EL MERCURIO
innovación

Fecha: 26/12/2024 Audiencia: 320.543 Sección: CONTRAPORTADA
Vpe: $11.865.043 Tirada: 126.654 Frecuencia: 0
Vpe pág: $18.442.944 Difusión: 126.654
Vpe portada: $18.442.944 Ocupación: 64,33%

LA VISIÓN DE 20 EXPERTOS:

¿Cuáles serán los desafíos en **ciberseguridad** para Chile en 2025?

Resiliencia, talento y cambios regulatorios en seguridad digital, privacidad y protección de datos están entre los principales retos. **EQUIPO INNOVACIÓN**

DINAMISMO

"Para 2025, la prioridad no es solo el cumplimiento normativo, sino la creación de una cultura de seguridad proactiva. Esto implica soluciones tecnológicas resilientes, capaces de adaptarse a amenazas emergentes y asegurar la disponibilidad, integridad y confidencialidad de los datos. Las empresas que prioricen la ciberseguridad como criterio de competitividad estarán mejor posicionadas para el éxito en la próxima década".

KATHERINA CANALES
Directora ejecutiva de la Corporación de Ciberseguridad Minera

PUESTA EN MARCHA

"La integración público-privada es la clave del éxito del despliegue del nuevo ecosistema regulatorio digital, teniendo siempre presente que en ciberseguridad no se compite, se colabora. En tal sentido la selección de los nuevos miembros del Consejo Multisectorial de Ciberseguridad será también una pieza clave en la nueva institucionalidad. Dos de ellos proveerán de la industria, dos del mundo académico y dos de la sociedad civil organizada".

KENNETH PUGH
Senador

TALENTO

"Cerrar la brecha de habilidades en ciberseguridad, que afecta especialmente a sectores como servicios financieros, industriales, consumo y tecnología, responsables del 64% del déficit. La falta de diversidad agrava el problema: aunque las mujeres ocupan el 36% de los empleos en tecnología, solo representan el 24% en ciberseguridad. Las empresas deben invertir en formación, diversificación y automatización, pero el factor humano seguirá siendo esencial para enfrentar amenazas crecientes y complejas".

MARCIAL GONZÁLEZ
Managing director y socio de BCG.

RESILIENCIA

"Uno de los principales desafíos es cómo las organizaciones adoptarán el concepto de resiliencia para enfrentar amenazas más evolucionadas. El dilema está en cómo responder frente a aquellas amenazas que sí o sí podrán afectar a la organización, y cómo esta estará preparada en todos los niveles para hacerle frente. Pero no solo desde lo técnico, también en lo comunicacional y reputacional. Esto es importante para generar un músculo ciberseguro en toda la cadena de la empresa (...)
La escasez de talento seguirá siendo un desafío muy importante en las organizaciones, por lo que los marcos regulatorios y la colaboración intersectorial podría permitir el sentar una base para cubrir este *gap*".

MARCELO DÍAZ
Socio Líder de Cyber en Deloitte.

CUMPLIMIENTO

"Las empresas e instituciones públicas tienen el desafío de acelerar su preparación para cumplir con la Ley Marco de Ciberseguridad y la Ley de Protección de Datos. Resiliencia: defender y responder a ciberataques a la infraestructura crítica y fuga de información seguirán siendo prioridad. Personas: el proceso más lento es el cambio cultural para fortalecer las defensas, mejorar la resiliencia y reducir el riesgo del incumplimiento legal y normativo".

RICARDO SEGUEL
Director del magíster en Ciberseguridad de UAI.

RESILIENCIA

"El principal desafío será fortalecer la resiliencia organizacional frente a amenazas cada vez más sofisticadas y persistentes. La gestión del riesgo continuará siendo prioritaria, ya que el factor humano sigue siendo el eslabón más vulnerable. En respuesta, la demanda de profesionales especializados en seguridad Zero Trust y automatización crecerá significativamente. Además, la formación de profesionales con competencias en detección, respuesta y mitigación de amenazas jugará un rol esencial. Se debe transitar desde un enfoque reactivo hacia una ciberseguridad proactiva".

ALEJANDRA ACUÑA
Directora de la Escuela de Informática y Telecomunicaciones Duoc UC.

CAPACITACIÓN

"Las organizaciones deben invertir en infraestructura que garantice la protección de su información y la continuidad del servicio, tanto de manera preventiva como reactiva. En ese sentido, las prioridades deben estar enfocadas en potenciar una cultura que fomente la capacitación del capital humano, reduciendo los riesgos de ciberataques causados por errores humanos. La ciberseguridad no es una opción, sino una necesidad para asegurar la competitividad y éxito en la economía digital".

LUZ MARÍA GARCÍA
Gerente general de ACTI

RESILIENCIA

"La resiliencia cibernética será el principal desafío. La sofisticación de amenazas obliga a las organizaciones a reforzar su preparación. El informe Pulse of Change de Accenture revela que solo 53% de las empresas se sienten listas para enfrentar estos ataques. Superar este reto requiere ser brillantes en lo básico, visibilidad y protección de datos críticos, priorizar la prevención con pruebas y capacitación continua, y fortalecer la respuesta modelando amenazas en la cadena de valor para la recuperación rápida y escalable".

LUIS PORTA
Director ejecutivo de Accenture Chile

ESTRATEGIAS

"La evolución de las amenazas, los cambios regulatorios, y nuevos enfoques en la gestión del riesgo, obligan a las organizaciones a una continua mejora en sus estrategias para mantener una seguridad corporativa que resguarde sus activos críticos y la resiliencia de sus operaciones. El ransomware, la IA generativa, la creciente adopción de la nube, entornos híbridos y la digitalización empresarial, han ampliado la superficie de exposición al riesgo que debe ser gestionada (...) Las organizaciones deben reforzar sus capacidades de ciberdefensa, priorizando la protección de identidades y datos".

ERNESTO TACHOIRES
Director regional de desarrollo de negocios de ciberseguridad de Sonda.

COORDINACIÓN

"La ley de ciberseguridad y la de protección de datos, junto a regulaciones sectoriales, exigen que las empresas desarrollen programas de seguridad coherentes para responder en forma oportuna. Un desafío clave será armonizar las políticas internas para clasificar y notificar brechas de seguridad, considerando plazos, criterios y autoridades distintas según la normativa aplicable. La automatización de procesos y la inversión en talento serán esenciales para cumplir con estas exigencias y fortalecer la resiliencia".

PAULINA SILVA ABOGADA
Socia de Bitlaw.

CULTURA

"La Política Nacional de Ciberseguridad y la Ley Marco de Ciberseguridad son claves para desarrollar una cultura en Chile, gracias al foco en las buenas prácticas digitales y tecnológicas, y por la Agencia Nacional de Ciberseguridad que deberá regular, fiscalizar y sancionar a entidades públicas y privadas que operan servicios esenciales. En ese contexto, el desafío será reducir la brecha de 35 mil profesionales de ciberseguridad con nuevos especialistas y una mayor participación femenina. Asimismo, desarrollar mayor conciencia en los directorios de empresas".

MARCO ANTONIO ÁLVAREZ
Presidente de la Alianza Chilena de Ciberseguridad

ADOPCIÓN

"El principal desafío será cómo una nueva generación de tecnologías para ciberseguridad se adopta y ejecuta en cada institución. Cumplir con las nuevas regulaciones de protección de datos es esencial para robustecer nuestros sistemas y garantizar la integridad de la información. La implementación efectiva requiere inversión en tecnología, capacitación del personal y una cultura organizacional orientada a la seguridad. Hoy existen soluciones robustas con tecnologías cuánticas para enfrentar ransomware, proteger datos en reposo y en movimiento, e incluso resistir ataques de computadoras cuánticas con algoritmos PQC, evitando penalizaciones, pérdidas monetarias y de reputación. El 2025 es el Año de la Cuántica, porque las organizaciones deberán empezar a revaluar sus sistemas para llevarlos al siguiente nivel".

PAULINA ASSMANN
CEO de SeQure Quantum

IA

"Para 2025 y 2026 será un desafío no menor, porque la inteligencia artificial es un gran avance, es muy positivo para la humanidad, pero también es muy negativo desde el punto de vista para la seguridad de la información y la seguridad de los sistemas y todo lo que significa la infraestructura eléctrica".

JORGE ATTON
Director ejecutivo en Attsons Consulting

ADAPTACIÓN

"Las empresas deberán revisar sus procesos para garantizar el cumplimiento de la ley de protección de datos, que se aplica de manera general, sin distinciones entre empresas esenciales y operadores vitales. Esta ley establece la obligación de implementar medidas de seguridad en el tratamiento de datos, incluyendo medidas técnicas y organizativas que aseguren la confidencialidad, disponibilidad, integridad y resiliencia de los sistemas. Esto implicará inversiones en infraestructura tecnológica robusta, estrategias de ciberseguridad proactivas y formación continua de los colaboradores".

ROMINA GARRIDO
Directora de Protección de Datos Personales de Prieto.

VULNERABILIDAD

"Es fundamental que los directorios evolucionen sus agendas para incluir de manera proactiva la ciberseguridad, no solo como una cuestión técnica, sino como una prioridad estratégica. Deben integrarla en decisiones clave, mitigando riesgos de manera efectiva y alineándose con los objetivos comerciales de la empresa. Por otro lado, es urgente que los directorios y altos ejecutivos comprendan y se capaciten en las normativas vigentes, para cumplir con los requisitos legales y evitar sanciones".

FADUA GAJARDO
Directora ejecutiva del Instituto de Directores de Chile

RESILIENCIA

"Chile enfrentará el desafío crítico de robustecer la resiliencia de infraestructuras críticas, especialmente su cadena de proveedores y suministro, quienes son un blanco más común de ataques. La pregunta hoy no es si estos sistemas serán atacados, sino cuánto será el tiempo de recuperación para garantizar la continuidad operativa de sectores como la banca, energía y logística. El riesgo es acentuado por la interconexión y la heterogeneidad de la ciber-madurez del país. Así, el desafío transversal será romper la lógica de silos y diseñar entrenamientos y prácticas conjuntas que aceleren aprendizajes".

ROCÍO ORTIZ M.
Subdirectora de Industrias del Futuro, Centro de Innovación UC

RESILIENCIA

"Construir resiliencia frente a amenazas cada vez más sofisticadas, aprovechando tecnología avanzada e IA. Los ataques futuros requerirán que las empresas integren agentes inteligentes, analítica y soluciones automatizadas capaces de detectar, analizar y neutralizar amenazas en tiempo real, como predicción de vulnerabilidades mediante aprendizaje automático, respuesta autónoma para aislar riesgos, entre otros. La clave será combinar tecnología con cultura organizacional robusta".

SANDRA GUAZZOTTI
Directora de Empresas y fundadora de Ready to Digital

NORMATIVA

"Los principales desafíos en ciberseguridad serán tres: la acelerada evolución y sofisticación de las ciberamenazas, como los ciberataques a cadenas de suministro o dispositivos IoT; la adaptación a la nueva ley marco que presenta un reto para las organizaciones en capacitación, inversión e infraestructura, y para el Estado crear la Agencia Nacional de Ciberseguridad, y la escasez de talento especializado. Es crucial mejorar la conciencia en ciberseguridad, invertir en formación, tecnología avanzada y cooperación público-privada".

RAFAEL RINCÓN-URDANETA
Líder Objetivos de Desarrollo Digital de Fundación País Digital

RIESGOS

"El riesgo a terceros o riesgo de cadena de suministro o proveedores, es una preocupación crítica y se espera que continúe creciendo. A medida que las empresas externalizan más servicios y dependen de proveedores externos, aumenta el riesgo de que las vulnerabilidades en estos terceros afecten la seguridad de las organizaciones, por lo que se deben realizar evaluaciones exhaustivas de los riesgos de ciberseguridad asociados con sus proveedores, especialmente quienes manejan datos sensibles. Los contratos con proveedores deben incluir cláusulas específicas sobre ciberseguridad y que exijan que los proveedores notifiquen inmediatamente sobre incidentes y colaboren en la resolución".

CAROLINA PIZARRO
Fundadora Red de Mujeres en Ciberseguridad.