DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
VIERNES 31 DE MARZO DE 2023



# LAS CIBERAMENAZAS A LAS QUE HAY QUE PONER ATENCIÓN EN 2023

**Con el aumento de las personas y empresas conectadas a Internet, se incrementan los ciberriesgos y, con ello, la necesidad de redoblar los esfuerzos para afrontar ataques cada vez más especializados.** POR FRANCISCA ORELLANA

El último informe semestral de las amenazas del laboratorio de inteligencia de datos FortiGuard Labs de la empresa de ciberseguridad Fortinet, reveló que Chile fue víctima de 14 mil millones de intentos de ciberataques en 2022. La cifra representó un incremento de 50% en relación a 2021, y no es la única alerta: a nivel mundial, según cifras de la plataforma de seguridad CVE Details, en 2022 los fabricantes de productos reportaron 25.226 nuevas vulnerabilidades, la cifra más alta desde 1999, cuando empezó la medición, y un aumento de 26,5% frente al año anterior.

"Son cada vez más las vulnerabilidades que quedan expuestas. Entre más sean, mayores posibilidades hay de que ocurran incidentes de seguridad graves, exponiéndonos a dejar el negocio fuera de operación. Esta situación no es ajena a Chile", comenta Walter Montenegro, gerente de Ciberseguridad en Cisco Chile.

La obsolescencia en las estaciones de trabajo con sistemas operativos desactualizados aumenta la exposición a las amenazas comprometiendo la operación, explica Montenegro. Y es que en ciberseguridad, los atacantes tienen ventaja: "Solo necesitan encontrar un punto débil en una organización. Los atacantes tienen menos terreno que cubrir que un defensor y pueden adaptarse más rápido que las organizaciones para defenderse", dice Claudio Ordóñez, director de Ciberseguridad de Accenture Chile.

Las tensiones geopolíticas podrían ser responsables de una mayor volatilidad para la ciberamenazas este año, añade, "con una mayor variación en los tipos de malware y phishing, así como cambios en tipo de activos o procesos de creación de valor de los ciberatacantes".

## Nuevos ataques

Hay consenso en que la mayor preocupación hoy debe estar en los ransomware, programas maliciosos que impiden a los usuarios ingresar a su sistema y archivos, para pedir un rescate por ellos.

Francisco Rodríguez, consultor en ciberseguridad de ITQ Latam, explica que ser víctima de un ataque de estas características puede dejar a la entidad sin acceder a sus recursos y afectar su operatividad.

Esto se complejiza cuando las empresas no tienen adecuados procesos de seguridad, dice Montenegro, y muchas veces no pueden hacerlo "porque sus hardware o sistemas operativos no los soportan".

Otra amenaza a la que hay que prestar atención es el BEC (Business Email Compromise), explica José Antonio Lagos, profesor Uejecutivos de la Facultad de Economía y Negocios de la U. de Chile, una amenaza diseñada para obtener información comercial crítica o extraer dinero, por medio de un correo electrónico falso suplantando a un proveedor habitual para solicitar un pago adelantado por un servicio, engañando al área de contabilidad o finanzas.

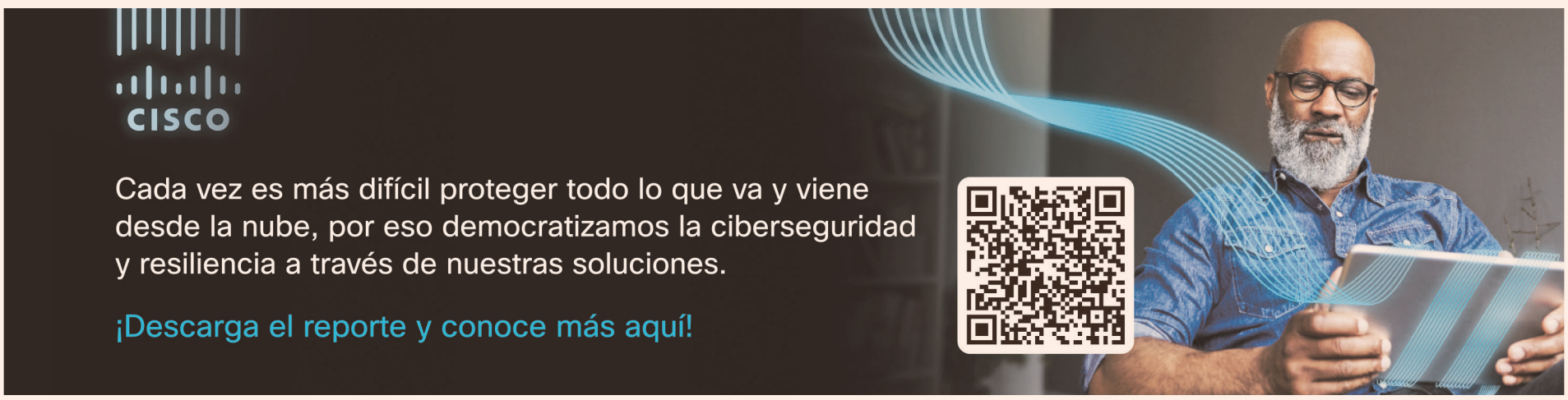
"Una organización mejor preparada puede enfrentar de forma más resiliente estos ataques. Una con menor preparación podría incluso desaparecer al no lograr restablecer sus operaciones", acota Marcelo Díaz, socio del área Cyber Risk de Deloitte.

## Adelantarse a los problemas

Lagos afirma que una de las dificultades es que la sofisticación de las amenazas avanza más rápido que la industria. Por lo mismo, ve relevante mejorar los temas técnicos y de gestión, por ejemplo, estableciendo una gobernabilidad corporativa de ciberseguridad e incorporando directores independientes expertos en el área.

Para Montenegro, es clave también sensibilizar a los usuarios de la importancia del resguardo e higiene cibernética al compartir y descargar información.

Otro reto, a juicio de Erich Zschaeck, gerente senior de Ciberseguridad de EY, es que las empresas omiten configuraciones y controles de seguridad en el diseño de los sistemas y soluciones tecnológicas: "No considerar la seguridad y la privacidad de los datos personales desde el diseño, representa uno de los mayores desafíos hoy, ya que una vez avanzado el proyecto podría ser muy difícil y costoso de corregir".



cisco SECURE

# Seguridad multicloud: protegiendo las cargas de trabajo y aplicaciones en la nube

**Entre la adopción y la maduración, las empresas en Chile siguen apostando por migrar su negocio para ganar agilidad, dinamismo, mayor control de la operación y competitividad.**

Las empresas y organizaciones entendieron el mensaje. La nube no es moda, sino un habilitador de negocio fundamental para sostener las operaciones modernas y responder ágilmente la administración de los datos.

Sin embargo, al invertir y adoptar plataformas en cloud o multicloud hay un desafío complejo: aplicar ciberseguridad a la migración. Se habla de Zero Trust, SASE, multi-autenticación, entre otros frameworks y soluciones, pero lo cierto es que la seguridad de las empresas al interior de sus nubes sigue siendo un eslabón crítico.

"La seguridad de las aplicaciones y cargas de trabajo no es un capricho. Si bien los clientes han ido migrando a la nube en etapas -algunos de forma más acelerada y con variadas experiencias-, la seguridad de las aplicaciones en la nube se convierte en un punto crítico de control, no solo por su relación con el negocio, sino que también por el dinamismo con que se modifican éstas en pos del negocio", explica Walter Montenegro, gerente de ciberseguridad en Cisco Chile.

Según datos de Valtix, el 95% de las organizaciones dice que el multi-cloud es una prioridad estratégica en 2023, pero solo el 58% confía firmemente en que tiene la arquitectura adecuada para respaldar su seguridad en el futuro.

Otro inconveniente que se presenta en la migración al cloud, es que cada proveedor de nube ofrece sus soluciones de protección, haciendo compleja la tarea de integración a cada cliente. Cada uno funciona de manera distinta, por lo que contar con aliados como Cisco resulta crítico. "Dado que la migración a la nube es mayoritariamente multicloud, es necesario integrar la seguridad bajo una única estrategia independiente del proveedor", precisa Montenegro.

**Seguridad y visibilidad**

La seguridad robusta en la nube es clave. Sin embargo, no hay seguridad sin visibilidad. Consolidando la integración, se evitan los silos, los problemas de ineficacia y una carga operativa sustancial para los equipos de seguridad.

"La red sigue uniendo a las nubes. Tenemos la necesidad de visualizar todo el tráfico que fluye entre las aplicaciones y los usuarios. Por lo tanto, debemos usarla como soporte para realizar una seguridad consolidada y consistente por la visibilidad, la telemetría y la aplicación de políticas que ofrece", detalla Montenegro.

**Walter Montenegro, gerente de ciberseguridad en Cisco Chile.**

Es el principio, por ejemplo, de Cisco Security Cloud, una plataforma de red y seguridad global, integrada y provista en la nube para organizaciones de cualquier forma y tamaño.

"Hablamos de simplificar la seguridad de la red sin importar en qué nube se creen o consuman las aplicaciones. Con un control nativo y fácil de usar, se busca ofrecer una experiencia fluida en entornos múltiples", aclara el ejecutivo.

**On premise y cloud: lo híbrido continuará**

Hay una premisa importante: el negocio nunca estará por debajo de la seguridad. Por esa razón, la migración al cloud es compleja ya que implica trasladar distintas cargas del negocio lejos del data center.

"On premise, las organizaciones tenían un tipo de segmentación, visibilidad y control. Pero al migrar al cloud, tienen que consolidar una nueva forma de organización y protección. Es fundamental iniciar ese proceso con la seguridad como eje y en Cisco estamos preparados para crear esa estrategia", aclara Montenegro.

"En Cisco entendemos que puede ser un proceso complejo. Por eso, ofrecemos una arquitectura de ciberseguridad cloud para simplificar y mejorar la experiencia, sin descuidar plataformas on premise de trabajo. Sin duda la nube es un habilitador de negocio que potencia, agiliza, controla y visibiliza la operación, mientras entrega competitividad, predicción e inteligencia a los mercados y países", menciona Montenegro.

Una cosa es cierta: los data center no dejarán de existir. "Es plausible que vivamos en la dualidad de ambos, dependiendo de las necesidades de cada empresa", sentencia Montenegro.

Cisco cuenta con todas las herramientas necesarias para acompañar a las organizaciones en su transformación tecnológica, securitizando la migración desde el on premise hacia la nube. Integrando y optimizando sin importar la ubicación de la aplicación o la carga de trabajo, para disminuir los riesgos y seguir potenciando el negocio de sus clientes.

La seguridad es y será un eslabón clave. Ignorarla puede traer dificultades ya que los ciberataques solo irán en aumento.

# LOS NUEVOS FOCOS DE CIBERSEGURIDAD QUE SE ABREN CON EL METAVERSO

**Aunque todavía falta para que el metaverso llegue a su punto más alto de popularidad, los expertos ya vislumbran los riesgos a los cuales esta tecnología se expone y para los que las empresas ya deben prepararse.**

POR PAULINA SANTIBÁÑEZ T.

Aún el metaverso no ha llegado a su punto de masificación, ni está disponible para todas las industrias. No obstante Fabio Assolini, director del Equipo de Investigación y Análisis para América Latina en Kaspersky, visualiza que al hacerse popular seguramente será aprovechado por diversos cibercriminales.

Para Luis Dujovne, director de Transformación Digital de BBK+-2Brains, este hecho se explica porque los ciberataques son actos de ingeniería social, que engañan y perjudican a la gente. Y dado a que el metaverso tiene un componente social, como avatares y representación virtual humana, "una persona se ve aún más expuesta, ya que alguien podría suplantar su identidad de forma virtual", dice Dujovne.

Y es que el metaverso es una plataforma vasta de posibilidades, por lo que inspeccionarla en detalle es complejo, dice Claudio Ordóñez, director de Ciberseguridad de Accenture Chile.

En este sentido, son varias las industrias que podrían ser afectadas utilizando el metaverso. Para Dujovne, hay dos áreas que deben tener especial cuidado: primero, las industrias que puedan tener información personal de los usuarios y que esa información sea relevante, como datos bancarios o de salud. Y la segunda corresponde a las empresas "donde se realicen transacciones, por ejemplo la industria de juegos".

## Las oportunidades

Pese a ello, el metaverso es una puerta de entrada para nuevas oportunidades de negocio, incluso para la ciberseguridad, ya que la protección de este espacio desde su diseño debe "centrarse en reforzar la infraestructura y el software frente a nuevas amenazas, en particular la ciberdelincuencia, el fraude y la desinformación", dice Ordóñez, impulsando con ello a las empresas a utilizar modelos de seguridad como Zero Trust adaptable.

En ese sentido, Dujovne destaca los diversos servicios que pueden nacer de estos modelos, con herramientas que abren espacios a la educación de los usuarios finales para identificar amenazas, añadiendo servicios de consultoría sobre cómo evitar fraudes en los canales que se manejan en el metaverso. "Existirá una gran oportunidad en la industria de softwares de seguridad", asevera.

Por otra parte, Fabio Assolini destaca la presencia de la web 3.0 como la base del metaverso, siendo una nueva iteración teórica basada en blockchain de la web. Esta, al ser más segura, "permitiría a los usuarios publicar contenido de medios ricos a una audiencia global y hacer que el metaverso sea más comercialmente viable".

GRUPO DF
DF · DFLIVE · DEMAS · FD · BAZARED

**Director:** José Tomás Santa María / **Subdirectora:** Teresa Espinoza / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo
**Coordinadora:** Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, piso 10, Las Condes, Fono: 23391000 / e-mail: buzondf@df.cl / **Impreso por** COPESA IMPRESORES S.A., que sólo actúa como impresor.
Se prohíbe la reproducción total o parcial de los contenidos de la publicación.

Vuelve a estudiar
para ir más adelante

DIPLOMADOS
UEJECUTIVOS
Universidad de Chile

ADMISIÓN
2023

FACULTAD ECONOMÍA Y NEGOCIOS
UNIVERSIDAD DE CHILE

ÁREA SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN


- Ciberseguridad
  *Inicio:* ***06 de junio***
- Estrategia y Planificación de Proyectos Informáticos
  *Inicio:* ***12 de junio***

Universidad de Chile U EJECUTIVOS DIPLOMADOS

AACSB ACCREDITED

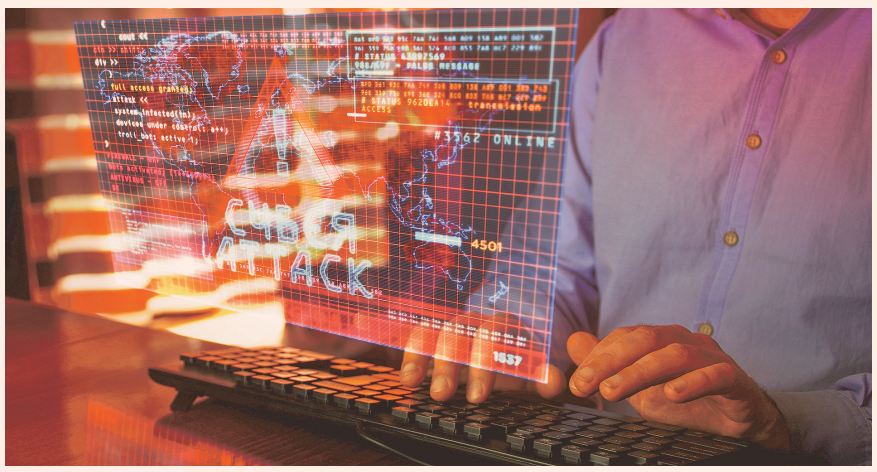
*Matricúlate anticipadamente y accede a descuentos especiales con rebaja de arancel*

+562 2 9783565 contacto@uejecutivos.cl uejecutivos.cl

PUBLIRREPORTAJE

# Automatizar la seguridad frente a las ciber amenazas es hoy un elemento crucial para resguardar la información y operación de las empresas

**Las nuevas amenazas son cada vez más accesibles de ejecutar y más complicadas de resolver para responder a la velocidad y capacidad de sistematizar y automatizar ataques con enorme impacto para las organizaciones.**




De acuerdo al tercer reporte de Ciberseguridad de Entel Ocean, Chile fue el séptimo país de Latam con más ciberataques en 2022 y para este año se espera que los riesgos y amenazas sigan en aumento, siendo el phishing, ransomware, data leak y databreach los ciberdelitos que más se pronostican.

Si el escenario es claro y las alarmas ya se han levantado, ¿cómo estar realmente preparados ante el aumento de las amenazas y la evolución constante de las acciones de la ciberdelincuencia? Según la consultora Internacional Gartner, para 2025 el 50% de las organizaciones utilizará los servicios de Managed Detection and Response (MDR) para las funciones de monitoreo, detección y respuesta de amenazas, mientras que un 60% de las soluciones EDR incluirán datos de múltiples fuentes de seguridad, como identidad, CASB y DLP.

Estas nuevas herramientas presentan enormes ventajas para el manejo de seguridad de las empresas, como son acelerar y mejorar la respuesta a Incidentes, obtener mayor visibilidad y control sobre todos los eventos de seguridad, visibilizar métricas vitales en tiempo real, en tareas complejas apoyar la intervención humana de remediación y automatizar el control de falsas alertas.

Anticipándose a esa realidad, Entel Ocean selló, a fines de 2022, una importante alianza con Palo Alto Networks –líder mundial en ciberseguridad- y hoy es la única empresa chilena certificada con especialización en Detección y Respuesta Extendida (XMDR) para la gestión de ciber amenazas con capacidades para brindar soporte local.

Cyril Delaere, Gerente de Ciberseguridad & Cloud de Entel Ocean, asegura que "administrar las amenazas de seguridad en entornos híbridos de manera efectiva es altamente complejo. Es aquí donde toma importancia que las organizaciones cuenten con servicios de detección y respuesta gestionada (XMDR), un servicio que es aplicable en todo tipo de organizaciones, éste adquiere aún más relevancia en organizaciones con requerimientos de seguridad complejos, como lo es el cumplimiento normativo".

Este servicio avanzado permitirá otorgar un enfoque más maduro y holístico para la gestión de amenazas de carácter proactivo, reduciendo los tiempos de detección y respuesta de días a horas, y en particular para enfrentar Incidentes de ciberseguridad (IR).

# "CIBERCRIMEN COMO SERVICIO", EL NUEVO MODELO DE NEGOCIO DE LOS DELINCUENTES DIGITALES

**La ciberdelincuencia es rentable. Y para probarlo, estos criminales están ofreciendo sus servicios a atacantes que ya no necesitan tener conocimientos técnicos, por lo que hoy las amenazas para las organizaciones se multiplican.**

**POR PAULINA SANTIBÁÑEZ T.**

Al igual que la industria de la ciberseguridad ha crecido, entregando nuevos y mejores servicios de protección, el sector delictual está avanzando no solo en sofisticación, sino hacia un modelo económico de entrega de servicios de cibercrimen.

Según el reporte Amenazas 2023 de Sophos, el año pasado este modelo "como servicio" se expandió para abarcar casi todas las herramientas de la ciberdelincuencia, en un mercado clandestino que incluso publica ofertas de trabajo para reclutar nuevos talentos.

Pero, ¿de qué se trata este modelo? Juan Alejandro Aguirre, senior manager Sales Engineering Latam de Sophos, explica que cuando se habla de cibercrimen como servicio (CaaS, por su sigla en inglés) se hace referencia a la transferencia de herramientas y capacidades digitales maliciosas muy sofisticadas a criminales "que no necesariamente deben tener un amplio conocimiento técnico". Es decir, cualquiera puede comprar el servicio de un ciberataque.

Entre las herramientas más conocidas, Benjamín Mera, director de CronUp Ciberseguridad, destaca la distribución de malware, ataques de denegación de servicio (DDoS) y phishing, entre otras. El modelo de negocio se puede dividir en cinco componentes: adquisición de datos, análisis de datos, extracción de datos, venta de datos y blanqueo de dinero.

A ojos de Camilo Sepúlveda, subgerente de Seguridad Operativa de NovaRed, con la existencia de CaaS ha aumentado el riesgo inherente hacia las corporaciones, gracias a la facilidad de tener estas herramientas. Por ello, "contemplar sistemas de detección y prevención se vuelve de suma importancia".

Esto principalmente porque el CaaS ya no se asocia solo a una persona, sino a mafias de crimen organizado cibernético, dice Mera. Y es que lamentablemente es considerado un negocio rentable, "tanto así que se ha advertido que los costos globales anuales asociados a estas bandas aumentarán un 15% por año durante los próximos cinco años, llegando a los US$10,5 billones (millones de millones) anuales", añade.

Con esta realidad, Sepúlveda destaca claves indispensables de protección, como tener "un equipo que realice actividad de Threat Intelligence" y que tenga como foco la notificación temprana de amenazas latentes.

No obstante, para Aguirre, contar con estos equipos es también un desafío para la industria: "Si bien existe una oferta amplia de tecnologías con capacidades de detección y respuesta, los recursos humanos para operar estas tecnologías son escasos y costosos".


PUBLIRREPORTAJE

MÁS DE 13 AÑOS DE TRAYECTORIA EN EL MERCADO DE CIBERSEGURIDAD:

## GlobalSecure amplía sus servicios de respuesta ante incidentes y ataques de Ransomware en países de Latinoamérica

**Esta empresa ha participado en la respuesta frente a los incidentes de ciberseguridad más importantes que ha tenido el país, incluyendo ataques en la banca y compañías multinacionales tanto en Chile como en el extranjero. En eventos de esta naturaleza, la experiencia del equipo de GlobalSecure es clave, porque les permite a sus clientes tomar decisiones rápidas para restaurar las operaciones en el menor tiempo posible.**

Los últimos 3 años han sido intensos para GlobalSecure, pues los ataques de Ransomware se han vuelto cada día más frecuentes y traspasan todas las medidas de seguridad de las compañías. "Hemos visto unos 30 casos los últimos 3 años, casi 1 por mes, y se nota cómo han evolucionado los atacantes. También ha ocurrido que empresas que no evalúan lo que pasó o cómo se efectuó el ataque, vuelven a ser vulneradas. En ese aspecto, es clave el análisis forense que se hace posterior a restaurar la operación de la compañía", señala Manuel Moreno, CEO y fundador de GlobalSecure.

**De izquierda a derecha: Manuel Moreno (CEO); Jaime Munita (Team Leader SOC); a rostro cubierto, consultor (Senior Red-Team); y Francisco Maureira (Team Leader Cyber- Security & DFIR), los cuatro de GlobalSecure.**

Los procesos de respuesta ante incidentes de GlobalSecure, están diseñados para que un equipo de elite con amplia experiencia en ataques avanzados, pueda llegar apenas se detecta el ataque para poder neutralizarlo, obtener inteligencia de quienes lo están realizando e implementar acciones dirigidas a este grupo.

"Ser atacado por un Ransomware es como tener una enfermedad grave como un cáncer", asevera el ejecutivo. Esto, porque la respuesta requiere de un equipo altamente especializado, multidisciplinario y con mucha experiencia para poder tomar las decisiones correctas en el momento correcto.

Manuel Moreno complementa: "No es lo mismo responder a un incidente a horas de sucedido, que responderlo en 24 horas y menos aún en 48 horas. Hay evidencia clave del ataque que se pierde, porque las áreas de informática de las empresas normalmente no saben cómo reaccionar y apagan o reinician servidores".

https://www.globalsecure.cl

PUBLIRREPORTAJE

FORTINET:

# Ciberseguridad de clase mundial para enfrentar un entorno digital cada vez más desafiante

**La evolución de la industria 4.0 a su siguiente nivel 5.0, abre inmensas posibilidades de progreso, pero a la vez, supone un crecimiento en la superficie de red y posibles nuevos escenarios para ciberataques. Ante esto, Fortinet ha desarrollado un modelo hiper especializado y segmentado, para que su ecosistema de partners cuente con las herramientas necesarias para responder a las necesidades de sus clientes, en función a sus desafíos, nivel de madurez digital o entornos híbridos de trabajo, entre otros. En este sentido, uno de sus partners más destacados es SONDA.**

La acelerada transformación digital plantea nuevos desafíos de cara a la surgente industria 5.0. En dicho escenario, la ciberseguridad se convierte en uno de los mayores desafíos, considerando que la digitalización inevitablemente implica un crecimiento en la superficie de red y, por ende, de las vulnerabilidades. “Hoy la postura de seguridad de la organización, más que nunca, forma parte de sus elementos diferenciadores y es claramente una ventaja competitiva en cualquier mercado en donde ésta se desenvuelva”, señala Jackeline Sulbaran, Gerente de Canales Fortinet Chile, la compañía líder global de ciberseguridad impulsando la convergencia entre redes y seguridad.

La ciberseguridad de los datos y plataformas han pasado a ser capacidades habilitantes fundamentales para la continuidad operativa y éxito de los procesos de empresas y organizaciones, y en dicha condición, deben ser capaces de acompañar la evolución del negocio.

Una tarea desafiante, dado que las ciberamenazas son cada vez más sofisticadas. Jackeline Sulbaran profundiza: “Los principales retos derivan de la extensión de superficie de red, los modelos ‘trabaje donde sea’, la migración de cargas de trabajo a la nube, la convergencia entre redes IT/OT, tendencias como ‘traiga su propio dispositivo’ y el uso de IoT e IIoT, entre otros. Por eso en Fortinet enfatizamos la importancia de contar con una arquitectura de ciberseguridad sólida y resiliente que abarque de forma integral desde puntos de acceso hasta hardware, software y aplicaciones”.

**Jackeline Sulbaran, Gerente de Canales Fortinet Chile.**

En ese contexto, las arquitecturas de ciberseguridad están evolucionando hacia plataformas integradas que permitan reducir la complejidad versus el uso de herramientas aisladas, debido a que “existe una escasez importante en cuanto a talento con habilidades de seguridad, por lo que se ha vuelto necesario contar con herramientas que simplifiquen la gestión”, observa la ejecutiva.

Con toda su experiencia y conocimiento, Fortinet registra variados casos de éxito junto a sus partners; entre ellos, su alianza con SONDA, compañía líder en transformación digital en Latinoamérica, que junto a Fortinet, han diseñado un ecosistema de ciberseguridad personalizado, escalable, automatizado y a la medida de cada cliente potencial.

“Para Fortinet, SONDA es un claro ejemplo de un partner referente con foco integral en soluciones de ciberseguridad para el mercado, desarrollando en conjunto una relación integrada de trabajo que ha producido buenos resultados, donde SONDA ha contribuido al posicionamiento de nuestra compañía en segmentos como el Retail, Industrial y el sector público”, señala Jackeline Sulbaran.


Cuenta con **Soluciones de Ciberseguridad Integral** para la protección de tu empresa y el respaldo del líder en transformación digital de la región.

Conoce más en
sonda.com

SONDA make it easy | FORTINET

# LAS CLAVES PARA EL AVANCE DEL ENFOQUE ZERO TRUST

**Invertir en educación en ciberseguridad para que los trabajadores estén capacitados y comprendan el enfoque Zero Trust. Ese será uno de los desafíos que las empresas chilenas deberán enfrentar para implementar estrategias maduras de confianza cero en los próximos años.**

POR ANDREA CAMPILLAY

Como una de las consecuencias de la pandemia, la aceleración de la transformación digital ha llevado a las organizaciones a buscar nuevas estrategias para protegerse de posibles ataques cibernéticos que puedan vulnerar sus centros de datos y sistemas informáticos.

En ese contexto, ha proliferado la utilización de metodologías de Zero Trust. "El porcentaje de empresas a nivel mundial con una iniciativa definida de este tipo, pasó del 24% en 2021 al 55% en 2022, lo cual fue un aumento considerable de más del doble", asevera Carlos Bustos, presidente de la Mesa de Ciberseguridad de ACTI y director corporativo de Servicios de Ciberseguridad en Sonda.

El porqué lo están prefiriendo las organizaciones tiene un motivo principal: este enfoque apunta a desconfiar de todo. Esto significa "ya no confiar en que alguien conoce una contraseña o tiene algo (como un token) y por eso puede acceder a todos los recursos. O que si alguien inicia sesión en un determinado lugar, por ejemplo, desde la oficina, puede tener acceso a toda la red", explica Nicolás Corrado, socio líder de Cyber Risk en Deloitte, quien afirma que este enfoque derriba el antiguo concepto de un castillo que tiene las murallas como perímetro y un lago alrededor para proteger el reino de TI.

A nivel nacional, el grado de implementación de enfoque ha ido creciendo paulatinamente, con algunas organizaciones que comienzan a interesarse y otras que ya están alineando sus estrategias bajo esta nueva mirada.

"Como consecuencia de la pandemia y el trabajo remoto, se han acelerado algunos puntos específicos como la microsegmentación y la autenticación multifactorial. Esto ha llevado a considerar con mucha fuerza el monitoreo de registros de usuarios, aplicando tecnologías que permitan detectar comportamiento de usuario, como el UBA (User Behavior Analytics)", comenta Camilo Sepúlveda, subgerente de Seguridad Operativa de NovaRed, añadiendo que las empresas locales han invertido de forma muy potente en puntos de gestión de accesos privilegiados (PAM, por su sigla en inglés), con el objetivo de aplicar un control adaptativo y de mínimos privilegios para todos los accesos y, de esta forma, acelerar el cambio a una estrategia Zero Trust.

### Proyecciones

Los analistas de Gartner predicen que para 2026, el 10% de las grandes empresas a nivel global tendrá un programa de confianza cero maduro y medible. Sin embargo, a nivel local aún queda camino por recorrer, pues los expertos coinciden en que se requiere una mayor conciencia sobre la importancia de la seguridad cibernética y la necesidad de implementar medidas de Zero Trust en las empresas. "Para lograr una implementación efectiva, las empresas deben asegurarse de contar con los recursos humanos y técnicos adecuados, además de implementar procesos claros y transparentes. De esta manera, podrán mejorar la seguridad y proteger sus activos digitales", puntualiza Eder Morán, docente de la carrera de Ingeniería en Ciberseguridad de AIEP.

**"Este concepto permitirá reducir la materialización de las amenazas, por lo que no comenzar a caminar este viaje, hará que los activos tecnológicos de la organización estén más expuestos ante los ciberriesgos", dice Nicolás Corrado, de Deloitte.**

Asimismo, la implementación de este modelo presenta retos a nivel de personas. "El principal desafío es educar al capital humano de las organizaciones en temas relacionados a la ciberseguridad", señala Sepúlveda, quien también destaca la brecha existente entre las áreas de seguridad corporativa y el concepto de "Bring your own device", en el sentido de que sean reconocidos o no los dispositivos personales como una parte permanente de la infraestructura de TI de las empresas. "El no considerar esto dentro de una implementación Zero Trust y no disponer de un manejo y políticas de los dispositivos que se ingresan a los entornos corporativos, creo que es un punto que puede poner en riesgo la implementación de esta estrategia", dice.

Por su parte, Morán acota que para superar estos desafíos "es fundamental contar con una estrategia de capacitación y concientización en seguridad cibernética, que asegure que todos los empleados tengan una comprensión clara de la estrategia y cómo pueden contribuir a su implementación".

Así, los expertos coinciden en que la proliferación de esta estrategia es el paso siguiente. "Sin lugar a duda, Zero Trust es hacia donde la ciberseguridad debe ir. Estos conceptos permitirán reducir la materialización de las amenazas, por lo que no comenzar a caminar este viaje, hará que los activos tecnológicos de la organización estén más expuestos ante los ciberriesgos", concluye Corrado.

# LEY DE PROTECCIÓN DE DATOS: CÓMO IMPACTARÍA UNA AGENCIA QUE FISCALICE SU CUMPLIMIENTO

**Se trataría de un organismo descentralizado con atribuciones para fiscalizar y proteger a las personas para que puedan ejercer sus derechos en esta materia. Un rol que los expertos valoran y que podría ver la luz antes de fin de año.**

El proyecto de ley que regula la protección y el tratamiento de los datos personales y que, además, crea la Agencia de Protección de Datos Personales, dio un paso importante este mes al ser despachado por la comisión de Constitución de la Cámara de Diputadas y Diputados. Se trata de un hito importante en esta materia, porque la Agencia propuesta sería un organismo descentralizado con atribuciones para fiscalizar el cumplimiento de la ley y emitir instrucciones para imponer las sanciones que la norma indica.

El tema, sin embargo, ha sido tramitado por cinco años sin ver luz verde. Y, si bien hay una ley vigente, "carece de la actualización suficiente para cumplir con los estándares internacionales", dice Carolina Cabrera, Legal Lead de Accenture Chile. Pese a ello, la ejecutiva valora la creación de una autoridad especialista en materia de datos, ya que está destinada a resolver conflictos, fiscalizar, determinar medidas mitigatorias, entre otros temas.

La extensa discusión que se ha dado en la Cámara ha permitido perfeccionar y esclarecer varios puntos del proyecto, como los límites máximos de las multas en caso de contravención a la legislación, y se perfeccionó la regulación relativa a los modelos de cumplimiento y la figura del delegado de protección de datos personales. Además, se definió el plazo para su entrada en vigencia una vez que el proyecto se convierta en ley.

Desde el punto de vista de los titulares de datos personales, Felipe Fernández, socio adjunto de Servicios Legales (Law) de EY, cree que contar con una Agencia de Datos Personales permitirá ejercer derechos sin tener que soportar la carga -tanto en tiempo como dinero- que supone tener que litigar ante tribunales ordinarios en el evento en que estos derechos puedan ser afectados.

"Contar con una autoridad con facultades para fiscalizar y potencialmente sancionar infracciones a la nueva normativa, les permitirá a los titulares de datos contar con una mejor protección, lo que requerirá necesariamente que entidades tanto públicas como privadas adecúen procesos y sistemas para poder responder requerimientos de los titulares como de la propia autoridad", opina.

## Más inversión

A juicio de Thierry de Saint Pierre, presidente de la Asociación Chilena de Empresas de Tecnologías de Información (ACTI), el proyecto es suficientemente flexible para que se siga desarrollando la economía digital en torno a los datos. "Chile podría llegar al nivel de adecuada protección de datos permitiendo que empresas europeas puedan instalarse o transferir datos al país", subraya.

El proyecto ahora será discutido por la comisión de Hacienda de esta instancia, para efectos de revisión presupuestaria. Cuenta con suma urgencia para su tramitación, lo que se traduce en que la revisión no debiera tomar más de 15 días. Con todo, Fernández concluye que "es altamente probable que el proyecto finalmente se convierta en ley durante este año".

COLUMNA DE OPINIÓN

# Urgencia de un frente común para enfrentar ciberataques

**Marcelo Pino Pérez**
**Vicepresidente de Asuntos Corporativos y Comunicaciones Huawei Latam y Caribe**

Los ciberataques se siguen incrementando y hoy representan una gran amenaza a la seguridad de la infraestructura en Chile, tanto del sector público como del privado. Los hackers pueden venir de cualquier lugar, dentro o fuera del país, y sus objetivos pueden variar: algunos están detrás de data sensible almacenada por servicios gubernamentales o información clasificada de industrias, mientras que otros se enfocan en los datos de los clientes para vender la información. Incluso, hay hackers que simplemente quieren causar caos, interrumpiendo el comercio y la vida cotidiana de las personas.

En vista de que los ataques son transversales y que todos los organismos internacionales advierten que aumentarán a medida que la digitalización avance, es urgente establecer un trabajo coordinado y compartido entre gobierno, industria, ciudadanos y academia, formando un verdadero ecosistema de ciberseguridad, donde cada actor tenga responsabilidades que consoliden este frente común. La experiencia de otros países demuestra que, si bien esta fórmula no es infalible, hasta ahora es la mejor alternativa en materias de ciberseguridad.

*"Es urgente establecer un verdadero ecosistema de ciberseguridad, donde cada actor tenga responsabilidades que consoliden este frente común. La experiencia de otros países demuestra que, hasta ahora, es la mejor alternativa contra el cibercrimen".*

Los gobiernos de Latinoamérica están entendiendo la necesidad de legislar y generar reglamentos, junto con preparar y disponer de policías especializadas en ciberataques de todo tipo. Pero lo anterior no es suficiente, los ciudadanos debemos conocer las leyes, aplicar las mejores prácticas de autocuidado y exigir altos estándares de seguridad a nuestros proveedores de servicios y fabricantes de tecnología. La academia, en tanto, no solo puede aportar con estudios y sugerencias luego de analizar experiencias de otras latitudes, sino también debe sumarse a este esfuerzo común preparando profesionales y técnicos con conocimientos actualizados en materias de delitos digitales.

La inversión en ciberseguridad, protección de datos y privacidad de la información de manera particular, se debilita si no está acompañada por un entorno que trabaja en conjunto por el mismo objetivo.