Proteger datos para sobrevivir como empresa: cinco consejos básicos

En un mundo cada vez más **digitalizado** y donde el **intercambio de información** sobrepasa las expectativas planteadas hace unos años, la ciberseguridad es un tema que nos tiene que interesar a todos los niveles.

Según *Radware*, proveedor de balance de carga y servicios de **ciberseguridad** para centros de datos, se estima que el 80 por ciento de las empresas reciben algún tipo de ataque cibernético.

Además se informa que el **costo** para una organización que no tuvo precaución de protegerse, superó en 2019 el **millón y medio de dólares**.

México es el tercer país con más **ciberataques** en el mundo, sólo detrás de Estados Unidos y el Reino Unido, indica el **Sistema Económico Latinoamericano y del Caribe** (SELA).

En el marco del **Día Internacional de la Internet Segura**, que se celebra el 10 de febrero, el director del **Hub de Ciberseguridad**, del Tec de Monterrey, Félix Barrio comparte cinco **consejos** para tomar más conciencia del uso seguro de nuestros datos.


width="900" loading="lazy">

1.- Es necesario **controlar los accesos** a los equipos de cómputo, las bases de datos y, en general cualquier sistema que almacene información en nuestras organizaciones.

Esto significa **asignar permisos** a los usuarios con claves y contraseñas robustas, que periódicamente se revisen y modifiquen.

Esto reducirá los riesgos de que un atacante pueda suplantar a los usuarios y obtener acceso a los equipos.

2.- Resulta esencial **realizar copias de seguridad** de los datos frecuentemente, de modo programado y siempre en un almacenamiento externo a la red corporativa, para poder recuperar aquellos en caso de un desastre.

3.- Las empresas deben **prever la destrucción** y borrado de los datos que ya no son necesarios, desechando los equipos y soportes obsoletos conforme procedimientos estandarizados que impidan su recuperación y uso por terceros.

4.- **Utilizar** algún tipo de **software** para cifrar los datos de los equipos para evitar fugas de información si se extravían los equipos por parte de los empleados, y para dificultar a los ciber atacantes la lectura de los datos en el supuesto de que accedan a nuestras redes y sistemas.

5.- Debemos de **apoyarnos en nuestros servicios jurídicos y legales** para que establezcan cláusulas y acuerdos claros y transparentes, tanto para nuestros clientes como para nuestros empleados.

Estas cláusulas ayudarán a **mitigar el riesgo** de que empleados o terceros hagan un uso inadecuado de la información y mejoren el tratamiento de los datos personales.

También **evitará** a la empresa el disgusto de **recibir sanciones** de tipo legal e incluso penal por no cumplir con la obligación de proteger adecuadamente los datos que maneja.

SEGURAMENTE QUERRÁS LEER TAMBIÉN: