LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **El mundo refuerza su defensa digital ante nuevas amenazas globales**

Pág. : 4
Cm2: 413,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

HYPO PHOTOS

MARÍA JOSÉ TAPIA, subeditora de Economía y Negocios domingo, junto a Orlando Garcés, José Luis Diego, Jesús Toledano y Néstor Strube.

PANEL 2

EN TIEMPOS DE INCERTIDUMBRE:

El mundo refuerza su defensa digital ante nuevas amenazas globales

Expertos de la OEA, la Comisión Europea y el sector privado, presentes en Cybertech South America 2025, coincidieron en que el desafío no es solo técnico, sino cultural, humano y estratégico.

RICHARD GARCÍA

Cómo se prepara un país, una empresa o un ciudadano frente a un ciberataque real fue el eje que cruzó las intervenciones del panel "Ciberinteligencia y ciberamenazas en contexto geopolítico", que se desarrolló durante el *summit* Cybertech South America 2025 en "El Mercurio".

Orlando Garcés, oficial de políticas de ciberseguridad del Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), afirmó que América Latina y el Caribe presentan avances dispares, aunque alentadores. "Hay países como Chile que están dando pasos muy interesantes en legislación e infraestructura crítica. Y otros están fortaleciendo capacidades humanas o cooperación internacional", afirmó, destacando que el 80% de las naciones de la región se ubican en niveles 3 o 4 del Cybersecurity Global Index de la Unión Internacional de Telecomunicaciones (UIT).

Néstor Strube, gerente general de ITQ Latam, abordó la dimensión cultural: "El 95% de los incidentes son por errores humanos. La cultura de ciberseguridad debe combinar capacitación constante con la aplicación real de ese conocimiento". A su juicio, el cumplimiento normativo ha sido clave, especialmente en el sector público. "No cumplir con regulaciones puede traer consecuencias legales y económicas graves", dijo.

Asimismo, planteó una metodología clara: identificar los activos críticos, evaluar su nivel de protección y aplicar medidas de vigilancia permanente. "El monitoreo 24/7 no puede detenerse nunca", recalcó.

CAMBIO ESTRATÉGICO

Jesús Toledano, *head* of Global Security Architecture en Intel para Google, explicó que "no se trata de evitar todo ataque, sino de saber que te van a atacar y estar preparado para responder", afirmó, comparando aquello con saber bloquear una tarjeta de crédito robada: acciones concretas, sin pánico.

Toledano alertó sobre el uso que hacen atacantes de la inteligencia artificial (IA), pero también destacó su potencial defensivo: "La IA acorta el tiempo de aprendizaje y permite respuestas más rápidas. Pero sin una cultura humana fuerte, perderemos la batalla".

José Luis Diego, inspector de policía y evaluador de proyectos para la Comisión Europea, en tanto, subrayó que la ciberseguridad exige un cambio estratégico en las fuerzas del orden. "Muchas veces escapa de nuestra competencia directa, pero no de nuestra responsabilidad. La ciudadanía espera respuestas concretas, incluso cuando las causas no sean evidentes o inmediatas", señaló.

Y relató que el reciente apagón que afectó a España y Portugal impulsó una revisión profunda de los protocolos de emergencia. "Nos dimos cuenta de que no basta con una reacción forense. Hay que actuar en tiempo real, con respaldo analógico, con telefonía satelital, con simulacros y preparación transversal", dijo.

PREPARACIÓN GENERAL

Diego comentó que los cuerpos policiales europeos están renovando sus estrategias para enfrentar tanto ciberataques como fenómenos híbridos. "Debemos asumir que a la ciudadanía le da igual si una catástrofe es provocada por un fallo técnico o un ciberataque; la expectativa es que estemos presentes, ayudemos y mantengamos funcionando los servicios esenciales", añadió.

Además, enfatizó en la importancia de preparar a la población y no solo a las instituciones: "Hay que fomentar una cultura de corresponsabilidad. La seguridad no puede depender exclusivamente del Estado. El individuo también debe tener un rol activo, estar informado, saber cómo actuar ante una emergencia digital".

El panel coincidió en que la amenaza que significa la falta de profesionales especializados. "En el mundo faltan cuatro millones, en América Latina 1,3 millón, y en Chile unos 28.000", señaló Strube. Garcés agregó que se debe actuar desde ambos extremos: formar desde la educación básica y mejorar las condiciones para contratar y retener talento, tanto en el sector público como en el privado.