

Prólogo

Dada la cantidad de vulnerabilidades, exploits y parches que han aparecido para Internet Explorer en estos dos últimos años es de vital importancia configurar nuestro navegador para evitar en la medida de lo posible futuros ataques y así poder mantener nuestros equipos más seguros.

En este tutorial no escucharás consejos "fáciles" como "utilizar otro navegador", principalmente porque un navegador bien configurado no debe dar grandes problemas, y si los da, como dice el refrán, "a grandes males, grandes remedios".

También decir que en Windows XP, Internet Explorer viene integrado con el sistema operativo, es decir, que NO se puede desinstalar. Así que conviene configurarlo, se vaya a utilizar o no.

Internet Explorer es un navegador que da, y sigue dando buenos resultados. Dependiendo de la configuración obtendremos mejores o peores resultados. Todo depende de la buena conducta al navegar por Internet. Internet es como la televisión. Hay cosas buenas y cosas malas. En televisión hay programas muy buenos y programas que sólo sirven para que puedan poner anuncios entre medio. En Internet pasa lo mismo. Hay sitios bien construidos y sitios potencialmente peligrosos. En el 90% de los casos depende del usuario final, es decir, de nosotros.

Los consejos que se van a dar aquí no son la solución a todos los problemas. Surgirán nuevas vulnerabilidades, exploits, etc... En cualquier caso son consejos para disfrutar aún más de la WWW (World Wide Web).

El portapapeles, al descubierto

Internet Explorer permite capturar los datos del portapapeles desde una página Web. Aunque el uso malicioso de esta característica ya fue denunciado a finales del 2002, todavía se puede explotar esta vulnerabilidad, ya que en una instalación por defecto deja esta opción activa.

Aunque evidentemente tiene usos prácticos, imaginemos esta situación:

Abrimos nuestro WebMail (Correo vía Web, como Hotmail por ejemplo). Tipeamos nuestro usuario, y cuando escribimos nuestra contraseña, la copiamos con el portapapeles (edición → copiar).

Causa: Copiamos nuestra password al portapapeles.

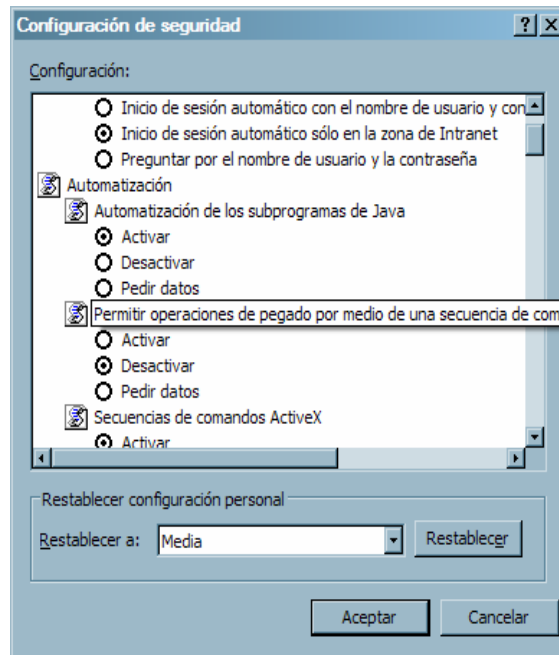
Efecto: Al entrar en una Web maliciosamente construida, ésta podría ver los datos que tenemos en el portapapeles, es decir, nuestra contraseña.

El objeto clipboardData es el que aporta esta funcionalidad. Se incorporó en la versión 5 de Internet Explorer. Básicamente admite tres métodos para interactuar con los datos del portapapeles, "getData" para capturar la información, "setData" escribe datos, y "clearData" para borrar el portapapeles.

Realmente no es una vulnerabilidad, es una opción más de Internet Explorer, y como usuarios que somos, tenemos la opción de utilizarla o no. En nuestro caso la vamos a deshabilitar, ya que yo personalmente no le doy ningún uso.

Para deshabilitar esta opción haremos lo siguiente:

- ✚ En el menú de IE, seleccionar "Herramientas" y acto seguido en "Opciones de Internet"
- ✚ Acto seguido pincharemos en la pestaña "Seguridad" y pulsaremos el botón "Nivel Personalizado"
- ✚ Deshabilitar la opción "Permitir operaciones de pegado por medio de una secuencia de comandos", tal y como se muestra en la imagen

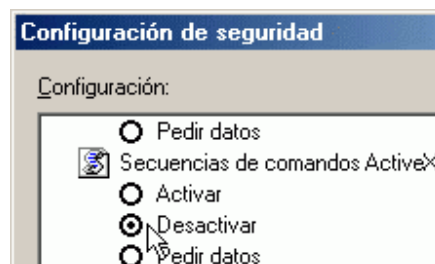


Podéis ver una prueba de concepto [aquí](#)

Deshabilitar el Active Scripting (JavaScript y ActiveX)

Los cambios que se hagan en este apartado influirán directamente en la visualización de muchos sitios de Internet. Generalmente casi todos los sitios de Internet pueden ser visualizados correctamente sin el uso de estos componentes (JavaScript y ActiveX). Para deshabilitar esta opción seguiremos estos pasos:

- 1.- En el menú de IE, seleccionar "Herramientas" y acto seguido en "Opciones de Internet"
- 2.- Acto seguido pincharemos en la pestaña "Seguridad" y pulsaremos el botón "Nivel Personalizado"
- 3.- Deshabilitar la opción de Active Scripting tal y como se muestra en la imagen.



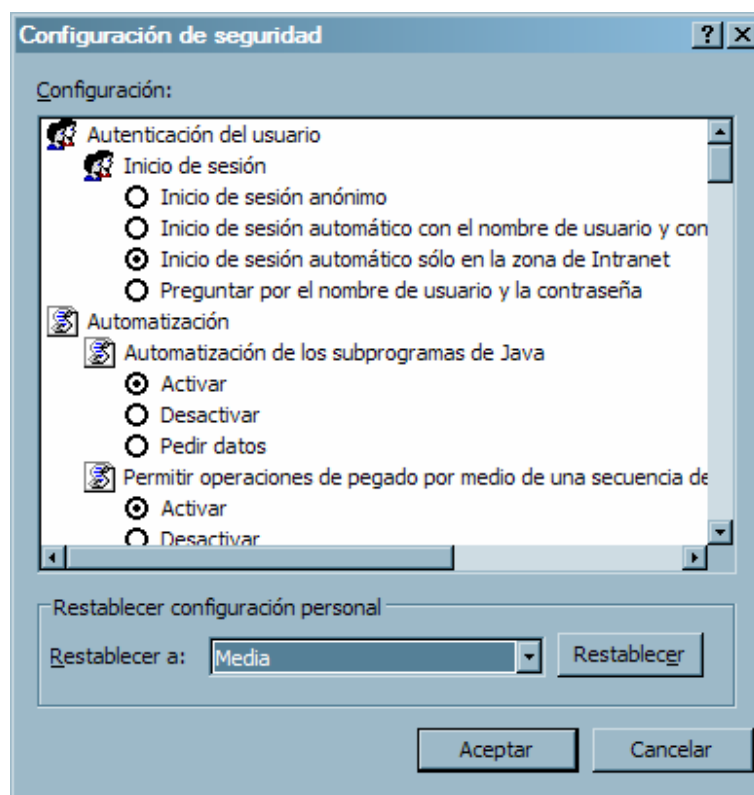
- 4.- Aceptamos y confirmamos cambios

Los que necesiten ActiveX, pueden agregar los sitios a una lista segura. Una solución es incluir estos sitios en la zona de "Sitios de confianza".

Configuración de la zona "Sitios de Confianza"

En esta zona se pondrán los sitios Web que sepamos en todo momento que no van a afectar a ni a nuestro equipo ni a la privacidad de nuestros datos.
Procederemos de la siguiente manera.

- 1.- En el menú de IE, seleccionar "Herramientas" y acto seguido en "Opciones de Internet"
- 2.- Acto seguido pincharemos en la pestaña "Seguridad", marcaremos la opción "Sitios de Confianza" y pulsaremos el botón "Nivel Personalizado"
- 3.- Seleccionaremos el nivel Mediano (medio) y pulsaremos el botón "Restablecer"
- 4.- Aceptamos y confirmamos los cambios.



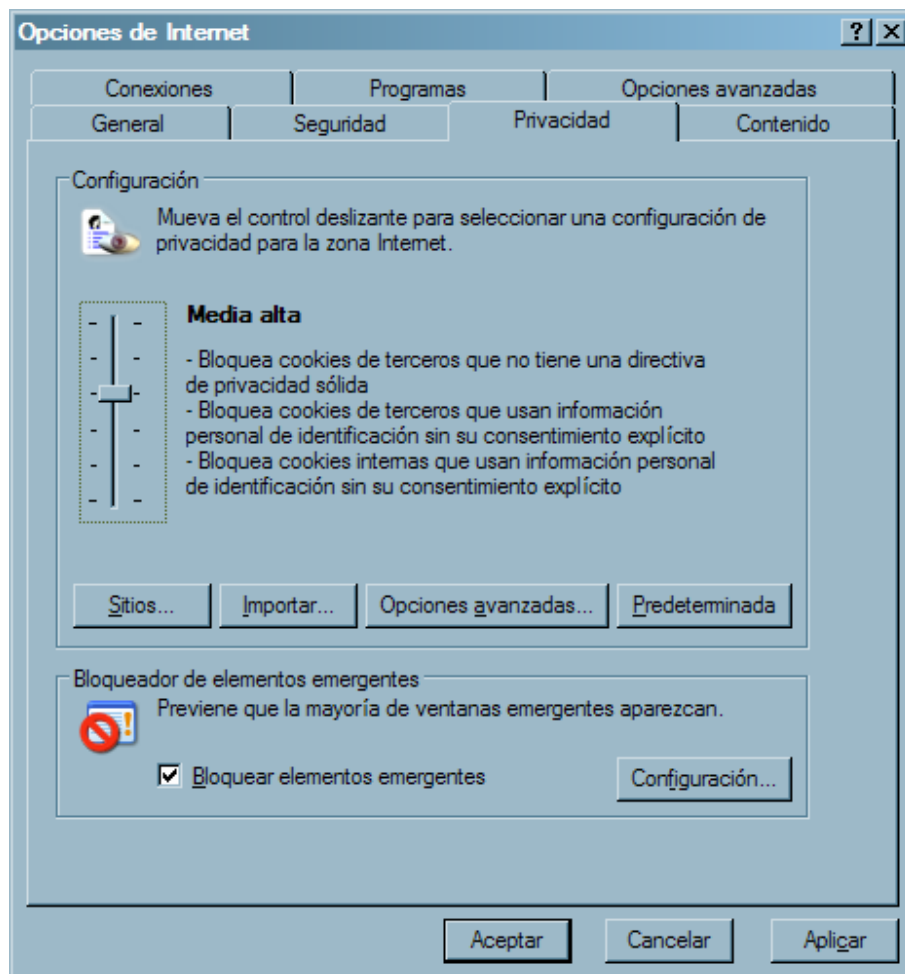
Una vez que realicemos estos cambios, podremos incluir en esa zona los sitios Web que consideremos "seguros".

Nota: Para incluir las zonas de Internet en la pestaña "Sitios de Confianza", desmarcaremos la casilla "Requerir comprobación del servidor (https:) para todos los sitios de esta zona".

Cookies

Una Cookie es un fichero de texto. En él se almacena información referente las páginas Web que hemos visitado que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, con información acerca de lo que hemos estado viendo, configuración del site, nombres de usuario y contraseñas, etc....

Por defecto Internet Explorer coloca la configuración de las Cookies en un nivel "Medio". Se recomienda ponerlo un nivel más alto, es decir, en el nivel "Medio-Alto", tal y como muestra la imagen.



Archivos Temporales e Internet Explorer

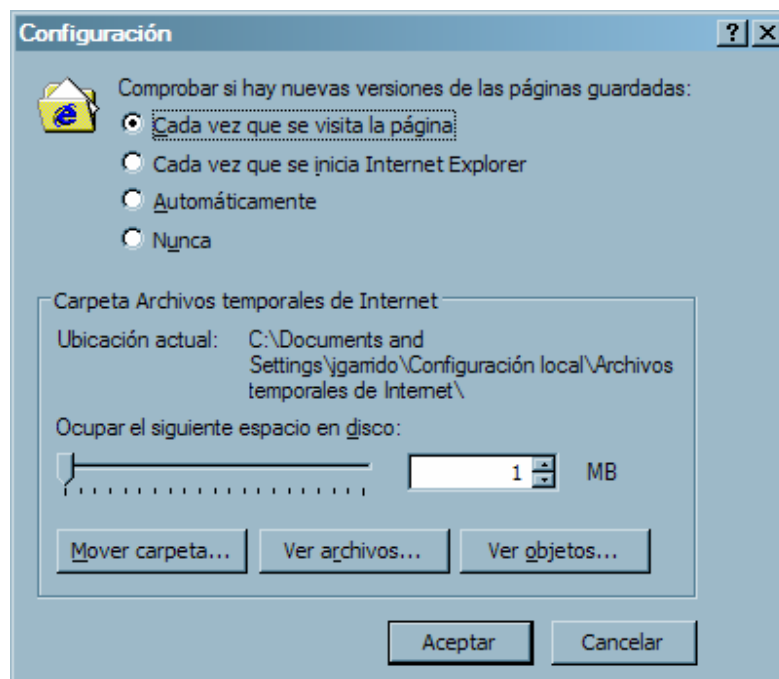
Cuando navegamos por Internet, nuestro navegador crea una caché con las páginas visitadas. Esto es útil cuando navegamos varias veces por los mismos sitios. Nuestro navegador mirará primero en esa caché. Si encuentra el sitio lo muestra desde la caché y si tiene que actualizarlo, lo actualizará al instante. Así conseguimos experimentar más rapidez a la hora de cargar las páginas.

Hoy en día, gracias a las velocidades de conexión, esta opción deja de tener protagonismo por muchos factores, de entre los cuales matizo los siguientes:

- ✚ Si visitamos páginas maliciosas (exploits) se guardarán en nuestra caché
- ✚ Los scripts que tengamos en la caché podrán ser invocados y ejecutados

Para solucionar esto podemos hacer dos cosas:

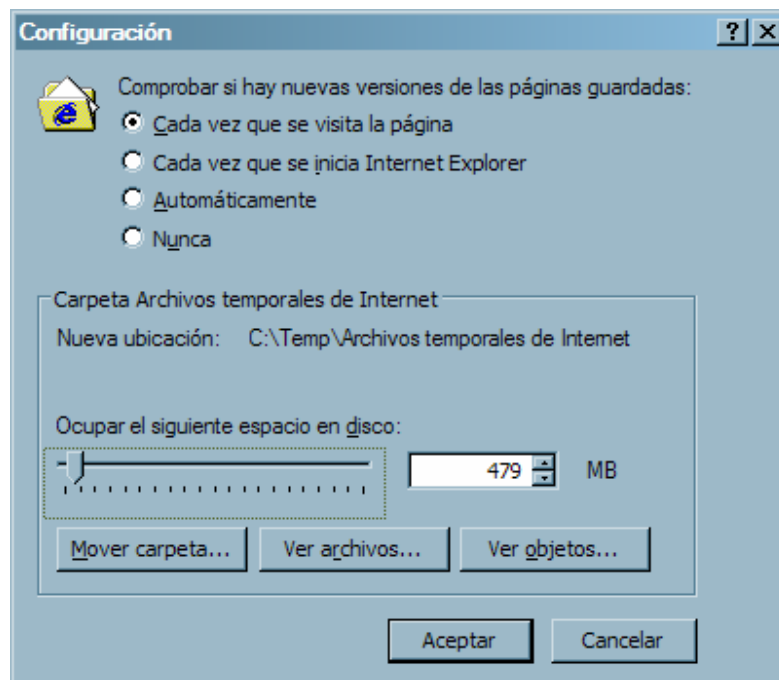
No dar opción a guardar archivos temporales



Esto lo conseguimos bajando la cuota de disco en lo que se refiere a Archivos temporales. Lo mínimo que podemos poner es 1MB, y marcamos la opción, “Cada vez que se visita la página”. Con esto conseguimos que cuando visitemos cualquier página nuestro navegador visualice la última actualización del site.

Problemas: Podemos experimentar una navegación más lenta, ya que no tendríamos caché para guardar páginas, pero gracias a las velocidades de conexión existentes en el mercado, prácticamente no existe diferencia.

Cambiar la ruta de acceso a Archivos Temporales



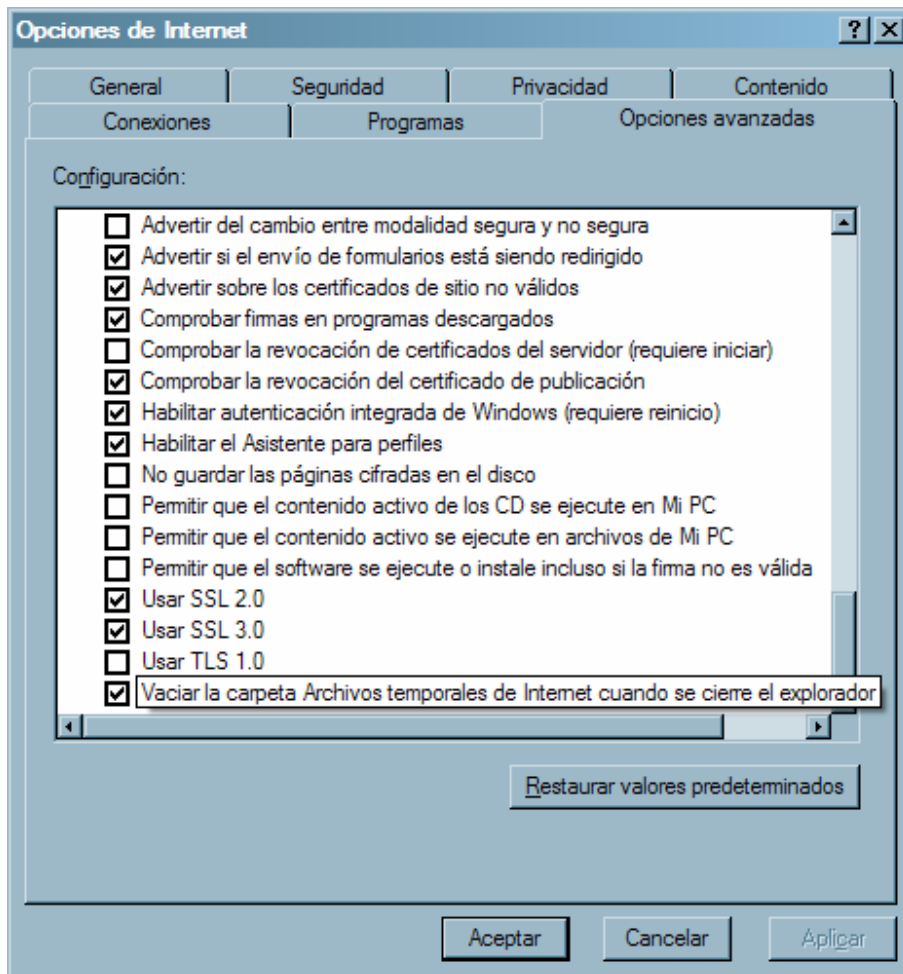
Todo script, sea malicioso o no, tiene que ser invocado por "ruta" completa y exacta. Podemos crear una carpeta nueva, y en las propiedades de Internet cambiamos la localización de los temporales de Internet a dicha carpeta. Al no encontrar una ruta exacta, los scripts no se ejecutarán.

Problemas: Recientemente me he encontrado con diversos Spyware y virus que creaban carpetas de Archivos temporales en las carpetas Temp de %SYSTEMROOT%, y del perfil de usuario. Con esto quiero decir que no es efectivo 100%.

Vaciar la carpeta Archivos Temporales

Tanto si aplicamos las opciones anteriores, como si no lo hacemos, esta opción es de obligado cumplimiento para el navegante.

Internet Explorer tiene una opción para borrar los archivos temporales una vez que se cierre el navegador. Con esta opción activada conseguiremos borrar scripts maliciosos que nos hayan inyectado desde cualquier Web.



Ejecutar Internet Explorer con permisos mínimos

Ejecutar nuestras aplicaciones con privilegios mínimos es fundamental en muchos casos:

- ✚ Ayudará a mantener nuestra privacidad
- ✚ Nos protegerá contra ataques
- ✚ Muchas vulnerabilidades no se ejecutarán, dado el mínimo nivel de privilegios

Para poder ejecutar el navegador Internet Explorer con permisos mínimos podremos utilizar la herramienta de [SysInternals psexec](#). Es una herramienta con la cual podremos ejecutar comandos y aplicaciones de forma local y remota. En este caso vamos a utilizarla de forma local. El comando resultante para lanzar Internet Explorer con privilegios mínimos será:

```
psexec -l -d "C:\Archivos de Programa\Internet Explorer\iexplore.exe"
```

Texto bajo Licencia Attribution 2.5 Spain License de Creative Commons

