

Trabajar de forma segura con Windows XP (I)

Introducción

Este material le brinda al lector algunas perspectivas básicas acerca de cómo hacer que el trabajo con Windows XP sea más seguro.

El material consta de dos partes:

- **Primera parte:**
Una descripción acerca de cómo asegurar el sistema por medio de herramientas disponibles de forma inmediata ofrecidas por el propio sistema operativo, sin la necesidad que el usuario recurra a la aplicación de programas de terceros.
- **Segunda parte:**
Se revela cómo fortalecer la seguridad aún más al agregar una capa adicional por medio del uso de programas auxiliares de terceros.

En esta entrega se verá la primera parte de este informe:

Actualización del sistema

En primer lugar, debería tratar de actualizar el sistema operativo, con los últimos parches y arreglos para erradicar errores conocidos y fallas de seguridad presentes de forma inevitable en todos los programas, incluyendo los de Microsoft.

Para empezar, es obligatorio que instale la más importante actualización acumulativa de WinXP conocida como **Service Pack 2** (SP2) antes de utilizar Windows ampliamente y, después de esto, es aconsejable que también se apliquen todas las posteriores actualizaciones publicadas después del SP2.

Todo esto puede realizarse, ya sea habilitando la característica Actualizaciones automáticas, la que como opción predeterminada de Windows se encuentra activa, realizando un pedido del disco gratuito de Microsoft (no se incluye el coste de envío) o consultando la dirección que aparece al final de este texto y descargando todas las actualizaciones manualmente de los sitios Windows Update o Centro de descarga de Microsoft.

Para verificar la versión actual de Windows y controlar si se encuentra instalado el SP2 en su sistema:

1. Presione la combinación de teclas **Windows** y **Pausa** (*Break*) después de lo cual aparecerá la ventana **Propiedades del sistema**.
2. En la pestaña **General**, verifique la versión de Windows y, también, puede habilitar las actualizaciones automáticas si se desactivaron de forma accidental.

Al finalizar el tema de las actualizaciones, los usuarios deber mantener su sistema al día, para lo cual, se aconseja el uso de las actualizaciones automáticas que provee el servicio **Windows Update**.

Control de ejecución de aplicaciones

Al igual que con todos los programas espía, los virus y otros programas que se ejecutan subrepticamente en el ordenador, no se exponen abiertamente y buscan ocultar su constante presencia y actividad.

Las formas estándar que aparecen en manuales para verificar qué es lo que está sucediendo en un ordenador no son suficientes y las personas deben realmente aprender otras formas de ver lo que está ocurriendo.

Para lograr esto, existe un utilitario integrado, simple y fácil denominado **Administrador de tareas** que puede invocarse:

1. Pulse simultáneamente las teclas **CTRL+Shift (Cambio) y ESC**, y le permitirá visualizar los programas y procesos que se estén ejecutando actualmente en el ordenador.
2. Pulse en la pestaña **Procesos** y aparecerá una lista de todos los procesos activos en el sistema.
Esta vista, de hecho, refleja en realidad todo lo que se está ejecutando en un ordenador en un momento determinado y, desde esta ventana, los usuarios pueden finalizar aquello que no necesitan.

Aunque los nombres de los procesos mostrados en la ventana podrían parecer un poco desconcertantes, una simple consulta en Google, Yahoo o MSN con el nombre específico del proceso ingresado en el campo de búsqueda, puede brindar amplia información necesaria para evaluar la validez del programa en cuestión.

Por otro lado, podría también hacer una búsqueda acerca de un archivo ejecutable del disco local, sobre el que quisiera tener más información.

Simplemente ingrese el nombre del proceso en el programa **Buscar archivos y carpetas de Windows** y, después de finalizar la misma, aparecerán los archivos encontrados.

Al pulsar, con el botón derecho, sobre el nombre del archivo y posteriormente en **Propiedades** aparecerá información acerca del proceso de su interés.

Algunas recomendaciones: los programas maliciosos a menudo tratan de imitar a los verdaderos y, en un esfuerzo por lograrlo, copian los nombres de los programas legítimos y se muestran con esos nombres como si fueran los originales.

Aunque complica en gran medida la tarea de verificación del programa, si se aplica el conocimiento suficiente, los programas sospechosos siempre se confirmarán.

Si, por ejemplo, hemos realizado una búsqueda y nos dimos cuenta que el archivo scvhost.exe se está ejecutando desde la subcarpeta **Sistema**, de la carpeta donde se ha instalado Windows, la situación sería bastante normal y, por el contrario, si el archivo se encontrare en otras ubicaciones en lugar de C:\WINDOWS\system32, o C:\WINDOWS\ServicePackFiles\i386, esto debería generar una alarma, dado que no es común hallar este archivo en otras localizaciones.

Una vez más, reúna datos en Internet acerca del proceso que aparece en el Administrador de tareas, ya que existe mucha información disponible que le brindará todos los detalles acerca del proceso sobre el que necesite averiguar.

Con el Administrador de tareas, puede finalizar los programas que considere inapropiados, pero se debe tener cuidado porque finalizar un programa válido podría generar una falla en el sistema o resultar en la pérdida de datos que no hayan sido guardados.

Siempre consulte una fuente de confianza de Internet para averiguar acerca de la aplicación que está a punto de cerrar.

Configurar aplicaciones y servicios de inicio

Para configurar cuáles programas deben ejecutarse cuando se inicia Windows, el utilitario **Configuración del sistema** es la herramienta correcta para realizarlo:

1. Pulse en el menú Inicio, **Ejecutar**.
2. Escriba **msconfig** y presione el botón Aceptar.
3. En la pestaña **Inicio** (a la derecha), puede configurar cuáles aplicaciones desea que Windows ejecute cuando se inicia y, restringir aquellas que no quiere que se inicien automáticamente.

De esta forma, no solamente podrá disminuir el consumo de memoria y tiempo de uso del procesador sino que, en casos extremos, podrá evitar la ejecución de aplicaciones peligrosas que procuran iniciarse automáticamente con Windows.

Una vez más, recoja la información acerca de posibles exclusiones ingresando en los motores de búsqueda de Internet y averiguando acerca del tema en cuestión.

También puede considerar desactivar un par de servicios redundantes de Windows, pero saber cuáles pueden desactivarse de manera segura requiere realmente cierto grado de aprendizaje, por lo tanto necesitará más información que podrá encontrar, una vez más, fácilmente en Internet para poder decidir si el servicio puede desactivarse o no.

El motivo por el cual se brinda tanta atención a los servicios es que eliminar los innecesarios podría influir de forma positiva en la seguridad general del sistema.

Al utilizar el comando **services.msc** ingresado en el menú **Ejecutar** puede configurar la operación de servicios y sus parámetros de inicio.

Configurar usuarios locales en el ordenador

Con la configuración predeterminada de la instalación de Windows XP, se activan algunas cuentas de usuario internas; tienen privilegios (nivel de control más alto posible) de raíz (administrador) y ni siquiera tiene protección mediante contraseña.

Esta situación debe ser revertida drásticamente y para ello los usuarios deben realizar lo siguiente:

1. Pulse en el menú Inicio, **Ejecutar**.
2. Escriba **lusrmgr.msc** y pulse en el botón **Aceptar**.

Aparecerá el módulo de programa **Usuarios locales y grupos** donde es posible especificar contraseñas de usuarios y desactivar cuentas de usuario innecesarias.

Se recomienda realizar los siguientes cambios:

- Seleccione la carpeta **Usuarios** y desactive todas las cuentas excepto la de Administrador y los usuarios creados manualmente.
Con muy poca frecuencia, o prácticamente ninguna, necesitará tener en ejecución las cuentas **Invitado**, **Asistente de ayuda** y/o **Soporte**.

Si todavía no estableció la contraseña del Administrador, deberá asignarla en el menú **Cuentas de Usuarios** del Panel de Control:

1. Pulse en el menú Inicio, **Ejecutar**.
2. Escriba **nusrmgr.cpl** y pulse en el botón **Aceptar**.
3. Introduzca contraseñas para la cuenta de Administrador y cuentas de usuario selectivas agregadas manualmente.

De esta forma, se complicaría sustancialmente la tarea de controlar el ordenador por parte de piratas que confían en una protección por medio de contraseñas poco estrictas.

Además, asigne permisos de usuario adecuados a los usuarios locales del ordenador colocándolos en los grupos de usuario específicos con credenciales diferentes.

Esto puede realizarse con el mismo menú **Cuentas de Usuarios**:

1. Seleccione el usuario al que desea asignar una nueva configuración.
2. Pulse en **Propiedades**.
3. En la pestaña **Miembro de** y en esa ventana coloque al usuario en el grupo de usuarios adecuado.

De esta forma, le habrá brindado al usuario permisos especiales para realizar ciertas acciones basándose en su criterio del estado de autoridad del usuario.

Conceptos básicos de seguridad de redes

Tal como aseguran los encargados de la seguridad, cuando usted está conectado a Internet, Internet también está conectada a usted.

Es ahí donde surgen todas las implicancias de mantener las conexiones de red de manera segura: configurando de forma correcta las propiedades, instalando un cortafuegos, actuando de manera inteligente y con conocimiento, mientras está conectado, entre otros temas.

Los agregados prácticos para la seguridad de la red serían:

- Desactivar la opción **Compartir archivos e Impresoras para todas las conexiones de Internet** o las seleccionadas.
Si usted, como muchas personas hacen normalmente, no tiene la intención de brindar a extraños acceso a archivos e impresoras locales, debe desactivar esta opción.
No dañará la calidad de su conexión a Internet.
- Activar el icono, en la barra de sistema, de conexiones de red para visualizar el estado de conexión actual.
- Activar el cortafuegos de Windows y actualizar de forma regular el sistema con los últimos parches (la repetición de lo que se dijo anteriormente subraya su importancia).

- Controlar la actividad de las conexiones actuales, en busca de irregularidades, tales como las que se observan cuando un usuario no carga o descarga ningún dato y, sin embargo, las luces de control del área de notificaciones permanecen encendidas permanentemente (la posible sospecha en ese caso sería la operación de un código malicioso astuto que envía datos)
- La velocidad y el rendimiento de la red podrían también verificarse con el Administrador de tareas mencionado anteriormente, esta información se puede localizar en la pestaña llamada Funciones de red.

Protección del navegador y correo electrónico

En realidad, el tema de esta sección podría abarcar demasiadas páginas, pero haciendo un pequeño resumen, se debería prestar atención a lo siguientes puntos básicos::

Establecer el nivel de seguridad adecuado para el navegador

Con el paquete de mantenimiento **SP2**, se han realizado grandes avances para mejorar la protección del navegador Internet Explorer (IE) pero, estableciendo manualmente el nivel de protección, se adaptaría mejor al estado de destreza del flagelo denominado código malicioso y demás virus modernos que infiltran los sistemas actualmente. Aunque con la configuración predeterminada de SP2 se ha vuelto más seguro, Internet Explorer, podría de todas formas, necesitar un poco de personalización manual.

Para maximizar la seguridad el navegador, se recomienda que se implementen las siguientes medidas:

1. Abra Internet Explorer.
2. Pulse en el menú Herramientas, Opciones de Internet, **Seguridad**.
3. Seleccione la **Zona de Internet** (con un signo de globo terráqueo) y asigne nivel de seguridad **Medio** moviendo el indicador.
4. Presione en el botón **Aplicar**.
5. Posteriormente, pulse en nivel **Personalizado** y seleccione:
 1. En **Ejecutar controles y complementos ActiveX, Preguntar**.
 2. En **Creación de guiones de aplicaciones Java, Preguntar**.
 3. Pulse en el botón **Aceptar**.

Después de realizar tales acciones su navegador y, por consiguiente, todo el sistema estará más seguro, pero necesitará más interacción con el operador, lo que se reflejará en la cantidad de consultas al usuario que mostrará. Para evitar estas persistentes ventanas de confirmación, los usuarios pueden indicar listas de exclusión para sitios de confianza cuyos guiones serán siempre permitidos.

Esto habilitará a los usuarios a navegar por los sitios seleccionados, con permisos completos, al mismo tiempo que si visitan sitios desconocidos o sin probar, gozarán de una amplia seguridad en el navegador.

Las listas de exclusión para sitios de confianza se definen en la misma pestaña **Seguridad**.

Para esto, simplemente pulse en el botón **Sitios** y agregue aquellos que considere por completo seguros y los mismos le serán más fáciles de acceder y navegar.

Mantener un uso seguro e informado de Internet

Estar protegido contra guiones de páginas de Internet, ejecutados automáticamente, por sí solo no garantiza una protección absoluta.

Se debe utilizar un comportamiento aceptable y lógico cuando se navega en Internet, incluyendo no abrir archivos desconocidos o no solicitados, no diseminar información privada en fuentes sin verificar, no confiar automáticamente en todos los contenidos de un sitio de Internet desconocido, entre otros.

La creciente amenaza que los usuarios de Internet deben ser capaces de detectar se refiere a las metodologías denominadas *Phishing* y *Pharming* (envenenamiento de DNS).

Esto requiere cierto nivel de conocimiento de Internet y, los usuarios, deben tener en cuenta medidas simples para no ser víctimas de tales amenazas.

Protegerse de la técnica **Phishing**: es sencillo, nunca reaccionar o por lo menos reaccionar cautelosamente a las solicitudes de datos secretos, provenientes supuestamente, de bancos u otras entidades que le ofrecen realizar ciertas acciones ingresando en algún sitio y realizando cierta acción hasta que cierto problema se haya solucionado. Los agresores utilizan técnicas de falsificación de direcciones IP para simular ser el sitio verdadero, utilizando uno de los creados por el agresor para estafar a las personas que consideran al sitio, como de confianza.

La técnica **Pharming**, que está relacionada con las mismas técnicas de falsificación de direcciones IP, involucra métodos más elaborados para atraer a la víctima, es más difícil de reconocer y más difícil para el usuario protegerse. En la actualidad, únicamente los cortafuegos más avanzados pueden ser de ayuda para defenderse contra esta técnica delictual.

Uso de correo electrónico seguro

Las mismas precauciones mencionadas en relación con el uso de Internet deben aplicarse al uso del correo electrónico, y además:

1. Desactive la opción **Descargar mensaje automáticamente al visualizarlo en el panel de vista previa**, en Outlook Express si está utilizando este programa para enviar correo electrónico.
En este caso para leer los mensajes entrantes deberá presionar la barra espaciadora en el teclado pero, por otro lado, ignorará los contenidos potencialmente innecesarios del propio correo electrónico.
2. En la pestaña **Seguridad** de Outlook Express realice las siguientes modificaciones:
 1. Marque la opción **Zona de sitios restringidos (Más segura)**
 2. Marque la opción **Mostrar advertencia cuando otras aplicaciones traten de enviar correo en mi nombre**
 3. Marque la opción **Bloquear imágenes y otro contenido externo en correo electrónico con formato HTML**

Recursos de Internet mencionados en el texto:

- Sitio de actualización de Windows: <http://windowsupdate.microsoft.com>