LITORALPRESS

Fecha: 19-06-2024
Medio: El Pingüino
Supl. : El Pingüino
Tipo: Noticia general
Título: **Especialistas en ciberseguridad y su relevancia actual**

Pág. : 9
Cm2: 231,6

Tiraje: 5.200
Lectoría: 15.600
Favorabilidad: No Definida

La columna de...

BENJAMÍN TOSELLI,
PRESIDENTE EJECUTIVO DE IT HUNTER INTERNATIONAL

Especialistas en ciberseguridad y su relevancia actual

Por estos días, los datos representan uno de los activos más valorados por las organizaciones y personas, siendo muy relevante el papel de expertos en ciberseguridad. De hecho, una brecha de seguridad en una empresa o institución puede generar pérdidas financieras, daños en su reputación y/o comprometer su información sensible.

Dada la transformación digital y el avance de las tecnologías emergentes, entre ellas la Inteligencia Artificial (IA), las áreas posibles de sufrir un ciberataque también están aumentando. Lo anterior exige que los profesionales y expertos ligados a la seguridad informática se mantengan actualizados respecto de las últimas tendencias y ciberpeligros que vayan emergiendo, para así adecuar sus estrategias y tecnologías antes las nuevas amenazas.

Si bien hoy existe un déficit no menor de especialistas TI en Chile (más de 10 mil al año), dicha escasez también afecta a los perfiles en ciberseguridad. De acuerdo a nuestra "XI Guía Salarial TIC - 2023", las principales posiciones ligadas con esta área corresponden a las de Gerente de Seguridad, Subgerente de Ciberseguridad, Oficial de Seguridad e Ingeniero de Ciberseguridad. Se trata de cargos que pueden percibir remuneraciones líquidas que van desde 1,9 millones hasta 8,5 millones de pesos mensuales, dependiendo del tamaño de la organización.

A nivel de responsabilidades de los profesionales de la Ciberseguridad, podemos afirmar que son variadas y están vinculadas con:

· La implementación de soluciones de seguridad para las diferentes áreas o departamentos de una organización, tales como antivirus, firewalls, y sistemas para la prevención y detección de intrusiones, por dar algunos ejemplos.

· La evaluación de las vulnerabilidades, con el fin de identificar las debilidades de la infraestructura y proponer correcciones.

· El cuidado de los datos, es decir, relativas a la infraestructura digital, redes, sistemas, aplicaciones y datos.

· La detección y respuesta a las amenazas informáticas, para lo cual es esencial el monitoreo constante de la red corporativa, a través de herramientas que detectan las intrusiones.

· El fomento de una mayor conciencia sobre el tema, mediante programas de capacitación que eduquen a los colaboradores en torno a las mejores prácticas y la relevancia de la ciberseguridad, así como sobre las últimas tendencias y amenazas.

· El desarrollo de políticas de seguridad informática, que establezcan prácticas y procedimientos que disminuyan el riesgo de incidentes.

· La gestión de incidentes de seguridad, con miras a investigarlos, mitigarlos y recuperar la normalidad en las operaciones de la empresa en el menor plazo posible.

· La actualización tecnológica, respecto de los últimos avances TI y soluciones de seguridad informática, así como sobre los riesgos más recientes en este ámbito.

· El cumplimiento de la legislación actual, según los estándares de seguridad de la industria donde se encuentre la organización.

En el fondo, el rol de estos especialistas es crucial en materia de protección de la infraestructura digital de una organización, lo que demanda una gran dedicación y la capacidad para adaptarse a un enorme volumen de ciberamenazas que son mutantes y cada vez más complejas.