# 10 Consejos prácticos para mejorar la seguridad informática

Las buenas prácticas de mantenimiento de computadoras no solo certificarán que tu ordenador funcione de manera óptima, sino que la **seguridad informática** que tengas, también protegerá tus valiosos datos de las amenazas.

Al igual que conseguir un cambio de aceite para tu automóvil, **el mantenimiento de tu ordenador es crucial para conservar las buenas condiciones de funcionamiento en tus aparatos.**

## Antes de tener acceso a internet mantén la seguridad informática de tus dispositivos al día

La evolución del uso de herramientas de las tecnologías de información y **el despliegue de Internet** r**equieren que establezcas sistemas de búsqueda altamente desarrollados.**

Sin embargo, **con el flujo creciente de información viene una mayor exposición a los ataques cibernéticos**, y debes tener un sistema de seguridad apropiado para proteger tus datos y tu red.

Ya que actualmente estás en confinamiento por la crisis del coronavirus y se te hace más fácil estar conectado a la red, puedes estar más propenso a riesgos por ciberdelincuentes, que podrían atacar tus ordenadores, móviles y tabletas.

Si a causa de la crisis de la pandemia debes teletrabajar de manera intensiva, **es importante que tengas en cuenta el grado de riesgo por el que pueden pasar tus datos.**

## Consejos de mantenimiento de dispositivos

Pero si no estás seguro por dónde empezar, a continuación se desglosan **10 consejos para el mantenimiento de tus dispositivos y la seguridad informática**, tanto a modo personal como a nivel empresarial.

### 1- Mantén el software actualizado

La instalación de actualizaciones de software para tu sistema operativo y tus programas es fundamental. **Instala siempre las últimas actualizaciones de seguridad para tus dispositivos.**

La mayoría de los sistemas operativos de las computadoras tienen medidas de seguridad integradas, por lo que **las actualizaciones a menudo incluirán mejoras en la seguridad de tu computadora**, así como correcciones de errores para tu sistema operativo.

**Mantenerte actualizado asegura que tu ordenador y tus datos están protegidos tanto de las amenazas de ciberseguridad, como de los problemas del sistema.** Utiliza navegadores web como Chrome o Firefox que reciben actualizaciones de seguridad, automáticas y frecuentes.


***Te puede interesar: 13 Consejos para proteger nuestro teléfono móvil***

### 2- Evita las estafas de phishing

Debes tener cuidado con los correos electrónicos y llamadas telefónicas sospechosas. **Las estafas de phishing son una amenaza constante.**

Los ciberdelincuentes intentarán engañarte para que divulgues información personal, como tu identificación de usuario y contraseña, información bancaria o de tarjeta de crédito.

Los engaños de phishing se pueden llevar a cabo por teléfono, mensaje de texto o sitios de redes sociales, pero más comúnmente por correo electrónico. **Sospecha de cualquier mensaje de apariencia oficial que solicite información personal o financiera.**

**3- Practica una buena gestión de contraseñas**

**Un administrador de contraseñas puede ayudarte a mantener tus rúbricas únicas y sólidas para todas tus cuentas.** Estos programas pueden generar contraseñas seguras, ingresar credenciales automáticamente y recordarte que actualices las claves periódicamente.

**Enfatiza la importancia de tener una contraseña segura. Utiliza más de 10 caracteres de complejidad y no los utilices en varios sitios.**


**4- Mucho cuidado a lo que haces clic**

Evita visitar sitios web desconocidos o descargar software de fuentes no confiables. **Estos sitios suelen alojar malware que se instalarán automáticamente (a menudo de forma silenciosa) y pondrán en peligro tu ordenador.**

Es recomendable usar Click-to-Play, funciones complementarias del navegador, que impiden la descarga automática de contenido de complementos (por ejemplo, Java y Flash) que pueden albergar códigos maliciosos.

**5- Nunca dejes los dispositivos desatendidos**

La seguridad física de tus dispositivos es tan importante como tu seguridad técnica. **Si necesitas dejar tu computadora portátil, teléfono o tableta durante un período de tiempo, ciérralo para que nadie más pueda usarlo.**

Si mantienes los datos protegidos en una unidad flash o un disco duro externo, asegúrate de que estén cifrados y bloqueados también. **En el caso de las computadoras de escritorio, bloquea la pantalla o apaga el sistema cuando no esté en uso.**

**6- Salvaguardar los datos protegidos**

**Mantén los datos protegidos con los que entras en contacto y tus restricciones asociadas.** Revisa el estándar de clasificación de datos para comprender los requisitos del nivel de protección de los mismos.

**Conserva los datos protegidos de alto nivel (por ejemplo, SSN, información de tarjetas de crédito, registros de estudiantes, información de salud, etc.)** fuera de tu estación de trabajo, computadora portátil o dispositivos móviles.

Elimina de forma segura los archivos de datos confidenciales de tu sistema cuando ya no sean necesarios. **Utiliza siempre el cifrado al almacenar o transmitir datos confidenciales.**

La falta de un carácter podría enviarte a un lugar en el que lograrás poner en peligro tus datos. **Compra siempre los artículos en un sitio web conocido y de buena reputación.**

El robo de identidad es realmente alto en estos días y comprar algo en un lugar del que nunca has oído hablar, podría conducirte al robo de identidad. **Además, cuando ves una oferta en Internet que es demasiado buena para ser verdad, generalmente no lo es.**


***Conoce como Recuperar ficheros Encriptados***

**7- Utiliza dispositivos móviles de forma segura**

Teniendo en cuenta, cuánto confías en tus dispositivos móviles y cuán susceptibles son a los ataques, querrás asegurarte de estar protegido siempre. **Bloquea tu dispositivo con un PIN o contraseña, y nunca lo dejes desprotegido en público.**

Instala sólo aplicaciones de fuentes confiables (Apple AppStore, Google Play). Mantén actualizado el sistema operativo del dispositivo. **Evita transmitir o almacenar información personal en el aparato móvil.**

La mayoría de las unidades portátiles pueden emplear cifrado de datos; consulta la documentación de tu dispositivo para conocer las opciones disponibles.

**Utiliza Find My iPhone de Apple o el Administrador de dispositivos Android, ya que tienen herramientas para ayudarte a prevenir pérdidas o robos.**

**8- Instala protección antivirus/antimalware**

Instala estos programas únicamente de una fuente conocida y confiable. **Protege las definiciones de virus, los motores y el software actualizados para garantizar que tus programas sigan siendo efectivos.**

Es muy importante que tengas un buen antivirus que escanee con regularidad el sistema. **Aparecen nuevos virus todo el tiempo, por lo que el escaneo regular mantiene tu computadora funcionando correctamente y tus datos seguros.**

**9- Haz una copia de seguridad de datos**

Realiza copias de seguridad con regularidad, si eres víctima de un incidente de seguridad, la única forma garantizada de reparar tu computadora es borrar y volver a instalar el sistema.

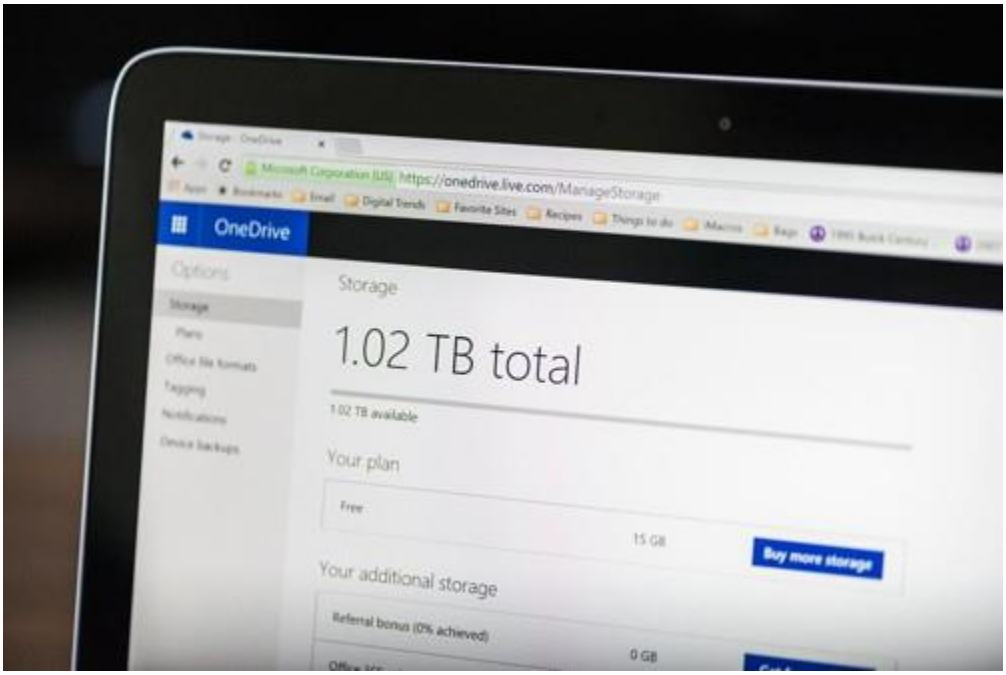
**Compra un par de discos duros externos para hacer una copia de seguridad de tu computadora.** En un Mac, el programa Time Machine realizará automáticamente un duplicado de tu computadora siempre que la unidad de respaldo esté conectada, esto es parte de la seguridad informática.

Puedes hacer lo mismo en tu PC usando Windows Backup. **Si algo le sucede a tu ordenador, puedes usar los discos duros para recuperar todo e incluso cargar los datos en una computadora nueva si es necesario.** También es una buena idea buscar en los servicios de respaldo en la nube.

**10- Espacio en el disco**

Vigila tu espacio en la computadora. Si el disco duro de tu procesador se llena, el software dejará de funcionar. **Puedes liberar espacio eliminando programas no deseados y excluyendo archivos que ya no necesites.**

**Si estás utilizando Windows 7, asegúrate de limpiar tus archivos temporales con regularidad.** Puedes hacerlo mediante la herramienta, liberador de espacio en disco. Afirma que la casilla etiquetada, archivos temporales está marcada, para concluir el barrido.




***Te invito a leer: No seas Víctima de la [estafa en Software a medida]***

**Para evitar riesgos es importante que obtengas toda la información necesaria de calidad sobre la seguridad informática.**

A parte de que puedas resolver dudas, podrás aprovechar esta época para consultar y contactar a expertos en el tema, como es el caso de José Luís Martir Millán, quien te podrá dar la información detallada en materia de ciberseguridad, ya que es un perito especializado en el tema.