El modo protegido en Internet Explorer

Debemos señalar que esta característica sólo existe desde Windows Vista y es fuente de muchos problemas. Examinemos cada una de sus particularidades.

1. Los niveles de integridad

Existen cuatro niveles:

- **Sistema**: se aplica a los componentes del sistema y no a las aplicaciones.
- **Alto**: se aplica a los procesos que se ejecutan con privilegios de administrador.
- **Medio**: se aplica a los procesos que se ejecutan en el entorno predeterminado.
- **Bajo**: lo utiliza Internet Explorer y Windows Mail cuando se ejecutan en modo protegido.

El nivel de privilegios se puede modificar una vez iniciado el proceso. El aislamiento de privilegios en la interfaz de usuario provoca tres consecuencias:

- Cualquier objeto "asegurable" que se haya creado mediante un proceso heredará el mismo nivel de integridad que el del proceso principal.
- Un proceso no podrá acceder a un recurso cuyo nivel de integridad sea más elevado que el suyo propio.
- Un proceso no puede enviar una ventana de mensaje a un proceso de nivel de integridad más elevado.

2. Funcionamiento del modo protegido

El aislamiento de privilegios en la interfaz de usuarios (*User Interface Privilege Isolation* o UIPI) impide a los procesos utilizar las API de usuario en modo de integridad elevada. De este modo, no será posible la instalación silenciosa de programas o la modificación de datos confidenciales. Cuando se ejecuta Internet Explorer en modo protegido se le asigna un nivel de integridad bajo. Por este motivo, no puede pasar de las operaciones de escritura en objetos que poseen un nivel de integridad más elevado.

En modo protegido, Internet Explorer sólo puede modificar los objetos ubicados en los siguientes directorios:

- \Documents and Settings\%USER PROFILE%
- \Local Settings\Temporary Internet Files
- \Local Settings\Temp
- \Local Settings\History
- \%USER PROFILE%\Favorites
- \%USER PROFILE%\Cookies

El esquema de funcionamiento obedece este principio:

- Internet Explorer se abre en modo protegido.
- El mecanismo de integridad (UIPI) se activa de forma automática.
- Las operaciones que necesiten privilegios de administrador utilizarán el proceso IEInstall.exe (Nivel de integridad alto).

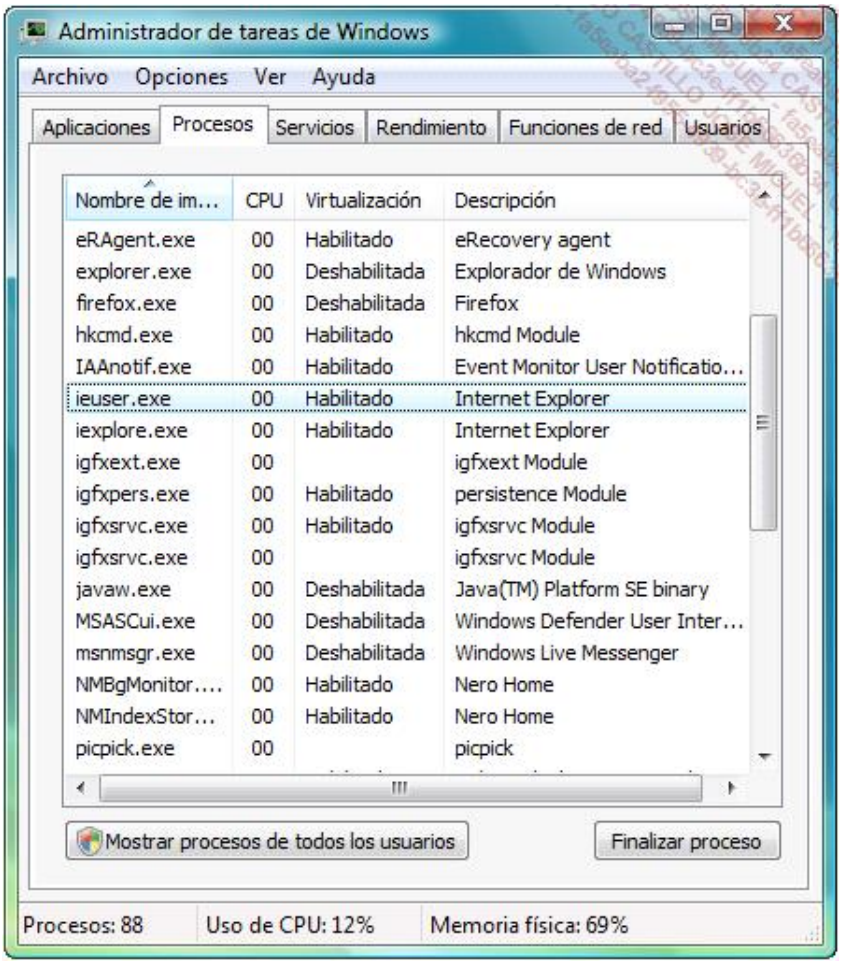
- Las operaciones que necesiten privilegios de usuario usarán el proceso IEUser.exe (Nivel de integridad medio).
- Finalmente, la capa de compatibilidad de aplicaciones ("Compatibility Layer") proporcionará unos privilegios de usuario bajos que permiten el funcionamiento del navegador.

Esta capa de compatibilidad le permite interceptar los intentos de escritura en objetos con un nivel de integridad medio y los redirige hacia las ubicaciones de nivel de integridad bajo:

- \%userprofile%\APPData\Local\Microsoft\Windows\TemporaryInternet Files\Virtualized
- HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Internet Registry

Los dos procesos (*IEInstall* et *IEUser*) provocan la aparición del cuadro de diálogo de elevación de privilegios en los casos siguientes:

- *IEUser.exe* le permite, por ejemplo, guardar los archivos en las ubicaciones con nivel de integridad alto. Tenga en cuenta que se trata de un proceso virtual.



- *IEInstal.exe* le permite instalar el Control ActiveX u otros módulos complementarios.

Mostramos un ejemplo práctico:

- Abra una página de Internet.
- Guarde la página en C:\Program Files.

Abra es mismo directorio.

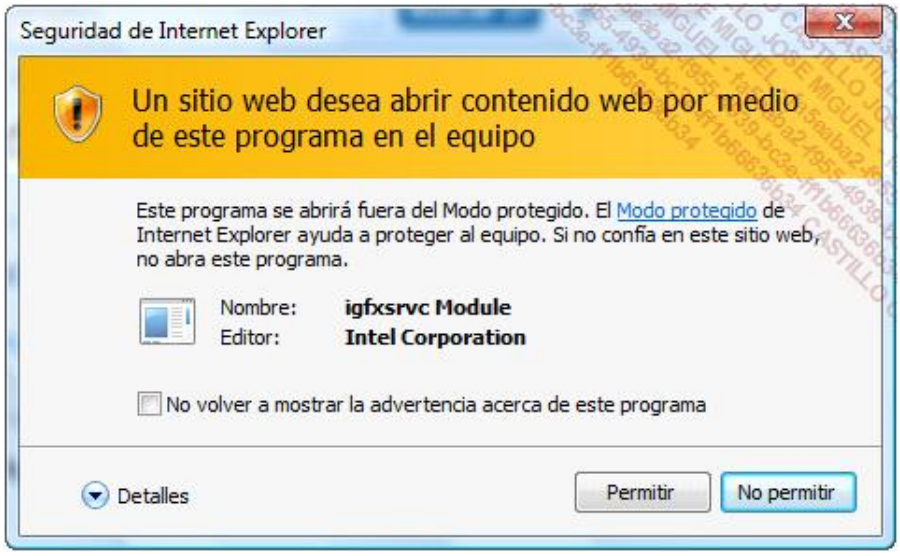
En el Explorador de Windows, la página HTML o MHT no se podrá encontrar. De hecho, el archivo se ha guardado de forma virtual en este tipo de árbol: C:\Usuarios\Nombre_de_usuario\AppData\Local\Temp\Low\lfg98KF.

Si desactiva el modo protegido y realiza la misma operación, la misma página se guardará, esta vez, en esta ubicación: C:\Usuarios\Nombre_de_usuario\AppData\Local\VirtualStore\Program Files.

El modo protegido se activa en las siguientes zonas de seguridad: *Internet*, *Intranet Local* y *Sitios Restringidos*, pero se desactiva en las zonas *Sitios de confianza* y *Equipo local*.

3. Otras consecuencias del modo protegido

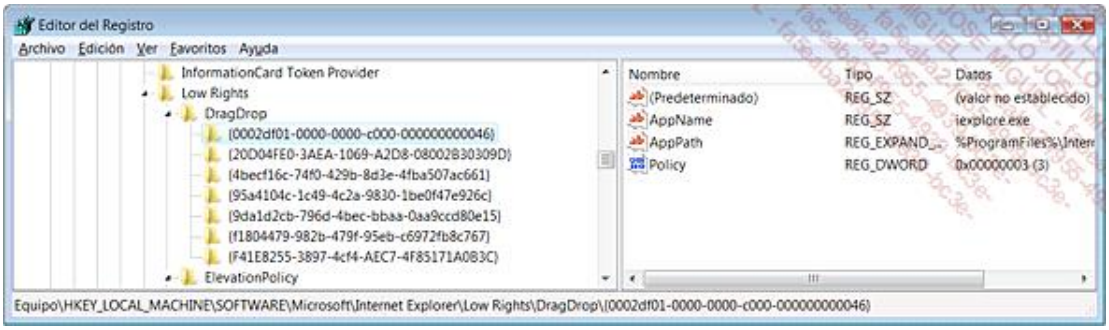
Internet Explorer incluye un mecanismo que impide que ningún código malicioso consiga comunicar o lanzar otro proceso. Por ejemplo, si una extensión del navegador intenta hacerlo, Internet Explorer le pedirá permiso antes de iniciar el proceso.



Si esta extensión posee su propio archivo ejecutable, podrá añadir una clave en el Registro que indique que el proceso es digno de confianza. El árbol de Registro que se modificará será el siguiente: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy.

En esta última clave, cree un nuevo GUID en el que añadirá estos tres valores:

- **`AppName`** (valor de cadena): nombre del archivo ejecutable.
- **`AppPath`** (valor de cadena): ubicación del archivo ejecutable.
- **`Policy`** (valor DWORD): la cifra 3 como información del valor.

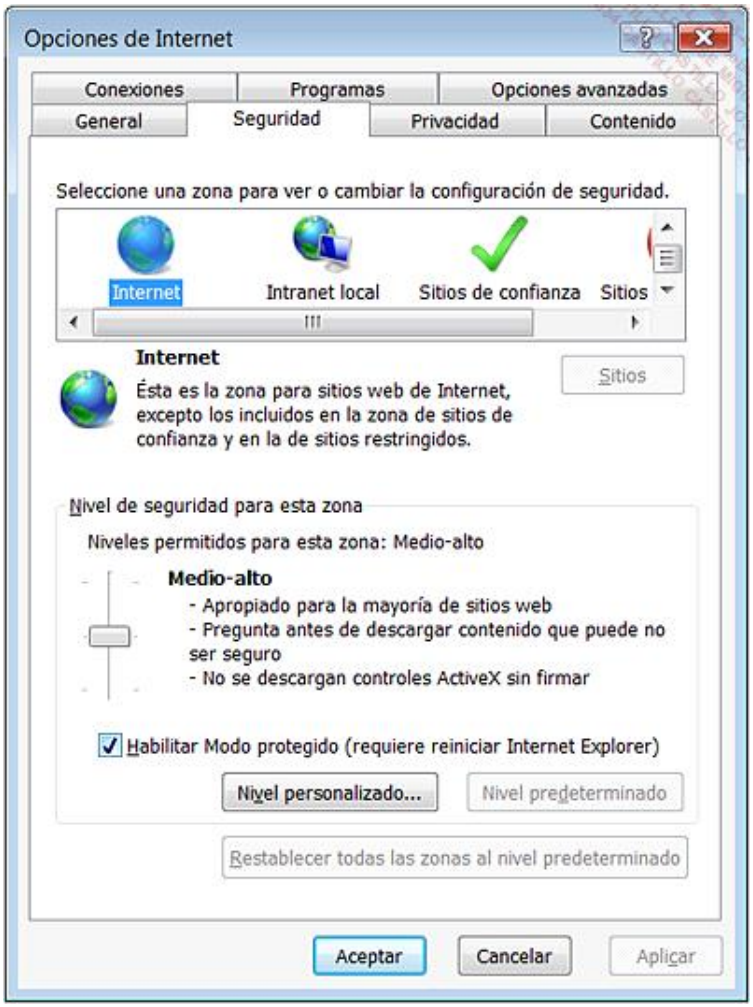


Le aparecerá el mismo cuadro de diálogo cuando intente mover el contenido de una página Web a otra aplicación. El mecanismo es idéntico al descrito anteriormente, con la única diferencia de que en este caso el árbol de registro correspondiente es: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Low Rights\DragDrop.

4. Desactivación del modo protegido

Para desactivar el modo protegido, siga el siguiente procedimiento:

- Haga clic en **Herramientas - Opciones de Internet**.
- Seleccione la casilla **Seguridad**.
- Marque o desmarque la casilla **Activar Modo protegido (requiere reiniciar Internet Explorer)**.



Observe que puede realizar esto para cada una de las zonas con esta característica.

La barra de estado de Internet Explorer, debajo de la ventana del navegador, indica el estado de la protección. Existen otras circunstancias que provocarán la desactivación del modo protegido:

- La desactivación del Control de cuentas de usuario.
- La ejecución de Internet Explorer en modo Administrador.
- Cuando se ejecuta Internet Explorer desde un archivo situado localmente en el disco. Esto no se aplicará si la página HTML se ha guardado en el disco pero proviene de la zona Internet.

Mostramos un resumen de casos particulares en los que el modo protegido no está activado:

- El Control de cuentas de usuario ("UAC") está desactivado.
- Internet Explorer se ejecuta como Administrador.
- La página se ha guardado desde una zona de seguridad que ya se considera como protegida.
- El modo protegido no está activado para la zona de seguridad en cuestión.

5. Modo protegido mejorado

Esta nueva funcionalidad de Windows 8 permite añadir una capa de seguridad complementaria al modo protegido existente desde Internet Explorer 7. Esta capa de protección ofrece seguridad contra los programas y scripts maliciosos que se ejecutan desde Internet Explorer, limitando la exposición de recursos del sistema operativo y sus datos personales. Uno de los efectos visibles de esta capa de protección es el bloqueo de la ejecución de plug-ins no compatibles con el modo protegido mejorado, por ejemplo el plug-in Adobe Flash en el momento de la redacción de esta obra.

En Windows 8, el navegador por defecto es Internet Explorer 10. Este navegador dispone de dos modos de funcionamiento. Si se ejecuta desde la pantalla de inicio, es decir en modo Interfaz de Usuario, el modo protegido mejorado está activo por defecto. En este modo de funcionamiento, Internet Explorer 10 no permite la ejecución de plug-ins, de este forma el modo protegido mejorado influye un poco en la experiencia de usuario. Desafortunadamente, todavía hay numerosos sitios web que necesitan utilizar plug-ins. Para permitir la visualización de este tipo de sitios, ejecute su navegador en el Escritorio de Windows. En este modo de funcionamiento, se permite utilizar plug-ins o módulos complementarios. Si el plug-in es compatible con el modo protegido no habrá mensajes de error. Por el contrario, en caso en que el plug-in sea incompatible con el modo protegido, un mensaje de notificación le pedirá que desactive el modo protegido solo para el sitio que quiere visitar.

Para desactivar el modo protegido mejorado para un sitio web:

- Desde el Escritorio Windows, navegue a un sitio que ejecute un módulo complementario no compatible con el modo protegido mejorado.
- Un mensaje de notificación indica que se ha bloqueado la ejecución del módulo complementario identificado y no compatible con el modo protegido mejorado.
- Haga clic en el botón **Desactivar** en la zona de notificación.

Para desactivar el modo protegido para el equipo:

- Desde el Escritorio Windows, abra las opciones de Internet Explorer 10.
- En la pestaña **Opciones avanzadas**, sección **Seguridad**, desactive la opción **Habilitar el modo protegido mejorado**.