CAS-CHILE®

LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

Cas-Chile® Conecta a las **Municipalidades** del País.

¿Por qué es importante la Ciberseguridad?

Marín Nº 0586 - Providencia | **Mesa Central:** + 600 570 00 20
Ventas: ventas@caschile.cl | **Comunicaciones:** comunicaciones@caschile.cl

Eran las 23:40hrs. Del 7 de abril del 2018 cuando los habitantes de Dallas se vieron sobresaltados por sirenas que solo se activan en caso de tornados o fuertes tormentas. A pesar del cielo despejado de aquella noche, esas 155 alarmas repartidas por toda la zona, no pararon de sonar durante casi dos horas, lo que desencadenó caos entre la población.

¿Qué había pasado? El sistema de sirenas de la ciudad había sido hackeado. Este es un caso ligado a la ciberseguridad. Cada día se hace más difícil resguardar nuestros sistemas de ataques por parte de hackers.

La empresa Trend Micro, ha elaborado una lista de pasos para comprobar la ciberseguridad en las organizaciones:

- Realizar test de penetración.
- Elaborar Acuerdos de Nivel de Servicio o SLA, con sus proveedores de tecnología.
- Establecer un equipo de respuestas a emergencias (CERT en inglés).
- Asegurar la coherencia y seguridad de las actualizaciones de Software.
- Encriptar las comunicaciones.
- Diseñar un sistema tolerante a fallos.
- Garantizar la continuidad de los servicios.
- Resguardar la privacidad de los datos.

Nuestras instituciones deben velar por su seguridad y tomar todas las medidas necesarias para implantar plataformas y soluciones de ciberseguridad. No olvidar que cualquier dispositivo conectado a la red puede ser atacado.

En Chile, se aprobó la Política Nacional de Ciberseguridad que tiene como objetivo resguardar la seguridad de las personas y sus derechos en el ciberespacio.

Últimamente, hemos visto casos de ciberataques en nuestro país, como a Correos de Chile (con el robo de datos de 14 mil tarjetas de crédito) y a Banco de Chile, con la pérdida económica de US $10MM.

Debemos tener en claro que la ciberseguridad debe ser una preocupación de todos, porque puede traer como consecuencia que las empresas pierdan clientes, su reputación caiga, que los empleados pierdan sus trabajos, los contribuyentes pierdan privacidad y su dinero.

Cada institución u organización debe desarrollar una cultura de ciberseguridad a través del desarrollo del capital humano. Las organizaciones deben contar con especialistas en ciberseguridad y tener la estructura adecuada que les permitan enfrentar cualquier incidente en seguridad de la información de la manera más expedita y rápida.

Hoy en día se están incorporando una serie de tecnologías donde la ciberseguridad tendrá mucho que decir, como BYOD (Bring Your Own Device), Cloud Computing, Big Data y la Internet de las Cosas (IoT).

Recomendación: libro de Ciberseguridad, La Protección de la Información en un Mundo Digital. Fundación Telefónica, 2016, editorial Ariel S.A.

Daniel P. Valdés Gómez