

# 5 hábitos para evitar ciberataques

Se producen ciberataques cada día, y la existencia este año de ataques muy sonados como el **WannaCry, en mayo, y el Petya, en junio**, han hecho a los ciudadanos más conscientes de la necesidad de protegerse. Recuerda la empresa Datos 101 que “estos ataques online afectan tanto a grandes como pequeñas empresas y ocasionan resultados muy negativos: pérdidas de datos, robos de información, perjuicio económico, etc”. Y destaca 5 buenos hábitos a considerar:



1. **Formar a los empleados.** La primera barrera para que el ataque no afecte al sistema es el propio empleado o usuario. “Los trabajadores deben estar informados y formados para no abrir nada que pueda ser un peligro para la empresa”. Muchos estudios apuntan a que gran parte de los ataques se ejecutan por culpa del usuario desinformado.

2. **Copias de seguridad.** Las copias de seguridad fuera de la base de datos son la solución más eficaz para luchar contra la amenaza de **ransomware, Cryptolocker** y la ciberdelincuencia en general.

3. **Equipos actualizados.** Es habitual que los ciberataques se cuelen por fisuras de seguridad que tienen los **softwares**. “En muchas ocasiones **los fabricantes corrigen esos errores, bugs y vulnerabilidades en actualizaciones, de ahí que la importancia de instalarlas por básicas que nos parezca**. Por supuesto, la actualización del equipo debe ir acompañada de un buen antivirus que también esté actualizado”, dice el informe.

4. **Contraseñas indescifrables.** Por miedo a olvidarnos, es **común usar contraseñas como el año de nacimiento**, el nombre de nuestros hijos o el equipo de fútbol. Para crear una contraseña fuerte es conveniente que incluya letras y números así como mayúsculas, minúsculas y algún símbolo.

5. **Dispositivos extraíbles.** Smartphones, smartwatches, usb... son una puerta de acceso a las empresas. Es común que simplemente para cargar la batería conectemos dispositivos a los ordenadores, sin embargo, **esta acción puede suponer un riesgo para el sistema de seguridad ya que pueden actuar como vía de acceso para los ciberdelincuentes**.