¿ESTÁ PROTEGIDO TU NAVEGADOR WEB?

Hoy en día, el navegador web se ha convertido en una parte imprescindible del uso de Internet. La mayoría de funcionalidades que hace algunos años se llevaban a cabo desde diferentes programas o con distintos protocolos, se han trasladado hoy a la WWW (World Wide Web) y por tanto, se realizan desde el navegador web.

La tecnología y conciencia social que ha permitido esto, es lo que se denomina Web 2.0. Para poder soportar técnicamente toda esta nueva carga de trabajo, los navegadores web han multiplicado en los últimos años su complejidad y funcionalidades, lo que implica que también se hayan multiplicado el número de riesgos por los que pueden ser atacados.

Además, la progresiva securización del resto de componentes de los sistemas operativos (por ejemplo, la introducción de cortafuegos de serie en Windows, o el filtrado de archivos potencialmente peligrosos en el correo) ha hecho que los atacantes necesiten explorar nuevas vías para poder infectar los sistemas. Así, el navegador web se ha convertido poco a poco en un método eficaz para infectar, puesto que es una herramienta ubicua y desde el punto de vista de los atacantes, permite entrar en el sistema sin tener que eludir otras restricciones de seguridad.

I La importancia de proteger el navegador web

Los atacantes han encontrado en los navegadores web una vía rápida para entrar en el sistema operativo que quieren comprometer por varias razones:

- Si el navegador web sufre de alguna vulnerabilidad, es posible que se pueda ejecutar código arbitrario en el sistema con solo visitar un enlace. Aunque muchos usuarios tomen las precauciones adecuadas en otros ámbitos (el correo), este problema todavía no está totalmente asumido en la navegación.

- El protocolo web, debido a su diseño, permite que solo una minuciosa exploración de una página web permita conocer qué se está visitando en cada momento.

- Cuanta mayor funcionalidad se pide a los navegadores web, mayores problemas de seguridad pueden sufrir. Actualmente, la configuración por defecto de muchos de estos programas no está especialmente alineada con la seguridad.

- Debido a las facilidades que les proporcionan, los atacantes se centran últimamente en buscar vulnerabilidades que afecten a los navegadores web. En los últimos tiempos, en el mercado negro de vulnerabilidades, las relativas a fallos graves en navegadores web son las más cotizadas.

- El navegador web y la navegación web en la era 2.0 se ha complicado hasta el punto que, para un usuario medio, resulta complicado entender todas las advertencias y mensajes de seguridad que muestra el navegador web, así como las tecnologías utilizadas (cada vez más complejas).

II Riesgos del navegador web

Para poder proteger el navegador web, primero es necesario conocer qué peligros intrínsecos están asociados a su utilización y las tecnologías que, en los últimos años, han sido aprovechadas en mayor medida para vulnerar su seguridad.

En un principio, los navegadores web fueron diseñados para interpretar páginas HTML[1] simples, pero poco a poco se le fueron añadiendo tecnologías para que la interacción con páginas web fuese mucho más completa y añadir así funcionalidades.

A continuación se describe una pequeña lista de tecnologías y características que están siendo utilizadas hoy en día para vulnerar los navegadores web.

JavaScript

JavaScript es una tecnología estándar (un lenguaje) que añade funcionalidad de programación a las páginas web. Con HTML no se pueden realizar programas en general, mientras que HTML+JavaScript permite crear todo tipo de funcionalidad. JavaScript se ejecuta del lado del cliente (navegador web) y no del servidor (página web que se visita).

En la práctica, con JavaScript se permite, por ejemplo, cargar contenido multimedia como Flash y muchos otros plugins[2]. JavaScript también suele ser utilizado para validar los datos antes de ser enviados a un formulario, y comprobar acciones del usuario: por ejemplo, se puede detectar cuándo se pasa el ratón por encima de una imagen, completar las sugerencias de un campo de búsqueda, etc.

JavaScript, por sus características básicas (ser responsable de la llamada a otros plugins y contener funcionalidades que permiten programar) se ha convertido en una de las funcionalidades con más riesgos (pero también indispensable) de los navegadores web modernos. La inmensa mayoría de los ataques de hoy en día son lanzados a través de llamadas a JavaScript.

Los navegadores web permiten deshabilitar JavaScript, pero el problema es que JavaScript es un estándar muy utilizado actualmente, por tanto, si se deshabilita, la

[1] Siglas de HyperText Markup Language (Lenguaje de Marcado de Hipertexto), es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes.

[2] Programa a modo de complemento que se añade al navegador web y permite interpretar nuevas funcionalidades.

funcionalidad de las páginas actuales se vería muy mermada. Con lo que es necesario establecer una política de confianza en la que se determine que ciertas páginas en las que se confían, podrán ejecutar JavaScript mientras que el resto, hasta que se demuestre que son confiables, no deberían poder hacerlo.

Java

Java es otro lenguaje de programación que añade funcionalidad a las web. Las páginas pueden alojar un código Java (llamado applet) que el navegador web recoge e interpreta en su máquina virtual Java (que previamente debe haber sido instalada en el sistema operativo).

Por tanto, se basa en que una página web envía código que será ejecutado en el cliente, y esto supone intrínsicamente una amenaza puesto que es necesario conocer qué intenciones tiene ese código y no permitir que pueda acceder a zonas del sistema operativo más allá de las que necesita la página web para funcionar.

La máquina virtual que ejecuta estos applets está diseñada para no permitir que este código acceda a las zonas sensibles del sistema operativo, pero en la práctica, los atacantes encuentran métodos y vulnerabilidades que permiten eludir la restricción.

ActiveX

ActiveX es una tecnología respuesta de Microsoft a Java. Su fin es el mismo, pero la forma de realizar las acciones es diferente.

En la práctica, se trata de archivos librería (los que poseen la extensión DLL) que son ofrecidos por una web y, una vez instalados, son ejecutados en local en el sistema para enriquecer la interactividad con esa página web. Al igual que Java, se basa en que una página web envía código que será ejecutado en el cliente, y esto supone una amenaza si no se conocen las intenciones del desarrollador.

Cookies

Las cookies son pequeños archivos de texto que el navegador web almacena y clasifica y que guardan información sobre una página web. Por ejemplo, cuándo ha sido la última vez que se ha visitado, el nombre de registro o el código de acceso para que no sea necesario introducirlo cada vez que se entra a una página.

Cada página puede dejar una cookie en el navegador web, y acceder a ella (y solo a ella) cuando lo necesite siempre que sea visitada. Por tanto, un dominio concreto solo puede acceder a una cookie y actualizarla, borrarla, etc.

Las cookies se convierten en un riesgo de seguridad en el momento en el que son utilizadas como elementos de rastreo (*tracking*) del usuario por empresas de publicidad. Las empresas de publicidad suelen emplazar los mismos anuncios incrustados en diferentes páginas. Según el diseño de las cookies, estos anuncios incrustados tienen acceso a una misma cookie independientemente de la página en la que se encuentren, puesto que los anuncios en sí, provienen todos de un mismo servidor. Son las llamadas cookies de terceras partes.

Por ejemplo, una página llamada pagina1.com puede contener un banner o anuncio publicitario cargado desde "anunciante.com/anuncio1.html". Pagina1.com puede almacenar en el equipo que la visite su cookie principal, mientras que la cookie de anunciante.com se llamará "de terceros".

Así, el problema surge cuando un mismo anuncio o dominio se encuentra alojado en diferentes páginas.

Por ejemplo, en el supuesto de que un anuncio de "anunciante.com/anuncio1.html" se encuentre incrustado en el dominio "pagina1.com" y otro anuncio del mismo domino "anunciante.com/anuncio2.html" alojado en "pagina2.com", ambos anuncios pueden acceder a la misma cookie de anunciante.com (puesto que pertenecen al mismo dominio) y saber desde qué dominio original (pagina1.com y pagina2.com) se ha realizado el acceso. Por tanto, anunciante.com podrá saber qué páginas visita el usuario y "rastrearlo". Esto le permite crear un perfil y usar esta información comercialmente.

Plugins

Parte de la funcionalidad de los navegadores web viene en forma de plugins. Estos son complementos adicionales que añaden funcionalidad extra al navegador web. En realidad, es un concepto parecido a los ActiveX o Java, pero en el caso de los plugins, solo pueden ser utilizados en el contexto del navegador web y nunca de forma independiente.

Pueden estar programados por terceras personas, lo que siempre añade un riesgo extra sobre su confiabilidad. Para mitigarlo, suele existir un repositorio oficial donde los desarrolladores pueden subir su complemento que, una vez validado oficialmente por la organización responsable del navegador web, se hace público para su utilización.

Aun así, existen plugins que, aun habiendo pasado la validación, han supuesto una amenaza de seguridad para los navegadores web.[3]

[3] http://www.hispasec.com/unaaldia/4284. Mozilla Firefox y la (in)seguridad de sus extensiones y complementos

Phishing

El navegador web es el medio por el que se consuma habitualmente el phishing. Cuando un usuario es víctima de un phishing, significa que ha ingresado a través de su navegador web en una página que simula ser la de su banco, y ha introducido en ella sus credenciales (que irán a parar al atacante). Los certificados y el SSL previenen de por sí esta técnica, pero debido al desconocimiento de la tecnología subyacente por parte del usuario medio, los atacantes tienen éxito en sus ataques incluso existiendo un remedio efectivo como son los certificados digitales.

Desde hace algunos años, todos los navegadores web incluyen una tecnología sencilla de lista negra de URLs para bloquear las direcciones catalogadas como phishing o peligrosas y así evitar que los usuarios puedan acceder a ellas. Esta tecnología suele estar basada en listas negras (y por tanto es reactiva y no preventiva).

Otros

El navegador web no deja de ser un programa que necesita ser actualizado para corregir los problemas de seguridad que surgen en él. Por tanto, como cualquier otra aplicación, necesita aplicar parches periódicamente para mitigar los potenciales riesgos, además de configurarlo preventivamente contra los fallos más comunes, que suelen ser aprovechados para estrechar la ventana de riesgo.

III Configuraciones básicas de seguridad de los navegadores web

La configuración básica de seguridad de un navegador web pasa por mitigar los principales riesgos expuestos anteriormente.

Se ofrecen a continuación unas claves sobre el uso y mantenimiento básico de los navegadores web más utilizados hoy en día: Microsoft Internet Explorer, Mozilla Firefox, Apple Safari y Google Chrome.

Tabla 1: Comparativa/Resumen de métodos de securización básica de navegador web

Riesgos	Microsoft Internet Explorer	Mozilla Firefox	Apple Safari	Google Chrome
JavaScript	Administrar las zonas de seguridad en las opciones de seguridad del navegador web	Instalar y administrar complementos de terceros como NoScript	Solo se puede, sin componentes adicionales, bloquear JavaScript por completo desde las opciones de seguridad	Opciones, Avanzadas, Configuración de contenido, JavaScript y administrar excepciones
Java	Administrar las zonas de seguridad en las opciones de seguridad del navegador web	Instalar y administrar complementos de terceros como NoScript	Solo se puede, sin componentes adicionales, bloquear Java por completo desde las opciones de seguridad	Es posible instalar complementos como NoScript
ActiveX	Administrar las zonas de seguridad en las opciones de seguridad del navegador web	No aplica, puesto que no son compatibles	No aplica, puesto que no son compatibles	No aplica, puesto que no son compatibles
Plugins	Descargar solamente plugins firmados desde páginas oficiales	Descargar solamente plugins firmados desde páginas oficiales	Descargar solo plugins desde páginas oficiales: https://extensions.apple.com/	Descargar solo plugins desde páginas oficiales: http://chrome.google.com/extensions/
Cookies	Herramientas, Opciones de Internet, Privacidad, No aceptar cookies de terceros	Herramientas, Opciones, Privacidad, No aceptar cookies de terceros	Preferencias, Seguridad, Aceptar cookies solo de sitios que visito	Opciones, Avanzadas, Privacidad, Ignorar las excepciones y evitar que se habiliten las cookies de terceros
Phishing	Herramientas, Opciones de Internet, Opciones Avanzadas, Activar SmartScreen	Herramientas, Opciones, Seguridad, Bloquear sitios reportados	Preferencias, Seguridad, Advertir al visitar un sitio web fraudulento	Opciones, Avanzadas, Privacidad, Habilitar protección contra phishing y software malintencionado
Actualizaciones	Panel de control de Windows, Activar las actualizaciones automáticas	Herramientas, Opciones, Avanzado, Buscar automáticamente actualizaciones	Actualizar con el sistema operativo	Mantiene su propio sistema de actualización silenciosa y automática
Otros	Herramientas, Opciones de Internet, Opciones Avanzadas	Escribir en la barra de navegador web about:config y filtrar por la palabra deseada		Dispone de una gran cantidad de extensiones, al igual que Firefox

Fuente: INTECO

Microsoft Internet Explorer

Las versiones anteriores a la actual (Microsoft Internet Explorer 8), no contenían métodos suficientes para prevenir amenazas y además, sufría de un gran número de

vulnerabilidades que permitían a atacantes ejecutar código de forma inadvertida (malware, normalmente) en el sistema. Esto ha cambiado sustancialmente con esta última versión (y sigue una evolución positiva en su inminente versión 9), puesto que estas se centran fundamentalmente en la seguridad.

La seguridad de Microsoft Internet Explorer está basada en las *zonas de seguridad*. Las zonas son una clasificación lógica que hace el navegador web de las distintas páginas que se visitan, de forma que a cada zona se le permiten ciertas licencias sobre el sistema. Cuando se visita un sitio, el sistema lo encaja dentro de una zona y se restringe la capacidad de acción según lo definido en cada zona.

Microsoft Internet Explorer permite la agrupación de la Red en general en varias zonas, según el nivel de confianza que se tenga en ellas. Las zonas son “Internet”, “Intranet Local”, “Sitios de Confianza” y “Sitios Restringidos”. Cada una puede ser configurada para que, a las páginas clasificadas en esa zona, se le aplique un nivel de seguridad "alto", "medio-alto", "medio", "medio-bajo" y "bajo". A su vez, cada nivel es configurable con otras opciones individuales de seguridad.

Tabla 2: Configuración de seguridad y características de las Zonas de seguridad Microsoft Internet Explorer

Zona	Configuración de seguridad por defecto/recomendada	Características
Internet	Seguridad Media / Seguridad Alta	Es la zona donde se clasifican todas las páginas por defecto. No se pueden añadir sitios específicos. Supone todo el resto de lugares que no encajan en las otras zonas y en los que, por tanto, no se debe confiar. Todas las direcciones o dominios que se introduzcan en el navegador web y que contienen un punto, por defecto, pertenecen a esta zona a no ser que se especifique lo contrario.
Intranet Local	Seguridad media-baja / Seguridad Media	Es la zona donde se clasifican las direcciones dentro de una red interna (por ejemplo, las páginas o elementos compartidos dentro de una empresa).
Sitios de Confianza	Seguridad Media / Seguridad Media	Es una lista blanca donde se pueden introducir las direcciones web de las páginas en las que se confía y por tanto, se les aplicará una configuración de seguridad específica (más relajada). Acepta "comodines" en forma de *.dominio.com, de forma que se clasifican en esta zona todos los subdominios de dominio.com de forma automática.
Sitios Restringidos	Seguridad Alta / Seguridad Alta	Es una lista negra donde se pueden introducir las direcciones web de las páginas en las que no se confía y por tanto, se les aplicará una configuración de seguridad específica (más restrictiva). Acepta "comodines". Es recomendable usar la opción de lista blanca y no utilizar los sitios restringidos, puesto que lo ideal es que todos sean restringidos con seguridad alta (en la zona de Internet) excepto los de confianza.

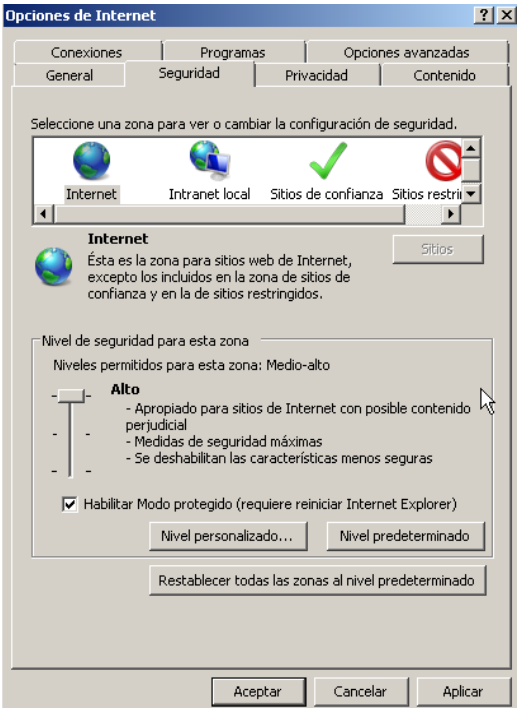
Fuente: INTECO

Para poder configurar el nivel de confianza que se tiene en estas zonas, desde IE, se debe ir a “Herramientas”, “Opciones de Internet” y pulsar sobre la pestaña de “Seguridad”. Es recomendable cambiar la configuración por defecto que ofrece Microsoft para aumentar la seguridad del navegador web Microsoft Internet Explorer.

JavaScript, Java y ActiveX

El consejo básico es restringir al máximo la zona de Internet, desactivando la mayoría de las posibilidades de ejecución de código. Es posible que esto vuelva incómoda la navegación, puesto que al restringir JavaScript, ActiveX, etc, las funcionalidades con las que fueron diseñadas las páginas pueden no funcionar. Para solucionar esto, es posible usar los "sitios de confianza". Es una lista blanca y concreta de lugares habituales de los usuarios y que sean de confianza. Por tanto, en estos sitios es relativamente seguro el uso de estas tecnologías. Así, la lista de sitios de confianza queda configurada con una seguridad más relajada que permite que funcionen correctamente.

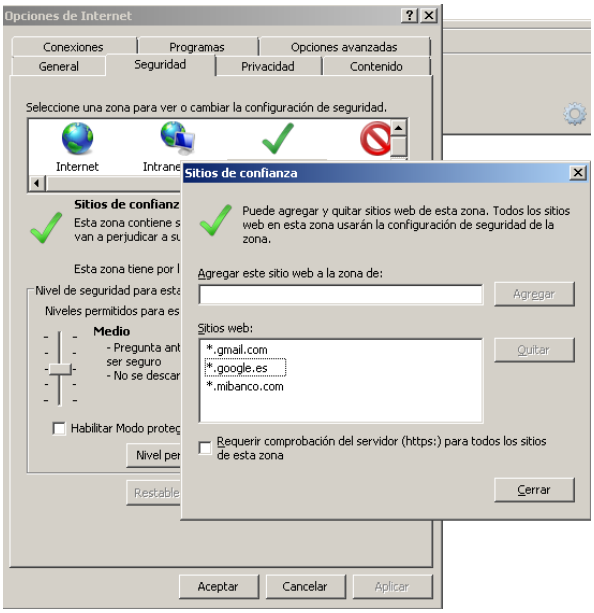
Ilustración 1: Nivel de seguridad "alto" en la zona de Microsoft Internet Explorer



Fuente: INTECO

No se considera una buena política de seguridad añadir dominios a la zona restringida, pues resulta una tarea tediosa (e impracticable, a la larga) de recopilación de posibles dominios. La combinación de la zona de Internet (a la que pertenecen todas las páginas por defecto) muy asegurada y una seguridad más relajada para los Sitios de Confianza es lo más recomendable una vez se han recopilado las páginas más visitadas que pueden no funcionar correctamente debido a las restricciones impuestas.

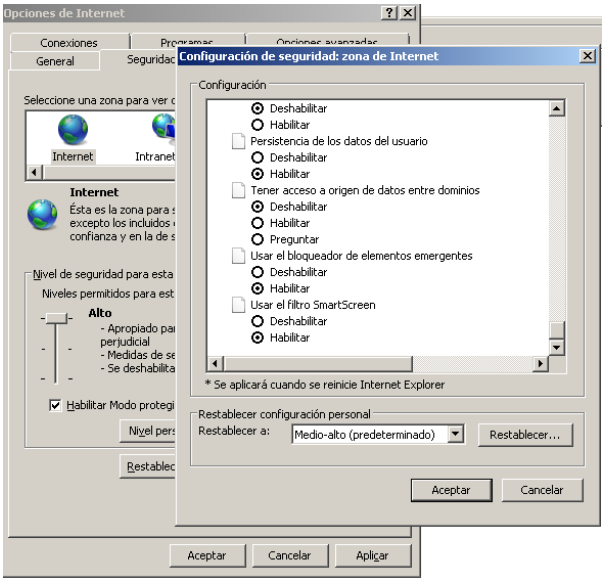
Ilustración 2: Añadir webs de confianza en la zona de Sitios de confianza de Microsoft Internet Explorer



Fuente: INTECO

Para una mayor granularidad en el proceso, además de los niveles "alto", "medio-alto", etc, se puede pulsar sobre "nivel personalizado" y modificar algunas opciones. En este panel es posible encontrar la configuración específica para controlar la ejecución de Java, ActiveX y JavaScript.

Ilustración 3: Niveles personalizados de configuración de las Zonas de seguridad de Microsoft Internet Explorer

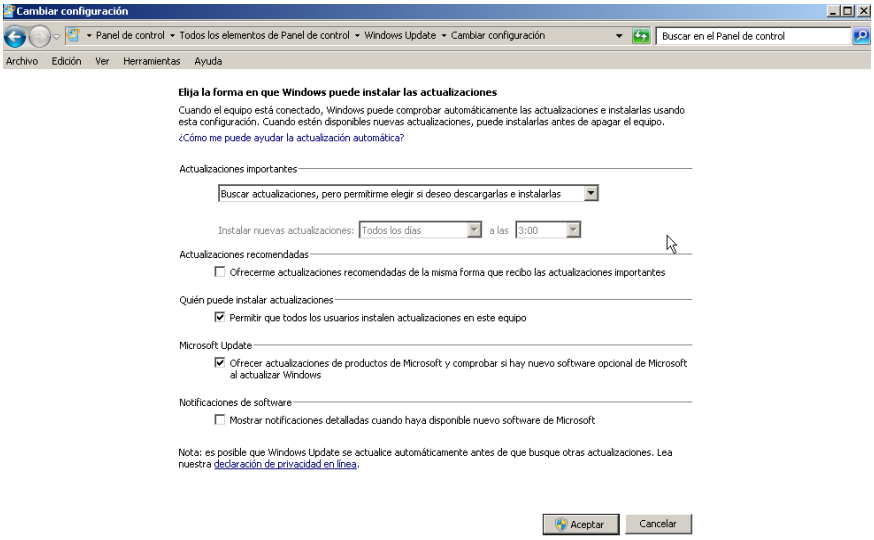


Fuente: INTECO

Actualización del navegador web

Para actualizar el navegador web, junto con el resto del sistema operativo, es recomendable programar las actualizaciones automáticas integradas. Es un sistema interno que comprueba la existencia de parches de seguridad y los instala de forma automática. Esto protege de los fallos de seguridad que, periódicamente, se encuentran en el navegador web.

Ilustración 4: Actualizaciones de seguridad en Windows 7



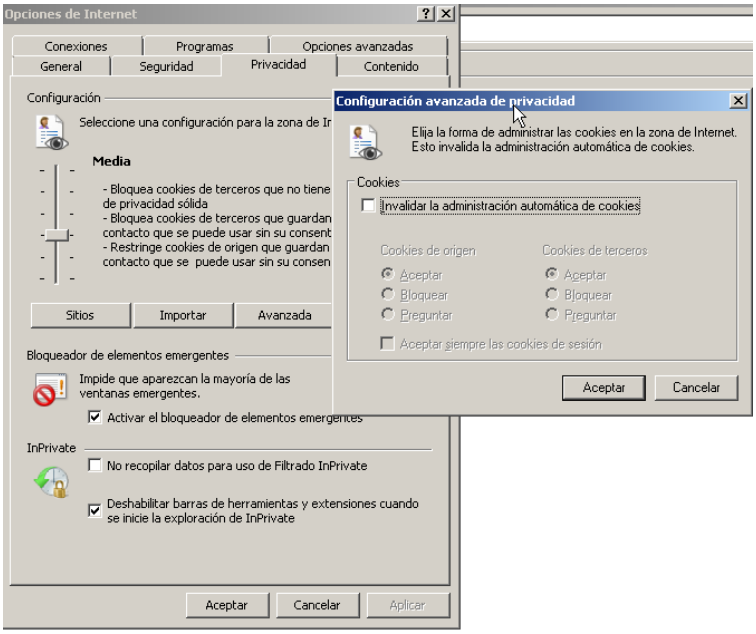
Fuente: INTECO

Bloquear cookies

Con respecto a las cookies, Microsoft Internet Explorer permite o bien la administración automática o bien personalizada. Cuando se elige la administración personalizada, se divide entre cookies de origen y cookies de terceros.

Como se ha explicado anteriormente, la situación ideal pasa por bloquear o preguntar antes de utilizar cookies de terceros. Esta configuración está disponible desde la pestaña de Privacidad, de las opciones del navegador web.

Ilustración 5: Configuración personalizada de cookies en Microsoft Internet Explorer



Fuente: INTECO

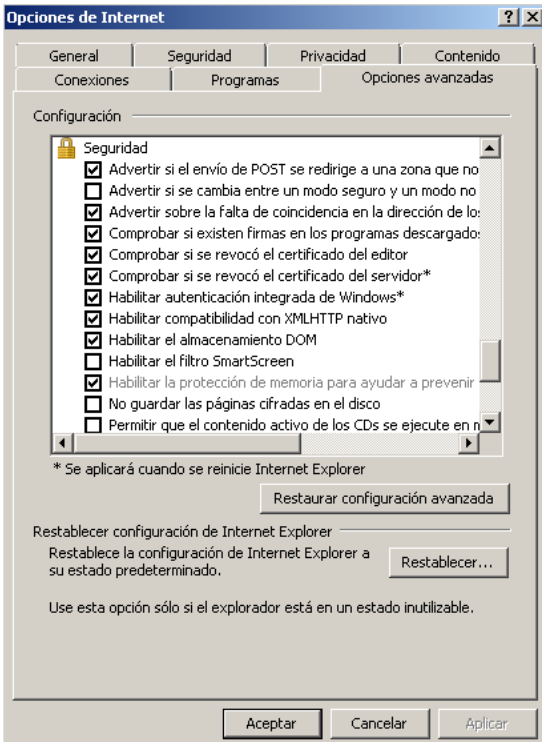
Contramedidas contra el phishing

Las opciones de seguridad de Microsoft Internet Explorer no acaban en las zonas. Existe una gran cantidad de opciones que pueden ser aprovechadas, en la pestaña de opciones avanzadas, clasificadas bajo el epígrafe de "Seguridad".

Entre ellas, se puede encontrar la opción de “Habilitar el filtro SmartScreen” (contra páginas de tipo phishing o potencialmente peligrosas) o "Habilitar la protección de memoria".

Esta última opción permite prevenir las vulnerabilidades que ejecutan código gracias a fallos de programación del propio navegador web.

Ilustración 6: Opciones de seguridad avanzada en Microsoft Internet Explorer



Fuente: INTECO

Mozilla Firefox

Mozilla Firefox es un navegador web gratuito, de código abierto y que ha ganado una gran popularidad en los últimos años[4]. Funciona bajo cualquier plataforma y ha demostrado una evolución positiva con respecto a la seguridad.

Mozilla Firefox es un navegador web muy modular para el que se ha tejido una importante comunidad en torno a la creación de plugins que añaden una gran potencia a la aplicación final.

Así, el navegador web "por defecto" no posee demasiadas funcionalidades de por sí, pero existen complementos desarrollados por terceros que han demostrado ser muy eficaces previniendo muchos problemas de seguridad potenciales.

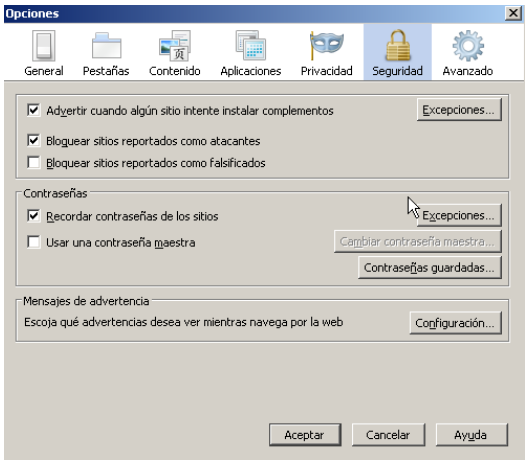
Contramedidas contra el phishing y otras opciones

Las opciones de seguridad básicas de Mozilla Firefox permiten muy pocas gestiones para asegurar el navegador web. En la Ilustración 7 se encuentra la opción "Bloquear sitios reportados como falsificados", que permite bloquear las páginas reportadas como

[4]Mozilla Firefox supera a Explorer como navegador web más usado en Europa. http://www.siliconnews.es/2011/01/04/Mozilla Firefox-supera-a-explorer-como-navegador web-mas-usado-en-europa/

phishing y a las que Mozilla Firefox de esta manera, no posibilita el acceso. En este sentido, Mozilla Firefox se ha mostrado bastante eficaz[5].

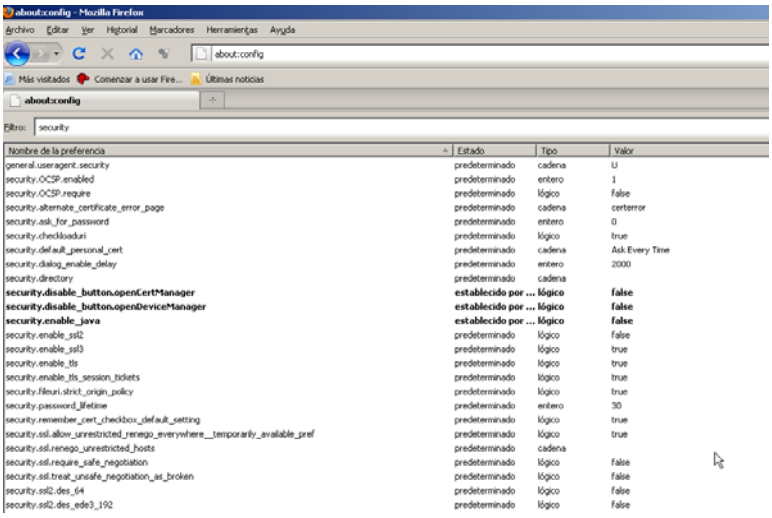
Ilustración 7: Configuración de Seguridad de Mozilla Firefox sin complementos



Fuente: INTECO

Sin embargo, contiene un sistema de configuración a bajo nivel (en el que realmente se controla el navegador web) que resulta mucho más potente (aunque también potencialmente peligroso si no se sabe a qué corresponde cada variable). A él se accede a través del comando about:config en la barra de direcciones. Con el filtro disponible, si se introduce "security" aparecen muchas otras opciones de seguridad que pueden ser modificadas.

Ilustración 8: Funcionalidad de configuración avanzada de Mozilla Firefox



Fuente: INTECO

[5] http://www.hispasec.com/unaaldia/4360. Mozilla Firefox el navegador web más seguro contra el fraude

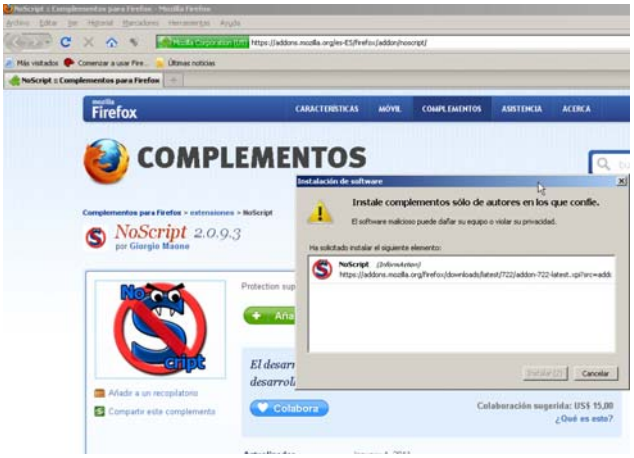
JavaScript y Java

Uno de los complementos más utilizados para Mozilla Firefox es NoScript, que permite bloquear Java, JavaScript y otras funcionalidades del navegador web potencialmente peligrosas. Puede ser descargado desde:

https://addons.mozilla.org/es-ES/Mozilla Firefox/addon/noscript/

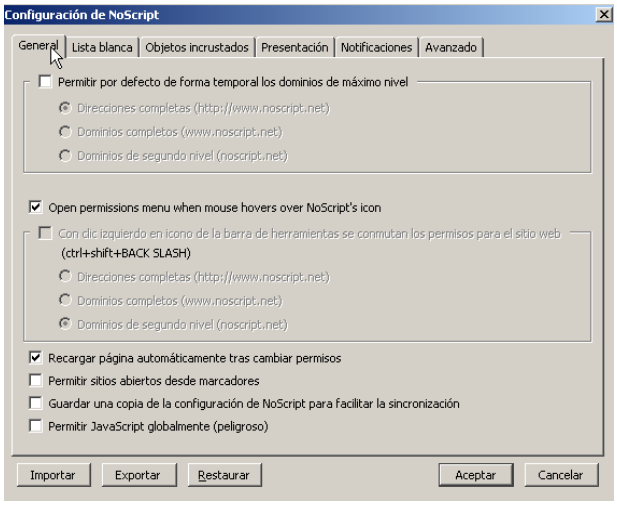
Este complemento permite una aproximación al bloqueo similar a la que ofrecen las Zonas de Microsoft Internet Explorer. Se puede configurar una lista blanca, o una lista negra de dominios a los que se les permite o prohíbe que ejecuten JavaScript, por ejemplo.

Ilustración 9: Descarga del plugin "NoScript" para Mozilla Firefox



Fuente: INTECO

Ilustración 10: Pantalla de configuración de NoScript



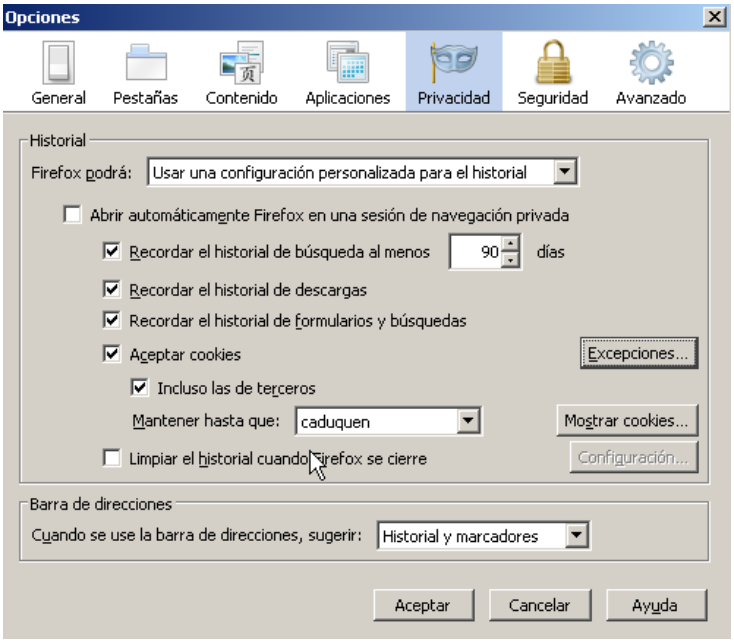
Fuente: INTECO

Bloquear cookies

Con respecto a las cookies y su configuración, Mozilla Firefox permite por defecto bloquear las de terceros, que son las cookies que pueden llegar a resultar peligrosas para la privacidad del usuario, como se ha mencionado anteriormente.

Esta opción está disponible desde las opciones de Privacidad de Mozilla Firefox. Desmarcando la opción "Aceptar Cookies incluso de terceros" se puede prevenir almacenar este tipo de información.

Ilustración 11: Configuración de las cookies en Mozilla Firefox

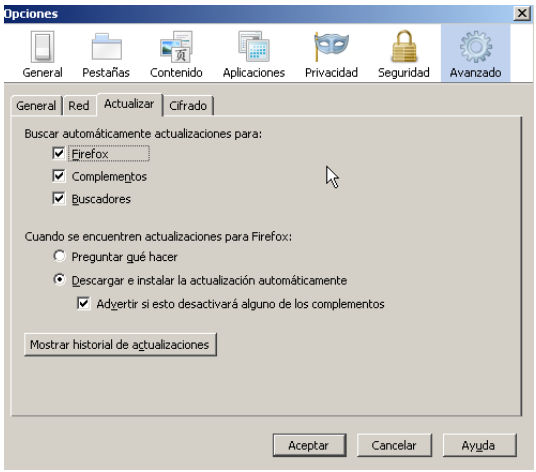


Fuente: INTECO

Actualización del navegador web y los plugins

Para actualizar el navegador web, es importante marcar las opciones del propio navegador web que permiten que busque las actualizaciones disponibles (tanto del propio navegador web como de los complementos) y las aplique lo antes posible. Esto permite estar protegido cuanto antes contra vulnerabilidades conocidas.

Ilustración 12: Opciones de actualización de Mozilla Firefox



Fuente: INTECO

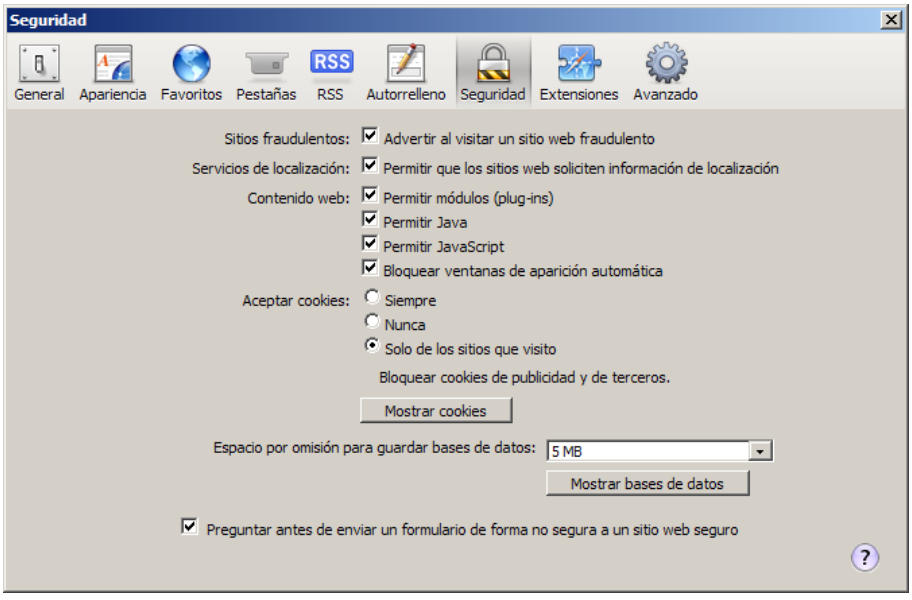
Apple Safari

Apple Safari es un navegador web gratuito de Apple, que tradicionalmente se utiliza en su sistema operativo Mac OS, aunque existe versión para Windows.

Contramedidas contra el phishing y otras opciones

Las opciones de seguridad básicas de Safari permiten muy pocas gestiones para asegurar el navegador web. En esta pantalla se encuentra la opción "Advertir al visitar un sitio web fraudulento".

Ilustración 13: Configuración de Seguridad de Safari sin complementos

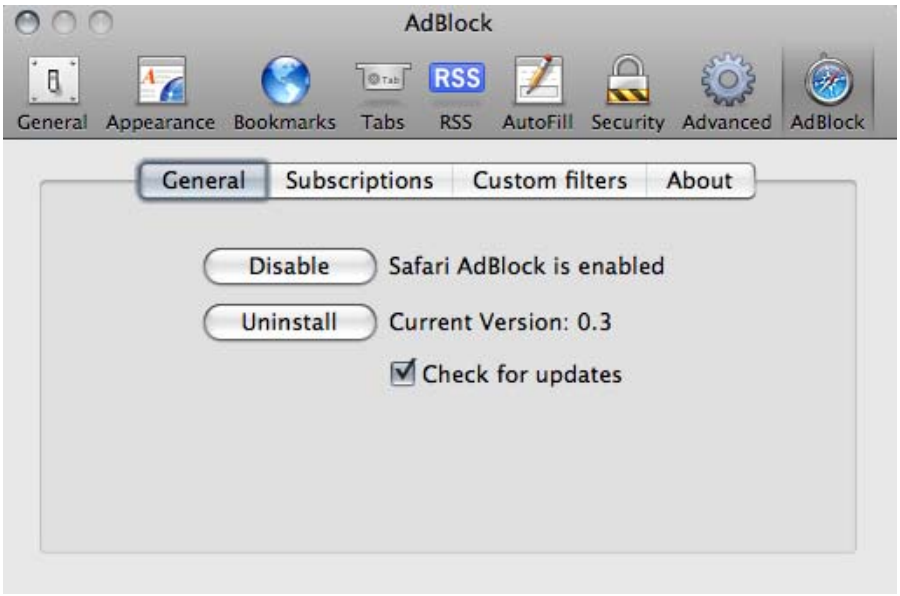


Fuente: INTECO

JavaScript y Java

No existe nada parecido a las zonas de Internet Explorer o al complemento NoScript para Apple Safari. Lo más aproximado en este aspecto es la extensión AdBlock compatible con Apple Safari que bloquea anuncios y banners publicitarios de las páginas web. Puede ser descargado desde http://safariadblock.com/

Ilustración 14: AdBlock en Safari

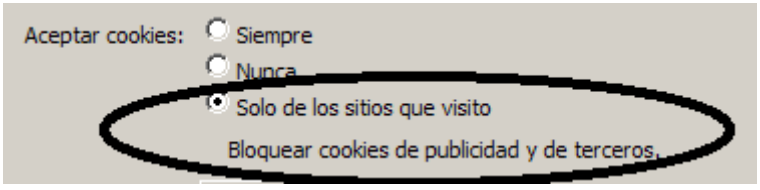


Fuente: UPFLYSOFT.COM

Bloquear cookies

Con respecto a las cookies y su configuración, Safari ofrece una opción que, en su traducción al español, puede llegar a confundir. La opción que se muestra es "Aceptar cookies sólo de sitios web que visito. Bloquear cookies de publicidad y de terceros". Pero su distribución en pantalla puede llegar a hacer pensar que se tratan de opciones diferentes. En su versión en inglés, la opción está correctamente redactada: *"Accept cookies Only from sites you navigate to. For example, not from advertisers on those sites".*

Ilustración 15: Configuración de las cookies en Safari



Fuente: INTECO

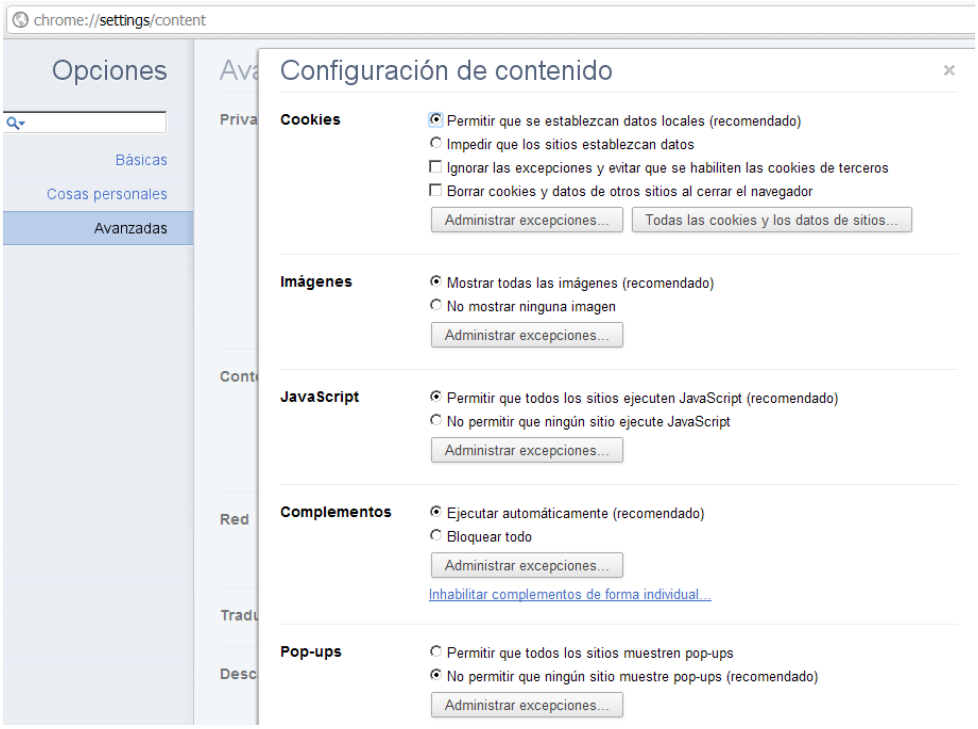
Google Chrome

Chrome es un navegador web gratuito de Google, que ha evolucionado mucho en un corto espacio de tiempo, y ha tenido gran aceptación entre los usuarios por su velocidad y sencillez.

Contramedidas contra el phishing y otras opciones

Las opciones de seguridad de Chrome están muy bien organizadas, con un sistema básico de excepciones muy potente. Es posible acceder directamente a estas opciones, no solo a través de las opciones del menú, sino también con el acceso directo en el navegador: chrome://settings/content

Ilustración 16: Configuración de Seguridad de Chrome



Fuente: INTECO

JavaScript y Java

Chrome cuenta, al igual que Firefox con la posibilidad de instalar el complemento NoScript y gestionar JavaScript y Java. Aun así, para JavaScript, cuenta de serie con un gestor capaz de administrar excepciones.

Bloquear cookies

Con respecto a las cookies y su configuración, Chrome permite o bien gestionar por excepciones, o bien ignorar las excepciones y bloquear directamente todas las cookies de terceros con la opción, "Ignorar las excepciones y evitar que se habiliten las cookies de terceros."

Actualización del navegador web y los plugins

Chrome introdujo un nuevo concepto de actualización totalmente silenciosa y poco intrusiva en el navegador, intentando mantener siempre al usuario con la última versión con los parches de seguridad incorporados.