GUIAS DE SEGURIDAD UJA

Uso seguro de la web

Servicio de Informática
Vicerrectorado de Tecnologías de la Información
y la Comunicación y Universidad Digital
Universidad de Jaén

Edición: **enero 2018**

Contenidos

1. Introducción

En la actualidad la navegación web es, con diferencia, una de las actividades a las que más tiempo dedicamos en nuestro uso habitual de Internet: redes sociales, contenidos multimedia, descargas de ficheros, lectura de blogs, comercio electrónico, banca on-line… Estos son solo algunos de los ejemplos de sitios webs por los que habitualmente nos movemos a diario.

Pero ¿es segura la navegación web? De entrada, navegar por Internet no es una actividad anónima, por lo que la privacidad y la seguridad son dos temas a los que debemos prestar máxima importancia, máxime cuando accedamos a sitios web especialmente sensibles por donde circulan nuestros datos personales, como pueden ser las webs de comercio electrónico o de banca on-line.

Es por este motivo por lo que debe haber una concienciación y la máxima información posible de los usuarios antes de lanzarse a abrir su navegador y surcar el océano de Internet.

En este documento se ofrecen algunos consejos básicos a tener en cuenta para que nuestra navegación diaria por la web sea más segura.

2. Peligros más frecuentes asociados a la navegación web

Entre las diferentes amenazas a los que nos podemos ver expuestos hoy en día cuando navegamos por Internet, se encuentran las siguientes:

- La posible instalación (la mayoría de las veces sin nuestro conocimiento) de **software malicioso de tipo *adware* (software comercial) y *spyware* (software espía)** que genera la apertura constante de ventanas emergentes desplegando publicidad no deseada, y que hace un seguimiento de nuestros hábitos de navegación, con finalidades diversas. La descarga e infección automática de **troyanos u otro tipo de malware** puede tener lugar simplemente visitando páginas web comprometidas e infectadas. Hace unos años, esto era exclusivo de páginas de dudoso contenido, pero hoy en día, cualquier sitio web que presente vulnerabilidades es susceptible de ser comprometido, infectando a los usuarios que lo visiten.

- Ataques llevados a cabo explotando **vulnerabilidades en los sistemas operativos y aplicaciones** instaladas, como por ejemplo los navegadores, con objeto de capturar contraseñas y otro tipo de información sensible.

- **Secuestradores de navegador (*browser hijackers*)**: se trata de un intento de terceros para tomar el control de nuestro navegador web y utilizarlo con fines maliciosos. Algunos simplemente se usan con fines publicitarios, pero no son realmente peligrosos. Sin embargo, en algunos casos, pueden ser malintencionados y robar información como contraseñas guardadas automáticamente en el navegador. Estos programas suelen agregar varios favoritos a la lista de marcadores del navegador sin nuestro conocimiento, y cambiar la página de inicio e incluso algunas claves del registro. Asociados a los secuestradores de navegador, en muchos casos también se instalan ***keyloggers* (capturadores de pulsaciones de teclado)** que registran todo lo que tecleamos,

incluyendo las contraseñas de sitios sensibles como servicios de banca por Internet y correo electrónico.

- Una de las modalidades de secuestro cada vez más habituales es el denominado ***ransomware*, o instalación de falsas aplicaciones (rogue)**. Esta amenaza se explica con más detalle más adelante en este documento. Algunos casos famosos de *ransomware* son el "virus de la Policía" y el "virus de la SGAE".

- Especialmente peligrosa es la **infección web denominada "*drive-by-download*"**, que permite infectar masivamente a los usuarios simplemente accediendo a un determinado sitio web. Mediante esta técnica, los creadores y diseminadores de malware propagan sus códigos aprovechando las vulnerabilidades existentes en diferentes sitios web e inyectando código dañino entre el código original. **Hace tiempo estos ataques eran casi exclusivos de sitios de dudoso contenido (software ilegal, hacking, pornografía…), pero en la actualidad, la tendencia es encontrarlos en todo tipo de sitios web, ya sea directamente o bien, a través de terceros en forma de banners publicitarios, por lo que no debemos bajar la guardia.**

  Por lo general, el proceso de ataque se lleva a cabo de manera automatizada mediante el uso de herramientas que buscan en el sitio web alguna vulnerabilidad. Una vez que la encuentran, insertan un script malicioso entre el código HTML del sitio vulnerado. Basta con que un usuario visite un sitio web infectado mediante esta técnica para que sea infectado. **En la mayoría de los casos, la infección intenta buscar agujeros de seguridad en el equipo del usuario infectado, por lo que la mejor protección pasa por tener el sistema operativo y las aplicaciones correctamente actualizadas, además de tener instalado y actualizado un antivirus o suite de seguridad (la mayoría de antivirus actuales protegen de todo este tipo de amenazas).**

- **Envío y uso de información personal a través de sitios web.** Esto es algo de sentido común. Muchos usuarios facilitan en páginas web todo tipo de información personal que en manos de personas inadecuadas puede ser usada de forma fraudulenta o poco ética. Como norma general, el mejor consejo es evitar proporcionar en Internet cualquier tipo de información que nunca ofreceríamos en el mundo real.

- **Clic en enlaces web maliciosos (*clickjacking*).** Últimamente esta es una de las amenazas más comunes. Se trata de una técnica fraudulenta utilizada en Internet que tiene como objetivo robar información personal del usuario o acceder a su equipo o dispositivo. Consiste en esconder bajo una página web con apariencia inocente e inofensiva enlaces fraudulentos, que si son pulsados por el usuario son capaces, entre otras cosas, de ejecutar código malicioso en su equipo. Todo ello aprovechándose de algún fallo de seguridad de los navegadores web. Se puede ver un ejemplo en:

  http://www.youtube.com/watch?v=jgAO8WU2lp0&list=UU7vjeSjyAgzUaQZF0NzFNsg&index=2

2.1. Falsas aplicaciones (*rogue/ransomware*) y barras de utilidades (toolbars)

Las **aplicaciones de tipo "rogue"** (también denominadas ***ransomware***) son falsos programas que simulan ser antivirus y suites de seguridad (las interfaces de usuario son muy similares a las de otras aplicaciones antivirus reales existentes en el mercado), pero

que en realidad esconden malware destinado a hacer un mal uso de nuestro ordenador y la información contenida en él. **Son especialmente peligrosas porque pueden ser el origen de un secuestro de navegador o del robo de nuestras contraseñas. Además, actualmente es uno de los métodos más difundidos y efectivos por lo que hay que tener un especial cuidado.**

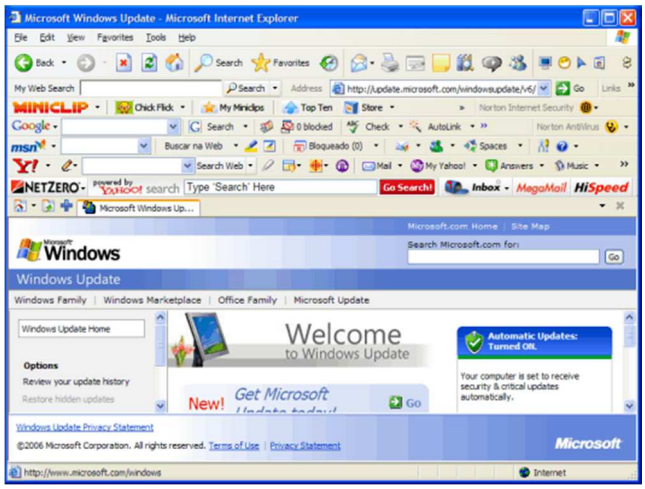
Un ejemplo de rogué antivirus es el siguiente:

Algunos consejos para detectar aplicaciones "rogue":

- La falsa aplicación por lo general **se descarga sin autorización del usuario** o solicita su descarga de forma muy insistente, justo después de acceder a algún sitio donde se realiza un falso análisis on-line de nuestro equipo. Dicha simulación de análisis SIEMPRE detecta amenazas e insiste en que nuestro equipo se encuentra en peligro.
- Al realizar la exploración desde la supuesta aplicación de seguridad, **siempre se encuentra una gran cantidad de amenazas** (lo que casi nunca es cierto), pero casi nunca se detalla puntualmente qué archivos se encontrarían infectados.
- Al querer realizar la limpieza de las amenazas **el programa nos "invitará" a comprar la licencia del producto**, generalmente por medio de una ventana emergente (pop-up) que nos llevará a un sitio donde poder realizar el pago con tarjeta de crédito. **Es muy importante que bajo ninguna circunstancia se indiquen dichos datos.**
- La aplicación "rogue", una vez instalada, **tiende a realizar ciertas modificaciones a nuestro sistema operativo para insistir en el riego que tenemos** y así apresurarnos a realizar la compra del producto. Estos cambios incluyen, por ejemplo, la modificación del fondo de pantalla, constantes y molestos avisos de alertas de seguridad, modificaciones en la pantalla de inicio del sistema operativo e incluso modificaciones a la barra de inicio.

- Si se intentamos desinstalar la herramienta desde la opción "Agregar o quitar programas" del panel de control, al reiniciar el equipo **la aplicación rogue puede volver a instalarse de forma automática**.

En cuanto a las **barras de utilidades (toolbars)** son barras de botones y complementos que se añaden a nuestro navegador, generalmente durante la instalación de cualquier otro software gratuito. Aunque algunas de ellas son totalmente legítimas e inofensivas, sin embargo hay muchas otras que esconden malware que puede afectar a nuestro equipo o espiar nuestros hábitos de navegación sin que seamos conscientes de ello.



Generalmente, todo está relacionado con un acuerdo económico. El desarrollador de la barra de herramientas llega a un acuerdo económico con desarrolladores de software para que incluyan dicha barra en sus instaladores, pagándoles una cantidad de dinero por cada instalación y uso que los usuarios hagan de la barra. De forma añadida, muchas de estas barras se usan para rastrear la navegación web del usuario que la instala, con fines puramente comerciales y de marketing.

Como norma general, se recomienda **NO instalar ninguna de estas barras, a menos que la conozcamos y realmente la necesitemos.** Igualmente, es aconsejable revisar desde el Panel de Control de Windows, en la lista de aplicaciones instaladas si hay alguna de estas barras (alguna aplicación que contenga la palabra "toolbar" y desinstalarla). Nos evitaremos sorpresas y problemas en el futuro.

Muchas aplicaciones anti-malware (como Malwarebytes Antimalware) permiten detectar y eliminar cualquier rastro de muchas de estas toolbars, por lo que se recomienda un análisis periódico del equipo con herramientas de este tipo.

3. Consejos para un uso seguro de la web

3.1. Consejos generales

- En primer lugar, la protección comienza por el sistema. Nunca nos cansaremos de repetir que antes de navegar por Internet, el equipo debe contar con un **antivirus** correctamente instalado y actualizado (en el caso de la Universidad de Jaén, el Servicio de Informática recomienda y da soporte a Panda AV), un **cortafuegos** (Windows ya incluye uno de serie que viene activado por defecto) y algún **software antimalware específico** (ej: Malwarebytes Antimalware).

- **Aplica las actualizaciones disponibles del sistema operativo.** En las últimas versiones de Windows, las actualizaciones se suelen descargar e instalar automáticamente. Además de las actualizaciones del sistema, también se recomienda actualizar los navegadores web con los parches y versiones más recientes publicados por los fabricantes. En el caso de Internet Explorer, las

actualizaciones del navegador se incluyen dentro de las actualizaciones del sistema.

- Utiliza "conexiones seguras" siempre que sea posible. Asegúrate que, al transmitir datos sensibles, la dirección web comienza por **HTTPS**, y en la parte inferior del navegador aparece algún tipo de candado cerrado que indica que hemos establecido una conexión segura.

- Comprueba los certificados de seguridad, en páginas que requieren datos personales.

- **Nunca hagas clic en enlaces sospechosos**. Uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los enlaces o hipervínculos. Evitar hacer clic en éstos previene el acceso a páginas web potencialmente capaces de infectar al usuario. Los enlaces pueden estar incluidos en un correo electrónico, una ventana de chat o un mensaje en una red social, por poner algunos ejemplos. La clave está en analizar si son sospechosos (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), que provienen de un remitente desconocido o remiten a un sitio web poco confiable.

- **No accedas a sitios web de dudosa reputación,** tales como páginas de software ilegal (warez), generadores de números de serie (keygens), etc. Estos ficheros son muy propensos a contener malware y pueden poner en serie peligro nuestro equipo de forma instantánea. Por otra parte, a través de técnicas de "ingeniería social", muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario, como descuentos en la compra de productos (o incluso ofertas gratuitas), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que estemos atentos a estos mensajes y evitemos acceder a páginas web con estas características. Hay que tener cuidado especialmente en evitar la instalación de aplicaciones "rogue", como se ha indicado anteriormente. Se recomienda descargar las aplicaciones de seguridad siempre desde los sitios web oficiales y con buena reputación.

- **Ten precaución con los resultados que ofrecen los buscadores web**. A través de técnicas denominadas "Black Hat SEO", los atacantes suelen posicionar sus sitios web maliciosos entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad o noticias curiosas. Ante cualquiera de estas búsquedas, debes estar atento a los resultados y verificar a qué sitios web está siendo enlazado. Para evitar esto, se recomienda la instalación de analizadores de enlaces, tales como AVAST Web report, AVG LinkScanner o páginas específicas como http://www.urlvoid.com/. Estos son complementos para el navegador que junto a cada enlace que aparece en el navegador incluyen un icono indicativo de su fiabilidad.

- **Usa plugins o extensiones en el navegador para eliminar las molestas ventanas emergentes** (pop-up) que aparecen durante la navegación, o configura tu navegador para evitar estas ventanas. En muchas ocasiones, estas ventanas son la vía de acceso a virus, troyanos y otros tipos de malware.

- Se debe **evitar entrar desde sitios públicos** (cibercafés, bibliotecas, cafeterías, aeropuertos y hoteles, entre otros) **en sitios web que requieran un nivel alto de seguridad**, como pueden ser las páginas de entidades bancarias y financieras En este sentido, si es totalmente necesario navegar desde lugares públicos, se

deben tomar todas las precauciones de seguridad necesarias, entre ellas: eliminar los archivos temporales, la información almacenada en caché, las cookies y nunca almacenar las direcciones URL, contraseñas y demás información crítica para no dejar rastro de nuestra navegación.

- Si algún sitio web ofrece la descarga de aplicaciones que no se solicitaron, no deben ser aceptadas sin antes verificar la integridad del mismo con un antivirus o aplicación de seguridad.

- Ten especial precaución con la **instalación de complementos extras para el navegador, tales como barras de utilidades (toolbars)**, sin verificar previamente su autenticidad. Instálalas solo si las conoces realmente y necesitas usarlas. Muchas aplicaciones software libres (de tipo freeware) incluyen durante la instalación la posibilidad de instalar utilidades extra y barras de herramientas indicadas en los apartados anteriores. Procura NO instalar ninguna de estas aplicaciones extra, ya que muchas de ellas contienen malware o *adware* y ponen en peligro la seguridad de nuestro navegador y nuestra privacidad. Además, conviene revisar periódicamente las aplicaciones instaladas en nuestro PC y eliminar cualquier aplicación de tipo toolbar (barra de herramientas) que nos resulte sospechosa o que no recordemos haber instalado.

3.2. Proteger nuestra privacidad

- **Nunca facilites datos personales** si no existe una completa seguridad sobre quién los va a recibir. Si no es estrictamente necesario, nunca facilites datos personales que no sean obligatorios.

- No incluyas en ninguna web **información personal sobre tus gustos, aficiones o preferencias**, si no quieres verte bombardeado de información comercial y publicidad relacionada con los datos registrados. Como norma general, se recomienda NO rellenar la información que no sea obligatoria cuando rellenemos algún formulario en Internet.

- Ten especial **cuidado con la información que compartes en Internet y con quién la compartes.** Esto es especialmente importante en determinados tipos de webs, como las redes sociales.

3.3. Uso de contraseñas

- Ten **precaución con las contraseñas que guardes en el navegador**, y utiliza siempre una contraseña maestra para que nadie más pueda acceder a ellas (en la ayuda de los navegadores se indica cómo hacerlo). En general, se debe evitar el almacenamiento por defecto de información crítica en el navegador, ya que esta información puede ser fácilmente robada a través de aplicaciones y códigos maliciosos.

- **Cambia tus contraseñas periódicamente y usa contraseñas robustas. No dejes las contraseñas guardadas en claro en su disco duro ni las anotes en un papel**. Muchos servicios en Internet están protegidos con una clave de acceso. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, que incluyen distintos tipos de caracteres (letras mayúsculas y minúsculas,

números, algún carácter especial (&, %, $...) y una longitud de al menos 8 caracteres).

- En general, es recomendable usar un buen gestor de contraseñas electrónico bien protegido con todas las medidas de seguridad que ofrece. Un buen ejemplo es KeePass (https://keepass.info/).

3.4. Descarga de software y aplicaciones

- Extrema la precaución en los archivos que recibes en sesiones de chat o desde cualquier otra página web o aplicación que se ejecute desde el navegador web.

- En general, ten mucha precaución con los ficheros que descargues desde redes de tipo P2P, descarga directa o enlaces de tipo Torrent. Es muy fácil que incluyan algún tipo de malware. Antes de abrirlos o ejecutarlos, analízalos con un buen software antivirus/antimalware actualizado.

3.5. Protegerse del *clickjacking*

- En primer lugar, hay que tener mucha precaución con las páginas que visitamos y con los enlaces que pulsamos. Use el sentido común.
- Debemos sospechar si alguna página web de las que frecuentamos, se comporta de forma extraña: solapa más de una ventana cuando la abrimos, muestra elementos muy diferentes a lo habitual, etc.
- Ten tu navegador web siempre actualizado.
- Instala y ten actualizadas herramientas indicadas en este documento, como antivirus, antimalware, analizadores de enlaces, etc.
- Si usas Mozilla Firefox para navegar por Internet, puedes instalar el complemento **NoScript** que incluye una funcionalidad llamada "ClearClick" que lanza una ventana al usuario avisándole si ha hecho clic sobre un elemento de la web que se encuentra escondido y que podría ser malicioso.

4. Seguridad en redes sociales

En la actualidad, las redes sociales constituyen uno de los usos más populares de la navegación web por los usuarios, que las utilizan de forma masiva. Esto hace que se conviertan en objetivos específicos para la rápida propagación de malware. Los beneficios de las redes sociales son innumerables, no solo para los usuarios sino también para los atacantes que han encontrado en ellas múltiples formas de aprovecharlas para engañar a los usuarios y propagar nuevas amenazas. Por este motivo, hay que tener muy en cuenta una serie de medidas específicas:

- Evitar publicar ningún tipo de información sensible y confidencial, porque esta información puede ser usada por terceros con fines maliciosos. También es muy recomendable evitar la publicación de imágenes propias y de familiares.

- Es muy importante aplicar los consejos para mantener la privacidad del perfil, configurándolo para que no sea público. En la ayuda de cada red social suele haber un apartado específico de seguridad y privacidad donde se indica cómo configurar nuestro perfil para tener las máximas garantías de seguridad. Conviene estar actualizado, ya que la política de privacidad y las opciones de privacidad y seguridad de las diferentes redes sociales suelen cambiar y actualizarse con bastante frecuencia.

- En general, se recomienda no responder a las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas.

- Ignorar los mensajes que ofrecen material pornográfico, pues suelen ser canales habituales para la propagación de malware.

- Como norma general de seguridad, también se recomienda cambiar periódicamente la contraseña en nuestros perfiles de redes sociales, para evitar que la misma sea capturada fácilmente.

- Denuncia cualquier uso abusivo que detectes en las redes sociales. Todas incluyen algún protocolo para realizar estas denuncias. Ante hechos graves, recurre a la Policía o la Guardia Civil, a través de sus unidades especializadas en delitos telemáticos.

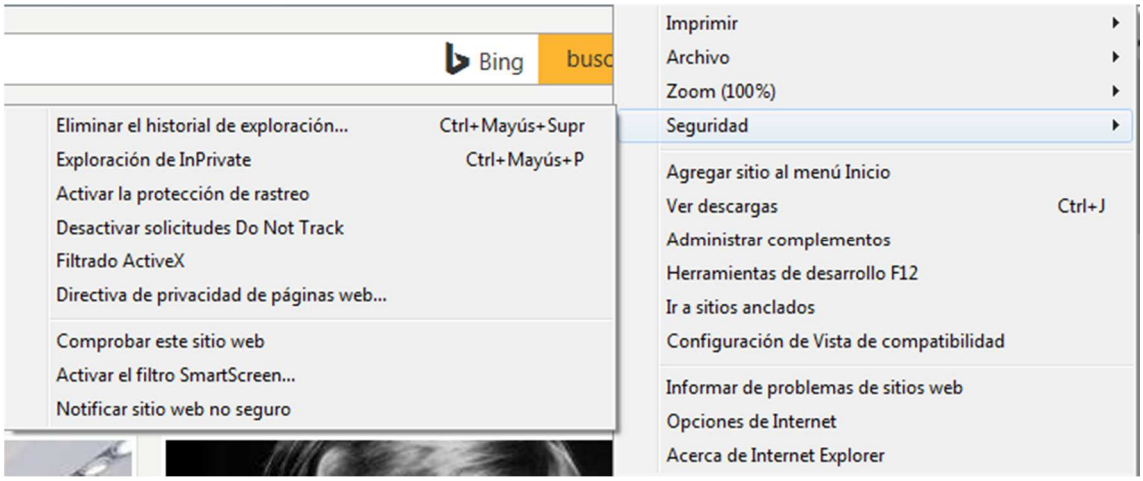
El Instituto Nacional de Ciberseguridad (INCIBE) dispone de una sección en su sitio web donde ofrece guías de seguridad y videotutoriales específicos para las diferentes redes sociales y sitios web 2.0 más habituales hoy en día (Facebook, Twitter, LinkedIn, Youtube…):

https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

5. Herramientas y complementos para hacer más seguro nuestro navegador

5.1. Seguridad y privacidad en Microsoft Internet Explorer

Las últimas versiones de Internet Explorer incluyen interesantes características de seguridad y privacidad, que se pueden configurar desde un menú específico ("Seguridad"):



Entre estas características están las siguientes:

- **Filtrado ActiveX**, que bloquea los controles ActiveX para todos los sitios y permite que después podamos volver a activarlos sólo para los sitios en los que confiemos.

- **Resaltado de dominios**, que muestra claramente la dirección web real de los sitios web que visitamos. Esto ayuda a evitar los sitios web que usan direcciones web engañosas, como los sitios web de suplantación de identidad (*phishing*). El verdadero dominio que visitamos aparece resaltado en la barra de direcciones.

- **Filtro SmartScreen**, que puede ayudar a proteger contra los ataques de suplantación de identidad en línea (*phishing*), los fraudes y los sitios web simulados o malintencionados. También examina descargas y nos advierte acerca de posible malware (software malintencionado). El filtro SmartScreen hace que Internet Explorer envíe una notificación cuando intentamos descargar un programa potencialmente peligroso. Además, el nuevo administrador de descargas proporciona una capa de seguridad extra para archivos que hayamos descargado de la web; realiza varias comprobaciones de seguridad en las descargas, tales como buscar virus y verificar la ubicación de la cual hemos descargado el archivo.

- **El filtro de scripts de sitios (XSS)**, que evita ataques de sitios fraudulentos que podrían intentar robar su información personal y financiera mediante ataques denominados *Cross Site Scripting* (XSS).

- **Una conexión SSL de 128 bits** para sitios web seguros. Esto ayuda a Internet Explorer a crear una conexión cifrada con los sitios web que manejan información personal, con unas garantías de seguridad adecuadas.

- **Notificaciones** que nos advierten si la configuración de seguridad se encuentra por debajo de los niveles recomendados.

- **Protección de rastreo (desactivar solicitudes Do Not Track)**, que limita la comunicación del explorador con ciertos sitios web, determinada por una lista de protección de rastreo para ayudar a que nuestra información siga siendo privada.

- **Exploración InPrivate**, que se puede usar para explorar la web sin guardar datos relacionados, como cookies y archivos temporales de Internet.

- Configuración de privacidad que especifica cómo el equipo debe tratar las cookies.

En relación a los sitios web fraudulentos, en sus opciones de Seguridad, Internet Explorer 9 ofrece dos opciones interesantes: la posibilidad de comprobar el nivel de fiabilidad de un sitio web (opción **Seguridad > Comprobar este sitio web**) o la posibilidad de informar a Microsoft de un sitio que detectemos como fraudulento (opción **Seguridad > Notificar sitio web no seguro**) para actualizar dinámicamente la base de datos de Microsoft de enlaces no fiables.

5.2. Seguridad y privacidad en Mozilla Firefox

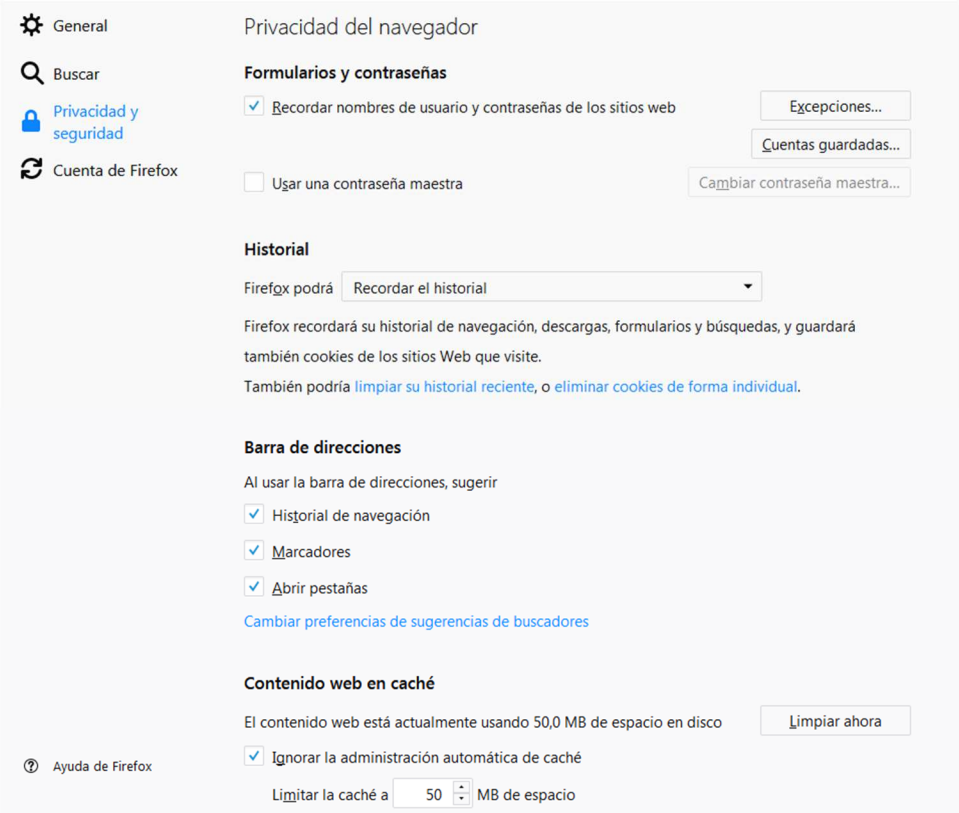
La página oficial de Mozilla Firefox donde se indican los consejos a seguir relacionados con la seguridad y la privacidad es la siguiente:

http://support.mozilla.org/es/products/firefox/privacy-and-security

Por otra parte, la URL oficial para descarga de complementos para Mozilla Firefox relacionados con la seguridad y la privacidad es la siguiente:

https://addons.mozilla.org/es/firefox/extensions/privacy-security/

Dentro de las opciones, Firefox cuenta con un apartado específico de privacidad y seguridad (**Opciones > Privacidad y Seguridad**):



donde podemos configurar aspectos como:

- Que nos avise cuando algún sitio web intenta la instalación de complementos sin nuestro permiso.
- El bloqueo se sitios informados como maliciosos, ya sea porque estén infectados o falsificados.
- Opcionalmente, podemos guardar las contraseñas que vamos introduciendo en los sitios web para que Firefox las recuerde, pero en este caso, es muy recomendable activar la casilla "Usar una contraseña maestra", ya que cualquiera que acceda a nuestro navegador tiene la posibilidad de ver todas nuestras contraseñas guardadas en claro, a menos que estén protegidas por una contraseña maestra.

En cuanto a las opciones de privacidad, Firefox permite:

- Indicar a los sitios web que no queremos ser rastreados.
- Poder indicar que no recuerde el historial (eliminar el rastreo de nuestra navegación) total o parcialmente.
- Evitar que el la barra de direcciones aparezcan sugerencias sobre sitios visitados anteriormente.

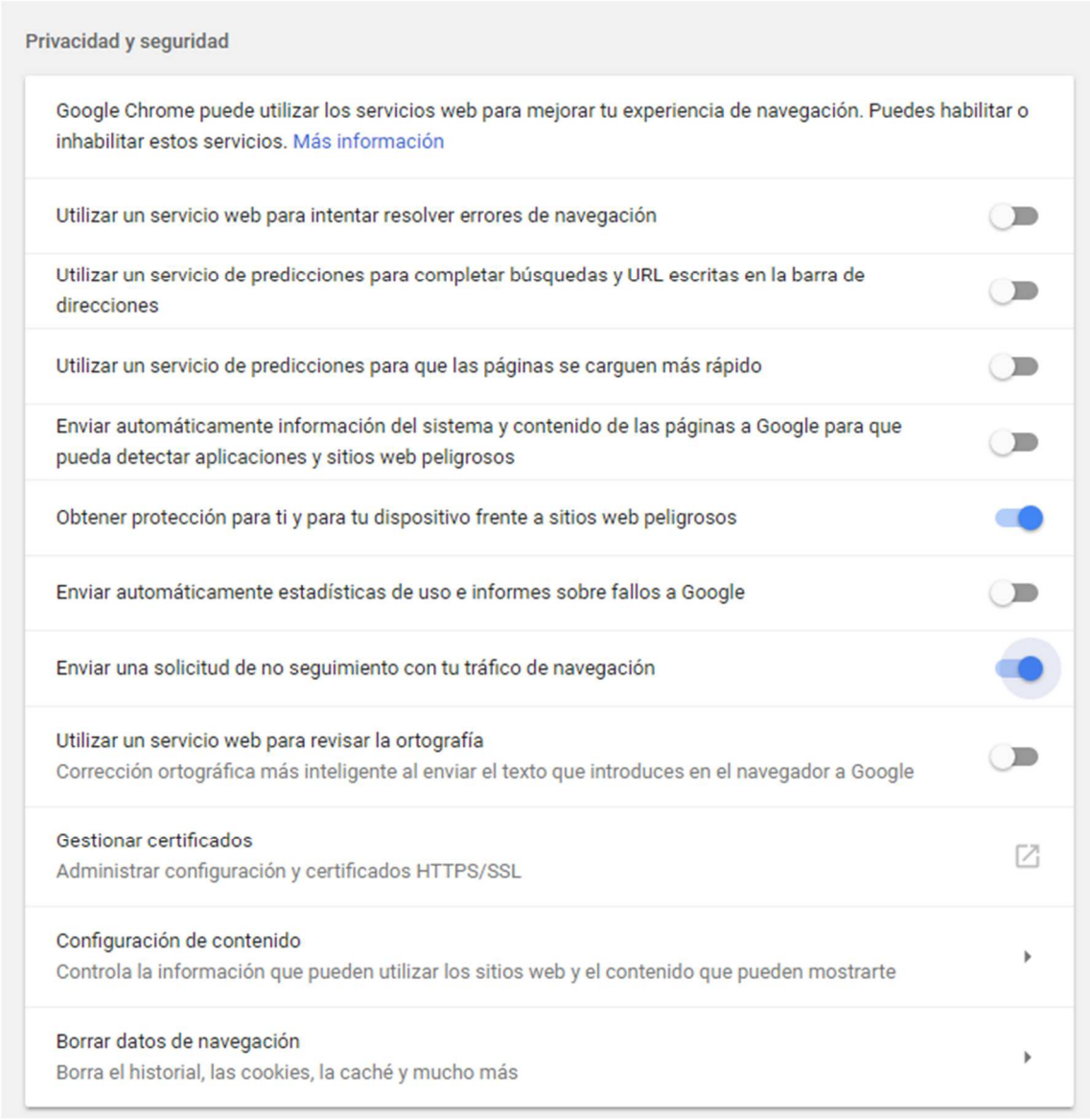
En el apartado de Contenido, contamos con la posibilidad de bloqueo de ventanas emergentes (pop-ups), así como desactivar elementos potencialmente peligrosos como la carga de imágenes o la ejecución de código javascript.

5.3. Seguridad y privacidad en Google Chrome

Google Chrome, por su diseño basado en un modelo denominado "sandbox", es de entrada uno de los navegadores más seguros en la actualidad, por lo que es muy recomendable su uso si estamos realmente concienciados respecto a la seguridad en nuestra navegación web.

La gestión de la seguridad y la privacidad se incluye dentro del menú Configuración, en las Opciones avanzadas. Hay todo un apartado dedicado a este tema:

Entre las opciones habilitadas por defecto, se encuentra la protección contra *phishing* y software malicioso que ya integra Chrome de serie, avisándonos cuando intentamos descargar algún fichero detectado como malware, o cuando entramos en un sitio web con una baja reputación según el análisis de fiabilidad.



De las opciones disponibles, conviene activar:

- **Obtener protección para ti y para tu dispositivo frente a sitios web peligrosos.**
- **Enviar una solicitud de no seguimiento con tu tráfico de navegación:** para evitar ser rastreados.

Por último, disponemos de la opción de borrar los datos de navegación.

6. Referencias en Internet

- Navegación Segura
  http://www.navegacionsegura.es/
- Guías de seguridad en el uso de las redes sociales (INCIBE)
  https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet
- ESET – Guía de buenas prácticas de seguridad informática
  http://www.eset-la.com/pdf/prensa/informe/buenas_practicas_seguridad_informatica.pdf
- Seguridad y privacidad en Mozilla Firefox:
  http://support.mozilla.org/es/products/firefox/privacy-and-security
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/es/actualidad/blog/2012/04/04/navega-mas-seguro-con-los-analizadores-de-enlaces-url
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html