LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Proteger la infraestructura crítica ya no es una opción, sino un deber ineludible**

Pág. : 12
Cm2: 449,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

BÁRBARA BRICEÑO, conductora de EmolTV, moderó el panel integrado por Karin Quiroga, José Daniel Garabito, Christian Ellsworth y Patricio Leighton.

PANEL 7

FORTALEZA DIGITAL EN JAQUE:

Proteger la infraestructura crítica ya no es una opción, sino un deber ineludible

Representantes del sector eléctrico, tecnológico y gremios de ciberseguridad presentes en Cybertech South America, coincidieron en que los ataques son una realidad. Uno de los anuncios clave fue la realización del primer simulacro de ciberataque con impacto en infraestructura crítica, liderado por el Coordinador Eléctrico Nacional.

RICHARD GARCÍA

Chile aún tiene desafíos pendientes en planificación, formación profesional y colaboración efectiva para proteger su infraestructura crítica frente a ciberataques y fallas sistémicas, reconocieron los representantes del sector eléctrico, empresas tecnológicas y gremios, durante el panel "Fortaleza Digital: Protegiendo la infraestructura crítica", realizado en el marco de Cybertech South America 2025.

El caso del apagón del 25F —y su paralelismo con fallas recientes en España y Portugal— marcó el punto de partida. "Probablemente, hace pocos años nadie hubiese pensado siquiera que la causa raíz de un *blackout* fuera un ciberataque. Eso cambió. De hecho, a dos minutos de ocurrido el evento, el 25F, me llamaron para preguntarme si fue un ciberataque; dos minutos", contó Patricio Leighton, director de la Unidad de Ciberseguridad e Infraestructura Crítica del Coordinador Eléctrico Nacional (CEN).

Leighton detalló que desde hace cinco años el CEN viene aplicando el estándar NERC, utilizado en Estados Unidos, Canadá y parte de México, para proteger la infraestructura crítica eléctrica tanto de ciberamenazas como de ataques físicos. "No es la solución definitiva, pero ayuda bastante a tener un lenguaje común, a tener una forma de operar estándar", explicó. Y advirtió que la amenaza al sistema eléctrico no es "multisistémica, porque tiene variables operacionales, tecnológicas, de negocio, de inestabilidad del sistema, hay diferentes desafíos de cambio climático, etc.".

Además, el ejecutivo anunció que el CEN está preparando un simulacro de ciberataque con impacto en el sistema eléctrico y otros servicios esenciales, que incluirá a Senapred, Defensa, PDI y diversas agencias públicas y privadas. "Vamos a articular un ejercicio que de alguna manera refleje la realidad", y del cual deben surgir aprendizajes que permitan establecer y transformar los planes de acción en un sentido de mejora, dijo.

José Daniel Garabito, responsable de Ciberseguridad de Infraestructuras Críticas para LATAM Insight, destacó que estos activos estratégicos se han vuelto más vulnerables por su creciente conexión con redes externas: "Antes eran sistemas aislados. Pero, ahora, ya tienen conexiones en las redes de TI, y en algunos casos llegan a internet. Eso hace que la superficie de ataque se amplíe".

Christian Ellsworth, *lead consulting engineer* de Corero, planteó una analogía: "Si no tienes los extintores en el edificio al momento del inicio del incendio, no hay nada que puedas hacer". Y añadió que la protección de infraestructura crítica no admite atajos: "Esto no existe, no hay una píldora básica y nadie de los que estamos afuera vamos a vender una caja que automáticamente resuelva el problema".

CAPITAL HUMANO

Respecto del capital humano, Karin Quiroga, cofundadora de la Alianza Chilena de Ciberseguridad, fue categórica: "La tecnología se enfrenta al componente de la actualización permanente. Y es demasiado rápido". Además, explicó que no solo el personal técnico necesita formación: "Hoy, las organizaciones también tienen que hacerse cargo de colaboradores que están en áreas no técnicas y que también son un punto focal de ataque o de amenaza".

Quiroga agregó que la nueva ley de ciberseguridad establece exigencias claras para las organizaciones que prestan servicios esenciales, señalando que "hay que desarrollar capacidades, focalizar la formación en sistemas de gestión de seguridad de la información, en planes de continuidad operacional, en certificaciones que nos va a determinar la agencia (de ciberseguridad, ANCI)".

PREPARACIÓN CONSTANTE

Garabito respaldó esa visión: "Tenemos que estar preparados para que nos pase. Es bastante importante. Todos tienen que buscar esa cultura de colaborar, de compartir, de aprender lecciones aprendidas".

Ellsworth enfatizó en que los ataques no son hipotéticos y que "si tienes algo conectado a internet, lo van a atacar. Eso no es un 'si', es un 'cuándo'", y coincidió en la falta de profesionales preparados: "Esto se enseña haciendo. Tienes que ensayar, tienes que probar, tienes que romper y arreglar".

Quiroga, en tanto, planteó que "hay dos mecanismos de solución: uno, a través de la educación formal, y la otra línea es la formación profesional". Y subrayó la necesidad de colaboración internacional: "Es probable que internamente o acá en Chile no vamos a tener todavía los profesionales preparados, pero sí tenemos países referentes".

Garabito ejemplificó con la experiencia colombiana: "Hemos venido trabajando en el Centro de Excelencia en Ciberseguridad Industrial (CESI). Estamos generando alianzas con universidades y también trabajando con fabricantes reconocidos".

Para Patricio Leighton, la solución exige mirar desde el principio: "La estrategia de capacitación y de formación tiene que partir desde los primeros niveles de educación, para que efectivamente tengamos primero conciencia y después jóvenes y niños interesados en estas temáticas".