

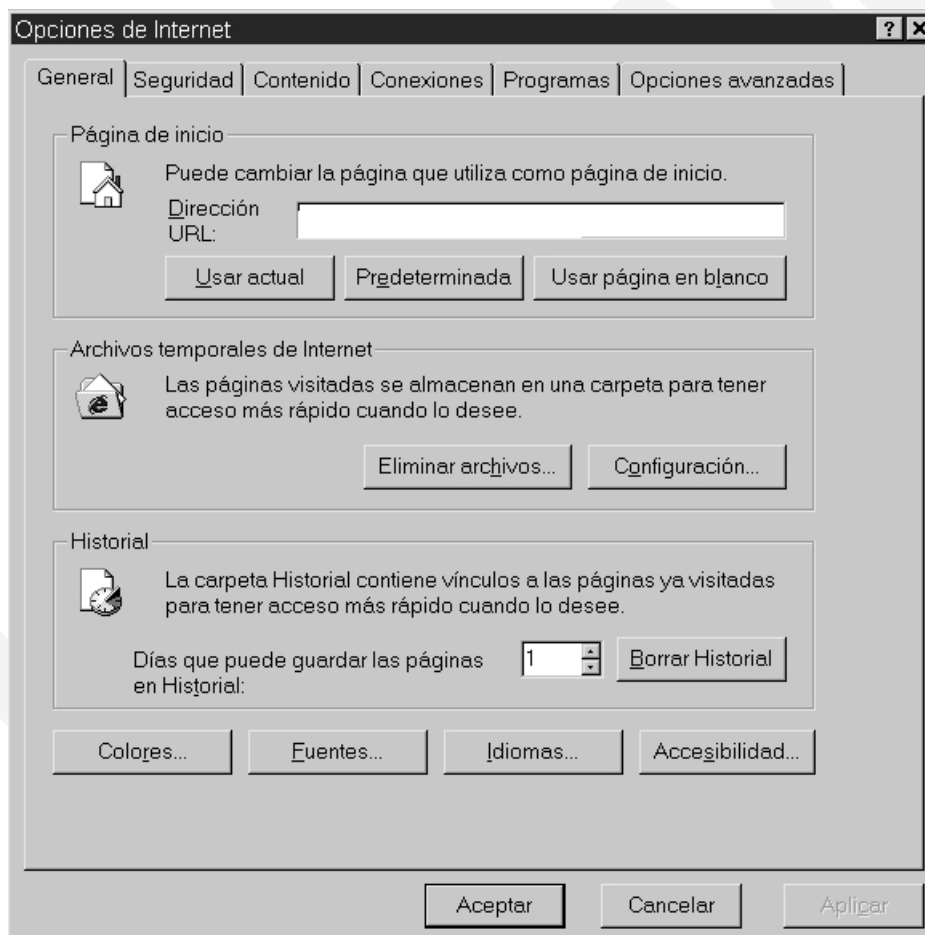
Configuración segura de Internet Explorer

A continuación, se examinarán las opciones que deben configurarse para aumentar la seguridad en la navegación con Internet Explorer. Se dejarán de lado otras características que no afecten directa o indirectamente a la seguridad e intimidad en la navegación.

En este navegador, estas opciones se encuentran agrupadas en el menú Herramientas, bajo el comando Opciones de Internet.... Nos iremos refiriendo a cada una de las seis pestañas que contiene la ventana desplegada, describiendo aquellas opciones relevantes para la navegación segura.

Pestaña General

En Archivos temporales de Internet se puede configurar el tamaño de cache de disco y su localización, pulsando el botón de Configuración. Se aplican los mismos comentarios y consejos que se vieron para Netscape.

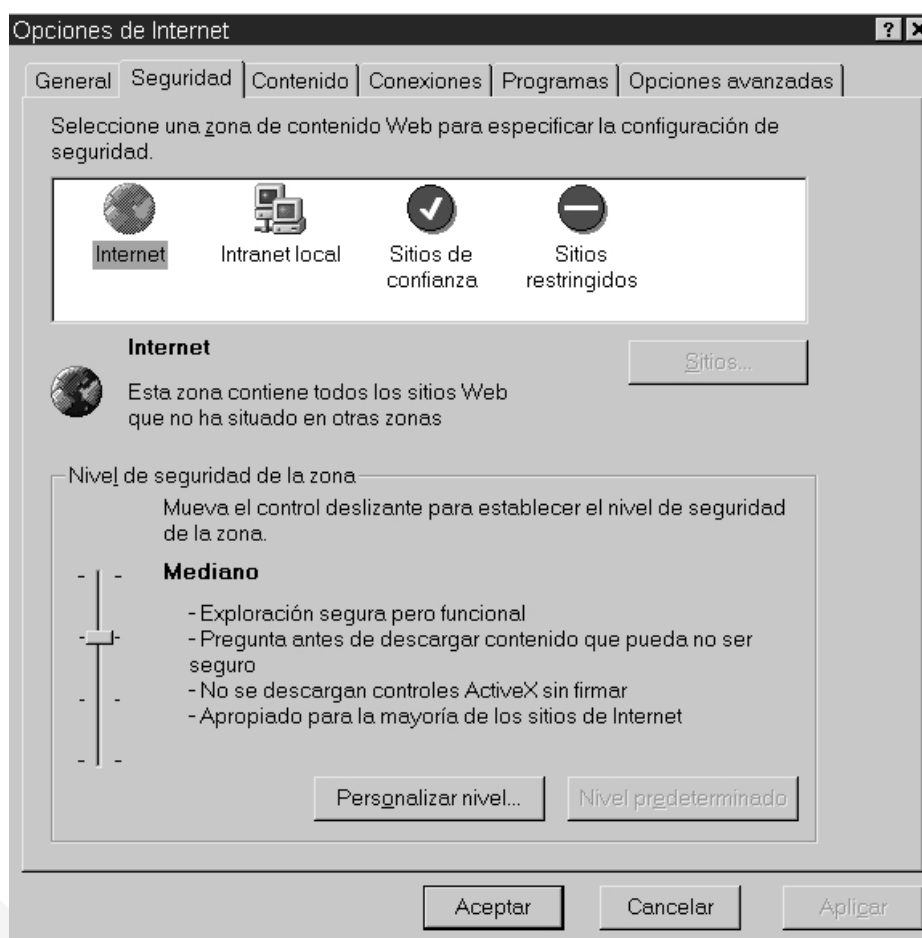


En Historial se puede configurar el número de días que Internet Explorer mantiene las páginas visitadas. Se aplican los mismos comentarios y consejos que se vieron para Netscape.

Pestaña Seguridad

Desde la versión 4.x de Internet Explorer, la seguridad al navegar se fundamenta en las zonas de seguridad, que constituyen un medio de reducir la complejidad de la seguridad del sistema al asignar políticas de seguridad a grupos enteros de sitios.

Microsoft Internet Explorer 4.0 ó superior divide el mundo de Internet en cuatro categorías o zonas, a cada una de las cuales se le puede asignar individualmente su propia configuración.



De ahí en adelante, cada sitio web sería asignado a su zona correspondiente con el nivel de seguridad adecuado.

El nombre de la zona de Internet en la que se está navegando aparece en la barra de estado en la parte inferior derecha.

De esta forma, cada vez que intente abrir un sitio o descargar contenido de la web, Internet Explorer comprobará la configuración de seguridad.

Además, se supone que los archivos de su equipo local son completamente seguros, por lo que no se les aplica la configuración de seguridad. Esta característica le permite abrir y ejecutar archivos y programas de su equipo sin preguntas ni interrupciones.

Para agregar sitios web a una zona de seguridad, en la lista Zona, seleccione Zona de sitios de confianza o Zona de sitios restringidos. Pulse en Agregar sitios y escriba la dirección URL del web y pulse en Agregar.

Por su parte, a cada zona se le puede asignar su propio nivel de seguridad. Estos niveles de seguridad se aplicarán a todo código descargado desde sitios de la zona en particular. En la tabla Niveles de seguridad para las zonas se listan los distintos niveles de seguridad.

En la Figura se muestra cómo se puede acceder al cuadro de configuración de las zonas de seguridad en Internet Explorer. En el menú desplegable Zona se puede elegir la zona que se desea configurar, con el nivel de seguridad Alto (el más seguro), Medio (seguro), Bajo (No recomendado normalmente) o Personalizar (sólo para usuarios expertos).

Si se elige Personalizar, se activará el botón Configuración..., que una vez pulsado abre la ventana más críptica de todas cuantas presenta Internet Explorer.



Desgraciadamente, la recomendación entre paréntesis (sólo para usuarios expertos) puede disuadir a muchos navegantes que no se consideran tales de configurar personalmente la seguridad. Si, a pesar de todo, decide entrar en la ventana de configuración, se encontrará con una jerga difícil, que puede terminar por confundirle. Se intentará arrojar luz sobre estas opciones, con el fin de que ningún usuario de Internet Explorer renuncie a la configuración personalizada de su seguridad por no entender las opciones que se le presentan.

Controles y complementos para ActiveX: especifica cómo reaccionará el navegador ante controles ActiveX. En el contexto de Internet, un control ActiveX es un objeto ejecutable que se inserta dentro de una página web. Este control se comporta como cualquier otro programa convencional que tenga instalado en su ordenador, sin ningún tipo de restricciones a lo que puede hacer.

Por su elevadísimo riesgo, se recomienda que en todos los casos se seleccione la opción de Pedir datos para que se solicite su aprobación antes de emprender acciones relacionadas con los controles ActiveX. Si no desea arriesgarse, desactive todos y si al navegar

por Internet se encuentra con uno, le aparecerá una ventana informándole de que no lo puede ejecutar porque su configuración de seguridad lo impide. Sopesese cuidadosamente si el sitio que lo envía es de fiar y si de verdad le merece la pena ejecutarlo, y en caso afirmativo, cambie la configuración activando los permisos. Recuerde que si lo ejecuta, le abre de par en par las puertas de su ordenador, permitiéndole hacer lo que quiera.

Autenticación del usuario: especifica cómo desea administrar las solicitudes de servidores que necesitan información de inicio de sesión. Los servidores de redes internas (intranets), y en algunos casos sitios web de Internet, requieren frecuentemente un nombre de usuario y una contraseña para limitar el acceso únicamente a los usuarios autorizados. Se recomienda que seleccione Preguntar por el nombre de usuario y la contraseña para conectar a un servidor y proporcionar un nombre y una contraseña cuando lo solicite.

Descargas: dado que al descargar archivos siempre se le pedirá confirmación, puede activar la descarga de archivos sin problemas. Eso sí, cuando le aparezca el cuadro preguntándole qué desea hacer con el archivo descargado, nunca responda que desea abrirlo directamente. En su lugar, guarde el archivo o programa en disco y ábralo o ejecútelo después de tomar precauciones como las siguientes:

- 1- Comprobar el archivo con un detector de virus.
- 2- Guardar su trabajo y cerrar los demás programas.
- 3- Desconectarse de Internet u otra conexión de red. Para mayor seguridad, asegúrese de que la casilla de verificación Preguntar siempre antes de abrir este tipo de archivo esté activada.

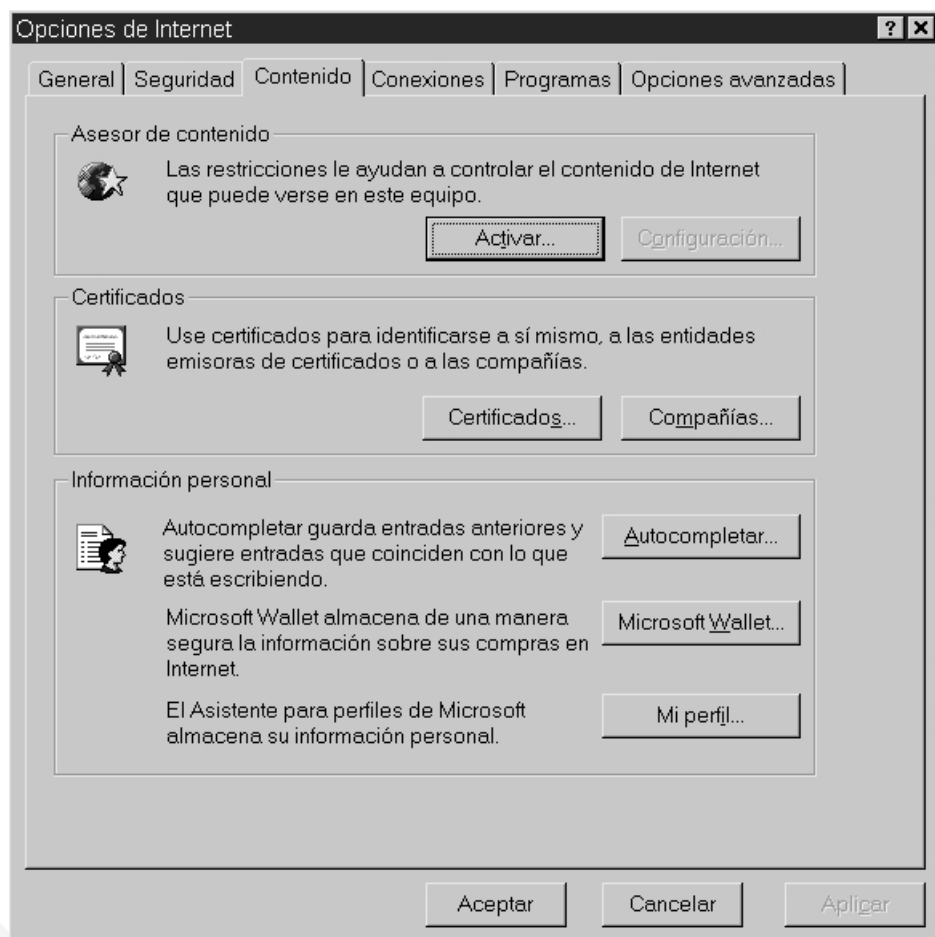
Java: especifica el nivel de seguridad con que permitirá que se ejecuten las applets de Java sin pedirle antes confirmación de los permisos necesarios. Normalmente, las applets de Java carecen de acceso a archivos, carpetas y conexiones de red del equipo, puesto que se ejecutan en un recinto de seguridad sin ningún privilegio. Ahora bien, si una applet de Java requiere un acceso mayor del que se ha especificado, se le pedirá que otorgue más permisos a la applet. Se pueden especificar configuraciones individuales para cada tipo de acceso que puede requerir una applet, seleccionando la opción Personalizada y pulsando a continuación en el botón Configuración de Java personal... que aparecerá. Sin embargo, esta configuración requiere conocimientos sofisticados de Java, por lo que se recomienda la opción más conservadora de seleccionar Seguridad alta. También se le ofrece la oportunidad de desactivar Java si así lo desea, lo cual sólo se recomienda en el caso de utilizar para navegar un ordenador con datos altamente sensibles.

Misceláneo: aquí se configuran una serie de rasgos diversos, como el nivel de seguridad que desea asignar a los canales de distribución de software de esa zona, que se recomienda sea Seguridad alta para permitir únicamente la notificación, pero no permitir la descarga e instalación automáticas. En todos los demás casos se recomienda la opción de Pedir datos para que se le pida aprobación antes de continuar.

Automatización: muchos usuarios tienen dificultades intentando desactivar JavaScript en Internet Explorer, sin llegar a encontrar por ningún sitio cómo hacerlo. Aquí se oculta la opción, en Automatización activa. Al igual que ha ocurrido con Netscape Communicator, la gran mayoría de agujeros de seguridad que se han descubierto en Internet Explorer están directamente relacionados con la forma de implantarse estos lenguajes en el navegador. Si, por precaución, selecciona la opción Pedir datos, cada vez que acceda a una página que albergue código de JavaScript se le presentará una ventana con la pregunta ¿Desea permitir la ejecución de los archivos de comandos?, que puede terminar resultando molesta si todas las páginas web de un sitio utilizan JavaScript. Dependiendo del riesgo que desee correr, puede activarlo o desactivarlo a su gusto.

Contenido

Al igual que NetWatch en Netscape, incorpora un Asesor de contenidos para ayudarle a controlar el tipo de contenidos de Internet a los que tiene acceso su equipo. Una vez activado el Asesor de contenido, sólo podrán mostrarse los contenidos restringidos que satisfagan o excedan los criterios que determine.



Con el fin de evitar que otros usuarios vean o cambien su configuración, ésta se protege mediante una contraseña. A partir del momento en que se activa el Asesor de contenido, nadie que use su navegador podrá saltarse las restricciones.

El inconveniente de utilizar el Asesor es que si no se activa la casilla Los usuarios pueden ver sitios sin clasificación (en la pestaña General dentro de Asesor de contenido), al ser tan pocas las páginas actualmente clasificadas, la navegación se volvería prácticamente imposible. Esto empuja normalmente a activar dicha casilla, con lo cual se podrá navegar por la casi totalidad de sitios Internet, especialmente con contenidos violentos o sexuales, los cuales con toda seguridad no incluirán una clasificación. Este obstáculo vuelve este sistema inservible en la práctica.

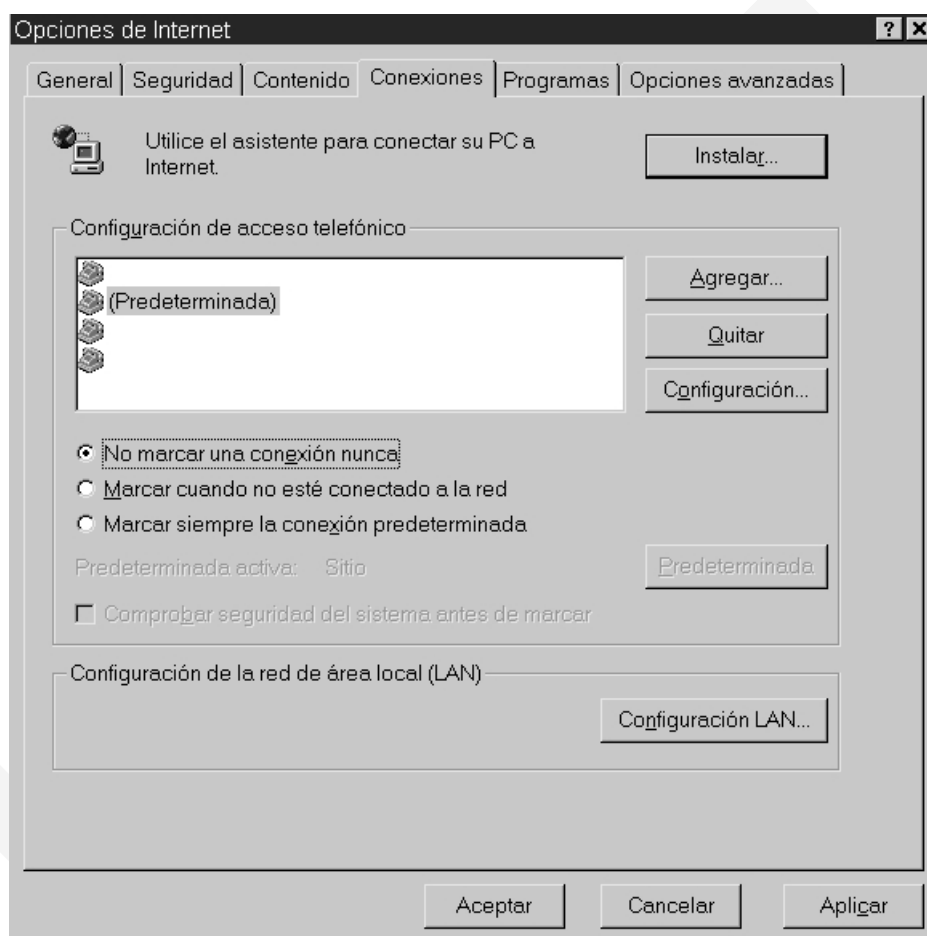
En Certificados se pueden examinar los certificados actuales.

En Información personal puede editar su perfil con toda la información acerca de su persona: nombre, domicilio, negocios, dirección de correo electrónico, certificados, etc. Esta

información se compartirá con páginas web que lo requieran, manteniendo su intimidad y seguridad. Mediante este método se le evita tener que escribir repetidamente la misma información, como su nombre o dirección de correo electrónico, cada vez que visite un nuevo sitio web. Al mismo tiempo, no se podrá ver esta información en su equipo ni se podrá compartir con otros sin su permiso. En la práctica, son tan pocos los sitios web que la solicitan que no merece la pena que rellene los datos. También dispone de la opción de pagos a través de Internet, que le permitirá trabajar con Microsoft Wallet. Respecto a los problemas potenciales de la función de autocompletado, consulte Cómo no recordar contraseñas en Internet Explorer.

Conexión

Desde esta pestaña se puede configurar el servidor proxy de acceso a Internet. Se aplican los mismos comentarios y consejos que se vieron para Netscape.

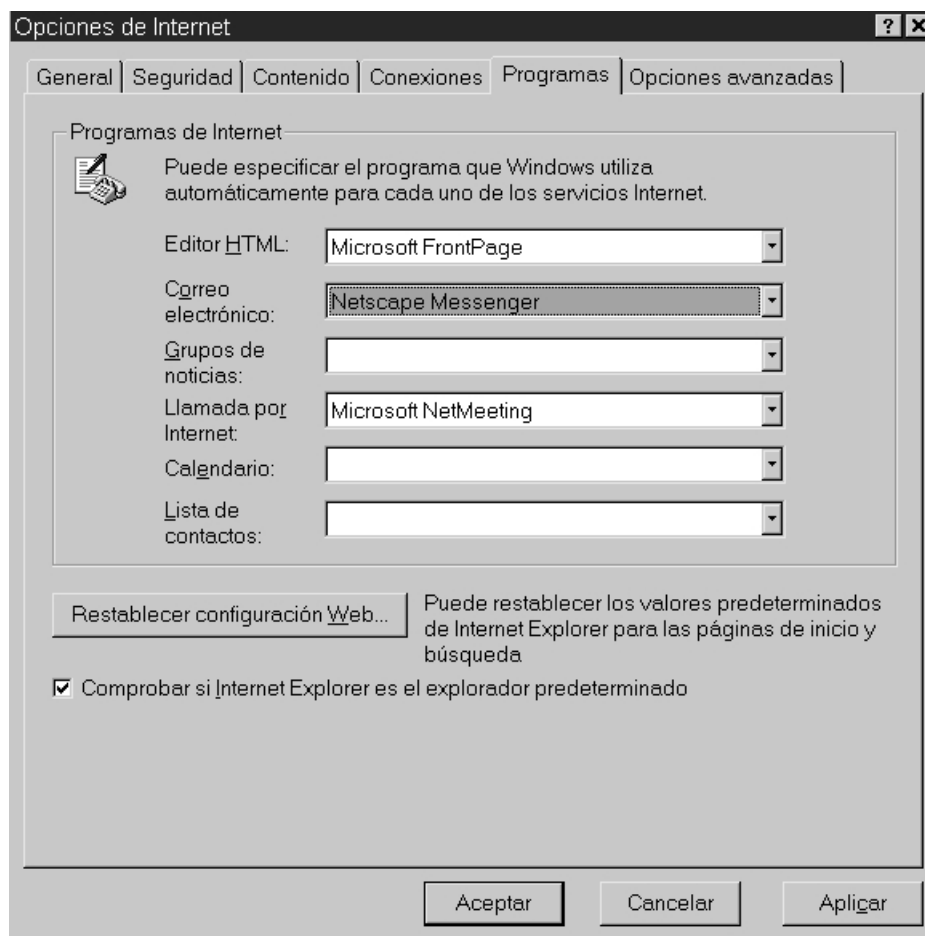


Programas

Ofrece la posibilidad de configurar qué programa de correo y lector de noticias desea utilizar integrado con Internet Explorer. Generalmente, al instalar la versión 4.x del navegador se instala asimismo el cliente de correo Outlook Express, que aparecerá como predeterminado, de manera que en el futuro, cada vez que envíe correo desde Internet Explorer se hará a través del programa que se haya especificado aquí.

Si no desea que sitios web obtengan inadvertidamente su dirección de correo, como se discutió al hablar de la Identidad en Netscape, debería configurar Outlook Express (o su

cliente preferido) con una cuenta falsa (en Outlook Express se hace en Herramientas/Cuentas.../Pestaña Correo/Botón Agregar/Correo...).



Por supuesto, resulta menos complicado leer las ventanas de aviso que se le presentan mientras navega, ya que Internet Explorer (a diferencia de Netscape Navigator, que lo hace desde las versiones 4.x en adelante) siempre le avisará antes de enviar correo automáticamente, en vez de enviar correos sin ton ni son.

Opciones avanzadas

Conviene activar todas las casillas que aparecen bajo Seguridad:

Avisar si el envío de formularios cambia de dirección, es decir, si la información rellena-da en el formulario se envía a un sitio web distinto del sitio que le presentó el formula-rio.

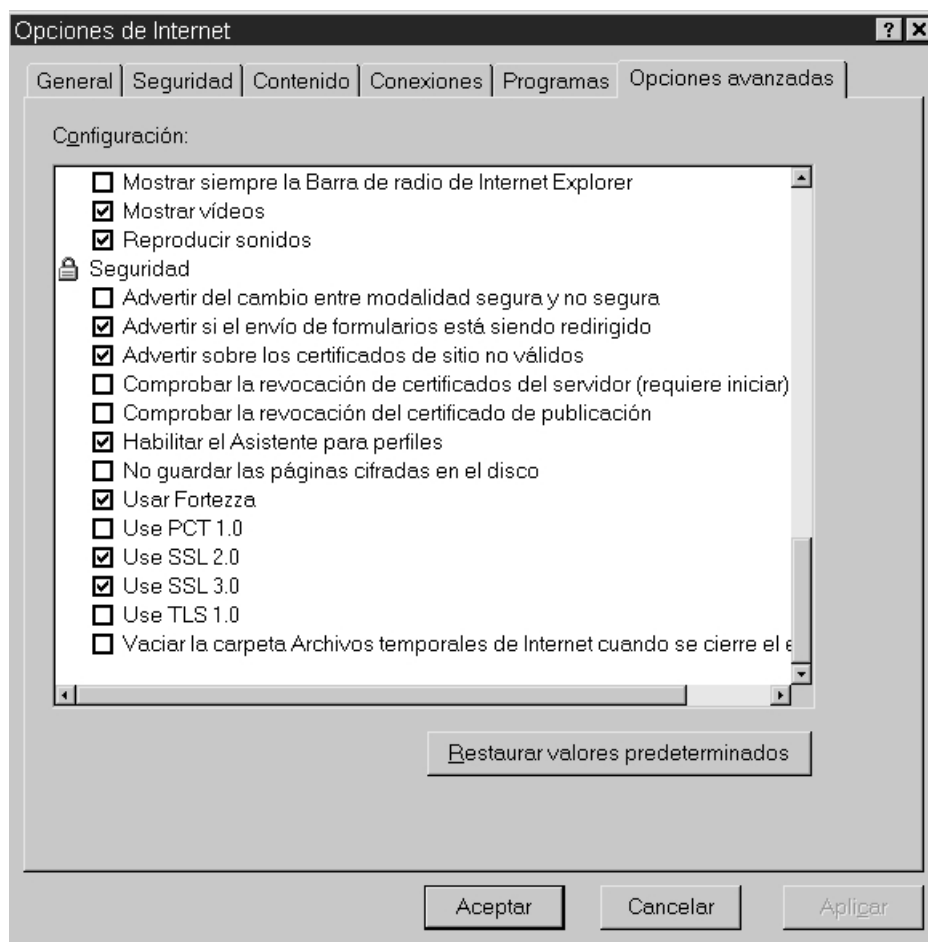
SSL 2.0 y SSL 3.0, para especificar que desea enviar y recibir información segura a tra-vés de Secure Socket Layer, versiones 2.0 y 3.0 respectivamente. Conviene activar am-bos.

Advertir sobre los certificados de sitio no válidos, cuando la dirección URL de un certifi-cado de seguridad de un sitio de Internet no sea válida.

Advertir del cambio entre modalidad segura y no segura, cuando se está moviendo en-tre sitios de Internet que no son seguros.

PCT 1.0, que especifica que desea enviar y recibir información segura a través de PCT (Private Communications Technology, Tecnología privada de comunicaciones), protocolo

desarrollado por Microsoft y mucho más seguro que SSL 2.0. Puede activarse sin problemas.



Al igual que en Netscape, por defecto las cookies se aceptan sin avisar. En esta opción se le ofrece la posibilidad de bloquearlas todas o avisar antes de aceptarlas. Se aplican los mismos comentarios y consejos que se vieron para Netscape al hablar de cookies.

Buscar revocación de certificado, con el fin de que Internet Explorer compruebe el certificado de un sitio para ver si se ha revocado antes de aceptarlo como válido.

No guardar las páginas a disco, que hace que la información segura no se guarde en el disco duro. Sólo se recomienda si está utilizando Internet Explorer desde un servidor compartido y no desea que otras personas vean su información segura.

Eliminar las páginas guardadas cuando se cierre el explorador, que permite borrar el contenido de la carpeta Archivos temporales de Internet cuando cierra el explorador. Sólo se recomienda si le preocupa el problema del cache, como se discutió más arriba.

Si desea que Internet Explorer cree un registro de toda la actividad de Java, active la casilla de verificación Consola Java activada. Esta opción le resultará muy útil en el caso de que una applet maliciosa ocasione algún desperfecto en su sistema, ya que le permitirá rastrear sus acciones.

Las mismas reflexiones que se hicieron con respecto a los plug-in en Netscape, se pueden aplicar al caso de Internet Explorer.