", concluye.

"La paradoja de esta etapa es que la herramienta que más productividad entrega es también la que más rápido está ampliando la superficie de ataque, y casi siempre sin que nadie lo decida formalmente", afirma la directora de la Alianza Chilena de Ciberseguridad, Claudia Santa Ana.

de Apiux Tech, Lucas Ovalle, coincide en que existe una ventaja táctica, pero matiza su alcance. "No diría que existe hoy un ganador definitivo", sostiene. Explica que, si bien los atacantes no necesitan respetar procesos internos, regulación o sistemas legados, las organizaciones cuentan con la ventaja de conocer el contexto de su operación, sus datos y sus patrones normales de comportamiento. A su juicio, en una carrera donde ambos lados disponen de IA, la ventaja será de quien la convierta

con esos recursos, como por ejemplo, analizar bases de potenciales víctimas, segmentarlas y preparar campañas adaptadas a distintos perfiles con mayor rapidez, precisión y efectividad.

Más capacidad para defender

Desde la vereda de la defensa, la automatización permite ampliar la capacidad de respuesta sin que los equipos crezcan necesariamente en la misma proporción.

De acuerdo con el CEO de Cy-

bertrust, José Antonio Lagos, esta puede aumentar las capacidades de ciberdefensa en actividades repetitivas como clasificar alertas, recolectar información de incidentes o resumir vulnerabilidades, permitiendo que los especialistas puedan dedicar su tiempo a actividades que generen más valor y que requieren funciones humanas no sustituibles como el pensamiento crítico y la toma de decisiones complejas. No obstante, aclara que "a priori mayor automatización

La capacidad de defensa cobra relevancia frente a ataques que también ganan velocidad. El investigador de seguridad informática de ESET Latinoamérica, David González, sostiene que la llegada de agentes de inteligencia artificial capaces de ejecutar tareas de manera autónoma representa uno de los cambios más importantes en ciberseguridad de los últimos años.

"Para los equipos de cibersegu-

PUBLIRREPORTAJE

Presencia internacional, operación local: Cyberpeace fortalece su presencia en Chile

Javier Núñez, Country Manager de Cyberpeace Chile, explica la estrategia de crecimiento de la compañía de origen mexicano en el país y su apuesta por la región de LATAM, respaldada por su experiencia y operación internacional.

Chile atraviesa una etapa de mayor exigencia en materia de ciberseguridad y protección de datos. Para las empresas, esto implica llevar el riesgo digital a las conversaciones de directorio y contar con mayor visibilidad sobre su exposición, sus capacidades de respuesta y la continuidad de sus operaciones. En este contexto, tener equipos que conozcan el mercado y puedan actuar localmente cobra especial relevancia.

Cyberpeace está reforzando su operación en Chile como parte de su estrategia de crecimiento en la región del Cono Sur. La compañía, de origen mexicano y liderada por su CEO, Alex Romero, ha desarrollado operaciones en Norteamérica, Europa y Sudamérica. Esta presencia permite trasladar al mercado chileno experiencia, conocimiento técnico y prácticas desarrolladas en distintos entornos, manteniendo al mismo tiempo una operación cercana a las necesidades locales.

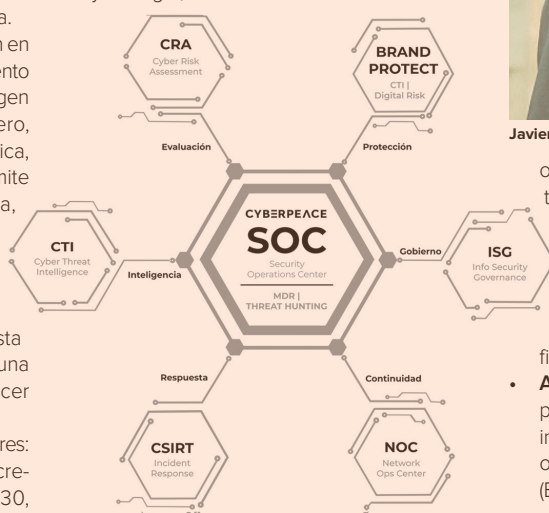
Chile es un mercado estratégico para esta nueva etapa. Nuestra intención es construir una operación con visión de largo plazo y crecer junto con las organizaciones del país.

Nuestro crecimiento se apoya en cuatro pilares:

- **Expansión en Chile.** Proyectamos un crecimiento del mercado para el año 2030,

acompañado de un plan de inversión a tres años enfocado en equipo, tecnología, capacidades especializadas y una mayor presencia local.

- **Foco sectorial.** Trabajamos con el sector público y privado, con énfasis en banca y servicios financieros, seguros, salud, retail y energía, sectores donde la continuidad



Javier Núñez, Country Manager Cyberpeace Chile

operacional y la protección de la información tienen un impacto directo en el negocio.

- **SOC360.** Nuestro ecosistema integra monitoreo, inteligencia de amenazas, respuesta ante incidentes, continuidad y gobierno, con capacidad de operación 24/7/365 y equipos especializados y certificados.
- **Agnósticos a la tecnología.** Nuestros equipos están preparados para trabajar con la infraestructura y las herramientas que cada organización ya utiliza, bajo un modelo BYO (Bring Your Own) y en colaboración con distin-

tos fabricantes. Esto permite aprovechar las inversiones existentes y adaptar la operación a las necesidades de cada cliente.

El objetivo es que las organizaciones tengan una lectura más clara de sus riesgos, sepan cómo actuar ante un incidente y cuenten con capacidad técnica para mantener su operación.

La expansión en Chile también responde a una visión regional. Buscamos desarrollar talento local y sumar las capacidades que Cyberpeace ha construido desde México y en otros mercados. La experiencia internacional aporta escala y conocimiento; la presencia local permite entender cómo aplicarlos a la realidad de cada organización.

Nuestra apuesta es consolidar a Cyberpeace Chile como un socio cercano para las empresas del país, con capacidad técnica local y el respaldo de una compañía internacional. Esa será también una de las bases para continuar nuestro crecimiento en la región Latam.

<https://www.cyberpeace.cl/>
<https://www.linkedin.com/company/cyberpeace-chile>



La conexión entre los sistemas de tecnologías de la información (TI) y las tecnologías operacionales (TO) está cambiando la ciberseguridad en industrias como minería, energía y manufactura. En estos entornos, un incidente puede comprometer procesos físicos, detener una operación y afectar servicios críticos.

De acuerdo con el análisis de Kaspersky ICS CERT para el tercer trimestre de 2025, en Chile, el 18,27% de los computadores de sistemas de control industrial registró el bloqueo de objetos maliciosos en ese período. Y, aunque disminuyó frente al 18,70% del trimestre anterior, la cifra muestra una exposición relevante.

“Los incidentes de ciberseguridad de los sistemas industriales no se relacionan únicamente con la capacidad de detectar ataques, sino también con la creciente conectividad de las operaciones”, analiza la gerente general para la Región Sur de América Latina en Kaspersky, Andrea Fernández.

Asegura que a medida que aumentan las conexiones en fábricas, plantas de energía y sistemas de transporte, también se amplían las posibles puertas de entrada para un atacante.

“En los sistemas más antiguos se podía ver como una ventaja: menos conectividad implicaba menos riesgo. Y hoy, potenciado por la

¿CÓMO SE PROTEGE LA OPERACIÓN DE LOS SECTORES CRÍTICOS?

El avance tecnológico de plantas, faenas e infraestructura esencial amplía los desafíos de resguardo digital y pone el foco en prevenir ataques sin afectar su disponibilidad.

POR VALENTINA CÉSPEDES



Capacidad global. Ejecución local

Inteligencia con Alma. Hacemos que las cosas ocurran.

AI
Cybersecurity
Cloud

hiberus

Authentic Intelligence

PUBLIRREPORTAJE

veeam

AUTOMATIZACIÓN, AGENTES IA Y ENTORNOS DIGITALES COMPLEJOS

Para Veeam la seguridad comienza con los datos

En el marco de Cybersecurity Awareness Month, el mensaje es claro: la concientización es fundamental, pero debe estar acompañada por tecnología, procesos y resiliencia.

Como líder en resiliencia y seguridad de datos, Veeam permite unificar controles de acceso y protección basados en políticas, flujos de gobernanza, salvaguardas de privacidad, reportes de cumplimiento y capacidades de recuperación resiliente. Esto es especialmente relevante en un contexto donde amenazas como ransomware, errores humanos, amenazas internas, agentes autónomos mal configurados o desastres pueden comprometer la continuidad del negocio.

“El aporte de Veeam está en ayudar a las organizaciones a reducir riesgos, fortalecer el control y asegurar la confianza en los datos durante todo su ciclo de vida”, sostiene Dmitri Zaroubine, Director de Ingeniería para Latinoamérica.

En efecto, Veeam ayuda a las empresas no solo a proteger sus datos, sino también a recuperarlos con precisión y confianza. Sus capacidades permiten restaurar operaciones rápidamente con datos limpios, confiables y validados, reduciendo el impacto operativo, financiero y reputacional de un incidente de ciberseguridad.

“Las organizaciones necesitan saber dónde están sus datos, quién accede a ellos, cómo se protegen y cómo pueden recuperarse de forma segura cuando ocurre un ataque”, destaca el ejecutivo.

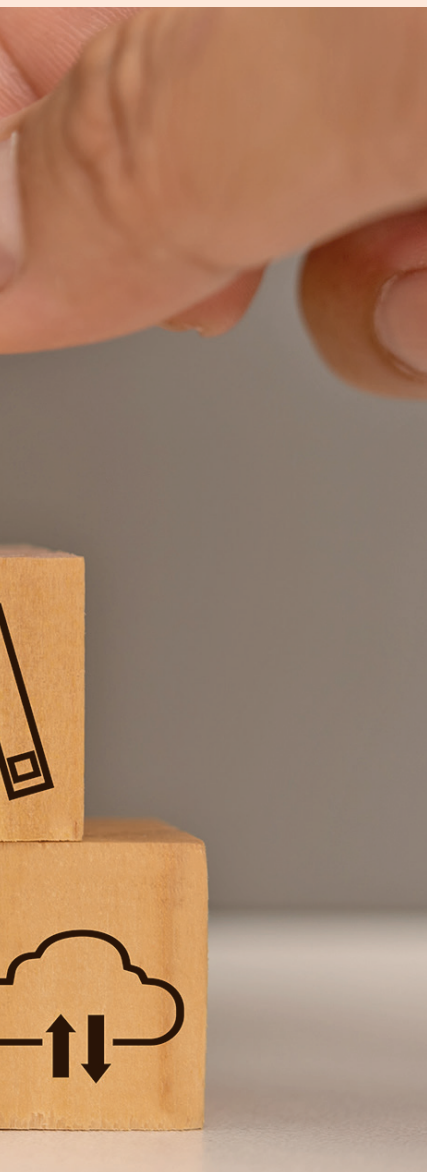
De cara al futuro, Veeam proyecta que



Dmitri Zaroubine, Director de Ingeniería para Latinoamérica.

la confianza en los datos será un habilitador central para la innovación, especialmente para la adopción de inteligencia artificial a escala. Las organizaciones que logren garantizar seguridad, privacidad, cumplimiento y resiliencia estarán mejor preparadas para aprovechar la IA de forma segura y responsable.

<https://www.veeam.com/es>



inteligencia artificial generativa, un experto en *hacking* en entornos tradicionales puede ser, al menos, un especialista también en estos entornos industriales”, complementa el líder de la plataforma estratégica del sector industrial de la Alianza Chilena de Ciberseguridad (ANCI), Carlos Vera.

Procesos críticos

El avance de la regulación también amplió en Chile el universo de organizaciones críticas. En julio de 2026, la ANCI informó que más de mil instituciones fueron calificadas como Operador de Importancia Vital (OIV). La segunda etapa incorporó otras 239 organizaciones, entre ellas empresas de combusti-

ble, agua potable, transporte y concesionarias de servicios públicos.

“Para una empresa, calcular el costo de una eventual interrupción operacional debería comenzar por identificar cuáles son sus activos y procesos más críticos”, sostiene Fernández. En una planta, faena minera o infraestructura crítica, la detención puede tener consecuencias directas sobre la producción o la entrega de servicios clave.

Si bien en Chile no existen cifras oficiales consolidadas sobre cuánto destinan las empresas a proteger sus ambientes industriales, Kaspersky estima que un ciberataque puede alcanzar un costo promedio de US\$ 1,5 millones, según la criticidad de cada operación.

“Uno de los vectores más explotados en estos últimos tiempos es usar a proveedores y servicios de terceros que están conectados a los sistemas industriales para poder acceder en forma remota a grandes corporaciones”, advierte Vera.

Para la gerenta general de la ACTI, Luz María García, la protección requiere combinar segmentación entre redes TI y TO, monitoreo continuo, gestión de identidades, respaldo y recuperación, detección de anomalías, inventario de activos y planes de respuesta a incidentes. A esto se suma la escasez de especialistas con conocimientos híbridos capaces de “entender simultáneamente redes, sistemas industriales,

US\$
1,5
MILLONES
PUEDE ALCANZAR EL
COSTO PROMEDIO
DE UN CIBERATAQUE,
SEGÚN KASPERSKY.

El nuevo estándar obligatorio que exige la Ley de Ciberseguridad

La Ley Marco de Ciberseguridad incorpora nuevas exigencias para las organizaciones calificadas como Operadores de Importancia Vital (OIV), particularmente aquellas cuya interrupción puede afectar la provisión de servicios esenciales. Según el líder de la plataforma estratégica del sector industrial de la Alianza Chilena de Ciberseguridad (ANCI), Carlos Vera, entre las exigencias se encuentra la implementación de un sistema continuo de gestión de seguridad de la información (SGSI), que permita identificar riesgos y evaluar tanto la probabilidad como el impacto de un incidente sobre redes, sistemas y continuidad del servicio. Los OIV también deberán contar con planes de continuidad operacional y ciberseguridad, sujetos a revisión periódica. “Las empresas sujetas a esta regulación, tendrán el desafío de prepararse, identificando activos críticos, mapeando dependencias IT/OT, definiendo escenarios de interrupción, estableciendo mecanismos de segmentación y recuperación, probando los planes y asegurándose que exista una estructura clara de responsabilidades y, por supuesto, en lo que la ley es muy explícita reportando en tiempo y forma todo incidente de ciberseguridad”, advierte Vera.

riesgo, regulación y operación”.

La necesidad de proteger sin alterar la operación también ha impulsado plataformas de visibilidad y monitoreo pasivo. El SOC manager de Grupo Tecnológico ITQ, Lelis Cuicas, señala que estas permiten analizar el tráfico industrial sin intervenir directamente en los procesos.

Para Fernández, lo relevante es combinar prevención y capacidad de recuperación, que vaya más allá del cumplimiento normativo:

“Un incidente que comprometa información de clientes, trabajadores o proveedores puede generar impactos económicos, reputacionales y operativos, por lo que la preparación debe considerar tanto la prevención como la capacidad de recuperación”. Esto, asegura, implica respaldo, inteligencia de amenazas, pruebas de penetración, recuperación previamente testeada y capacitación de los colaboradores.

PUBLIRREPORTAJE

NIVEL4 impulsa la ciberseguridad de las empresas frente a la transformación digital

En un escenario de transformación tecnológica acelerada, NIVEL4 apoya a sus clientes a proteger sus sistemas y crecer de forma segura, combinando innovación permanente y criterio experto.

La cuarta revolución industrial avanza a gran velocidad, con una vertiginosa digitalización y virtualización de procesos que transforma la cultura de trabajo, las normativas y el intercambio comercial. Para seguir siendo competitivas, las empresas han renovado sus infraestructuras tecnológicas con nuevos servicios, plataformas y aplicaciones, lo que ha vuelto sus sistemas más complejos e interdependientes y exige a sus equipos de seguridad un apoyo especializado.

NIVEL4 Cybersecurity tiene como propósito apoyar a sus clientes en el desafío de mantener el control sobre la seguridad de sus sistemas informáticos, reducir el riesgo ante su alta exposición y enfrentar ciberamenazas cada vez más versátiles. “En NIVEL4 llevamos más de una década evolucionando al ritmo de la tecnología, pero siempre con un propósito claro: estar un paso adelante en ciberseguridad. La innovación ha sido parte de nuestro ADN desde el primer día, y la inteligencia artificial representa hoy una nueva etapa de esa evolución. No solo la estamos incorporando para potenciar nuestros servicios, sino también para ayudar a las organizaciones a aprovechar todo su potencial de manera segura”, comenta su CEO, Fernando Lagos Berardi.

En NIVEL4 se innova permanentemente en nuevas capacidades tecnológicas de forma transversal en todas sus operaciones, mirando tanto los desafíos de hoy como los de un escenario de ciberseguridad global cada vez más complejo. Esa apuesta se refleja, por ejemplo, en sus servicios de monitoreo, donde herramientas de análisis automatizado apoyan la detección y respuesta ante amenazas, agilizando procesos que antes exigían muchos profesionales y tiempo.

Una distinción clave de NIVEL4 es su política de automatización responsable, que busca un equilibrio entre el uso eficiente de nuevas tecnologías -como la IA- y el rol irremplazable de sus especialistas. Como resultado, la empresa optimiza la capacidad de sus equipos para atender y resolver proyectos, mejorando los tiempos de respuesta sin perder su sello de calidad en la entrega de servicios.

El objetivo de NIVEL4 es robustecer el ecosistema de la ciberseguridad a través de los servicios que entrega, asegurando una calidad que impacte positivamente en las empresas y en las personas, y permitiéndoles adaptarse al ritmo de la transformación digital.



En NIVEL4 llevamos más de una década evolucionando al ritmo de la tecnología, pero siempre con un propósito claro: estar un paso adelante en ciberseguridad. La innovación ha sido parte de nuestro ADN desde el primer día, y la inteligencia artificial representa hoy una nueva etapa de esa evolución. No solo la estamos incorporando para potenciar nuestros servicios, sino también para ayudar a las organizaciones a aprovechar todo su potencial de manera segura

FERNANDO LAGOS BERARDI
CEO - NIVEL4



NIVEL4.COM

MES DE LA CIBERSEGURIDAD: Cómo defenderse de la IA en la era de la IA

La inteligencia artificial está cambiando las reglas del negocio y también las de la ciberseguridad. Para enfrentar este nuevo escenario, Gtd con su centro de excelencia en Ciberseguridad, Secure Soft, combina talento especializado, monitoreo continuo, ciberinteligencia y tecnologías avanzadas para fortalecer la resiliencia de las organizaciones frente a amenazas cada vez más sofisticadas.

La adopción de inteligencia artificial está transformando procesos, acelerando la innovación y generando nuevas oportunidades para las empresas. Sin embargo, la misma tecnología que impulsa la productividad también está siendo utilizada por los ciberdelincuentes para sofisticar sus ataques, automatizar campañas de fraude y aumentar su capacidad de evasión. Hoy, defenderse de la IA se ha convertido en uno de los principales desafíos de las organizaciones.

Los ciberataques globales crecieron un 44% durante el último año, impulsados por la profesionalización de los grupos criminales y la adopción masiva de herramientas basadas en inteligencia artificial.

Frente a este escenario, las empresas necesitan capacidades para anticipar amenazas, monitorear riesgos y responder con velocidad.

“Los grupos cibercriminales hoy operan con estructuras cada vez más sofisticadas, similares a empresas, donde la automatización y la inteligencia artificial han hecho que el crimen digital sea más eficiente, persistente y difícil de detectar”, explica Juan Carlos Beltrán, Chief Technology Officer de Secure Soft.

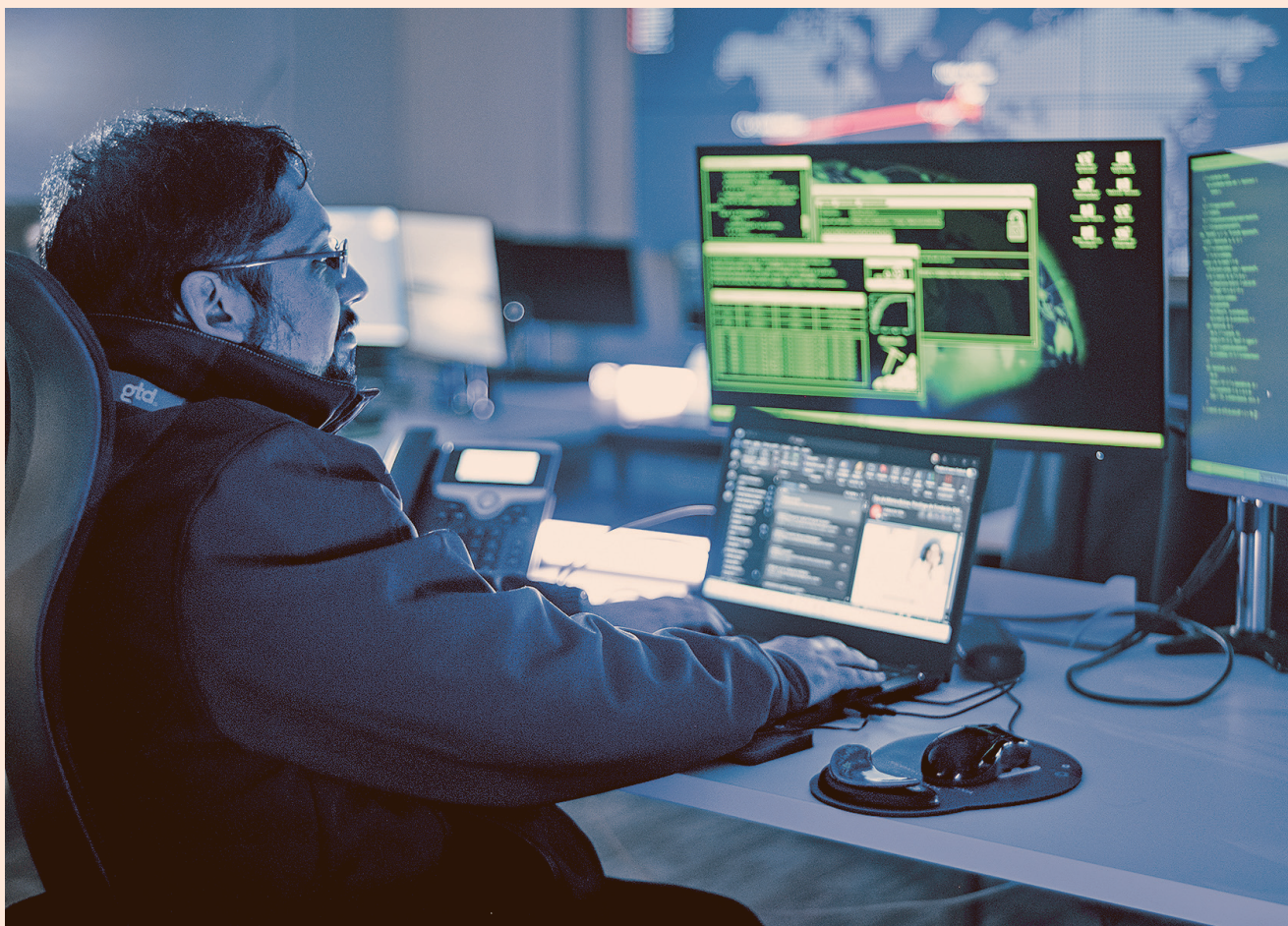
Cuando la IA se transforma en un riesgo para el negocio

La transformación digital ha multiplicado la cantidad de usuarios, dispositivos, aplicaciones, APIs y servicios conectados dentro de las organizaciones. En paralelo, la incorporación acelerada de inteligencia artificial ha ampliado aún más la superficie de exposición.

Hoy es necesario administrar identidades digitales, accesos privilegiados, cuentas de servicio, bots y agentes impulsados por IA que interactúan con información crítica y sistemas de negocio. En este contexto, la identidad se está convirtiendo en el nuevo perímetro de seguridad.

“Hoy los atacantes ya no necesitan vulnerar complejas barreras tecnológicas; muchas veces simplemente inician sesión utilizando credenciales legítimas. Eso obliga a las organizaciones a cambiar completamente su enfoque de protección, poniendo la identidad en el centro de la estrategia de seguridad”, afirma Juan Carlos Beltrán.

La tendencia se refleja en los datos. Investigaciones de Check Point Research registran un aumento de 160% en las credenciales comprometidas durante 2025, consolidando al robo de identidades como uno de los mecanismos de



ataque más utilizados por los ciberdelincuentes.

Hoy las organizaciones requieren una ciberseguridad mucho más avanzada que controles de acceso tradicionales. A partir de su experiencia acompañando a empresas de distintos sectores en Latinoamérica, Secure Soft ha fortalecido la protección de identidades, datos, aplicaciones, redes y entornos cloud mediante estrategias Zero Trust, capacidades avanzadas de gestión de identidades (IAM), administración de accesos privilegiados (PAM), monitoreo continuo, ciberinteligencia, detección y respuesta gestionada (MDR) y servicios CyberSOC impulsados por inteligencia artificial

Estas capacidades permiten aumentar la visibilidad sobre los riesgos, proteger los activos más críticos del negocio y responder con mayor rapidez frente a amenazas cada vez más sofisticadas, contribuyendo directamente a fortalecer la resiliencia digital y la continuidad operacional de las organizaciones.

La importancia de anticiparse

La ciberinteligencia permite identificar amenazas emergentes y campañas activas antes de que impacten al negocio, entregando información clave para una respuesta preventiva.

“Hoy la diferencia entre una organización resiliente y una vulnerable muchas veces está en la capacidad de anticipación. Comprender quiénes son los atacantes, cómo operan y cuáles son sus objetivos permite tomar decisiones más rápidas y efectivas”, señala Juan Carlos Beltrán.

Más allá del cumplimiento: el nuevo estándar regulatorio en ciberseguridad y protección de datos

La inteligencia artificial no es el único factor que está elevando las exigencias de seguridad. La entrada en vigencia de la Ley Marco de Ciberseguridad marcó un punto de inflexión para las organizaciones en Chile, incorporando nuevas responsabilidades en materia de gestión de riesgos, reporte de incidentes y resiliencia operacional. A ello se suman los desafíos que traerá la futura implementación de la nueva Ley de Protección de Datos Personales, elevando aún más los estándares de gobernanza de la información.

Sin embargo, la adaptación no ha sido ni será sencilla. Históricamente, muchas organizaciones han abordado la protección de datos y la ciberseguridad desde una perspectiva de cumplimiento mínimo, con distintos niveles de madurez en materias como clasificación de información, gestión de accesos, monitoreo continuo y respuesta

ante incidentes. Las nuevas regulaciones elevan significativamente el estándar y exigen una mirada mucho más integral sobre cómo se recopilan, almacenan, procesan y protegen los datos, así como sobre la capacidad de prevenir, detectar y responder ante incidentes de seguridad.

Las empresas deberán acreditar medidas adecuadas para resguardar la información que administran, gestionar riesgos, mantener trazabilidad sobre accesos y responder eficazmente frente a incidentes de seguridad. Asimismo, sectores definidos como críticos o estratégicos deberán fortalecer sus capacidades de monitoreo, continuidad operacional y gestión de incidentes, alineándose con las nuevas exigencias regulatorias.

Para muchas compañías, el principal desafío no será incorporar nuevas tecnologías, sino desarrollar capacidades de gestión, visibilidad y control que les permitan demostrar un adecuado tratamiento de los datos personales y una respuesta efectiva frente a incidentes.

“La nueva regulación representa una oportunidad para que las organizaciones fortalezcan su resiliencia digital. El desafío ya no es únicamente cumplir con una obligación legal, sino desarrollar capacidades que permitan proteger adecuadamente la información y responder frente a un entorno de amenazas cada vez más complejo”, señala Juan Carlos Beltrán.

En este contexto, servicios como protección de identidades, clasificación de información, evaluación de vulnerabilidades, monitoreo continuo, respuesta ante incidentes y consultoría especializada adquieren un rol estratégico no solo para proteger el negocio, sino también para cumplir con los nuevos requerimientos regulatorios.

Para muchas organizaciones, la ciberseguridad está dejando de ser una iniciativa tecnológica para convertirse en un imperativo de gestión, cumplimiento y continuidad operacional.



Una **amenaza se esconde** en millones de datos

En Gtd te **ayudamos a encontrarla**

Identificar un riesgo a tiempo exige precisión absoluta. Con nuestro Centro de Excelencia de Ciberseguridad, analizamos millones de eventos y datos en tiempo real para neutralizar cualquier amenaza antes de que afecte a tu organización. Contamos con tecnología de estándar mundial y el respaldo de expertos enfocados en proteger la continuidad de tu empresa.



**Centro de Excelencia
de Ciberseguridad**



+20 años de experiencia



**+480 expertos de
ciberseguridad**



**+100 incidentes
críticos resueltos**

CONOCE MÁS



Tecnología para simplificar **tu vida**

 gtd.cl

 company/gtdchile

LOS DESAFÍOS DE SEGURIDAD QUE ENFRENTA LA CADENA DE PROVEEDORES



Cumplir con controles, auditorías y certificaciones puede abrir o cerrar el acceso a grandes contratos. Las pymes enfrentan el desafío de financiar esa adaptación sin quedar fuera de la cadena.

POR ANAÍ PERSSON

Con el avance y la sofisticación de los ciberataques también aumentan las precauciones en ciberseguridad de las empresas y, por lo tanto, las que exigen a su cadena de suministro. No obstante, todavía hay brechas, pues, según un informe publicado en enero de este año por el Foro Económico Mundial, el 65% de las grandes empresas identificaba las vulnerabilidades de terceros y proveedores como su principal desafío para alcanzar resiliencia cibernética. En el reporte anterior, publicado en 2025, la cifra era menor, llegando al 54%.

“Las organizaciones están avanzando hacia esquemas basados en criticidad y riesgo, dejando atrás el enfoque de exigir lo mismo a todos los proveedores”, afirma Ernesto Tachiores, director corporativo de desarrollo de negocios de ciberseguridad de Sonda. La clasificación, dice, considera el acceso a información, los privilegios, la integración tecnológica, la dependencia operacional y el impacto potencial de una interrupción.

El riesgo detrás de esa clasificación ya se está materializando. Según una encuesta global de Kaspersky realizada entre septiembre y noviembre de 2025, el 31% de las empresas había sufrido un ataque a su cadena de suministro en los 12 meses previos. Entre las grandes corporaciones, la propor-

ción alcanzó el 36%.

Para Tachiores, una ruta gradual puede comenzar con autenticación multifactor, gestión de parches, respaldos, privilegios mínimos, capacitación y protocolos para reportar incidentes. A mayor criticidad, se incorporan monitoreo, planes de continuidad, auditorías y evidencias de cumplimiento. Para los terceros con mayor exposición, los requisitos pueden incluir la certificación ISO 27001 o SOC 2, monitoreo, pruebas de penetración, auditorías y planes de continuidad.

Este modelo ya se observa en empresas de servicios esenciales. Aguas Andinas, por ejemplo, clasifica a sus proveedores según el riesgo y el impacto potencial de un incidente, aplicando un enfoque Zero Trust, bajo el cual ningún acceso se considera confiable por defecto, según cuentan desde la compañía.

“No es lo mismo un proveedor que entrega insumos sin acceso a sistemas, que uno que accede a información sensible, procesa datos o participa en procesos

operacionales críticos”, explica su oficial de ciberseguridad (CISO), Juan Francisco Huechucura.

Según cuenta, la evaluación comienza desde el diseño y contratación del servicio, incorporando diversos requisitos de ciberseguridad, confidencialidad y gestión de accesos. Posteriormente, estos controles se mantienen durante toda la relación mediante monitoreo, revisiones periódicas, auditorías y obligaciones de reporte ante cualquier incidente o cambio relevante. Ante deficiencias de seguridad, dice que se establecen planes con responsables y plazos, además de medidas compensatorias durante la corrección.

Una nueva barrera de entrada

En el caso de las pymes, la brecha de partida es relevante. En Chile, el 46% de las empresas encuestadas para el estudio Mastercard 2026 SME Cybersecurity Outlook no cuenta con un plan de ciberseguridad. A nivel regional, una de cada cinco pymes carece de un plan de respuesta o recuperación ante incidentes.

Para una empresa de este tamaño, avanzar no implica contratar desde el inicio a un CISO de jornada completa. Fernando Lagos Berardi, CEO de Nivel4, explica que la función puede externalizarse o contratarse por horas, aunque alguien debe asumir la responsabilidad.

Tachiores dice que el problema aparece cuando se trasladan a una pyme las mismas exigencias diseñadas para un proveedor crítico de gran escala. “La seguridad de la cadena no mejora excluyendo proveedores más pequeños, sino definiendo requisitos coherentes con el tipo de servicio que prestan y acompañando su madurez”, afirma.

Lagos señala que cuando el proveedor sí maneja datos personales o se conecta a la red de una gran compañía, las exigencias aumentan e incorporan pruebas de seguridad y capacidades para investigar y reportar incidentes. Según explica, el costo inicial tiende a ser alto y después disminuye en la mantención: “Generalmente uno empieza cuando no hay mucha visibilidad de la tecnología que se maneja y su estado de ciberseguridad. Entonces, cuando se hace un análisis principal, suelen aparecer muchos hallazgos y cosas que mitigar”.

Ante un incidente que comprometa a un proveedor conectado a su red, una gran empresa puede suspender el acceso hasta conocer su origen, alcance y contención. Sin inventarios, procedimientos ni datos catalogados, la pyme tendrá dificultades para entregar ese reporte, recuperar la conexión y continuar prestando el servicio, lo que convierte la falta de preparación en un costo operacional, advierte Lagos.

65%

DE LAS GRANDES EMPRESAS IDENTIFICA LAS VULNERABILIDADES DE TERCEROS Y DE LA CADENA DE SUMINISTRO COMO SU PRINCIPAL DESAFÍO PARA ALCANZAR RESILIENCIA CIBERNÉTICA, SEGÚN EL FORO ECONÓMICO MUNDIAL.

CÓMO SE BLINDAN LAS TRANSFERENCIAS INTERNACIONALES FRENTE AL FRAUDE DIGITAL



Mientras los riesgos crecen y las exigencias regulatorias aumentan, la industria financiera fortalece la seguridad de sus transacciones, con procesos que van desde autenticación reforzada hasta la detección de anomalías en tiempo real. POR FRANCISCA ORELLANA

La rapidez de las transferencias de dinero internacionales plantea un desafío para la industria financiera: detectar y frenar el fraude antes de que el monto llegue a destino. La participación de bancos, fintech e intermediarios en distintos países multiplica los puntos vulnerables y obliga a reforzar los controles frente a estafas y suplantaciones de identidad.

"El fraude en transferencias internacionales combina cada vez más ingeniería social, suplantación de identidad, uso indebido de credenciales y manipulación de las personas que autorizan las operaciones", dice Diego Veroiza, gerente gremial de FinteChile y miembro de la Alianza Chilena de Ciberseguridad.

Los riesgos ya no están únicamente en el acceso a las cuentas, añade, pues "una transacción puede estar correctamente autenticada y, aun así, ser fraudulenta si el atacante consiguió que el propio usuario la ejecutara".

Para la managing director cybersecurity de Accenture Chile, María Luisa Acuña, el fraude en este negocio rara vez responde a una táctica, sino que "combina amenazas del ecosistema digital, como ingeniería social, compromiso de correo electrónico, phishing, entre otras, con fallas

en controles básicos dentro de las propias organizaciones".

En este escenario, el desafío es "combinar regulación con monitoreo, prevención y coordinación entre instituciones financieras, empresas y proveedores tecnológicos", dice la gerente general de la ACTI, Luz María García, agregando que, según la Comisión para el Mercado Financiero (CMF), el monto promedio de las transferencias no reconocidas reclamadas pasó de \$ 143 mil a \$ 450 mil entre enero de 2023 y diciembre de 2024.

Controlar los riesgos

Si bien Chile cuenta con un ecosistema financiero robusto en autenticación, monitoreo, prevención y cumplimiento, la gestión de riesgos se ha desarrollado incluso antes de las exigencias regulatorias, Veroiza indica que eso no significa que estén ajenas al fenómeno: "El fraude es cada vez más sofisticado, digital y transnacional".

Aunque el riesgo está presente, la industria ha ido robusteciendo sus soluciones para blindarse y dis-

minuir el riesgo. García destaca que la Ley Marco de Ciberseguridad creó una institucionalidad especializada y, desde agosto de 2026, la CMF exige autenticación reforzada para las transferencias electrónicas.

Veroiza agrega que muchas empresas avanzaron en esto antes de las exigencias regulatorias, al entender que la confianza es clave para operar. "La industria está pa-

transaccional y análisis del comportamiento del usuario, que permiten levantar alertas frente a un dispositivo nuevo, cambios de ubicación, incorporación repentina de beneficiarios, montos poco habituales o intentos reiterados de autenticación", detalla García. Este análisis, complementa Veroiza, debe acompañar la transacción de punta a punta.

Es un avance relevante, dice la gerente de riesgo y ciberseguridad de Klap, Sandra Ferrada, que debe complementarse con monitoreo transaccional basado en comportamiento, para reforzar "la trazabilidad y la capacidad de detectar comportamientos anómalos en tiempo real en todo el proceso".

Desafíos

Reforzar la seguridad sin agregar fricción innecesaria a la experiencia del usuario es uno de los retos que tiene la industria hoy. "A medida que los pagos se vuelven más rápidos, interoperables y automatizados, las instituciones financieras necesitan equilibrar velocidad, control y confianza, incorporando la gestión del riesgo dentro de la propia experiencia de pago", dice Acuña.

No todas las operaciones requieren el mismo nivel de control, advierte Veroiza: "Mientras mayor sea la calidad de la información disponible, mejor pueden funcionar los sistemas de detección y menor es la necesidad de imponer fricciones

"El fraude en transferencias internacionales combina cada vez más ingeniería social, suplantación de identidad, uso indebido de credenciales y manipulación de las personas que autorizan las operaciones", dice Diego Veroiza, gerente gremial de FinteChile y miembro de la Alianza Chilena de Ciberseguridad.

sando de un modelo de seguridad centrado en verificar quién está operando, a uno que busca qué operación se está realizando, en qué contexto y si es consistente con el comportamiento habitual del usuario", destaca.

"Hoy la detección combina autenticación reforzada, monitoreo

"Bancos, fintechs y plataformas de pago han avanzado en motores antifraude con análisis en tiempo real, autenticación reforzada de clientes y verificación de identidad mediante biometría del comportamiento", destaca Acuña.

indiscriminadamente".

Aquí la colaboración público-privada es fundamental: "Ninguna institución tiene por sí sola toda la información necesaria para enfrentar un fenómeno que es transnacional y que evoluciona rápidamente", concluye el gerente gremial de FinteChile.

Ria consolida su posición en Chile y apuesta por un futuro omnicanal para las remesas

Con el canal digital como principal vía de operación en Chile, Ria Money Transfer apuesta por un modelo que integra tecnología y atención presencial. La compañía sostiene que la transformación de las remesas no pasa por reemplazar un canal por otro, sino por entregar más alternativas a un cliente que exige inmediatez, precios competitivos y libertad para elegir cómo mover su dinero.



Las remesas son mucho más que mover dinero de un país a otro. Son una forma de mantener conectadas a las personas y de hacer posible que el dinero llegue donde se necesita, independientemente de la distancia. Hoy, más de 1,6 millones de personas nacidas en el extranjero viven en Chile, manteniendo vínculos con sus países de origen.

“En Ria creemos que nuestro rol es facilitar esas conexiones, haciendo que mover dinero entre países sea cada vez más simple, rápido y accesible. La tecnología es fundamental para lograrlo, pero también lo son la cercanía, la confianza y la posibilidad de elegir”, comenta Ana Dresdner, Managing Director South America, Ria Money Transfer.

Por eso la compañía que forma parte de Euronet Worldwide, ha construido un modelo donde lo digital y lo presencial conviven. En Chile, el canal digital es su principal vía de operación, pero se complementa con 20 tiendas propias y una red cercana a 300 sucursales a través de su socio estratégico Turbus y sus marcas asociadas -Starken, Cónдор Bus, JAC y Bio Bio-.

“Nuestros clientes se mueven naturalmente entre ambos mundos: pueden utilizar la aplicación en una ocasión y preferir la atención presencial en otra. Para nosotros, innovar no significa llevar a todos los clientes hacia un mismo canal, sino ampliar sus posibilidades y permitirles elegir. Por eso creemos que el futuro de las remesas será omnicanal”, afirma.

Y es que se trata de una industria que ha cambiado. Hace diez años las personas estaban mucho más dispuestas a adaptarse a la forma en que la industria les ofrecía enviar dinero. Hoy ocurre lo contrario. Además, el cliente es más informado, exigente y, sobre todo, quiere elegir.

Asimismo, las transferencias internacionales ya no responden únicamente al concepto tradicional



“Estamos fortaleciendo la infraestructura de Ria en la región y desarrollando nuevas conexiones. La apertura de nuestra operación en Colombia durante 2025 y de nuestra operación directa en Panamá en 2026 son parte de esa estrategia regional”, indica Ana Dresdner.

de remesa familiar. Cada vez existen más personas en Chile que necesitan mover dinero hacia otros países por diferentes razones y que buscan alternativas simples, transparentes y competitivas frente a los mecanismos tradicionales.

“Nuestro desafío es responder a esa diversidad de necesidades sin perder aquello que ha caracterizado históricamente a este negocio: confianza, cercanía y la certeza de que el dinero llegará a destino”, asegura la ejecutiva.

Más allá de la inmediatez

La inmediatez dejó de ser un elemento diferenciador para transformarse en una expectativa básica. En efecto, Latinoamérica está viviendo una transformación especialmente interesante. Infraestructuras y ecosistemas como Pix en Brasil, Bre-B en Colombia o Pago Móvil en Venezuela



“Estamos preparando una nueva etapa: ampliar nuestra propuesta hacia el segmento B2B, llevando nuestra experiencia e infraestructura internacional a empresas que también necesitan mover dinero entre países de una manera más eficiente”, señala Juan Cristóbal Bianchi.

La industria seguirá creciendo y transformándose, pero la competencia ya no estará determinada por quién tiene la mejor aplicación. Precio, velocidad, seguridad, capilaridad y capacidad de elección serán fundamentales.

están cambiando la manera en que las personas reciben y utilizan su dinero, mientras Chile avanza hacia un ecosistema de pagos cada vez más digital, abierto e interoperable.

“Digitalizar no significa obligar al cliente a utilizar un solo canal. Para nosotros, la verdadera innovación consiste en darle más opciones”, sostiene Ana Dresdner.

Esta visión forma parte también de la estrategia global de Euronet. Juan Cristóbal Bianchi, Executive Vice President & CEO, Cross-Border Payments Segment of Euronet Worldwide, chileno y radicado desde hace años en Los Ángeles, California, mantiene una conexión directa y permanente con Chile y con la operación local. Esa cercanía le permite conocer de primera mano la evolución del mercado chileno y, al mismo tiempo, observarla desde la perspectiva de una industria global que está cambiando aceleradamente.

Por otro lado, a nivel global, Ria está desarrollando nuevas experiencias que permiten integrar las transferencias de dinero en plataformas que las personas utilizan habitualmente. WhatsApp es un ejemplo de esta evolución, y Chile está entre los mercados donde Ria proyecta incorporar este tipo de experiencias.

Adicionalmente, Ria anunció una alianza para integrar sus servicios en la aplicación de Uber para conductores en Reino Unido.

Mirando hacia el futuro, Euronet también está explorando el potencial de tecnologías como las stablecoins para hacer más eficientes procesos de liquidación, tesorería y movimiento internacional de fondos.

“La tecnología seguirá cambiando, pero nuestro objetivo permanece: hacer que enviar dinero sea cada vez más sencillo, rápido, seguro y accesible”, enfatiza Ana Dresdner.

BIOMETRÍA: UNA LLAVE DE SEGURIDAD QUE TAMBIÉN NECESITA PROTECCIÓN

El uso creciente de rostros, huellas y voces para autenticar identidades plantea nuevos desafíos de ciberseguridad. Frente al avance de la IA y mayores exigencias regulatorias, las empresas deben reforzar la protección de estos datos.

Cuando se filtra una base de datos que contiene contraseñas, el usuario normalmente se entera por una alerta y basta con cambiarlas para reducir el riesgo. Pero, ¿qué ocurre cuando la información robada es una huella, un rostro o una voz? Para Sebastián Avila, jefe CSIRT del Grupo Tecnológico ITQ, se trata de un problema mayor: advierte que la exposición de los datos biométricos "te acompaña de por vida".

"Hay un segundo factor que solemos pasar por alto: la biometría no es secreta. Dejamos huellas en cada vaso que tomamos y nuestra

cara y voz están en redes sociales, videollamadas y audios de WhatsApp. Por eso el riesgo no es solo que una empresa sufra una filtración. Esos datos también se pueden reutilizar en otro lugar, por ejemplo, para hacerse pasar por alguien ante su banco. Es, en la práctica, una vulnerabilidad que no caduca. Eso obliga a quienes manejan estos datos a protegerlos con un estándar más alto que cualquier otro dato

personal", puntualiza.

El Dr. José Fernández, vicepresidente de Pro Salud Chile en colaboración con la Alianza Chilena de Ciberseguridad, acota que esta protección debe comenzar antes de implementar la tecnología. La Ley 21.719 considera los datos biométricos sensibles y obliga al titular a informar qué sistema se usa, garantizar su seguridad y evaluar previamente los tratamientos de

alto riesgo

"En la práctica, cada organización debería poder demostrar cuatro cosas respecto de cada dato biométrico que recoge: que tiene una finalidad legítima, que es necesario para cumplirla, que está bien protegido y que hay reglas claras sobre quién accede, cuánto tiempo se conserva y cuándo se elimina. Y esa responsabilidad no se externaliza. El proveedor tecnológico puede cometer el error, pero quien responde es el responsable del tratamiento", asegura Fernández.

A estas exigencias se suma el avance de la IA, que permite imitar rostros y voces o generar identidades sintéticas. Alan Shomaly, gerente de desarrollo de ecert, explica que existen tecnologías para detectar intentos de suplantación y verificar que quien intenta autenticarse sea una persona real. "Se realizan análisis tanto a la información capturada como a los dispositivos involucrados en el proceso y hay laboratorios especializados en estudiar las distintas técnicas de suplantación y diseñar mecanismos de detección y prevención", sostiene.

Así, el desafío para las empresas ya no consiste únicamente en incorporar sistemas biométricos cada vez más sofisticados, sino en garantizar que la información utilizada para autenticar identidades no se convierta, a su vez, en una nueva fuente de vulnerabilidad.

VITRINA EMPRESARIAL



Verificación de identidad: el requisito silencioso de la nueva Ley de Datos Personales

El debate corporativo se concentra en consentimientos y políticas de privacidad. Pero hay un eslabón previo que condiciona todo el modelo: saber con certeza, quién está al otro lado.

Sin duda, la Ley 21.719 conlleva nuevos desafíos y es ahí donde radica la relevancia de la trayectoria y estrategia de identidad digital, firma electrónica y biometría de ecert, compañía de certificación electrónica con operaciones en Chile y Perú, dedicada a generar firmas electrónicas avanzadas y verificar remotamente la identidad de quienes firman. En efecto, a la fecha, gestiona 14 millones de firmas avanzadas en Chile, operación que produce importantes beneficios sociales al reducir traslados y tiempos de espera.

"Llevamos años verificando identidad y hoy esa capacidad pasa de ser un detalle operativo a ser el centro del cumplimiento. Si la pregunta

de quién está al otro lado no se responde con un estándar robusto, todo el resto queda sobre una base frágil", indica Alfredo Guardiola, gerente general de ecert.

Ante la nueva ley, la discusión se centra en las restricciones y riesgos asociados a la identificación, incluyendo la posibilidad de fraude. En ese marco, los datos biométricos son sensibles y las soluciones deben reducir el almacenamiento de patrones, proteger la información indispensable y cumplir estándares elevados de seguridad, infraestructura y ciberseguridad.

Asimismo, la nueva ley exige gestionar consentimientos específicos y solicitudes de modificación, eliminación u olvido de datos personales. "La verificación de identidad en esos procesos puede apoyarse en la firma electrónica avanzada, su carácter de no repudio legal y la combinación de distintas tecnologías biométricas y factores complementarios", destaca Hugo Espinoza, CRO de ecert.



Para Alfredo Guardiola y Hugo Espinoza, la tecnología no garantiza por sí sola el éxito de los proyectos, de ahí la importancia de servicios de valor agregado, la implementación y el acompañamiento a los clientes.

Para ello, ecert provee acompañamiento experto e infraestructura de confianza para orquestar acuerdos digitales y gestionar la identidad en procesos masivos. La estrategia de ecert se articula en torno a la identidad como plataforma, con más de diez métodos disponibles y una orquestación adaptativa para verificar a las personas sin introducir fricción.

En esa línea, la empresa especializada lanzó una nueva solución de biometría dactilar que compara la huella del usuario con la registrada en su cédula de identidad.

Por último, para Alfredo Guardiola el punto de fondo no es regulatorio: "Lo que la ley termina haciendo es poner la confianza en el centro. Y la confianza no se declara: se acredita. Una organización que elige un proveedor con biometría y verificación de identidad robustas tiene menos fraude, menos litigios y más capacidad de crecer. Eso es un activo".

www.ecertia.com

EL NUEVO ROL DE LOS PARTNERS TI EN UN ENTORNO DE CIBERSEGURIDAD COMPARTIDA

Ante la proliferación y sofisticación de los ataques digitales, las nuevas exigencias regulatorias y la escasez de especialistas están transformando el rol de los partners tecnológicos. Por ello, las empresas chilenas están pasando de contratar servicios puntuales de ciberseguridad a buscar apoyo permanente en prevención, monitoreo y respuesta a incidentes.

Esta mayor dependencia exige definir responsabilidades. "El proveedor también tiene un rol activo en la seguridad. Debe mantener las soluciones actualizadas, detectar vulnerabilidades y responder ante incidentes. La empresa, por su parte, debe tener claro qué riesgos asume, quién accede a sus sistemas y qué responsabilidades corresponden a cada actor", señala al respecto la gerenta general de ACTI, Luz María García.

Coincide la managing director cybersecurity de Accenture

Las amenazas digitales, la IA y las nuevas exigencias regulatorias impulsan una relación más estrecha entre empresas y proveedores tecnológicos. La colaboración permanente y la gestión de riesgos entre ambas partes se vuelven fundamentales.

Chile, María Luisa Acuña, mientras advierte que la IA está permitiendo a los atacantes reducir de semanas a horas los tiempos de ejecución de sus ataques, lo que exige una colaboración continua.

"El partner está pasando a tener una participación permanente en todo el ciclo, desde la prevención y el monitoreo hasta la detección,

respuesta y recuperación. En ese modelo, la IA permite automatizar parte de las tareas más rutinarias y acelerar la identificación de amenazas, mientras los equipos humanos se concentran en decisiones de mayor complejidad y en la gestión estratégica del riesgo", explica Acuña.

Pero externalizar también abre

vulnerabilidades. El CEO de Cybertrust, José Antonio Lagos, identifica ocho aspectos que las empresas deben evaluar al elegir y supervisar a sus proveedores: estándares de seguridad, accesos privilegiados, trazabilidad, protección de datos, respuesta ante incidentes, seguridad de subcontratistas, resiliencia operacional y una estrategia de salida que asegure la revocación de accesos y el resguardo de la información.

Para Lagos, estas medidas son

fundamentales porque delegar la operación de la seguridad no implica delegar la responsabilidad. "Externalizar ciberseguridad no significa transferir el riesgo. El proveedor puede operar controles, monitorear amenazas e incluso responder técnicamente a un incidente, pero la organización sigue siendo responsable de saber qué está protegiendo, qué riesgo está aceptando y si el tercero al que entregó acceso continúa siendo confiable", concluye.

PUBLIRREPORTAJE

LION Consulting se consolida como el partner de referencia en la capa de integración e innovación del ecosistema SAP



Con la adopción de RISE y el enfoque de clean core, todo el desarrollo que antes vivía dentro del ERP se está moviendo hacia SAP BTP. "Habilitamos capacidades de IA, convencidos de que rinden en la medida en que los datos y las integraciones estén ordenados", comenta Claudio León, director gerente.

Hoy las empresas que operan sus procesos sobre SAP tienen el desafío constante de mantener la plataforma actualizada, más aún ahora que la inteligencia artificial (IA) se está transformando en una capacidad clave para competir. A eso se suma una necesidad permanente de integrarse con otros sistemas y arquitecturas que complementan las funcionalidades de sus distintos procesos: HCM, logística, ventas, compras. Para lograrlo, las empresas necesitan el apoyo de un partner SAP que conozca el abanico completo de capacidades que provee el ecosistema y que sea capaz de llevar esos objetivos de negocio a resultados concretos, en tiempo y forma.

De ahí la relevancia de LION Consulting, una empresa boutique con más de 9 años de experiencia en proyectos de transformación digital: un equipo de arquitectos y consultores

que se diferencia por el conocimiento, la calidad y el compromiso con los requerimientos de cada cliente. "Conocemos tanto el core de SAP como la plataforma SAP BTP —hoy SAP Business AI Platform (BAIP)—, que es donde se resuelve buena parte de la innovación: integraciones, extensiones y aplicaciones móviles. Eso nos permite proponer soluciones que aprovechan lo que el cliente ya tiene, en lugar de empujar reimplementaciones completas", explica Claudio León, director gerente de LION Consulting.

Asimismo, agrega el especialista, "trabajamos con alcances acotados y medibles, con entregas en semanas y no en años, y documentamos cada configuración para que el conocimiento quede instalado en el cliente. Nuestro valor está en acompañar al negocio de principio a fin, desde la definición de la arquitectura hasta el soporte



posterior a la puesta en marcha", destaca.

Acompañamiento continuo

Ahora, su proyección es consolidarse como el partner de referencia en la capa de integración e innovación del ecosistema SAP. Y es que, con la adopción de RISE y el enfoque de clean core,

todo el desarrollo que antes vivía dentro del ERP se está moviendo hacia SAP BTP, y ahí la firma seguirá creciendo. "Sobre esa base, estamos habilitando capacidades de IA en los ambientes SAP de nuestros clientes, convencidos de que rinden en la medida en que los datos y las integraciones estén ordenados. En esa línea, tenemos considerado crecer como empresa en los próximos meses, incorporando una mayor cantidad de especialistas a medida que se sumen nuevos clientes, para sostener la calidad de nuestros servicios", afirma Claudio León.

Por último, la firma avanza hacia un modelo de acompañamiento continuo, con equipos que conocen la solución del cliente y lo apoyan de forma permanente, dentro y fuera de Chile. Parte de ese camino lo compartirá en el próximo encuentro de ASUG Chile, en octubre, donde estará presentes para conversar con la comunidad SAP.

<https://www.lionconsulting.cl/>
<https://www.linkedin.com/in/claudioleon/>
<https://asug.cl/>