BÁRBARA BRICEÑO, conductora de EmolTV, junto a Juan Carlos Beltrán, Rocío Ortiz y David Nieto.

PANEL 5

REQUIERE UN MANEJO INTEGRAL Y TRANSVERSAL:

La gestión de crisis es un músculo que debe entrenarse

Los incidentes de ciberseguridad no se manejan solo desde el interior de las organizaciones. Hoy es fundamental la colaboración de todos los sectores, permitiéndoles prepararse a nivel nacional, como ecosistema y como industria.

BÁRBARA LICHNOVSKY

Un estudio del Foro Económico Mundial indica que nueve de cada diez organizaciones sufrieron al menos un ataque cibernético en 2024. Además, las pérdidas globales asociadas a la ciberdelincuencia podrían alcanzar los US$ 10.500 millones anuales para 2025.

Un panorama que según Rocío Ortiz, subdirectora de Industrias del Futuro UC, requiere que las empresas anticipen la crisis de ciberseguridad no solo desde el punto de vista técnico, sino que también de un manejo más integral y transversal. "Las crisis no se manejan solamente desde una organización, sino que tenemos que prepararnos a nivel nacional como ecosistema y como industria. Somos una cadena económica, entonces no podemos pensar que vamos a manejar la crisis nosotros solos internamente en la casa, bajo la alfombra", explicó.

En el panel "Incidentes y gestión de crisis: ¿Qué hacer cuando todo falla?", efectuado en el marco del Cybertech South América 2025 en "El Mercurio", participaron también Juan Carlos Beltrán, CTO del Centro de Excelencia Ciberseguridad de GTD, y David Nieto, *country manager* de Telefónica Tech Chile. Todos coincidieron en la necesidad de contar con un plan de manejo de las crisis centrado en la educación, la comunicación y la colaboración entre los distintos sectores.

Según Juan Carlos Beltrán, la inteligencia artificial (IA) tendrá un papel protagónico en el futuro inmediato, ya que permite tener capacidades de respuesta más rápidas frente a los ataques, además de reducir los falsos positivos (cuando un sistema de seguridad identifica incorrectamente una actividad o un archivo legítimo como malicioso). Una apreciación con la que coincidió Rocío Ortiz: "Nos puede ayudar a filtrar la información, a detectar patrones, porque estamos recibiendo una sobre estimulación de distintos ataques. Con la cantidad de señales, indicadores de compromisos y alertas que recibimos, no podemos tener a un analista leyendo uno a uno", afirmó.

FLUJOS DE INFORMACIÓN

Por otra parte, David Nieto agregó que la IA también juega un rol importante luego de declarar el incidente de ciberseguridad, ya que permite generar reportes, hacer fluir esa información al interior y exterior de la organización y ayudar a los empleados a saber cómo responder. "Tienes que mantener informado a todo el entorno, al gobierno, aprender del incidente y esa lección aprendida debe estar disponible para futuros sucesos tanto proactiva como reactivamente", señaló.

El ejecutivo destacó que la gestión de crisis va más allá del uso de una tecnología. Aspectos como la comunicación, el entrenamiento, la educación y el compartir información entre las empresas son clave, tanto en ciberseguridad como en la restauración de los sistemas una vez producido el incidente. A ello se suma la importancia de tener inmutabilidad de al menos el último estado sano de la organización, en el caso de que todo falle.

Para Beltrán, es básico contar con un plan de continuidad probado que involucre a toda la organización. "Cuando existe un incidente, hay que saber qué acciones se deben tomar mientras recupero los servicios, contengo el ataque, expulso al actor de las amenazas; mientras hago lo técnico, qué hago para seguir atendiendo a mis clientes, para comunicar a mis grupos de interés lo que está sucediendo, cómo y cuándo lo comunico, etc.", detalló.

Según Rocío Ortiz, aunque existe talento, tecnología y conocimiento, uno de los retos es fortalecer la colaboración entre el sector público, privado y la academia, ya que muchos aprendizajes pueden integrarse a nivel nacional. "Lo importante es articular y, sobre eso, generar modelos neutrales que nos permitan ir avanzando y, sobre todo, ejercitar. La gestión de crisis no se improvisa, es un músculo. Como yo entreno para una maratón, yo entreno también para gestionar crisis", señaló.

Como ejemplo de esta colaboración, el año pasado, el equipo del CiberLab —perteneciente al Centro de Innovación UC y el Ejército de Chile—, junto a DreamLab Technologies Latam, el Programa de Derecho, Ciencia y Tecnología de la UC, y Duoc UC, convocaron al primer ejercicio de gestión de crisis, donde más de 100 miembros de distintos sectores participaron en la simulación de un ciberataque en tiempo real. A ello se sumó, este año, un ejercicio en conjunto con el Coordinador Eléctrico Nacional. Pruebas claves, afirmó Nieto, ya que permiten un mayor aprendizaje frente a los incidentes de ciberseguridad, otorgando modelos de recuperación consensuados.