LITORALPRESS

Fecha: 05-06-2025
Medio: El Mercurio de Calama
Supl. : El Mercurio de Calama
Tipo: Noticia general
Título: **Recomendaciones urgentes en ciberseguridad**

Pág. : 12
Cm2: 224,2

Tiraje: 2.400
Lectoría: 7.200
Favorabilidad: No Definida

Columna

Iván Jirón Araya
Departamento de Matemáticas UCN

Recomendaciones urgentes en ciberseguridad

Recientemente asistí en Santiago a la conferencia y exposición internacional "Summit Cyber & Technology South America 2025", organizada por el diario El Mercurio en conjunto con la red Cybertech, donde se llevaron a cabo charlas y paneles con la participación de expertos reconocidos a nivel mundial, además de una exposición de productos y soluciones tecnológicas ofrecidas por destacadas empresas en el ámbito de la ciberseguridad. Este encuentro internacional se ha celebrado desde el año 2014 en ciudades como Singapur, Tokio, Roma, Panamá, Los Ángeles, Washington D.C. y Toronto.

"Se debe promover la notificación y el reporte de incidentes y ataques sufridos, junto con las estrategias aplicadas".

En este evento se realizaron numerosas recomendaciones en materia de ciberseguridad que resultan de gran utilidad para organizaciones y empresas, como por ejemplo elaborar un documento que oriente claramente las buenas prácticas; y que, al utilizar la inteligencia artificial (IA) es fundamental considerar tres escenarios específicos: la ciberseguridad aplicada a la IA, la IA utilizada para mejorar la ciberseguridad, y los riesgos del uso indebido de la IA.

Asimismo, se debe asumir que todas las organizaciones enfrentarán, al menos una vez, algún tipo de ciberataque; además de reconocer que en esta área el eslabón más débil suele ser el factor humano; por lo tanto, es esencial educar y concientizar continuamente en materia de ciberseguridad. Junto con ello, hay que proteger los propios perímetros, asegurando que los proveedores también implementen medidas adecuadas.

Otra recomendación es contar con un plan integral -reactivo y proactivo- para la gestión de crisis, que aborde los aspectos tecnológicos y humanos involucrados, y que involucre simulacros. Durante una crisis es indispensable disponer de medidas efectivas que permitan responder rápidamente y mantener operativos los procesos esenciales mientras se mitiga la amenaza.

Se debe promover la notificación y el reporte de incidentes y ataques sufridos, junto con las estrategias aplicadas para enfrentarlos, a fin de compartir conocimientos valiosos que puedan beneficiar a otras instituciones; así como fomentar una cultura sólida de ciberseguridad como una práctica cotidiana, no sólo durante situaciones críticas; y gestionar respaldos frecuentes de datos e información en medios inmutables que garanticen iniciar la recuperación de operaciones.

Finalmente, es deseable diseñar e implementar una estrategia efectiva de comunicación en situaciones de crisis, que incluya claramente quién lidera la gestión, los puntos de contacto designados, el equipo responsable y los procedimientos para generar reportes precisos sobre incidentes e identificar vectores de ataque; además de que todas las organizaciones deben considerar la rotación regular de empleados como un factor de riesgo y, por lo tanto, debe ser incluida como parte de sus prácticas de seguridad para reducir riesgos internos.