LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **“La democracia también se sostiene con la ciberseguridad”**

Pág. : 4
Cm2: 472,3

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

miento normativo ha sido clave, espe- ponsabilidad. La ciudadanía espera res- en el privado.

CAMBIO CULTURAL:

# “La democracia también se sostiene con la ciberseguridad”

**Con el impulso de las nuevas leyes, Chile ha mejorado su preparación ante ciberataques, pero aún falta seguir avanzando y tomar conciencia de su valor estratégico y reputacional.**


**OCTAVIA RIVAS**, editora de Radio Universo, junto a Daniel Álvarez, Kenneth Pugh, Nicolás Goldstein y Rodrigo Valenzuela.

FELIPE RAMOS

Solo en los nueve primeros meses de 2024 Chile fue víctima de 6.400 millones de intentos de ciberataques contra organizaciones y personas, según un informe de Fortinet. Los métodos más utilizados son el *phishing* y el *malware*, mientras que los ataques de *ransomware* continúan en ascenso, pero se diseñan especialmente para objetivos seleccionados. De acuerdo al mismo reporte, 44% de las muestras de *ransomware* y *wiper* apuntaron a sectores industriales, siendo salud, manufactura, automotriz y transporte y logística los más atacados.

Para discutir sobre el estado de preparación del país en esta materia, en Cybertech South America 2025 se realizó el panel “Ciberseguridad en Chile: ¿Estamos listos para el próximo ciberataque?”, en que participaron Daniel Álvarez, director de la Agencia Nacional de Ciberseguridad (ANCI); Kenneth Pugh, senador por la Región de Valparaíso; Nicolás Goldstein, presidente ejecutivo de Accenture Hispanoamérica, y el teniente coronel Rodrigo Valenzuela, jefe del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) del Ejército.

Actualmente, Chile es el cuarto país de Latinoamérica con más ciberataques, después de Brasil, México y Argentina. Dentro de los casos más recordados están el hackeo del Banco de Chile en 2015, la intrusión a los correos privados del Estado Mayor Conjunto en 2022, y ataques al sistema de Chile Compra. En el panel se comentó que hasta hace dos años habían unos tres eventos importantes al año, y llegaron a más de 80 en 2023. Solo en lo que va de 2025 se han registrado 30 incidentes. “El hecho de ser muy conectados nos transforma en un objetivo interesante para los ataques”, dijo Daniel Álvarez.

## UN ASUNTO POLÍTICO

Ante la posibilidad de un nuevo ciberataque masivo, el senador Pugh sostuvo que “nos estamos preparando para ese escenario y estamos evangelizando. La dependencia es total y eso requiere tener conciencia de aquello. Esto no es un tema tecnológico, sino un asunto político. La democracia también se sostiene con la ciberseguridad”. Goldstein añadió que “la reputación de las empresas pasa por la ciberseguridad. Hoy hay que hacer un clic cultural que es lo más importante y difícil. Un *pendrive* o un QR en una carta pueden provocar un ciberataque”.

El panel estuvo de acuerdo en que el país está mejor preparado que antes para un eventual ciberataque. Por ejemplo, el Ejército ha apostado por nuevas tecnologías, como el cifrado cuántico, y el sistema financiero está bien protegido. Pero no se sabe qué pasa con otros sectores productivos o claves para el país, como el eléctrico. En ese sentido, el senador Pugh señaló que “la madurez es esencial. El año pasado estábamos en pañales, hoy estamos gateando. Eso pasa por la colaboración. Hay que entrenarse, pero también saber responder”. Por su parte, el teniente coronel Valenzuela sostuvo que “hemos avanzado en la legislación, pero esto depende de los usuarios. Estamos avanzando, porque al tener una normativa se ordena la casa. Otro punto es que la preparación de profesionales en ciberseguridad es costosa, y hay que intentar retenerlos”.

## CERO CONFIANZA

Una mayor preparación, tanto a nivel de empresas como de usuarios, pasa por un mejor comportamiento digital. “Somos malos gestionando contraseñas y debemos estar conscientes del riesgo, ya que estamos muy expuestos. En lo que va de 2025, ya emitimos la misma cantidad de alertas por ataques vía SMS que en todo 2024. Debemos usar gestores de contraseñas y actualizar los sistemas operativos de nuestros equipos”, recomendó Álvarez.

“Hay que estar muy preparados y actuar con cero confianza. Ninguna máquina es segura y tampoco lo es ninguna persona. Hay que cuidarse”, concluyó Goldstein.

PANEL3