LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Progresos y desafíos en la protección de la infraestructura crítica**

Pág. : 20
Cm2: 425,5
VPE: $ 5.589.944

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

LA PERIODISTA VERÓNICA SCHMIDT moderó el panel integrado por Diego Macor, Jorge Atton, Katherina Canales y Esteban Fuenzalida.

PANEL

FRENTE A LAS AMENAZAS DIGITALES:

Progresos y desafíos en la protección de la infraestructura crítica

Expertos coinciden en que se han registrado avances en el país, pero hay que reforzar iniciativas para mejorar las coordinaciones, aumentar los recursos y fortalecer los planes que enfrenten esta nueva realidad.

CLAUDIA BETANCOURT M.

El reporte "Cyber Threat Landscape" indica que Chile registró un total de 813.191 detecciones de ciberamenazas entre febrero y abril de este año. Estos números equivalen al 7,8% del total regional y significan un aumento del 53% respecto al mismo período de 2024. Esto posiciona a nuestro país como el segundo más atacado de Sudamérica, después de Brasil.

Los sectores más vulnerables son el bancario, financiero en general, público y de salud, que son afectados por una serie de incidentes, incluyendo ataques de *ransomware*, *malware*, *phishing*, y otros tipos de ciberdelitos.

SITUACIÓN EN CHILE

¿Cuán preparado está Chile para enfrentar estos ataques a su industria crítica? ¿Cómo se puede enfrentar una contingencia como esa? ¿Son suficientes las inversiones actuales? Estas fueron algunas de las interrogantes que aparecieron en el panel "Ciberseguridad en industrias críticas" durante el Cybertech South América 2025, organizado por "El Mercurio".

En la conversación participaron Katherina Canales, ex directora ejecutiva de la Corporación de Ciberseguridad Minera; Esteban Fuenzalida, gerente de Operaciones de Ciberseguridad Claro Empresas-SCITUM Chile; Diego Macor, *country manager* Chile NeoSecure by SEK; y Jorge Atton, exsubsecretario de Telecomunicaciones y director ejecutivo de Attsons Consulting.

Diego Macor planteó que los niveles de seguridad en sectores críticos dependerán en gran medida de las inversiones que se hayan hecho. Y ahora, con la nueva Ley Marco de Ciberseguridad, "va a subir notablemente el nivel de exigencias a las industrias para responder a los ataques de ciberseguridad, gestionar los riesgos y estar preparados para notificar y colaborar".

Jorge Atton estimó que se han producido avances importantes en los últimos años. "Está la agencia (Agencia Nacional de Ciberseguridad), la Ley de Protección de Datos Personales y la Ley de Delitos Económicos; tenemos varios procesos de implementación y ha existido un gran trabajo y conciencia".

No obstante, admitió que un riesgo son las escasas inversiones que se observan, y es necesario que el Ministerio de Hacienda destine mayores recursos para que la ciberseguridad se convierta en un tema país. Lo mismo debe pasar en los directorios de las empresas. "Si sumamos todos los cambios que está trayendo la inteligencia artificial (IA), la verdad es que estamos frente a un tsunami desde el punto de vista de seguridad de la información", señaló.

Un factor determinante de los niveles de protección es la inversión de las empresas, la cual debería aumentar ante las nuevas exigencias de la ley de ciberseguridad.

Katherina Canales opina que falta una mayor interconexión y comunicación entre los diferentes servicios, ya que en cada incidente "hay personas atrás; y detrás de ellas hay organizaciones. Como hoy estamos tan interconectados, necesariamente vamos a depender de otros, y en esa dependencia también debemos entender que la estructura crítica debe actuar coordinada".

AÚN EN TRANSICIÓN

A su juicio, Chile muestra importantes avances en Latinoamérica, pero todavía estamos en una etapa de transición. Esteban Fuenzalida concordó en que es necesario nivelar las experiencias de las diferentes empresas, y en el período de transición se debe fortalecer esta cultura de estructura crítica para definir planes de continuidad. "Es un proceso que va paso a paso, pero con un buen acompañamiento. Debemos tener buenos KPI (*Key Performance Indicator*) para poder construir un rol más apropiado, y, en esa línea, se va a fortalecer la cultura dentro de una organización".

En definitiva, ¿está preparada la infraestructura crítica para un ciberataque a gran escala? Katherine Canales afirmó que "no vamos a estar preparados nunca", por lo que hay que practicar todos los días.

Para Jorge Atton, "las respuestas deben ser rápidas y asertivas, por lo que aparte de las exigencias de la ley, una de las grandes tareas para las empresas o las instituciones es crear comités de crisis, tener planes de contingencia y planes especiales de comunicaciones".

Esteban Fuenzalida puntualiza que "se debe impregnar la gestión de riesgo y la ciberseguridad dentro de todas las organizaciones. El camino va, también, en compartir información y mejorar los temas de ciberinteligencia en la infraestructura crítica".