

## Seguridad de sistemas en verano

En estos momentos, el verano está en su esplendor.

El clima cálido y las oportunidades de ir a la playa y divertirse, hacen que nos olvidemos con facilidad de nuestras tareas rutinarias y de los quehaceres diarios; del hogar, y de nuestros sistemas informáticos.

Estos días, probablemente llevemos el ordenador portátil a lugares remotos, para publicar nuestro diario de viaje, y descargar las fotografías que tomamos con la cámara digital.

Pero el simple hecho de estar en vacaciones, no debe hacernos olvidar de la seguridad.

Nadie quiere que sus recuerdos digitales sean eliminados por un gusano, o que un delincuente informático robe el dinero de sus cuentas bancarias.

Registrarse dentro de una red inalámbrica insegura, o confiar en la conexión del hotel, podría causar este tipo de trastornos y arruinar por completo las vacaciones de la víctima.

También puede suceder, que por distracción dejemos nuestro ordenador portátil olvidado en un café, o en el tren. Obviamente, este habrá desaparecido antes que notemos el descuido.

### Protección física de los datos

Al viajar con un ordenador portátil, siempre hay que recordar y tratar de aplicar las siguientes recomendaciones:


- **Utilizar la protección por contraseña del BIOS**

El sistema básico de entrada y salida (BIOS, *Basic Input-Output System*) es el responsable de todas las operaciones entre los componentes físicos del ordenador, antes de que se inicie el sistema operativo.

Se instala en la máquina antes de salir de la fábrica, se carga antes que Windows y comienza a funcionar en el mismo momento en que se enciende el ordenador.

Casi todos los sistemas BIOS tienen una opción que permite definir una contraseña, que será solicitada durante el proceso de inicio del ordenador. Si el usuario introduce una contraseña inválida, el sistema operativo no se cargará.

Habilitar esta opción, y definir una contraseña única, es un método sencillo para evitar que los ladrones accedan a la información guardada, en el supuesto caso que el ordenador sea robado.

 **Importante:** esta es una protección primaria y efectiva en el primer momento, ya que un experto que tenga el tiempo y el equipamiento suficiente, podrá acceder a la información contenida en el disco duro del ordenador portátil.

Para configurar el sistema BIOS, hay que presionar la tecla **Del (Supr)**, o **F4**, o **F10** (esto dependerá del modelo del ordenador) durante el proceso de inicio. En el manual del usuario del ordenador encontrará más detalles.

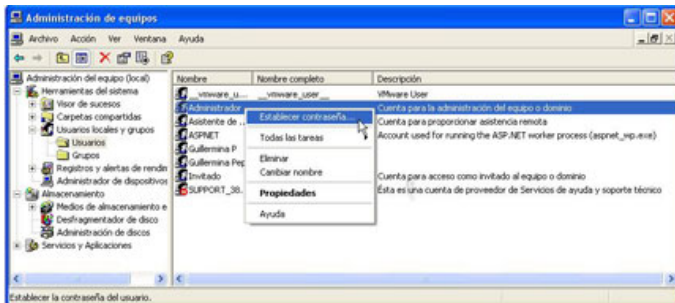
- **Proteger por contraseña todas las cuentas de usuario.**  
**Utilizar una clave robusta para la cuenta del Administrador.**

Es importante que todas las cuentas registradas en el ordenador estén protegidas por contraseña.

Es fácil olvidarse de definir una clave de seguridad especialmente fuerte para la cuenta del Administrador, pero esta es la que en realidad necesita mayor nivel de protección, porque es la que brinda acceso al resto de las cuentas del ordenador.

Las contraseñas de estas últimas pueden modificarse desde la consola de administración del equipo:

- Pulsar el botón **Inicio** y abrir el **Panel de control**.
- Seleccionar **Herramientas administrativas**, y pulsar sobre el acceso directo a **Administración de equipos**.
- En **Herramientas del sistema**, abrir la carpeta **Usuarios locales y grupos**, y seleccionar **Usuarios**.
- En el panel de la derecha, pulsar con el botón secundario del ratón sobre **Administrador**, y seleccionar **Establecer contraseña**.



● **Utilizar el sistema de archivos NTFS en lugar de FAT32**

NTFS (*New Technology File System*, Sistema de archivos de nueva tecnología) fue diseñado para resistir fallas del sistema, y permite bloquear el acceso a los discos y carpetas especificados, previniendo que usuarios no autorizados los vean o los copien. Este sistema es compatible con otras características de seguridad y auditoría, como la configuración de límites para el espacio del disco, el uso de registro de eventos y demás.

Los ordenadores portátiles actuales, tienen NTFS preinstalado. En aquellos casos que no sea así, nuestra recomendación es dejar la máquina como está, o llevarla para que un profesional haga la modificación, porque los experimentos con las estructuras de datos existentes son extremadamente riesgosos.

En general, se sugiere no convertir los discos que contienen datos críticos (documentos, o el sistema operativo), transformar los discos libres al nuevo formato NTFS, y finalmente mover allí la información que se desea proteger, y configurar los permisos de acceso.

Esto puede realizarse con la ayuda de la utilidad de Windows presente en la consola de administración de equipos:

- Pulsar el botón **Inicio** y abrir el **Panel de control**.
- Seleccionar **Herramientas administrativas**, y pulsar sobre el acceso directo a **Administración de equipos**.
- Expandir la carpeta **Almacenamiento**, y seleccionar **Administración de discos**.

Los permisos de acceso, pueden configurarse utilizando el Explorador de Windows.

● **Hacer copias de seguridad de los documentos y datos críticos**

Windows permite copiar cualquier archivo o carpeta a un CD o DVD, para resguardar los datos críticos. Es conveniente guardar estas copias en un lugar seguro, y dejarlas allí cuando se sale de viaje.

La herramienta **Restaurar sistema**, es muy útil para guardar una imagen de la configuración actual de Windows. Si el sistema falla, o se congela, esta aplicación deshacerá todas las modificaciones realizadas desde el punto de restauración, para volver a la última configuración estable.

Para acceder a Restaurar sistema, hay que:

- Pulsar el botón **Inicio** y seleccionar **Ejecutar**.
- En la ventana **Ejecutar**, escribir `%SYSTEMROOT%\system32\Restore\rstrui.exe`.

Existen herramientas desarrolladas por terceros para realizar esta tarea, por ejemplo [Acronis True Image 10](#).

- **Utilizar el sentido común**

No hay que olvidarse de algunos otros detalles, como no dejar el ordenador portátil en un lugar desconocido, nunca prestarlo a un extraño o a una persona que no es de confianza, y apagarlo cuando no está en uso. También es aconsejable configurar un bloqueo temporal, presionando una combinación de las teclas <> cuando es necesario desatender el ordenador por un momento.

Otras medidas adicionales que conviene tener en cuenta son:

- **Cifrado de discos**

El cifrado de los discos asegura que solo el usuario autorizado tendrá acceso a los datos contenidos en él. Esto es muy seguro, pero tiene una pequeña desventaja: si se pierde o se daña la clave de cifrado, la información guardada será inútil porque no hay forma de descifrarla.

El cifrado al instante consume recursos del procesador y del disco, y podría ser compatible solo con algunos dispositivos físicos. Aun así, es una herramienta muy poderosa y se puede experimentar con ella, si se es valiente. Windows Vista Ultimate incluye una herramienta para cifrar los discos, llamada **BitLocker**.

- **Suscribirse a un servicio de rastreo de ordenadores portátiles**

Existen servicios comerciales que pueden localizar un ordenador portátil, cuando este se ha perdido o ha sido robado. Trabajan utilizando una aplicación especial, o colocando un chip de rastreo en el ordenador, que se conecta con la estación de base de la compañía, e informa la ubicación actual de la máquina, siempre y cuando esta esté encendida y habilitada para acceder a Internet.

Conocemos casos de algunos afortunados dueños de ordenadores portátiles que han encontrado sus máquinas gracias a estos sistemas, de modo que vale la pena averiguar su disponibilidad.

## Seguridad de la red

Si bien las recomendaciones mencionadas son válidas para todo tipo de usuario o entorno de red, es útil recordar los siguientes puntos cuando nos vamos a conectar a la red más grande del mundo: Internet.

- Nunca abrir un archivo descargado sin analizarlo previamente en busca de virus, gusanos y programas espía.
- Aplicar siempre las actualizaciones de seguridad de Windows y demás aplicaciones habilitadas para Internet, tan pronto como estas estén disponibles.
- Asegurarse de [utilizar las redes inalámbricas de forma segura](#).
- Utilizar una [red privada virtual](#) para asegurar las conexiones móviles.
- Usar un programa que analice los sitios de Internet en busca de contenido o aplicaciones maliciosas, y bloquee automáticamente el acceso a ellos.
- Realizar transacciones con tarjetas de crédito solo con organizaciones de confianza, aprender a reconocer los intentos de robo de datos sensibles en línea (*phishing*), y asegurarse de introducir información personal únicamente en sitios que utilizan el protocolo HTTPS. Los navegadores web muestran esta característica con el icono de un candado en la barra de direcciones, o cerca de ella. Verificar los certificados de seguridad en los sitios web, y asegurarse que provienen de las compañías que cuyos nombres representan.

## Conclusiones

Este fue solo un breve documento, para recordar algunas de las precauciones de seguridad básicas que deben tenerse en cuenta al viajar con un ordenador portátil.

Es conveniente tratar de poner en práctica los consejos más importantes, después hacer el equipaje, y... ¡buen viaje!