DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
MARTES 17 DE OCTUBRE DE 2023

SOLO UNA DE CADA DIEZ EMPRESAS CHILENAS DESTINA LA MAYOR PARTE DE SU PRESUPUESTO DE CIBERSEGURIDAD A LA DETECCIÓN DE INCIDENTES

Un estudio de la consultora EY reveló que en el país las acciones están enfocadas a la capacidad de respuesta y recuperación ante ataques, justo al revés de la tendencia mundial, lo que muestra la falta de visibilización de la importancia de las acciones preventivas de manera transversal. POR ANDREA CAMPILLAY

Cuando Chile aceleró su camino de transformación digital hubo pruebas de fuego para las estrategias de seguridad de empresas de diversos rubros y varias fueron víctimas de emblemáticos ataques cibernéticos.

La industria financiera fue una de las más afectadas, cuando en mayo de 2018 un hackeo al Banco de Chile tuvo como consecuencia la sustracción de casi US$ 10 millones. Seis meses después, Banco Consorcio también reportó ser víctima de un ataque que terminó con el robo de aproximadamente US$ 2 millones. El retail también ha sido blanco de estos incidentes y bien recordado es el caso de Cencosud de septiembre de 2021, que derivó en la filtración de información sensible de sus clientes.

"En los últimos cinco años hemos visto una mayor cantidad de ataques, muchos de ellos sofisticados y dirigidos. Esto hace que las empresas reconsideren sus estrategias de ciberseguridad e inversiones", asegura Walter Montenegro, gerente de Ciberseguridad en Cisco Chile, agregando, sobre la base de estimaciones de IDC, que en 2022 el gasto en Chile en esta área aumentó en casi un 10%, alcanzando los US$ 156 millones aproximadamente.

Pero el aumento de las inversiones no necesariamente indica que los esfuerzos se están concentrando en prevenir los ataques. De hecho, es todo lo contrario, según el recién publicado estudio EY 2023 Global Cybersecurity Leadership Insights, de la consultora EY, que reveló la cantidad de recursos financieros que las empresas chilenas destinan a acciones de detección y prevención de los ciberataques: solo un 10% destina más del 40% de su presupuesto a estas funciones, contrario a lo que ocurre a nivel mundial, donde un 27% de las empresas de 25 países de América, Asia-Pacífico, Europa, Oriente Medio, India y África hace uso de la misma cantidad de fondos para estos temas.

Facundo Jamardo, socio

→ CONTINÚA PÁG. 26

→ VIENE DE PÁG. 25

líder de Ciberseguridad de EY, explica que esto se debe, por un lado, a que la distribución de empresas chilenas que formaron parte de la muestra del estudio incluyó a un tercio de organizaciones con capacidades avanzadas y dos tercios con capacidades en desarrollo. "Esto explica las dificultades que tienen las organizaciones para integrar mejores procesos de detección, incluyendo la dificultad de integrar tecnologías que permitan mejorar el monitoreo de la superficie de ataque y prevenir mejor los incidentes", dice, sobre uno de los desafíos que vislumbra en el ecosistema corporativo. Otro obstáculo relacionado, añade, es que estos distintos niveles de madurez están relacionados con el apoyo ejecutivo a los equipos de seguridad y el presupuesto disponible para mejorar las capacidades de ciberseguridad.

El reporte también muestra que la proporción de organizaciones locales con capacidades de ciberseguridad avanzadas es mucho menor aquí que en otros países (30% en Chile versus 45% a nivel global), lo que repercute en aspectos como la experiencia de los equipos y las tecnologías de gestión de seguridad.

Además, destaca que entre 2019 y 2023 hubo un aumento de un 75% de los ciberataques más conocidos y, a nivel mundial, un 76% de las organizaciones tardaron seis meses o más en detectar y responder a estos incidentes. "Las organizaciones con capacidades avanzadas pueden detectar los incidentes en rangos que van desde menos de un mes hasta seis meses, sin embargo, las organizaciones con capacidades en desarrollo se concentran fuertemente en el rango de más de seis meses", añade Jamardo.

Cambio de estrategia

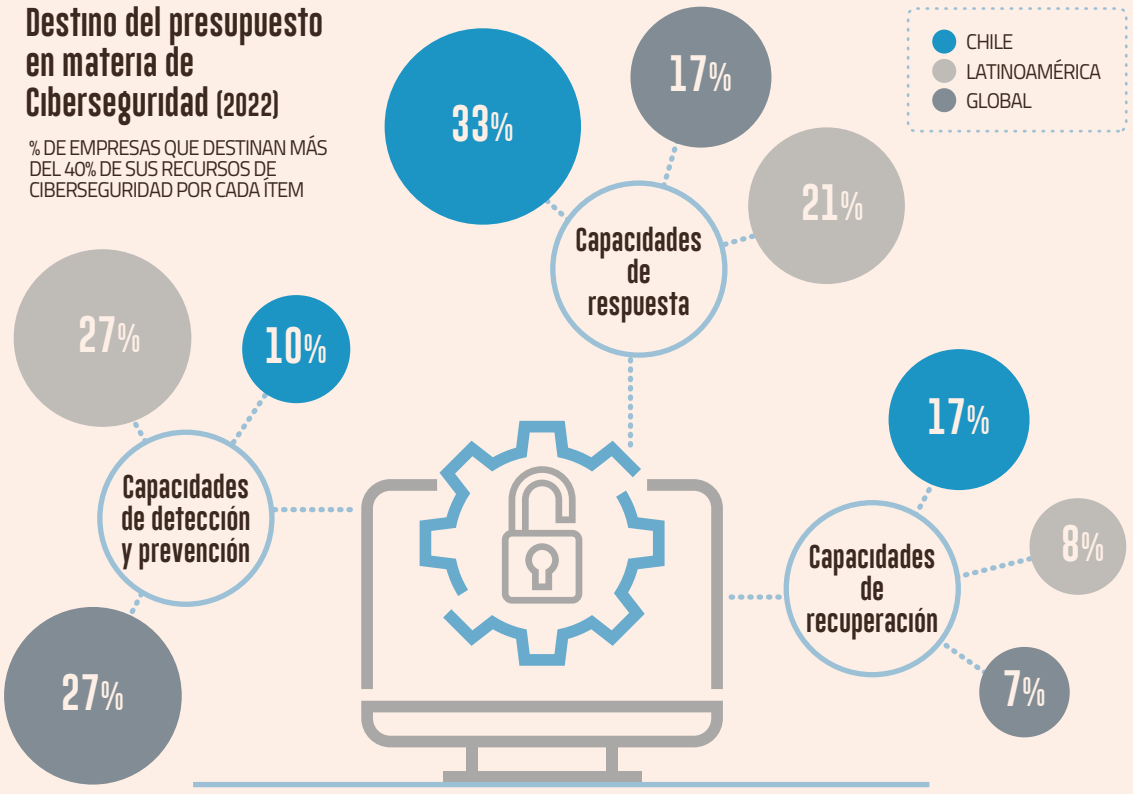
"El gran desafío es avanzar a un esquema preventivo en términos de ciberseguridad, pues hoy la tendencia nos muestra que los esfuerzos están puestos en la respuesta y recuperación", afirma Carlos Melo, CEO de Baseline Cybersecurity.

Martina López, investigadora de Seguridad Informática de ESET Latinoamérica, subraya que para buena parte de las organizaciones a nivel mundial, la detección de un incidente cuando ya ocurrió no es tanto una prioridad, como sí lo es prevenir que suceda. Asimismo, resalta la importancia de que organizaciones grandes y pequeñas puedan contar con herramientas para estar preparadas ante un eventual ataque. "Es complejo y es difícil asumir que seguramente vamos a ser víctimas de algún ataque informático o un intento alguna vez en nuestra vida operativa, pero es así", sostiene.

En este escenario, los expertos coinciden en que actualmente los ciberatacantes trabajan sigilosamente y explotan cada vulnerabilidad interna que encuentran en las compañías, razón por la cual se requiere avanzar en la implementación de tecnologías que permitan visualizar tempranamente las amenazas. "No solo en una solución, sino en las distintas que utilicen de cara al usuario, acceso a Internet, data center, nube, cargas de trabajo", complementa Montenegro. Un hecho que toma relevancia considerando que durante el año pasado, el 18% de los ataques generaron costos de entre US$ 3,1 millones y US$ 6 millones para el país, según cifras del estudio de EY.

Destino del presupuesto en materia de Ciberseguridad (2022)

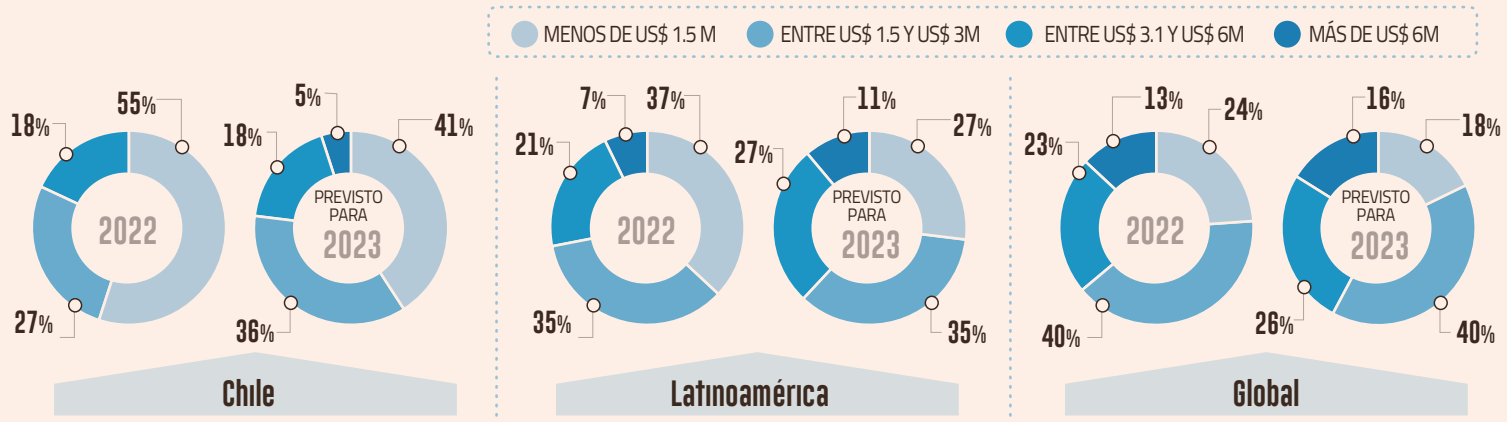
% DE EMPRESAS QUE DESTINAN MÁS DEL 40% DE SUS RECURSOS DE CIBERSEGURIDAD POR CADA ÍTEM



FUENTE: EY 2023 GLOBAL CYBERSECURITY LEADERSHIP INSIGHTS STUDY

Costo de los incidentes en las compañías por periodos de tiempo

COSTOS EN US$ MILLONES



Cómo está cada sector

Si bien Chile se encuentra levemente sobre el promedio mundial (30% vs 27%) con respecto al uso de la inteligencia artificial, automatización y orquestación de la nube y autenticación sin contraseña, estos avances no se han dado con la misma fuerza en todos los sectores y por eso unos son más vulnerables que otros.

"Las industrias más atacadas son las que han tenido que desarrollar más acciones: retail, banca, finanzas, energía. No obstante, hay sectores en los que los ataques están en aumento, como el sector público y el sector salud", asegura Francisca Heine, gerenta de Marketing y Nuevos Negocios de ITQ Latam.

Así, las estrategias para hacer frente a los ciberdelincuentes son diversas y varían según la industria: "La banca, por ejemplo, ha generado acciones más drásticas a nivel interno y de cara a los clientes por los diversos ataques al sector financiero en Chile en los últimos años (...). Por su parte, el retail y la minería buscan mejorar sus niveles de productividad y la experiencia de usuario con altos niveles de seguridad, cuidando siempre la operación y a los colaboradores", puntualiza Montenegro, para quien también se deben reconocer los avances desarrollados en la industria de telecomunicaciones.

53%

DE LAS EMPRESAS EN CHILE SE ENFRENTARON A MÁS DE 50 ATAQUES EN EL ÚLTIMO AÑO, SEGÚN EY.

Sin embargo, estas acciones están orientadas generalmente a la mejora de los sistemas de acceso a las aplicaciones mediante múltiples factores de autenticación; integrar las soluciones de ciberseguridad para disminuir los riesgos tanto en la detección como en la operación; y también generar campañas de concientización de los empleados.

"Lo que muchas compañías están haciendo es partir por una base estándar que permita ir a un primer nivel de madurez en ciberseguridad, adoptando e implementado normativas y estándares internacionales para seguridad de la información y ciberseguridad", complementa Melo.

De esta manera, para Heine, "entender que la ciberseguridad es transversal a toda organización y que requiere un esfuerzo permanente de concientización, capacitación, expertise y tecnología, es todavía un desafío importante en el país". Un hecho que se refleja en que, según el estudio de EY, en Chile las decisiones de alta dirección consideran en menor medida aspectos de ciberseguridad en comparación a otros países de Latinoamérica y el mundo.

Marcelo Díaz, director del área Cyber en Deloitte, asegura que a nivel local muchas organizaciones aún no han logrado tomar conciencia del riesgo de este tipo de ataques, lo que hace que ni siquiera hayan podido establecer "una línea base de ciberseguridad higiénica", lo que considera fundamental como desafío, mientras advierte que la falta de personal capacitado para hacer frente a estas amenazas es clave y sigue siendo un reto para todas las industrias.

GRUPO DF
DF · DFLIVE · DFMAS · FD · BAZARED

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: 23391000 / e-mail: buzondf@df.cl / **Impreso por** COPESA IMPRESORES S.A., que sólo actúa como impresor.