

# 7 errores que no debe cometer en sus equipos informáticos

## 1. No deje que cualquiera toque

Existen una gran cantidad de supuestos “entendidos” en sistemas informáticos, incluso puede que alguien con parentesco cercano tenga conocimientos de usuario avanzado, pero tenga en cuenta que estos conocimientos de ámbito doméstico no los capacitan para resolver cualquier problema, sobre todo si los equipos o programas afectados son de índole empresarial.

Tenga también en cuenta que es relativamente fácil provocar pérdidas IRREPARABLES de datos si se manipulan de forma incorrecta archivos de cualquier tipo, como también es posible que un tratamiento incorrecto de una avería puede suponer aumentar sensiblemente el trabajo del técnico que, al final, acaba por hacerse cargo del problema.

Recuerde, aunque sea bienintencionado, es peligroso que cualquier persona no capacitada opere en sus ordenadores.

## 2. No realizar copias de seguridad

Como todos conocemos, las máquinas tienen la posibilidad de averiarse. Los equipos informáticos, dada su complejidad, son más susceptibles de dejar de funcionar por fallos mecánicos, eléctricos o electrónicos. Algunos de estos fallos pueden provocar la pérdida de TODA la información almacenada.

Pero, estadísticamente, la mayoría de las averías en computadores son fallos de software, es decir, infecciones víricas, uso incorrecto de las aplicaciones, actualizaciones mal realizadas, etc. Todos estos fallos son atribuibles al factor humano.

En menor medida afectan a nuestra informática las contingencias propias de cualquier otro bien: robos, golpes, incendios, inundaciones...

Cualquiera de las fatalidades anteriores afectan a los datos contenidos en sus equipos, estos datos son, muchas veces, el efecto más valioso de la organización, es por esto que la pérdida de información es la más irreparable que podemos sufrir.

Es relativamente sencillo establecer un sistema de copias de respaldo para que, pase lo que pase, nuestros ficheros estén a salvo, y podamos recuperarlos. La copia de seguridad ideal es la que permite volver al estado anterior a la catástrofe, aunque estemos en otra ubicación y con equipos distintos.

Desde Infoestrella aconsejamos realizar, al menos, una copia en un soporte distinto al original y otra en una ubicación distinta a la de trabajo (Internet, por ejemplo). La frecuencia del respaldo ha de programarse en función de los datos y como éstos varían. Estas copias se realizan de forma automática, evitando así el factor humano (olvidos).

De forma periódica hemos de comprobar que nuestra copia de respaldo se está realizando correctamente, realizando una restauración de los datos. Se han dado multitud de casos en los que, durante años, se ha estado realizando una copia de seguridad que ha resultado inservible el día que ha hecho falta.

### **3. No realizar mantenimiento de nuestros programas**

En nuestros ordenadores usamos multitud de aplicaciones para todo tipo de tareas, éstas se quedan obsoletas por multitud de razones: nuevas amenazas de seguridad, nuevas funcionalidades, cambios de legislación en programas de gestión y contabilidad...

Quizás la razón más importante para mantener nuestro software al día es que si queremos compartir información con otros usuarios, hemos de trabajar con las mismas versiones de los programas que usan la mayoría, si no nos encontraremos con problemas a la hora de trabajar en equipo.

Especialmente importante es tener nuestro sistema operativo (sea cual fuere) actualizado, bien por las mejoras que vayan apareciendo, bien por los parches de seguridad que se vayan aplicando.

### **4. Instalar demasiadas aplicaciones**

Dada la curiosidad por probar otras herramientas, los usuarios informáticos somos dados a instalar en nuestro ordenador multitud de programas recomendados por otros usuarios, o por simple curiosidad.

Los archivos utilizados por estas aplicaciones van llenando progresivamente nuestro disco duro y añadiendo información inútil a los registros de nuestros sistemas operativos, ralentizando nuestro equipo.

Incluso si desinstalamos las aplicaciones siempre quedan rastros que bajan el rendimiento del sistema.

Por todo esto, recomendamos encarecidamente tener instaladas sólo las aplicaciones que necesitamos en nuestros puestos de trabajo.

### **5. Confiado en internet y e-mail**

Internet y el correo electrónico se han posicionado como herramientas indiscutibles para nuestro trabajo diario. A la vez son la mayor fuente de problemas para los sistemas de información. Un uso descontrolado puede desbaratar, en pocos minutos, horas de trabajo.

Hay una simple norma en el uso de información proveniente de internet: desconfianza TOTAL. Realmente no sabemos quién está al otro lado de esa web de descarga de software “gratuito”, como tampoco conocemos las intenciones de la persona que ha confeccionado ese correo electrónico tan entretenido.

Normalmente usamos unas pocas páginas webs en el trabajo: bancos, proveedores, fabricantes... Pues intentemos no salirnos de estas páginas, que ya conocemos, para explorar por sitios en los que no sabemos qué nos vamos a encontrar. Sólo hay que aplicar la lógica que usamos cuando vamos por la calle: en un banco no nos van a intentar estafar (normalmente), ya que perderían clientes y reputación. Pues en su página web siguen la misma política. En el lado opuesto nos encontramos con sitios de descarga de programas “gratuitos” y relacionados con actividades ilícitas. Aquí no es de extrañar que intenten estafarnos, robarnos o, en el mejor de los casos, sólo fastidiarnos.

Si realiza descargas y utiliza programas P2P asuma la responsabilidad de que cualquier descarga conlleva un riesgo y que está introduciendo al enemigo en casa. La única protección es tener el antivirus actualizado y las copias de seguridad al día, y aún así es más que probable que sufra alguna infección de forma periódica.

Precauciones con el correo electrónico: Por principio, desconfíe de todo y de todos.

- No abra ningún correo del que no reconozca al remitente, o incluso si lo conoce pero el asunto suena raro (en otro idioma, por ejemplo). Bórrelo directamente sin almacenarlo en la papelera de reciclaje.
- Desactive la vista previa en su cliente de correo.
- No participe en cadenas de correo tipo “si envía este email a 10 de sus amigos...”. El 99,999% son mentira y sólo sirven para captar direcciones de correo a las que luego se le envía publicidad.

## **6. No establecer contraseñas seguras**

Una correcta política de acceso hace casi inexpugnable a nuestro sistema. Una contraseña robusta ha de:

- Incluir números y letras, mayúsculas y minúsculas
- No tener ningún significado, para evitar los ataques por el “método diccionario”
- No ser igual a ninguna otra contraseña que usemos en otro sitio
- Ser cambiada periódicamente
- Sólo es conocida por los usuarios autorizados
- No es introducida en equipos públicos (ciber cafés, portátil del vecino...) para evitar que se quede almacenada
- No estar anotada en un fichero en nuestro ordenador llamado “contraseñas.doc”. En todo caso en papel guardado en un cajón bajo llave.

Somos conscientes de la dificultad de cumplir estas normas, pero mientras más nos acerquemos a la contraseña ideal, más difícil se lo pondremos a piratas que deseen acceder a nuestros datos.

## **7. Antivirus inexistente o inadecuado**

Sobre todo si usamos sistemas operativos Microsoft, nuestros equipos son susceptibles de ser atacados por miles de virus que pululan por la red y ponen en peligro nuestros datos. De aquí la necesidad de contar con una solución antivirus que haga de primera barrera ante los ataques.

No es necesario realizar un gran desembolso para protegernos, es más, existen varias soluciones gratuitas igual de eficaces (o mejores) que las de pago. A tener en cuenta que el antivirus, para que cumpla su función, ha de estar al día, con lo que es imprescindible configurar correctamente las actualizaciones y tener la licencia en regla.

Usuarios extremadamente precavidos optan por instalar más de una aplicación antivirus. Supuestamente la lógica nos dice que es una opción correcta, pero en la práctica resulta desastroso para nuestro sistema. En muchas ocasiones los dos programas se detectan como infecciones y se atacan mutuamente, teniendo un resultado fatal para nuestro equipo. En el mejor de los casos veremos mermado considerablemente el rendimiento de nuestra máquina sin ninguna mejora de seguridad.

Es más que aconsejable complementar a nuestro antivirus con un cortafuegos, también disponibles con licencia freeware y, si lo requieren nuestras necesidades, alguna solución antispam.

Aun cuando cumplamos todas las normas anteriores con respecto a nuestras protecciones, no debemos bajar la guardia, ya que el antivirus perfecto aún no se ha inventado y siempre existen ataques e infecciones que pueden saltar la barrera.

Es altamente recomendable que no cometa ninguno de estos 7 errores si quiere que sus sistemas informáticos de verdad le ahorren trabajo y le produzcan satisfacciones. La mayoría de las averías atendidas por servicios técnicos son ocasionadas por alguno de los fallos anteriores, siempre atribuibles al factor humano.

Si usted no posee los conocimientos necesarios para realizar estas tareas, es aconsejable que acuda a un servicio con personal técnico profesional. Aplicamos el símil del coche: Si quiere que su vehículo funcione correctamente, le realiza las operaciones de mantenimiento aconsejadas (aceite, neumáticos...) y las reparaciones las atiende un mecánico de confianza, no el hijo de la vecina.

*“La precaución y la sopa no le hacen daño a nadie” (Dicho popular)*