



EL MERCURIO

SE CELEBRA EN OCTUBRE:

**Ejecutivos plantean los
desafíos corporativos
en el Mes de la
Ciberseguridad**

FELIPE PALMA, gerente de Servicios de ITQ Latam

SE CELEBRA EN OCTUBRE:

Ejecutivos plantean los desafíos corporativos en el Mes de la Ciberseguridad

Por sexto año consecutivo, Chile festejará el Mes de la Ciberseguridad, instancia propicia para analizar los retos que enfrenta el país en esta materia. Aquí, cuatro ejecutivos se refieren a las tareas pendientes en términos de seguridad informática y a los desafíos corporativos, que van desde la concientización y capacitación de los colaboradores hasta la automatización de controles para el resguardo de datos, entre otros.

DIEGO AGUIRRE

FERNANDA MATTAR,
subgerenta de
Ingeniería de
Ciberseguridad de Entel



“Estamos en el comienzo de una nueva era, en la que el 5G será el primer paso hacia diferentes formas de comunicación entre humano y máquina, siendo la base sobre la cual despegará el verdadero potencial del internet de las cosas. En este punto, debemos ser conscientes de que la ciberseguridad es un punto

medular en el despliegue del 5G, por lo que se vuelve fundamental adoptar buenas prácticas e incorporar la seguridad en todo el ciclo de vida digital. Una de ellas es el diseño de infraestructura de seguridad y la automatización de controles para la protección, resguardo de datos y resiliencia de las telecomunicaciones”.

JAIME CHANAGA,
field CISO en Fortinet
para Latinoamérica y
el Caribe



“Es vital buscar las maneras de disminuir el rezago que existe respecto al entrenamiento y concientización en ciberseguridad para trabajadores, que puede dejar expuestos a los empleados a ataques de phishing, vulnerando la seguridad de los entornos corporativos. Las organizaciones deberían considerar implementar

programas de concientización y capacitación para sus empleados sin importar el área o puesto que desempeñen y asegurar así a las personas, los datos y los dispositivos, sin importar su ubicación, convirtiendo a sus colaboradores en la primera línea de defensa en contra del cibercrimen”.

ERICH ZSCHAECK,
gerente sénior
de Ciberseguridad
de EY



“Uno de los mayores desafíos en los próximos años se encuentra en la cadena de suministro, que es una parte vital de las operaciones empresariales, pero también es un eslabón vulnerable. Con múltiples proveedores y procesos fuera de su control, las empresas deben ser proactivas. Realizar

auditorías de seguridad en proveedores, gestionar el acceso a sistemas críticos y educar a los proveedores sobre buenas prácticas de ciberseguridad son acciones esenciales. La seguridad de la cadena de suministro es esencial, ya que cualquier eslabón débil puede poner en peligro toda la cadena”.

FELIPE PALMA,
gerente de
Servicios de
ITQ Latam



“La inteligencia artificial nos genera una gran posibilidad de robustecer las capacidades de identificación, detección y repuesta ante amenazas, pero también ha traído una serie de nuevas herramientas para que los ciberdelincuentes puedan utilizar técnicas avanzadas de ingeniería social, como las deepfake para generar contenido malicioso con videos falsos

muy realistas que aumentan las posibilidades de comprometer a las organizaciones a través de los usuarios finales. El desafío es colaborar de la mano de los avances tecnológicos para la ciberseguridad, sabiendo cómo usarlos y dónde integrarlos para optimizar los resguardos y disminuir la superficie de ataque en las organizaciones”.