
El adoptar **medidas de ciberseguridad, así como proteger datos y redes informáticas** puede ser vital para evitar que empresas y organizaciones sean víctimas de un ciberataque, señaló **Miguel González,** coordinador de Identidad y Privacidad del Tec de Monterrey.

*“A simple vista, la **ciberseguridad** no es tan palpable como los riesgos del mundo físico, como dejar la puerta de la casa abierta o nuestros documentos donde cualquiera los pueda tomar",* alertó el experto.

Cotidianamente, las personas ingresan información a sus computadoras o teléfonos, como **contraseñas** o **números de tarjetas bancarias**, algunas veces sin cuidar aspectos de **seguridad**.

El experto comparte conceptos importantes de seguridad informática y lo que puedes hacer para prevenir **vulnerabilidades** en tus **equipos** o tu **información digital.**

## La magnitud del daño determina si es incidente o brecha

Casi en el 70% de los casos, los ataques son perpetrados por actores externos como ***hackers* y grupos cibercriminales**.

La información que manejas en tu empresa, como **credenciales, usuarios, contraseñas, bases de datos o números de cuentas** es el objetivo de estos piratas informáticos.

El experto dijo que el daño o riesgo que pueda llegar a sufrir tu empresa en sus sistemas informáticos se puede identificar según su magnitud. Estas se clasifican como: **incidentes y brechas.**

### - Incidente de ciberseguridad

Este se da cuando es detectado uno o varios eventos que pudieran **comprometer o generar vulnerabilidad de la información**, su confidencialidad e incluso su disponibilidad para los diferentes procesos de tu negocio.

### - Brecha

Se determina en condiciones donde se ha **confirmado el daño**, que hubo una exposición, mal uso, robo o también cambio de datos de tu empresa.

## Los tipos de ciberataques más comunes

Los *hackers* pueden perpetrar un ataque a través de **técnicas de engaño** (también conocida como **ingeniería social**) y **códigos maliciosos (malware)** para crear vulnerabilidades en tus archivos y sistemas informáticos.

Entre las técnicas más comunes que usan los hackers están **virus, gusanos, troyanos y ransomware** para secuestrar tus datos o redes informáticas completas; además del ***phishing*** que es un **fraude por correo electrónico** o incluso por llamadas telefónicas o mensajes SMS.

También están los **ataques DDoS (denegación de servicio distribuido)** que saturan la capacidad de tus servidores o los **ataques XSS (Cross-Site Scripting)** que introducen códigos maliciosos desde páginas web.

## Errores humanos: otra fuente de vulnerabilidad

Los ataques de seguridad no siempre son ejecutados por *hackers*, también pueden ocurrir por **vulnerabilidades generadas por errores humanos** ante la falta de una cultura de ciberseguridad.

Alrededor del **30% de los incidentes pueden ocurrir a causa de errores humanos** que pueden ser prevenidos a través de acciones sencillas.


## Consejos para contraseñas seguras y otras medidas de ciberseguridad

El experto recomendó las siguientes **medidas de ciberseguridad:**

- Tener computadoras y equipos móviles con las últimas **actualizaciones de seguridad instaladas**.

- Implementar **contraseñas con varios niveles de seguridad** y uso de más de 10 caracteres, como el uso de mayúsculas, minúsculas, números y algunos signos.

- Evitar **contraseñas que contengan información personal** del usuario, por ejemplo, fechas de nacimiento.

**- Cambia las contraseñas** de manera frecuente **cada 3 o 6 meses.**

- Evitar utilizar las mismas **contraseñas y passwords en varias plataformas**.

- No abrir **correos sospechosos,** con mensajes engañosos como premios o noticias no esperadas.

- No dar **click a links o abrir archivos adjuntos** de mensajes que parezcan **sospechosos.**

- Evita **instalar software gratis** o que haya sido descargado de **páginas poco confiables.**

- Respalda la información importante usando **herramientas que tengan protección contra malware**.

- Implementa una **autenticación con pasos adicionales**, por ejemplo, con **Google Authenticator** o **Microsoft Authenticator.**

*“Pequeños pasos como **cambiar passwords**, no repetirlos en diversos sitios, usar **factores de autenticación** y **desconfiar de sitios** y **ofertas increíbles** que nos puedan*

*instalar cosas en nuestros dispositivos, son un gran avance para* ***proteger tu información****",* comentó González.

Incluso datos que aparentemente no puedan ser de utilidad para un ciberdelincuente pueden ser **vendidas en el mercado negro** a otros delincuentes con diferentes intereses, alertó el experto.

En el peor de los casos, con esta información, **los delincuentes pueden tomar el control** de tu red informática. Así, pueden restringir el acceso, cambiar información o incluso **secuestrar tu sistema**.

Tan solo en 2020, la **Lotería Nacional**, el **ISSSTE**, el **Banco de México**, el **SAT** y **Pemex** fueron algunas de las dependencias mexicanas que **sufrieron ciberataques,** que incluso dejaron **expuesta la información de usuarios**.

***"Cambiar passwords, no repetirlos en diversos sitios, usar factores de autenticación y desconfiar de sitios y ofertas increíbles (...) son un gran avance para proteger tu información".***

## Tecnologías para fortalecer tu ciberseguridad

Pese a que algunos ataques son a causa de la tecnología o utilizan esta vía, también hay herramientas o **aplicaciones que pueden servir para fortalecer tu seguridad** y prevenir vulnerabilidades en tus servidores.

**- Firewalls de última generación** para bloquear el acceso a intrusos y ataques desde otras redes.

**- Escáners** para analizar y detectar **vulnerabilidades de seguridad.**

**- Web Application Firewall (WAF)** para proteger tu servidor de ataques a través de aplicaciones web y el tráfico HTTP.

**- Administrador de usuarios privilegiados** con sistemas avanzados de autenticación y almacenamiento de sus credenciales en un entorno seguro.

- Programas antivirus actualizados con herramientas para **detectar y eliminar malware y ransomware.**

**Con información de Kaspersky y Verizon.*