DE MANERA DE PRESERVAR SU CONTINUIDAD:

Ciberdefensa, esencial para cuidar la infraestructura crítica

Una estrategia de múltiples capas de protección de los datos permite proteger la información, identificar los ataques, ralentizarlos y activar medidas específicas en su contra, para actuar a tiempo y anular o minimizar los daños en la organización.

ANA MARÍA PEREIRA B.

Con la creciente sofisticación del cibercrimen, se presentan nuevos desafíos a organizaciones de todos los sectores, entre ellos, el de infraestructura crítica, que comprende los servicios y operaciones esenciales para el funcionamiento de un país, como telecomunicaciones, energía, agua y salud, entre otros.

La respuesta recomendada es la ciberdefensa o ciberseguridad en profundidad, "una estrategia que aplica múltiples capas de protección de los datos de una organización. En cada una de estas capas se aplican sectorizadamente distintos controles y soluciones específicas, con medidas de ciberdefensa especializadas para proteger la información de los activos críticos", explica Néstor Strübe, gerente general de ITQ Latam.

El experto agrega que la principal ventaja es que esta estrategia "no solo apunta a proteger la información, sino que a la vez busca ralentizar los ataques para que tarden más en avanzar hacia su objetivo, vayan siendo claramente identificados y se activen medidas específicas en su contra, para proteger a tiempo y anular o minimizar los daños en la organización".

Rocío Ortiz, subdirectora de Industrias del Futuro del Centro de Innovación UC Anacleto Angelini, agrega que en dicha área, la ciberdefensa permite "responder de mejor manera a distintos ataques; reducir la superficie de impacto y el nivel de susceptibilidad a diferentes vulnerabilidades y, sobre todo, un mejor tiempo de recuperación ante un ataque, lo que facilita una continuidad operacional y una mayor seguridad de los servicios básicos".

A juicio de los expertos, Chile se encuentra bien avanzado en la materia, gracias a la institucionalidad que se ha ido desarrollando con la Ley de Ciberseguridad, por ejemplo. Además, hay industrias más desarrolladas, como la banca y el sector energético, a través del Coordinador Eléctrico Nacional.

CRISTIÁN CARVALLO

EL COORDINADOR ELÉCTRICO NACIONAL ha guiado la adopción de la norma internacional de ciberseguridad para el sector energético en Chile.

Pero existen desafíos. Para Strübe, entre los más relevantes está "el creciente paso de los negocios y sus tecnologías a ambientes *cloud*", aspecto en que se requiere "superar la concientización y entrenamiento de todos los colaboradores".

Ortiz destaca los retos que enfrentan algunas industrias como salud o logística, que tienen una gran infraestructura física, y donde es necesario integrar las tecnologías de la información con las de operaciones, así como actualizar los sistemas, sobre todo por la existencia de versiones anteriores ("sistemas legados") que pueden tener vulnerabilidades desconocidas.

"También hay un tema asociado a la interoperabilidad de los sistemas y las infraestructuras críticas, pensando que todo es una cadena de actividades conectadas. Y, finalmente, el tema del talento es fundamental: se requiere conocimiento especializado no solo en temas de ciberseguridad o ciberdefensa, sino que también conocimiento específico técnico de estas distintas industrias, lo que es cada día más desafiante", afirma Ortiz.