There are no translations available.
El objetivo de este artículo es guiar de forma sencilla al usuario común de Windows sobre cómo proteger su equipo..

El objetivo de este artículo es guiar en forma sencilla, en algunos casos paso a paso (con captura de pantallas), al usuario común de Windows sobre cómo proteger su equipo y guardar sus documentos frente a diversas amenazas que atentan contra sus valiosos datos almacenados en su PC. Para ello hemos redactado varios puntos a tener en cuenta para proteger lo máximo posible sus datos en caso de cualquier problema que puedan encontrarse como pueden ser (virus, gusanos, caballos troyanos) o spyware, estos son programas espías en los que se encontrarían: Cookies, ActiveX y páginas dinámicas o Scripts.

Los actuales discos duros son bastante confiables para guardar información, pero eso no es excusa para no tener actualizadas las copias de respaldo. La razón es muy sencilla: solo basta un sencillo comando para destruir la información de un disco duro y hacerla en extremo difícil o imposible de recuperar, así que cualquier medida a tomar debe estar encaminada para minimizar el riesgo de ataques.

Para ello trataremos los siguientes puntos:

1.- Servipack 2

2.- Backup

3.- Restaurar Sistema

1.- SERVIPACK 2

Un **Service Pack** es un conjunto de actualizaciones que corrigen características del sistema operativo Windows. Los Service Pack pueden contener también correcciones de problemas internos y de cambios de diseño. Las actualizaciones se usan para corregir o mejorar los productos software publicados por Microsoft. Todas estas actualizaciones se pueden hacer vía

Web:

Una parte muy importante es la seguridad y Windows XP **Service Pack 2 (SP2)** aporta mejoras a la seguridad diseñadas para proporcionar una mejor protección contra piratas informáticos, virus y gusanos. También mejora la capacidad de administrar las herramientas de seguridad en Windows XP proporcionando más información para ayudar a los usuarios.

En este punto entenderemos por **seguridad** en informática la protección frente a ataques a recursos del equipo por parte de intrusos a los que no se permite el acceso a dichos recursos, como pueden ser una carpeta compartida, los buzones de correo
La
política de seguridad
es un documento mediante el cual se especifican distintas normas referentes a la seguridad informática de una empresa (cuantas letras han de tener las contraseñas de los usuarios corporativos, quien va a poder iniciar la conexión, como se va a permitir el acceso recursos internos).

Una definición importante para entender la protección de nuestros ordenadores es la de **cortafuegos**
(del inglés, Firewall), que es un elemento físico o programa que sirve para prevenir a los equipos de amenazas por intrusión externa, controlan el acceso (de entrada y de salida) para que nadie dañe nuestro ordenador malintencionadamente. Una distinción importante consiste en:

1- cortafuego personal: un programa que normalmente controla el tráfico que entra o sale de un ordenador.

2- un cortafuego tradicional: cortafuego que controla el tráfico que entra o sale de una red.

Una de las novedades que aporta Windows service pack 2 es **Windows Firewall** que proporciona protección para los ordenadores que están conectados a una red, como puede ser a Internet. El cortafuego, se activa por defecto cuando se instala el Service Pack 2, también protege al equipo de cualquier ataque mientras éste se inicia o se apaga .

Otra medida de seguridad que aporta WINDOWS SP2 es un nuevo servicio que determina si los archivos adjuntos al correo o abiertos a través de Internet Explorer son seguros. Cualquier archivo adjunto que no sea seguro será aislado para que no pueda afectar a otras partes del sistema.

En **Internet Explorer** también se ha mejorado la seguridad, lo que permite bloquear la zona de seguridad local (Mi PC), para protegerla de la ejecución de secuencias de comandos malintencionadas y reforzarla ante descargas Web perjudiciales.

Otra seguridad que aporta Service Pack 2 es el bloqueo de contenido peligroso de Internet: applets de Java, controles ActiveX, cookies, etc. Permite bloquear los pop up (ventanas emergentes de publicidad) de las páginas de Internet añadiendo una barra y permitiendo aceptarlos o rechazarlos pinchando sobre ella.

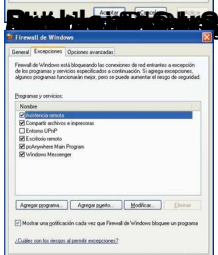
Herramientas para la gestión de la seguridad

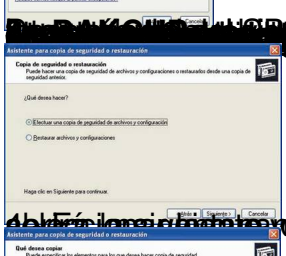
Se han creado mejoras para la gestión de la seguridad, como puede ser el **Centro de Seguridad de Windows**
: El Panel de Control añade un icono de configuraciones de seguridad. Hace una serie de comprobaciones: Comprueba si Windows Firewall está activado o no, también comprueba la presencia de otros, comprueba la presencia de programas antivirus. También comprueba que las actualizaciones automáticas estén activadas.

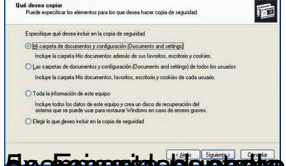
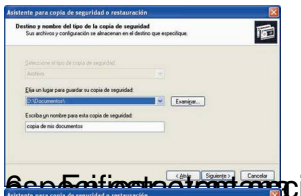
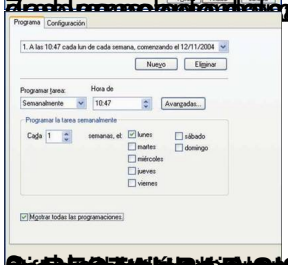
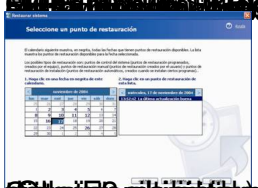
Mediante el centro de seguridad puedes activar el nivel de seguridad en Internet.

2. Firewall de Windows:

Es Actualizaciones automáticas. Permite que se active una opción para que Windows busque







Es Entrada para que nos pueda crear un nombre a la copia