DF
DIARIO FINANCIERO®
SANTIAGO DE CHILE /
JUEVES 2 DE OCTUBRE DE 2025
df.cl

EDICIÓN ESPECIAL

MES DE LA CIBERSEGURIDAD

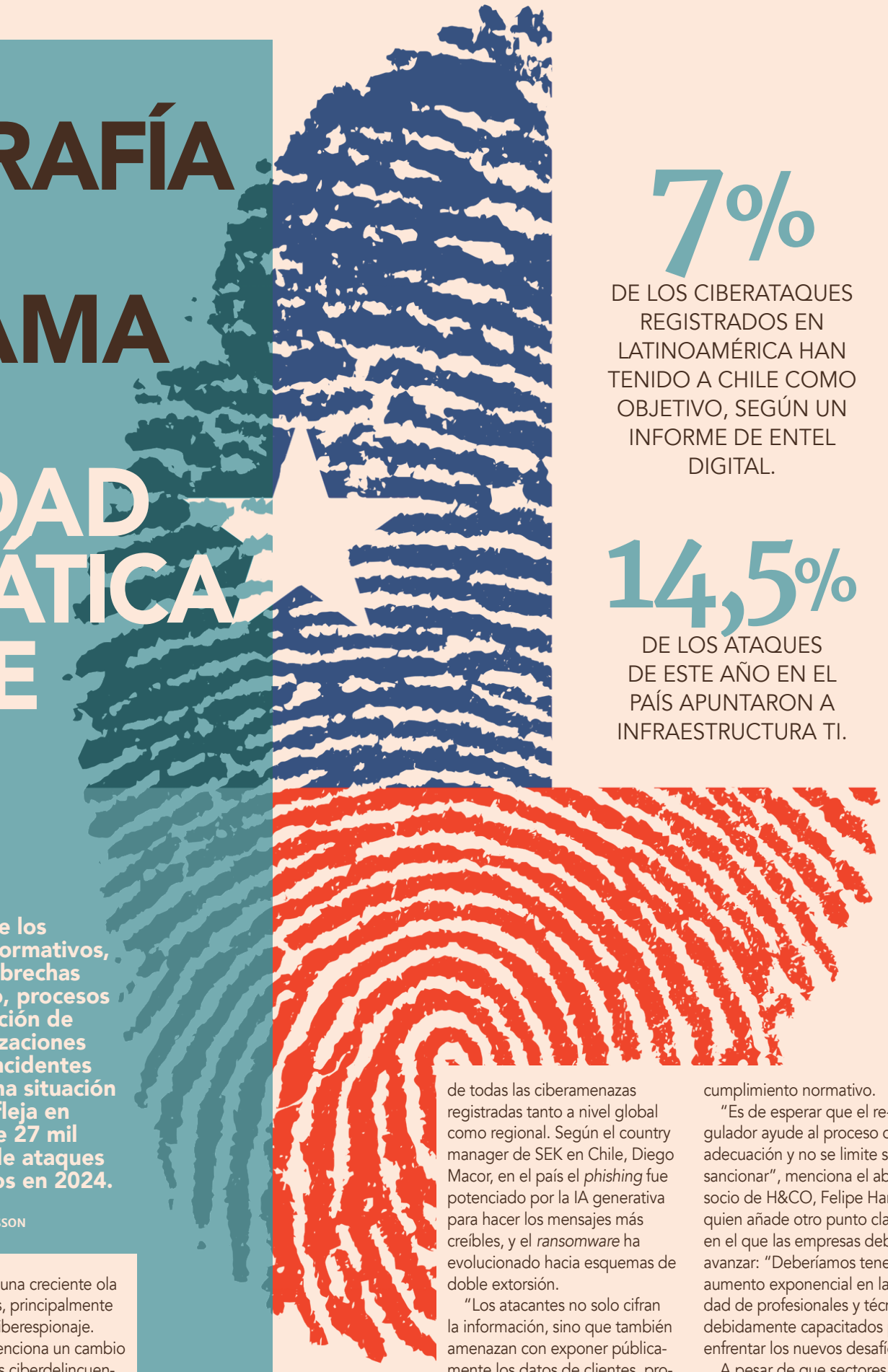
Lo que viene para los Operadores de Importancia Vital definidos por la ANCI
PÁG. 06

¿Qué tan preparados están los aeropuertos ante un ataque cibernético?
PÁG. 10

Los riesgos que trae el uso de la IA para la protección de datos
PÁG. 08

Aumentar la conciencia en la ciudadanía sobre la importancia de la seguridad digital e impulsar la educación sobre las medidas clave que tanto las personas como las organizaciones deben tomar es el objetivo del Mes de la Ciberseguridad, hito que se conmemora en octubre y que Chile celebra desde 2018. Aquí, una mirada a los desafíos y avances del país para enfrentar estas amenazas.

RADIOGRAFÍA AL PANORAMA DE LA SEGURIDAD INFORMÁTICA EN CHILE



7%

DE LOS CIBERATAQUES REGISTRADOS EN LATINOAMÉRICA HAN TENIDO A CHILE COMO OBJETIVO, SEGÚN UN INFORME DE ENTEL DIGITAL.

14,5%

DE LOS ATAQUES DE ESTE AÑO EN EL PAÍS APUNTARON A INFRAESTRUCTURA TI.

A pesar de los avances normativos, persisten brechas en talento, procesos y preparación de las organizaciones frente a incidentes graves, una situación que se refleja en los más de 27 mil intentos de ataques registrados en 2024.

POR ANAÍS PERSSON

Chile fue el primer país de Latinoamérica en instaurar octubre como el mes de concientización en ciberseguridad. Hoy, el país enfrenta un escenario complejo: los intentos de ciberataques pasaron de 6 mil millones en 2023 a 27.600 millones en 2024, según Fortinet, y durante la primera mitad de 2025 ya se registraron 4,2 mil millones de incidentes.

Este aumento se explica, en gran parte, por el uso creciente de inteligencia artificial (IA) y automatización por parte de los cibercriminales. Según el Reporte de Ciberseguridad 2025 de Entel Digital, Latinoamérica concentró el 25% de las detecciones globales, impulsada por un mercado de ciberdelito como servicio que comercializa credenciales, *exploits* y accesos en la *dark web*.

El panorama nacional refleja avances significativos, como la puesta en marcha de la Ley 21.663, que busca estructurar y fortalecer la seguridad digital en el país. No obstante, también hay desafíos persistentes. Chile se situó como el cuarto país más afectado de Latinoamérica, concentrando un 7% de los ataques regionales.

Según el director del Centro de Ciberinteligencia (CCI) de Entel Digital, Eduardo Bouillet, los sectores económicos clave de Chile enfrentan una creciente ola de ciberataques, principalmente *ransomware* y ciberespionaje.

El experto menciona un cambio en el foco de los ciberdelincuentes dentro del país: "En 2024, los sectores más golpeados fueron infraestructura de TI (21% de los incidentes) y banca y finanzas (17%). Para lo que va de 2025, si bien infraestructura de TI sigue liderando con un 14,5%, la amenaza se ha diversificado. Ahora, los sectores de transporte (8,6%) y manufactura (8,1%) figuran entre los más atacados, mientras que banca y finanzas representa un 5,3% de los casos".

Principales amenazas

Según Bouillet, el panorama regional es caracterizado por una creciente sofisticación, la automatización impulsada por IA y un cambio geopolítico clave "que indica que Latinoamérica ha dejado de ser un 'teatro secundario' para convertirse en un 'escenario principal de ciberespionaje'".

Los vectores de ataque más comunes en 2025 fueron la explotación de accesos remotos (38,5%) y vulnerabilidades no parcheadas (36%), con un 80% de estas últimas clasificadas como críticas en sistemas de control industrial. Además, el CCI de Entel Digital reporta un aumento del 23,2% en amenazas persistentes avanzadas (APT), con 85 grupos identificados, muchos apuntando a la infraestructura crítica de Latinoamérica, incluyendo Chile.

El *ransomware* fue la principal amenaza, representando el 38% de todas las ciberamenazas registradas tanto a nivel global como regional. Según el country manager de SEK en Chile, Diego Macor, en el país el *phishing* fue potenciado por la IA generativa para hacer los mensajes más creíbles, y el *ransomware* ha evolucionado hacia esquemas de doble extorsión.

"Los atacantes no solo cifran la información, sino que también amenazan con exponer públicamente los datos de clientes, proveedores o socios de la empresa víctima, buscando que sean estos mismos quienes presionen a la organización para pagar el rescate", señala Macor.

Avances y desafíos

Chile ha dado pasos importantes para proteger su infraestructura digital. La Ley Marco de Ciberseguridad, promulgada en abril de 2024, consolidó al país como el primero en Latinoamérica en adoptar esta iniciativa y estableció un marco regulatorio que protege las infraestructuras críticas de la información. Además, creó la Agencia Nacional de Ciberseguridad, encargada de coordinar políticas y supervisar el cumplimiento normativo.

"Es de esperar que el regulador ayude al proceso de adecuación y no se limite solo a sancionar", menciona el abogado socio de H&CO, Felipe Harboe, quien añade otro punto clave en el que las empresas deberían avanzar: "Deberíamos tener un aumento exponencial en la cantidad de profesionales y técnicos, debidamente capacitados para enfrentar los nuevos desafíos".

A pesar de que sectores regulados como la banca, la energía o las telecomunicaciones han mostrado grandes avances, Macor apunta a que la preparación promedio de las empresas y entidades del Estado en Chile frente a incidentes graves "es todavía heterogénea".

"Las mayores brechas no están en adquirir más tecnología, sino en personas y procesos: existen roles críticos sin cubrir, entrenamiento insuficiente y protocolos que rara vez se prueban en escenarios reales. En tecnología, el reto no es solo comprar herramientas *world-class*, sino usarlas plenamente, con recursos y competencias adecuadas", concluye el ejecutivo.

PUBLIRREPORTAJE

Ciberseguridad: ¿Tecnología o Conocimiento con Buenas Prácticas?

Una gestión adecuada de ciberseguridad conlleva Implementación para sacar el máximo provecho de la tecnología, el máximo ROI, desde el primer momento, considerando sus actualizaciones y mejoras. "También implica Operación con Visibilidad, Control y Reportería, con acciones de servicio predefinidas; y cumplimiento normativo, tanto interno como externo", señala Pedro Oyarzún Recabarren, CEO de Egs-Latam.

Durante años, la narrativa dominante en la industria ha sido que la seguridad digital depende casi exclusivamente de la tecnología. Las marcas líderes han invertido millones en posicionar sus softwares y soluciones como el "escudo definitivo". Sin embargo, los datos desmienten esta hipótesis y muestran que confiar solo en la tecnología nunca ha sido suficiente.

"La verdadera brecha en ciberseguridad no está enmarcada en las herramientas, sino en el conocimiento que se debe tener para administrarla y la capacidad de implementar buenas prácticas en el proceso", indica Pedro Oyarzún Recabarren, CEO de Egs-Latam.

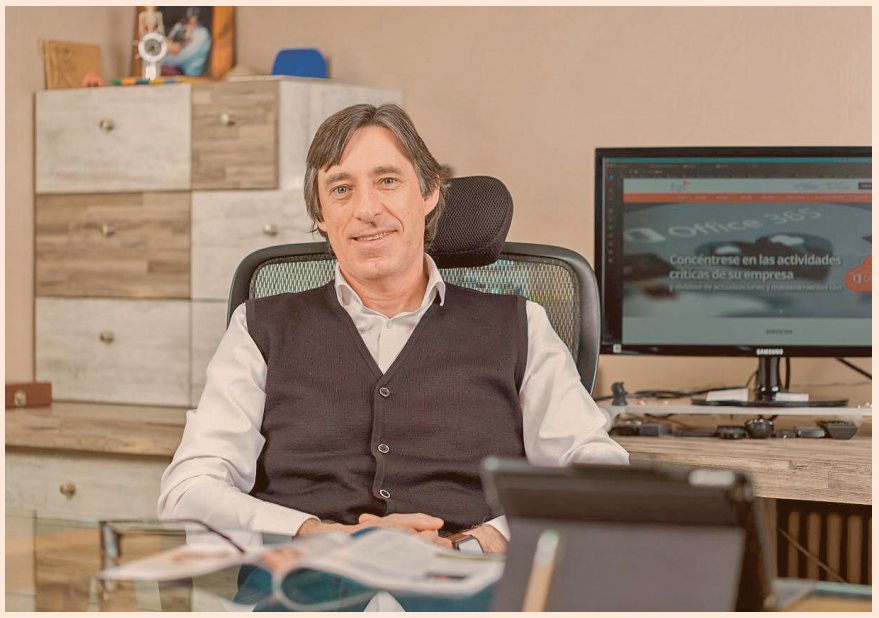
En efecto, el 90% de las organizaciones en Chile no está suficientemente preparada para defenderse de ataques informáticos, lo que se relaciona directamente con la falta de capacitación y concienciación sobre ciberseguridad. Asimismo, el 70% de los ataques en Chile afecta a Pymes, con pérdidas anuales estimadas por sobre los US$120 millones por ciberataques.

"La conclusión es clara: la falta de capacitación, el desconocimiento tecnológico y las malas prácticas de gestión son los principales puntos débiles que siguen exponiendo a las empresas", asegura el especialista.

Una visión distinta: lo básico puede cambiarlo todo

Con una vasta trayectoria, Egs-Latam hace más de 10 años que comparte la visión de los "hackers éticos" —aquellos profesionales especializados en seguridad, que buscan exponer vulnerabilidades para corregirlas y no para explotarlas— insistiendo en dos conceptos clave: Do-The-Basic y Low Hanging Fruit. El primero apunta a la importancia de hacer bien lo esencial, y el segundo recuerda que un ciberdelincuente siempre entrará por el camino más fácil.

Hoy esa mirada también la comparte La Agencia Nacional de Ciberseguridad de Chile (ANCI), delatando que esta postura puede reducir hasta en un 70% la probabilidad de incidentes graves.



"Es importante contar con un Plan en el tiempo que se revise cada 3 meses (dinámico), para crear concientización y priorización con dirección, eso mejora el estado del arte de las empresas en la Ciberseguridad", precisa Pedro Oyarzún Recabarren, CEO de Egs-Latam.

El desafío, entonces, es implementar un plan dinámico, que combine debida diligencia, presupuesto y desarrollo de competencias, para elevar progresivamente el estado del arte de la ciberseguridad en la organización.

www.egs-latam.com

LA CIBERSEGURIDAD SE TOMA LA AGENDA DE OCTUBRE

JUEVES 02

08:00 Inicio del 8.8 Computer Security Conference, un evento técnico y académico que abordará los desafíos globales y cooperación transfronteriza en ciberseguridad, estrategias de defensa y técnicas de ataques emergentes.

10:35 En el marco del Summit País Digital 2025, la gerenta de marketing y producto B2B de Movistar Empresas, Annie Fernández, abordará las amenazas digitales y soluciones para pymes en ciberseguridad.

12:03 Vivien Piddo, CEO de UpSociative, realizará en el Summit País Digital la charla "La confianza es el nuevo *currency*: protección de datos como ventaja competitiva", que busca derribar el mito de que la privacidad es un gasto.

VIERNES 03

09:30 La Universidad Técnica Federico Santa María dará inicio a "Campo de Marte", una competencia de ciberseguridad donde los participantes deben resolver problemas y explotar vulnerabilidades para encontrar y "capturar" una "bandera" (un código o dato oculto) para ganar puntos.

10:45 En el marco de la competencia de la UFSM el especialista en ciberseguridad ofensiva, Lukas Gaete, dictará la charla "Cómo comenzar y mejorar en ciberseguridad ofensiva en 2025", donde mostrara qué caminos seguir, qué recursos aprovechar y cómo la inteligencia artificial puede convertirse en un gran aliado en esta materia.

MARTES 07

09:00 El SummIT Ciberseguridad, organizado por Duoc UC en la sede San Joaquín, reunirá a líderes empresariales, académicos y especialistas para compartir conocimientos y debatir en torno a los desafíos de la ciberseguridad en empresas, instituciones y analizar el rol que tienen las personas en esta materia.

MIÉRCOLES 08

8 y 9 de octubre: Se realizará la octava versión del Seminario Internacional de Ciberseguridad, organizado por la Policía de Investigaciones junto a la Universidad Técnica Federico Santa María. El evento tendrá lugar en la Escuela de Investigaciones Policiales, en la comuna de Estación Central. La temática central será la computación cuántica y su impacto en el ecosistema digital, pero también abordará ejes como: marco regulatorio para el desarrollo de tecnologías cuánticas, avances en la inteligencia artificial y machine learning, ciberdelincuencia y criptografía y ciberseguridad.

08:30 Seminario "Un Estado digital: acelerando el valor público para Chile". El evento, organizado por la Secretaría de Gobierno Digital (SGD), la Asociación Chilena de Empresas de Tecnologías de Información (ACTI), la Asociación de Empresas Chilenas de Tecnología (Chiletec), el Banco Interamericano de Desarrollo (BID), la Pontificia Universidad Católica de Chile (PUC) y la Universidad de Chile, tendrá un programa enfocado en siete ejes estratégicos: inteligencia artificial (IA), identidad digital, gobernanza de datos, plataformas digitales integradas, ciberseguridad, talento digital y compras públicas en tecnologías.

VIERNES 10

10:00 La Agencia Nacional de Ciberseguridad (ANCI) transmitirá a través de Zoom y en su canal de Youtube la charla "Controles CIS, mejorando la seguridad de las instituciones", que dará a conocer un conjunto de buenas prácticas que buscan prevenir ataques de ciberseguridad. Inscripciones disponibles en el sitio web de la ANCI.

MARTES 14

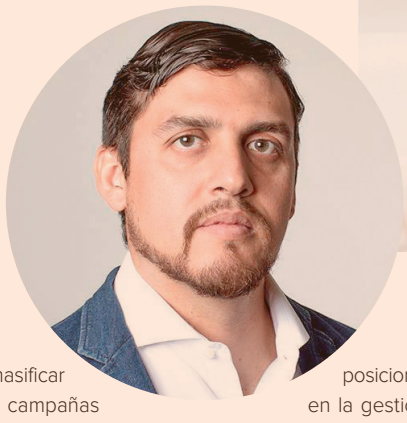
08:30 Mind The Sec Chile 2025: este evento latinoamericano de Seguridad de la Información y Ciberseguridad llega por primera vez al territorio nacional y busca reunir a líderes, especialistas y profesionales del sector en una experiencia inmersiva con enfoque en la innovación tecnológica y networking para promover el desarrollo del mercado de la ciberseguridad.

PUBLIRREPORTAJE

BSC CONSULTORES:

Ciberseguridad en Chile: desafíos, brechas y la necesidad de concientización

El 2025 ha sido un año complejo para Chile en materia de ciberseguridad. Instituciones públicas y privadas se han visto expuestas a incidentes que afectaron la continuidad de sus operaciones, desde ataques de ransomware que paralizaron servicios municipales, hasta filtraciones de datos sensibles en organismos del Estado. Estos episodios no solo generan pérdidas económicas y reputacional, sino que también exponen información de la ciudadanía.



Claudio Valdés, CEO de BSC Consultores.

Según un informe de Pronodo (julio 2025), el 56 % de las compañías chilenas víctimas de ciberextorsión han pagado rescates, con un promedio de USD 675.000 por incidente. Además, un estudio de The Clinic (enero 2025) reveló que seis de cada diez empresas han experimentado fugas de datos en los últimos dos años, con el sector financiero y las telecomunicaciones entre los más golpeados.

La realidad demuestra que ninguna organización está libre de amenazas. Los cibercriminales han perfeccionado sus métodos, utilizando desde inteligencia artificial para masificar estafas hasta sofisticadas campañas de phishing dirigidas a funcionarios.

Frente a este escenario, la prevención y la preparación son claves: concientizar a los equipos, contar con tecnologías de protección actualizadas, y realizar periódicamente análisis de riesgos y vulnerabilidades. La ciberseguridad debe ser entendida como un proceso continuo y estratégico, más que como una reacción aislada ante incidentes.

En este contexto, BSC Consultores se ha posicionado como un aliado clave en la gestión de la seguridad de la información. La empresa ofrece asesorías en la norma ISO 27001:2022, ciberseguridad, análisis de riesgos y vulnerabilidades, protección de datos personales, programas de capacitación y talleres de concientización para organizaciones públicas y privadas. Toda la información está disponible en www.bscconsultores.cl.

Para el CEO de BSC Consultores, Claudio Valdés, la clave está en las personas: "La concientización es el pilar fundamental para construir una verdadera cultura de ciberseguridad. Los empleados son la primera barrera, el primer firewall frente a las ciberamenazas. En BSC creemos firmemente que el éxito de cualquier estrategia de protección radica en capacitar y empoderar a los funcionarios en todos los niveles de la organización".

BSC Consultores refuerza así su compromiso de acompañar a las organizaciones en el camino hacia una gestión robusta, proactiva y alineada con los estándares internacionales de seguridad de la información.

PUBLIRREPORTAJE

MES DE LA CIBERSEGURIDAD 2025

“Siéntete como tu cliente” para navegar y operar con confianza

Octubre es el Mes de la Ciberseguridad y vuelve a recordarnos algo simple: hoy toda empresa depende de su conexión para vender, atender y colaborar. En Chile hemos visto incidentes recientes en organismos públicos, salud y retail que interrumpieron servicios y expusieron datos. El patrón se repite: correos de phishing cada vez más creíbles, sitios falsos que capturan credenciales, malware que cifra información y redes mal configuradas.

¿Qué escuchamos cuando nos sentamos con nuestros clientes?

“Mi equipo trabaja híbrido”, “usamos más SaaS”, “El foco debe estar en el crecimiento del negocio, no en atender incidentes puntuales”. Con esa mirada creamos Internet Seguro de Entel Empresas: una solución que agrega una capa de protección en la red para reducir la exposición a amenazas comunes y acompañar la operación diaria.

¿Cómo ayuda en la navegación segura?

- Bloqueo preventivo de dominios y enlaces maliciosas conocidos para disminuir el riesgo de phishing y descarga de malware.
- Políticas por perfiles (áreas/horarios) para ordenar el acceso y limitar superficies de ataque.
- Reportería clara y periódica sobre intentos de ataque, accesos bloqueados y el estado de la red, para tener visibilidad y poder tomar mejores decisiones.
- Actualizaciones y buenas prácticas aplicadas en la red para que el equipo no deba “ser experto”.

Carolina Riquelme – Product Owner Servicios Avanzados Fijo.

Es un complemento a soluciones como antivirus, respaldos y formación, entregando a tu equipo una experiencia de navegación más segura, simple y confiable.

En los últimos meses hemos visto titulares como “ataque masivo de phishing afectó a decenas de entidades financieras”, “filtraciones de datos de clientes en plataformas de salud” y “campañas suplantando servicios de mensajería que engañan a usuarios finales”; esos escenarios muestran lo común que son estas vulnerabilidades hoy. Internet Seguro ayuda a que esos riesgos no alcancen tu operación con la misma facilidad: filtra, alerta y acompaña.

En este mes, parte por lo esencial: contraseñas seguras, autenticación multifactor, reconocer y reportar estafas, y capacitar a tu equipo de forma constante.

La experiencia reciente nos enseña que la prevención marca la diferencia. Invertir en hábitos seguros y contar con herramientas que acompañen ese esfuerzo es la mejor forma de proteger tu operación y a quienes confían en ti.

LO QUE VIENE PARA LOS "OPERADORES DE IMPORTANCIA VITAL" DEFINIDOS POR LA AGENCIA NACIONAL DE CIBERSEGURIDAD

Especialistas advierten que, si bien contar con un listado preliminar de organizaciones entrega certezas y permite priorizar la protección de infraestructuras críticas, persisten desafíos en estándares técnicos y en la capacidad de cumplimiento de algunos sectores.

POR FRANCISCA ORELLANA

Una nómina de 1.712 empresas e instituciones públicas y privadas fueron catalogadas de forma preliminar como Operadores de Importancia Vital (OIV) por parte del Ministerio de Seguridad Pública, transformándose en entidades de relevancia esencial para la seguridad digital del país.

La Agencia Nacional de Ciberseguridad (ANCI) del ministerio analizó más de 60 mil entidades para determinar las más relevantes para la prestación de servicios y de importancia vital, donde se seleccionaron a 326 prestadores de salud, 307 empresas ligadas a generación, transmisión o distribución eléctrica, 111 instituciones financieras, 52 ligadas a telecomunicaciones y 146 organismos de administración del Estado, entre otros. "Este listado es fundamental porque le permite al país identificar a aquellos actores del sector público y privado que son esenciales para el normal funcionamiento del país y de su economía", destaca el director de la ANCI, Daniel Álvarez Valenzuela.

En la actualidad, se está en plena consulta pública y ciudadana para hacer observaciones a este primer listado, lo que es importante porque existen "altas posibilidades de falsos positivos en aquellos segmentos que no son regulados", comenta el gerente senior de Deloitte Legal, Oliver Ortiz.

El director del Centro de Ciberinteligencia (CCI) de Entel Digital, Eduardo Bouillet, agrega que la ANCI ejercerá plenamente sus facultades de fiscalización sobre estas entidades: "Los OIV quedarán sujetos a un riguroso deber de reportar incidentes de seguridad en plazos muy acotados, permitiendo una respuesta coordinada a nivel nacional. El incumplimiento de estas nuevas y exigentes normativas podrá acarrear multas, que tienen como propósito desincentivar la falta de preparación y proteger la infraestructura crítica del país".

El 30 de noviembre comenzará el segundo proceso de calificación de OIV para considerar otros sectores de la economía, dice el director de la ANCI, Daniel Álvarez Valenzuela.

Próximos pasos

El director de la ANCI dice que el 30 de noviembre comenzarán el segundo proceso de calificación de OIV, que considera otros sectores de la economía y la sociedad. "Además, debemos avanzar en la definición de estándares técnicos generales que nos permitan avanzar como país con una base común de seguridad digital", apunta, y añade que, tal como define la ley, también avanzarán en medidas diferenciadas que permitan apoyar a las pymes, por ejemplo, para adaptarse a las nuevas medidas de ciberseguridad.

Una vez que se publique el listado final, se espera que a finales de 2025 o inicios de 2026 ya entre en vigor la medida. "A partir de ese momento, se entrará en una fase de cumplimiento y fiscalización, donde estas organizaciones deben adoptar un estándar de protección digital significativamente más alto que el actual", detalla Ortiz.

Bouillet indica que, entre los puntos más importantes, las empresas calificadas deberán implementar un Sistema de Gestión de Seguridad de la Información, además de implementar planes de continuidad operacional y ciberseguridad, los cuales deben ser certificados, junto a realizar operaciones continuas de revisión, ejercicios, simulacros y análisis para detectar amenazas. Además, dice que "deberán cumplir con tiempos más acotados para el reporte de incidentes, debiendo entregar actualizaciones al CSIRT nacional en un máximo de 24 horas si el incidente afecta la prestación de sus servicios esenciales", y subraya que aquellas organizaciones que no logren adaptarse y cumplir con los estándares exigidos se enfrentarán a la posibilidad de recibir multas".

Ortiz indica que, para que todo funcione como corresponde, "persiste la necesidad de definir estándares técnicos concretos, guías de implementación prácticas para sectores con menor madurez en ciberseguridad y clarificar el proceso de revisión trienal de la lista de OIV, así como las implicancias de entrar o salir de ella".

Protección de Datos Personales: ¿Está dispuesto a exponer su empresa a multas millonarias?

Víctor Barrera, Subgerente de Ciberseguridad, junto a Carlos Norambuena, Gerente General, ambos de S&A Chile, entregan una visión estratégica y técnica respecto de los desafíos que enfrentan las empresas chilenas.

A menos de 15 meses para la entrada en vigencia de la Ley 21.719 sobre Protección de Datos Personales, conversamos con Víctor Barrera, Subgerente de Ciberseguridad, y Carlos Norambuena, Gerente General de S&A Chile, empresa integradora líder en soluciones de ciberseguridad, para entender cómo las organizaciones deben prepararse ante este nuevo marco regulatorio.

"La ley no solo protege datos de clientes, sino de toda persona vinculada a la organización", afirma Víctor Barrera.

¿Cuál es el verdadero alcance de la Ley 21.719 y por qué las empresas deben actuar ahora?

La Ley 21.719, que entra en vigencia en diciembre de 2026, establece un marco robusto para el tratamiento de datos personales. Su alcance va más allá de los clientes: incluye colaboradores, proveedores y cualquier individuo relacionado con la empresa. La normativa se basa en ocho principios clave, como seguridad, confidencialidad y trazabilidad. Las organizaciones deben comenzar hoy a identificar sus activos de datos, definir políticas de acceso y adoptar tecnologías que aseguren el cumplimiento. Postergar esta tarea puede derivar en sanciones millonarias, pérdida reputacional y riesgos operacionales.

¿Qué desafíos tecnológicos enfrentan las organizaciones?

Muchas bases de datos —especialmente aquellas con licencias gratuitas— carecen de funcionalidades nativas para cifrar, anonimizar o monitorear datos sensibles. Incluso en plataformas licenciadas, estas funciones suelen estar desactivadas por su alto consumo de recursos. En S&A Chile hemos detectado que la mayoría de las empresas aún no han asignado recursos ni definido estrategias para cerrar esta brecha tecnológica.

¿Qué soluciones recomienda S&A Chile para abordar estos desafíos?

Nuestra recomendación es IBM Guardium, una solución escalable y robusta que permite descubrir, monitorear, cifrar y anonimizar datos personales en entornos como Oracle, SQL Server, MySQL y MongoDB. Guardium opera sin afectar el rendimiento de las plataformas productivas, y se integra tanto en datacenters locales como en nubes públicas o privadas. Ofrece trazabilidad completa, aplicación de políticas de seguridad y cumplimiento normativo desde una consola centralizada.

¿Cómo ayuda IBM Guardium a cumplir con los principios de la ley?

Guardium identifica la ubicación exacta de los datos personales en archivos, servidores y estaciones de trabajo. A través de sus módulos de control de acceso, permite autorizar o denegar interacciones según las políticas definidas. Además, genera trazabilidad detallada de cada acción, facilitando auditorías y cumplimiento regulatorio. En S&A Chile hemos implementado esta solución en múltiples industrias, adaptándola a los requerimientos específicos de cada cliente.

Víctor Barrera, Subgerente de Ciberseguridad, y Carlos Norambuena, Gerente General de S&A Chile.

"La urgencia es real, y el costo de no actuar será exponencial", asegura Carlos Norambuena.

¿Qué distingue a S&A Chile como socio estratégico en este proceso?

Nuestra trayectoria de más de 35 años en el mercado, junto a una alianza estratégica con IBM que supera los 25 años, nos posiciona como líderes en ciberseguridad y cumplimiento normativo. Contamos con más de 70 profesionales TI altamente capacitados, que combinan experiencia técnica con visión estratégica. En S&A Chile no solo implementamos tecnología: diseñamos soluciones que integran seguridad, eficiencia operativa y alineación con los objetivos de negocio. Acompañamos a las empresas en su evolución digital, protegiendo lo más valioso: sus datos.

¿Cómo ha sido la adopción de esta ley por parte de sus clientes?

A nueve meses de la publicación de la ley, muchas empresas aún no dimensionan el impacto ni la urgencia. La Ley 21.719 contempla sanciones que van desde 5.000 UTM en casos leves, hasta 20.000 UTM en infracciones graves. Pero lo más crítico es que, en caso de reincidencia, las multas pueden alcanzar entre el 2% y 4% de los ingresos anuales o hasta el triple de la sanción base. Si las empresas postergan la decisión de implementar soluciones como IBM Guardium, enfrentarán dos grandes problemas: tiempos insuficientes para ejecutar proyectos y una alta demanda que elevará los costos. En este escenario, ser proactivo no es una opción, es una necesidad estratégica.

Si quieres conocer más sobre como S&A Chile junto a IBM pueden ayudar a enfrentar este gran desafío, te invitamos a escanear el QR para que te contacte uno de nuestros expertos.

LOS RIESGOS QUE TRAE EL USO DE IA PARA LA PROTECCIÓN DE DATOS

Frente a un uso cada vez más intensivo de inteligencia artificial en las empresas, expertos creen que es crucial contar con políticas que regulen la interacción de los colaboradores con estas plataformas.

POR ANDREA CAMPILLAY

Si bien los beneficios que trae el uso de la inteligencia artificial (IA) para la productividad laboral son bien conocidos en todas las industrias, su masificación trae consigo una mayor exposición y responsabilidad para la protección de información sensible en las compañías.

Un estudio realizado por WeWork y PageGroup, reveló que actualmente el 65% de los trabajadores chilenos utiliza la IA por iniciativa propia y solo un 5% asegura que cuenta con políticas y plataformas promovidas por su empleador para su uso.

A nivel regulatorio, esto abre un desafío pues "hoy, por una parte, las empresas no tienen bien definida ni delimitada la usabilidad, no están entrenando, entonces lo que están haciendo la gran mayoría de los trabajadores es que por cuenta propia están usando y poniendo datos en un universo abierto y eso trae consecuencias en materia de seguridad de datos, ciberseguridad y ética empresarial", plantea la associate director de Michael Page, Alejandra Cruzat.

El gerente regional de ciberseguridad en Cisco, Walter Montenegro, explica que los riesgos son diversos, pues dado que los usuarios interactúan con plataformas de IA públicas, podrían compartir información privada y sensible, incluso sin intención, la cual se vuelve de dominio público. "Esto significa que cualquier persona puede consultar un dato y la plataforma lo proporcionará, asumiendo su carácter público", detalla el ejecutivo, y añade que se han documentado casos en Chile donde actas de directorios que contenían información sensible fueron subidas íntegramente, comprometiendo así la privacidad de los individuos e información de la empresa.

"No solo debemos usar la IA para proteger, sino también proteger a la IA misma, resguardando la integridad de sus datos y monitoreando sus resultados", asegura el country manager de SEK en Chile, Diego Macor.

Soluciones de seguridad con IA

En el área de desarrollo de software, hace un par de años que la IA marcó un punto de inflexión con el uso de asistentes de código potenciados por esta tecnología. De hecho, según un informe elaborado por la división de investigación DORA de Google, el 90% de los profesionales de la industria tecnológica utiliza IA en sus actividades diarias, pero solo el 46% confía parcialmente en la calidad del código generado.

En el ámbito de la ciberseguridad, por un lado está el uso de la IA para crear soluciones propias, como plataformas de detección y respuesta basadas en agentes o bajo esquemas más avanzados de *IA agentic*, donde los modelos pueden tomar decisiones y ejecutar acciones de manera autónoma. "Allí el riesgo principal es la calidad del código y la gobernanza del modelo: si no se valida y supervisa, puede incorporar vulnerabilidades, errores o falsos positivos que afecten la eficacia de la defensa", expone el country manager de SEK en Chile, Diego Macor. También señala que muchas soluciones comerciales de seguridad ya integran IA en sus productos —desde *firewalls* y EDR hasta plataformas de identidad— y añade el riesgo creciente de la manipulación intencional de la IA, donde si un modelo es atacado, puede incorporar datos falsos o sesgos adicionales, alterando sus resultados y debilitando la defensa. "Por eso hoy no solo debemos usar la IA para proteger, sino también proteger a la IA misma, resguardando la integridad de sus datos y monitoreando constantemente sus resultados", acota Macor.

Para Montenegro, es crucial asegurar que el código utilizado no comprometa la información sensible de la empresa, y para ello delinea que es fundamental evitar la inclusión de datos sensibles o credenciales de acceso, como contraseñas de API, que requieran autenticación.

PUBLIRREPORTAJE

RESILIENCE ACCELERATION PROGRAM ASEGURA RESULTADOS REALES, MEDIBLES Y SOSTENIBLES

RAP, el nuevo modelo desarrollado por SEK que acompaña a sus clientes en todo el ciclo de ciberseguridad

La empresa líder en América Latina integra estrategia, ejecución y operación en un solo modelo de resiliencia que responde tanto a las brechas internas como a los desafíos globales de ciberseguridad, convirtiéndose en un socio estratégico para transformar la regulación y las amenazas en una ventaja competitiva.

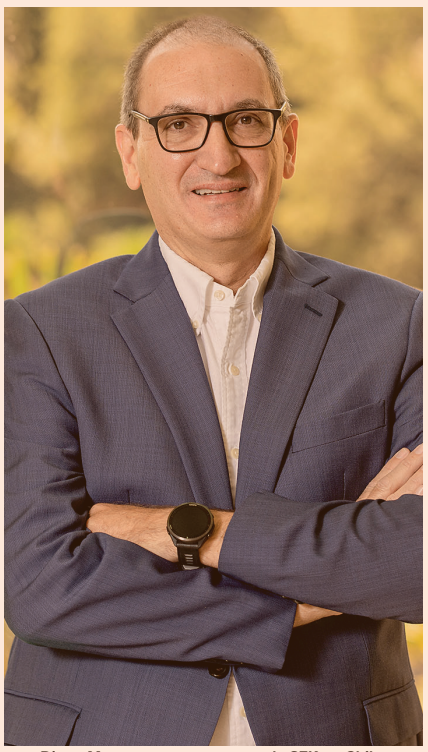
La mayor exposición por el acelerado proceso de digitalización del país, el aumento de ciberataques cada vez más sofisticados con IA y la presión por cumplir nuevas regulaciones, como la Ley Marco de Ciberseguridad, la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos, tienen a las empresas en un punto de inflexión.

Por eso SEK -que tras la reciente adquisición de Dreamlab Technologies Latam reforzó su posición como la empresa líder de ciberseguridad en América Latina- desarrolló el Resilience Acceleration Program (RAP). Un acelerador de negocio a través de resiliencia digital que acompaña a las organizaciones desde la definición de la estrategia de seguridad digital hasta la operación continua, asegurando resultados reales, medibles y sostenibles.

"Con RAP ejecutamos pruebas reales de resiliencia, simulaciones de ataques, stress tests de infraestructura y ejercicios de respuesta a incidentes que validan la capacidad real de respuesta de la organización. Es la diferencia entre tener un plan en papel y saber que funcionará cuando más lo necesite", afirma Diego Macor, country manager de SEK en Chile.

El programa incluye un componente único de Security Advisory continuo que funciona como el "Waze de la gobernanza de riesgos cibernéticos": orienta a los ejecutivos en tiempo real sobre las mejores rutas para navegar el complejo panorama de amenazas, regulaciones y decisiones de inversión en seguridad.

Un diferencial clave de RAP es su sistema de métricas de gestión y resiliencia basado en las Outcome Driven Metrics de Gartner, que mide el impacto real de las inversiones en ciberseguridad en los resultados del negocio. Sigue frameworks reconocidos internacionalmente, pero con la flexibilidad de adaptarse al modelo de gestión específico de cada cliente. Otro valor agregado es su plataforma de inteligencia unificada que entrega una visión única y centralizada de toda la postura de seguridad de la organización.



Diego Macor, country manager de SEK en Chile.

Características del programa:

- Assessment y estrategia: evaluación profunda basada en frameworks NIST/CIS y definición de roadmap estratégico
- Testing real de resiliencia: simulaciones prácticas que validan la capacidad de respuesta ante incidentes
- Métricas y KPIs de Negocio: Indicadores basados en Outcome Driven Metrics que conectan seguridad con resultados empresariales
- Plataforma de Inteligencia Unificada: visibilidad y control centralizado de toda la postura de seguridad
- Security Advisory Continuo: orientación estratégica permanente para la toma de decisiones
- Operación 24x7: Monitoreo y respuesta a través del SOC más avanzado de la región

Con operaciones en seis países de América Latina, SEK es considerado en Chile un Operador de Importancia Vital (OIV) por la Agencia Nacional de Ciberseguridad. Su portafolio integral, alianzas con los principales fabricantes tecnológicos del mundo y una metodología práctica de validación continua con métricas orientadas a resultados, le otorgan presencia local, expertise global y visión estratégica. "Invitamos a las empresas a ver a la ciberseguridad como una inversión estratégica para crecer con confianza, con métricas claras de retorno y una visión unificada de su postura de seguridad", concluye Macor.

¿QUÉ TAN PREPARADOS ESTÁN LOS AEROPUERTOS ANTE UN ATAQUE CIBERNÉTICO?

ATON

Los recientes ciberataques a aeropuertos europeos abren la discusión sobre la preparación de Chile ante amenazas digitales. Expertos advierten brechas en detección, respuesta y coordinación operativa, además de falta de capacitación y personal calificado.

POR VALENTINA CÉSPEDES

La reciente ola de ciberataques que paralizó operaciones en al menos cinco aeropuertos en Europa, provocadas por un ataque de *ransomware* que afectó a un proveedor estadounidense de sistemas de facturación y embarque, dejó en evidencia la fragilidad de la infraestructura digital de la aviación moderna. En este contexto, surge la pregunta sobre cuán preparados están los aeropuertos en Chile frente a ataques similares.

Según el digital industries cybersecurity manager de Siemens Sudamérica sin Brasil, Alfredo Rolando, "la infraestructura aeroportuaria en Chile enfrenta riesgos digitales cada vez más complejos, que amenazan la continuidad de un ecosistema vital para la economía y la conectividad del país".

Citando cifras del Grupo ADP, el ejecutivo destaca que el Aeropuerto Internacional Arturo Merino Benítez movilizó más de 26 millones de pasajeros en 2024, y solo en enero de este año registró casi 16 mil operaciones de despegue y aterrizaje, lo que da cuenta de su rol estratégico y de interconectividad. En paralelo, advierte que los principales riesgos se concentran en ataques de *ransomware* capaces de paralizar sistemas críticos, denegaciones de servicio (DDoS) -como sucedió en Europa- y tácticas de *phishing* que apuntan al "eslabón humano" para obtener accesos indebidos.

El asociado de la Alianza Chilena de Ciberseguridad, Hugo Galilea, complementa el análisis y apunta que la preparación local en esta materia es "heterogénea y todavía insuficiente frente a ataques sofisticados". Añade que, según simulaciones del Laboratorio Ciberlab de la U. Católica junto con el Ejército de Chile, grandes terminales cuentan con medidas básicas como *antimalware*, *firewalls* y acuerdos con proveedores (SLA), pero la mayoría presenta brechas críticas en detección de amenazas, segmentación de redes y respuesta coordinada.

Estas debilidades, explica Galilea, sumadas a la dependencia tecnológica, el uso de equipos antiguos difíciles de actualizar y una baja conexión con el CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática) nacional, hacen que los aeropuertos estén expuestos a interrupciones de servicios clave, como el check-in, manejo de equipaje o las comunicaciones internas. Además, subraya la limitada preparación operativa del personal ante crisis digitales.

En Bruselas, 140 de los 276 vuelos programados para el pasado domingo 21 de septiembre fueron cancelados, tras un ciberataque contra ese y otros terminales europeos. Ya hay un detenido por el caso.

Infraestructura más robusta

En 2024, Chile sufrió 27.600 millones de intentos de ciberataques, un 360% más comparado con los 6 mil millones de intentos en 2023, según el reporte FortiGuard Lab, de la multinacional Fortinet. La cifra refuerza la necesidad de fortalecer infraestructuras críticas como los aeropuertos.

Rolando plantea que es clave reforzar la cadena de suministro digital, invertir en detección avanzada y capacitar constantemente al personal. También recomienda adoptar normas internacionales como ISO/IEC 27001 —que establece los requisitos para un sistema de gestión de la seguridad de la información— y valora avances como la creación de la Agencia Nacional de Ciberseguridad (ANCI) y la Ley Marco de Ciberseguridad, aunque advierte que estos deben ir acompañados de vigilancia activa y compromiso sostenido.

"Proteger la seguridad digital de nuestros aeropuertos significa proteger la economía, la confianza y la reputación del país", afirma.

Mientras que Galilea propone una hoja de ruta que contempla desde medidas técnicas como la segmentación física y virtual de redes, el control estricto de accesos administrativos con autenticación biométrica y monitoreo de sesiones, hasta políticas de ciberseguridad en la relación con proveedores, incluyendo cláusulas contractuales, auditorías y gestión de vulnerabilidades.

A esto suma la necesidad de fortalecer la coordinación con el CSIRT nacional y la DGAC (Dirección General de Aeronáutica Civil), establecer responsables de ciberseguridad en cada aeropuerto y fomentar una cultura de prevención que alcance también al personal no técnico, como quienes operan en el manejo de equipaje o en los controles de acceso.

Para el CTO de ZeroQ, Hervis Pichardo, el país debe ir más allá de la prevención. "La lección es clara, no basta prevenir, hay que garantizar resiliencia. En Chile debemos reforzar la detección temprana, realizar simulacros de respuesta y asegurar colaboración público-privada para contener incidentes. Además, capacitar al personal en ciberseguridad sigue siendo clave para reducir riesgos humanos", concluye.

GRUPO DF

Director: José Tomás Santa María / **Subdirectora:** Paula Vargas / **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: 2 23391000 / e-mail: buzondf@df.cl / **Impreso por** Gráfica Andes Limitada, que sólo actúa como impresor.