

Cinco elementos clave para el plan de seguridad de PC

Sin un plan de seguridad interno para los equipos de la empresa, cualquiera de la oficina puede consultar todos los archivos que se almacenen en ellos, incluso documentos de estrategia, archivos financieros o fichas de personal. Seguro que no es eso lo que quiere. Y, a pesar de ello, muchos pequeños empresarios carecen de un plan de estas características y acaban por pagar las consecuencias. Así ponen en peligro la información de su negocio pero, además, corren el riesgo de faltar a su compromiso de confidencialidad con empleados y clientes.

Es preciso formalizar un plan de seguridad para PC sencillo de entender y aplicable por parte del personal.

A continuación explicamos cinco actuaciones básicas que se deben incorporar al plan de seguridad.

1. **Emplear protección con contraseñas**

Al proteger los archivos con contraseñas, se garantiza que sólo los abran los usuarios que estén autorizados para ello. Con casi absoluta certeza, su sistema operativo dispone de un sistema integrado de protección con contraseña y la mayoría de aplicaciones de software, también Microsoft Office, permite proteger los archivos y las carpetas mediante palabras clave.

2. **Elegir contraseñas imaginativas**

Hay que prohibir el uso del nombre del cónyuge, del hijo o del perro, por ejemplo, como contraseñas. El motivo es que los demás empleados los saben y no tardarían en adivinar la contraseña. Igual sucede con cumpleaños, direcciones, cantantes o grupos preferidos u otras palabras que se asocian fácilmente al interesado. Además, recuerde que resulta más complicado averiguar contraseñas compuestas de cifras y letras en mayúscula y minúscula o si se cambian con frecuencia. Facilite el uso de contraseñas dando instrucciones a todo el personal sobre cómo crearlas, cuándo cambiarlas y cómo proteger archivos y carpetas.

3. **Usar la función de cifrado**

Una manera de proteger la información valiosa guardada en los equipos informáticos de la empresa consiste en cifrar los datos. El software de cifrado convierte los datos en cadenas ininteligibles que se descifran con una clave. Este tipo de software se suele emplear para estos fines: restringir el acceso a archivos confidenciales como informes financieros o listas de clientes; salvaguardar los equipos portátiles para su uso fuera de la oficina; u ocultar mensajes confidenciales de correo electrónico.

4. **No dejar datos a la vista**

Algo tan sencillo como recordar al personal que cierre los archivos en uso cuando se aleje de su mesa resulta útil para reducir los riesgos de seguridad. Si no se toma esta precaución, la hora del almuerzo se transforma en una invitación para que cualquiera que pase lea los archivos abiertos. Favorezca la seguridad de los equipos con normas que exijan a los empleados cerrar los documentos que no les sirvan en el momento.

5. **Limitar los ataques a dispositivos portátiles**

El uso de equipos portátiles aumenta la productividad pero, al mismo tiempo, amenaza la seguridad de la empresa si no se toman las precauciones adecuadas. Avise a quienes trabajen a distancia de que no deben olvidar la seguridad fuera de la oficina; por ejemplo, una medida sencilla sería elegir un tipo de letra pequeño cuando trabajen en papeles confidenciales en lugares públicos como cafés o aviones. Si los empleados utilizan recursos tecnológicos públicos, enséñeles a asegurarse de que los documentos permanezcan en el disco duro del portátil y no en los equipos del recurso. Asimismo, el cifrado supone una medida más de seguridad en portátiles que se usan fuera de la oficina. Si roban un equipo pero el software de cifrado está activo, el ladrón no podrá leer los documentos guardados en él.