Recomendaciones Generales de Seguridad

Medidas de Seguridad Preventivas

A continuación se detallan las recomendaciones básicas para prevenir que su equipo se vea afectado por cualquier tipo de malware:

1. **No abra ningún correo de remitentes desconocidos con ficheros adjuntos sospechosos**. La distribución de ficheros adjuntos a través del correo electrónico es uno de los métodos más utilizados hoy en día para la propagación de virus y malware en general.

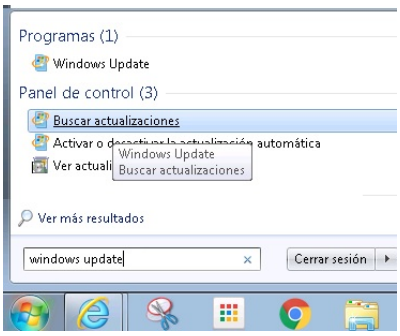
2. **Sea especialmente cuidadoso con la navegación web**.
   Navegue solo por sitios web fiables y necesarios para el desempeño de su trabajo.

3. **Compruebe que su sistema está actualizado**.
   - **En Mac:** Siga estas instrucciones acerca de **cómo actualizar el software en el Mac**.

   - **En Windows**: Si su equipo se lo ha entregado e instalado el Servicio de Informática, ya estará configurado de forma que las actualizaciones importantes del sistema se descargan de forma automática cuando Microsoft las publica y, por tanto, no estaría en riesgo.

     No obstante, realice esta comprobación, ya que, es posible que dado que Ud. es administrador de su sistema, en algún momento haya modificado esta configuración o bien, no haya querido o podido instalar estas actualizaciones.

     Teclee “Windows Update” en el control de búsqueda y, después, pulse sobre “Buscar actualizaciones”

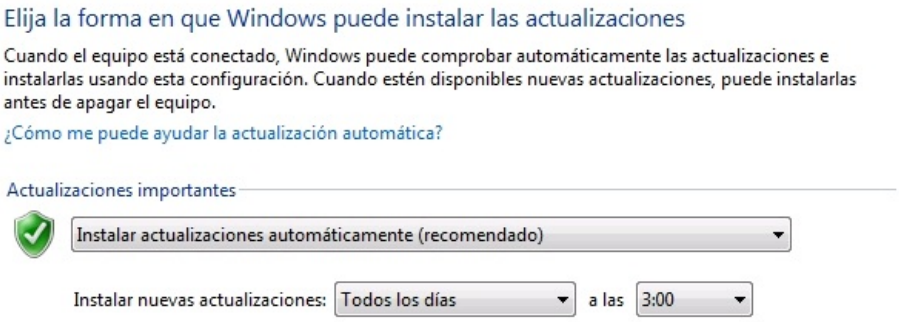
     

     Si tiene todas las actualizaciones importantes instaladas verá lo siguiente:

     Si no fuera así, pulse sobre “buscar las actualizaciones” importantes disponibles e instálelas.

4. **Compruebe que tiene activada la instalación automática de actualizaciones importantes**:



5. **Compruebe que tiene su antivirus actualizado**.
   Recuerde que puede instalar la última versión del antivirus Panda de la UJA desde el siguiente enlace:
   Antivirus Panda para equipos particulares

6. **Realice copia de seguridad periódica de su información personal**.
   Recuerde que si su equipo se infecta y sus ficheros son eliminados o cifrados, la única solución posible actualmente de recuperar su información es a partir de una copia de seguridad.

   En cuanto pueda, realice una copia de seguridad de su información en un dispositivo externo y desconéctelo de su equipo una vez realizada la copia. Puede seguir las recomendaciones del Servicio de Informática publicadas en la siguiente guía práctica:
   Cómo hacer una copia de seguridad de su información personal

Enlaces relacionados

- SPAM (Correo no solicitado)
- Phishing (correo fraudulento)
- Malware (software malicioso)
- Seguridad en el correo electrónico
- Uso seguro de la web
- Ransomware