SERVICIOS INFORMÁTICOS
Microinformática y C.A.U.
Torre de Control - Campus
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 5112
Fax: 91 885 5111
cau@uah.es

Consejos básicos para que su equipo sea más seguro

1. **Actualice Windows y aplicaciones con los parches de seguridad:** Las vulnerabilidades que se detectan en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, etc.) suelen ser, por su gran difusión, un blanco habitual de los creadores de virus. Para evitarlo, una vez detectada una vulnerabilidad, las compañías fabricantes de software ponen rápidamente a disposición de sus clientes actualizaciones, llamadas 'parches de seguridad'. Por esto, es de gran importancia actualizar nuestros equipos cuanto antes.

   Para actualizar el equipo, debe visitar periódicamente el sitio Web de Microsoft http://windowsupdate.microsoft.com e instalar las actualizaciones necesarias. Tiene un acceso directo a este enlace en Internet Explorer -> Herramientas -> Windows Update. Debe hacerlo desde una cuenta con permisos de administrador.

   También puede configurar en su equipo las actualizaciones automáticas de Windows, de modo que le avise cada vez que haya actualizaciones críticas, así se evita tener que acordarse de entrar en esta dirección. Para configurar las actualizaciones automáticas:

   En **Windows 8** → Configuración → Windows Update

   En **Windows 7** → Inicio → Panel de Control → Sistemas y seguridad → Windows Update

   En **Windows XP** → Inicio → Panel de Control → Actualizaciones automáticas

2. **Revise el antivirus:** El antivirus OfficeScan, diariamente se conecta con nuestro servidor y se actualiza automáticamente. No obstante, es aconsejable verificar periódicamente que está activo y se ha actualizado correctamente, para ello sitúe el cursor sobre el icono del antivirus y compruebe el motor y versión del fichero de firmas.

3. **Active el Cortafuegos.** Un cortafuegos o 'firewall' es un software que bloquea las entradas sin autorización a su ordenador y restringe la salida de información. Los sistemas operativos Windows (Xp, Vista, 7, 8) tienen incluido en el sistema operativo un cortafuegos que es conveniente tener activado.

4. **Contraseña en las cuentas.** Es importante que todas las cuentas existentes en el equipo estén protegidas por contraseña.

5. **Mantener copia de seguridad.** Es muy importante realizar periódicamente copia de seguridad de todos nuestros documentos, así como de los ficheros de correo (buscar ficheros con extensión *.pst* si utiliza Outlook 2003, Outlook 2007, Outlook 2010 u Outlook 2013.

SERVICIOS INFORMÁTICOS
Microinformática y C.A.U.
Torre de Control - Campus
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 5112
Fax: 91 885 5111
cau@uah.es

6. Y en general, respetar unas reglas elementales:

- Asegúrese de que todo el software instalado en su ordenador proviene de una fuente conocida y segura.
- No instale software pirata.
- Nunca facilite una contraseña ni datos bancarios o personales por correo electrónico. Ninguna institución seria va a pedirle que lo haga.
- No confíe en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus.
- No facilite su cuenta de correo a desconocidos, ni conteste correo electrónico de dudosa procedencia.
- No abra nunca ficheros adjuntos de un mensaje procedente de remitentes desconocidos, ni de remitentes conocidos si los ficheros son sospechosos. No comparta carpetas en su ordenador sin contraseña, ni siquiera temporalmente.
- Si utiliza Outlook, desactive la vista previa de mensajes.