

# *Cómo mejorar la seguridad de tus navegadores*



Desde hace ya algunos años, navegar por Internet se ha convertido en algo habitual en la mayoría de las personas. A la hora de buscar cualquier tipo de información o adquirir algún producto que necesitemos, acudimos a la red de redes para encontrarlo. Esto también ha traído consigo la llegada de **amenazas** que pueden causarnos importantes problemas.

Muchos ya conocéis las reglas básicas que siempre debemos tener presente a la hora de navegar por la red, pero hoy queremos hablar sobre otro tipo de elementos menos conocidos por la mayoría de los usuarios y que pueden ofrecernos una **seguridad** extra. Nos estamos refiriendo a los complementos de seguridad para los navegadores.

A lo largo de este documento veremos cómo podemos mejorar la seguridad de los navegadores Chrome, Firefox e Internet Explorer con la ayuda de estos complementos.

## 3 sencillos pasos con los que mejorar la seguridad de tu navegador

En la red nos podemos encontrar con multitud de amenazas como puede ser el Spam, el **Phishing**, robo de contraseñas o malware entre otras. Algunas de ellas están estrechamente ligadas al navegador que utilizamos para movernos por la red. Entre las amenazas que podemos destacar y que afectan al navegador destacan 3.

### a) Privacidad y exposición de datos personales

Cuando navegamos por la red, es muy importante estar concienciados de la información privada que nuestro navegador está exponiendo a terceros mientras navegamos. Acciones como restringir el uso de **cookies** de terceros o borrar el historial de navegación de forma periódica puede suponer ya una cierta mejora.

### b) Bloqueo de malware

En este caso nos estamos refiriendo a la posibilidad de que el navegador sea capaz de realizar filtrados y bloquear aquellos sitios que supongan una amenaza para nosotros.

Muchos de los principales navegadores web ya ofrecen algún tipo de sistema de filtrado basado en el uso de listas negras que han sido reportadas por otros usuarios como sospechosas o maliciosas.

### c) Control de ejecución de scripts

Otro de los aspectos importantes que no podemos dejar pasar es el control de ejecución de scripts ya que estos se han convertido en una de las principales puertas de entrada para la realización de ataques hacia nuestro navegador. Ataques como el denominado 'Cross-Site Scripting' o 'Clickjacking', se sirven de la ejecución de ciertos scripts.

En este sentido, una de las principales recomendaciones y que todo el mundo debería tener presente es la de tener siempre actualizado el navegador a la última versión estable disponible, así como cualquier complemento que podamos tener instalado en él.

## ¿Qué es un complemento para un navegador web?

Los complementos para los navegadores web no son más que pequeños programas que se integran con el navegador y que ofrecen funcionalidades extras que por defecto no incluyen. En la actualidad nos podemos encontrar multitud de estos complementos o plugin de forma gratuita, que pueden ser instalados en pocos segundos. El único problema que nos podemos encontrar es que no todos los complementos están disponibles para todos los navegadores, por lo que dependiendo de cuál sea nuestro navegador favorito, deberemos buscar aquellos que hagan la función que necesitamos.

## Mejorar la seguridad en Chrome

Google Chrome ha sido uno de los últimos navegadores en llegar al mercado, pero esto no le ha impedido convertirse en el más utilizado en la actualidad en casi todo el mundo. A pesar de su popularidad, Chrome pasa por ser uno de los navegadores que presentan más problemas de seguridad, pero el gran equipo que tiene detrás y los suculentos premios que ofrece Google a todos aquellos que descubran vulnerabilidades en su herramienta hace que continuamente vayan apareciendo nuevas versiones, donde se corrigen problemas encontrados.



Por defecto, este navegador ofrece soporte para luchar contra el Phishing y el software malicioso, cosa que podemos activar o desactivar entrando en "**Configuración**", "**Configuración avanzada**" y luego visitando la zona de "**Privacidad**".

## Privacidad

Configuración de contenido...    Borrar datos de navegación...

Google Chrome puede utilizar servicios web para mejorar la experiencia de navegación de los usuarios. Puedes inhabilitar estos servicios si quieres. [Más información](#)

- Utilizar un servicio web para intentar resolver errores de navegación
- Utilizar un servicio de predicción para completar las búsquedas y las URL introducidas en la barra de direcciones o en el cuadro de búsqueda del menú de aplicaciones
- Predecir las acciones de la red para cargar las páginas más rápido
- Enviar a Google automáticamente información sobre posibles incidentes de seguridad
- Habilitar protección contra phishing y software malicioso
- Utilizar un servicio web para revisar la ortografía
- Enviar automáticamente estadísticas de uso e informes sobre fallos a Google
- Enviar una solicitud de no seguimiento con tu tráfico de navegación

A continuación os dejamos algunos complementos que siempre deberíamos tener en cuenta para mejorar la seguridad de nuestro navegador.

## 1.- ScriptSafe



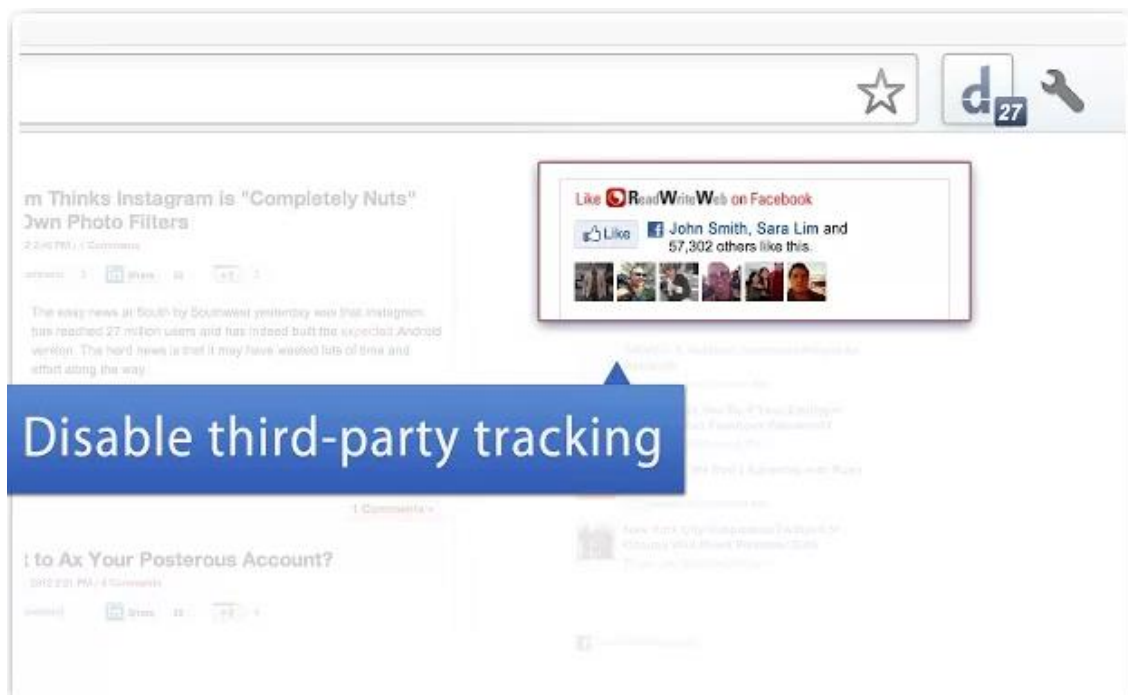
Se trata de una extensión que nos avisa en tiempo real de los script que se están ejecutando, bloqueando todos aquellos que puedan suponer una amenaza para nosotros. De esta forma evita ataques que podamos sufrir por la ejecución de este tipo de código.

## 2.- HttPs EveryWhere



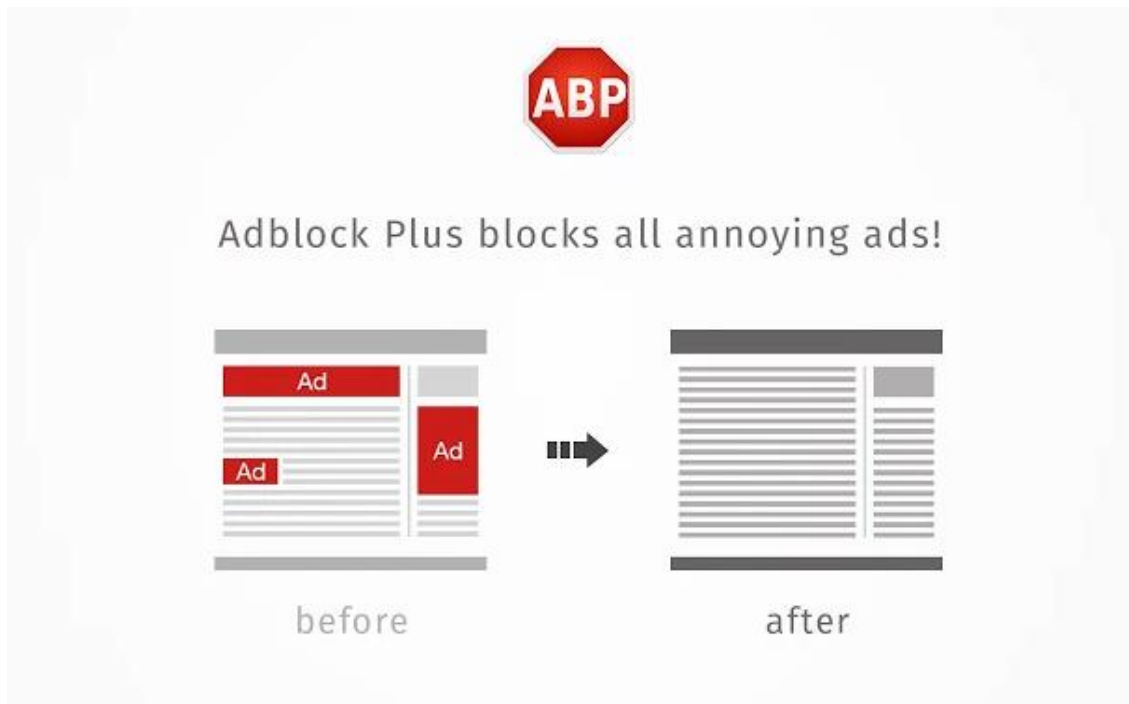
La funcionalidad que ofrece esta extensión es la de cifrar la mayoría de nuestras conexiones mediante el protocolo HTTPS, siempre y cuando la **página web** a la que nos conectemos lo permita. De esta forma estaremos consiguiendo que toda la información que se envíe desde nuestro navegador esté cifrada y por lo tanto más segura.

## 3.- Disconnect



Se trata de un complemento desarrollado por antiguos trabajadores de Google y permite bloquear multitud de servicios dedicados al rastreo de datos. Su uso es muy sencillo ya que una vez que lo instalemos empezará a bloquear por defecto aquellos servicios que se dediquen al rastreo, como a redes sociales tales como Facebook o Twitter.

#### 4.- Adblock Plus



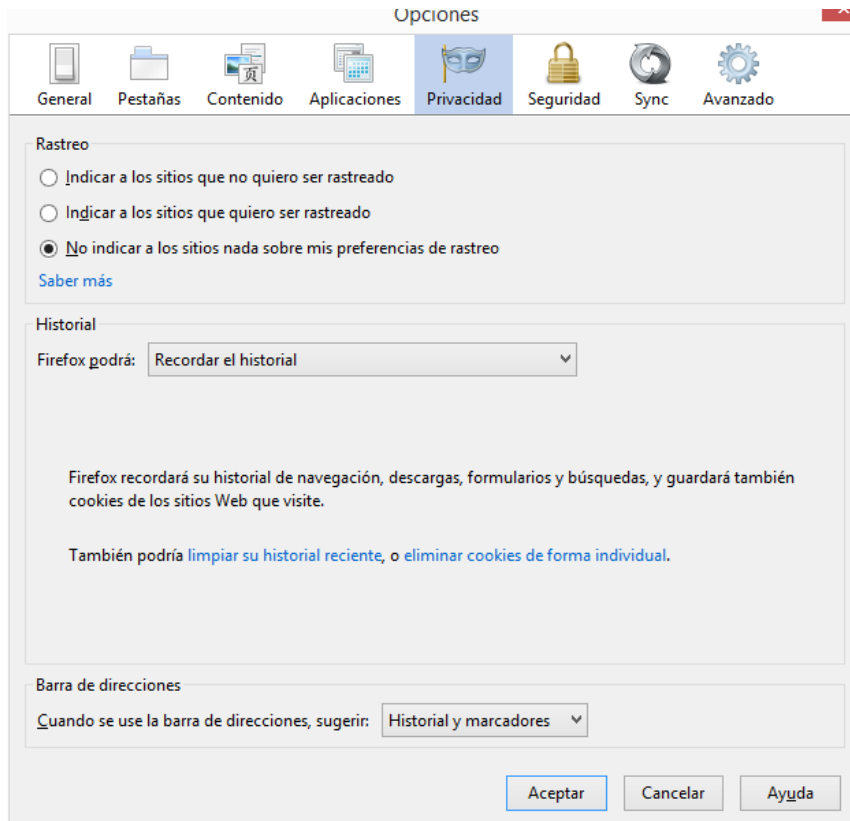
Esta extensión funciona para bloquear toda la publicidad que puede aparecer en una [página web](#), pero en versiones recientes también ofrece un filtro de privacidad, aunque no es tan completo como puede ser el caso explicado anteriormente, aunque sí que puede ser una buena opción si no queremos instalar nada más.

## Mejorar la seguridad en Firefox

Firefox se caracteriza por lanzar continuamente nuevas actualizaciones que vienen a solucionar ciertos problemas de seguridad. Esto es debido en gran medida al gran equipo de desarrollo que tiene detrás de él, que trabaja constantemente para mejorar la estabilidad y la seguridad de Firefox.



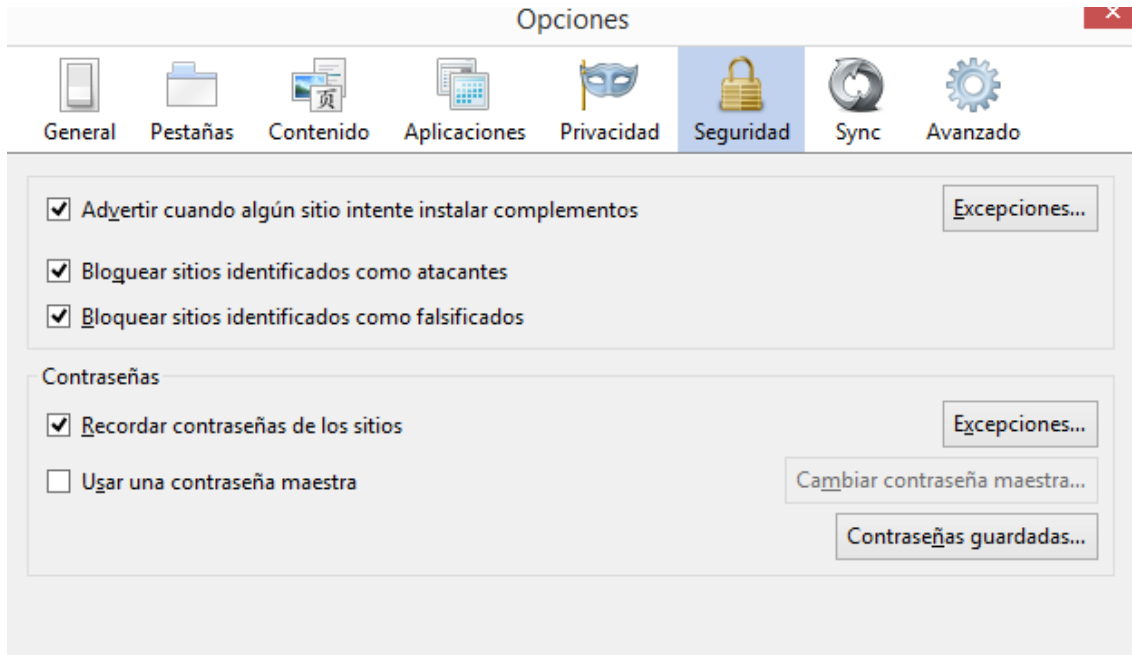
Antes de realizar la instalación de ningún complemento, podemos realizar una configuración básica que nos ayude a tener una mayor privacidad a la hora de utilizar este navegador. Para ello podemos entrar en "Opciones" e irnos a la pestaña de privacidad.



Aquí podemos hacer varias cosas.

- Podemos activar la opción "Indicar a los sitios que no quiero ser rastreado".
- En el menú desplegable seleccionar la opción "Usar configuración personalizada para el historial".
- Entre las opciones que nos aparecerán, podemos elegir "Modo permanente de navegación privada". De esta forma siempre que naveguemos no dejaremos rastro de las páginas que hemos visitado.
- Marcar la opción de "Aceptar cookies", pero no así las de terceras partes.

A continuación debemos acceder a la pestaña "**Seguridad**", pero en este caso no hace falta que hagamos nada, sino únicamente asegurarnos de que están marcadas las tres primeras opciones.



Dentro de los plugins que nos podemos encontrar desarrollados para Firefox podemos destacar.

### 1.- NoScript



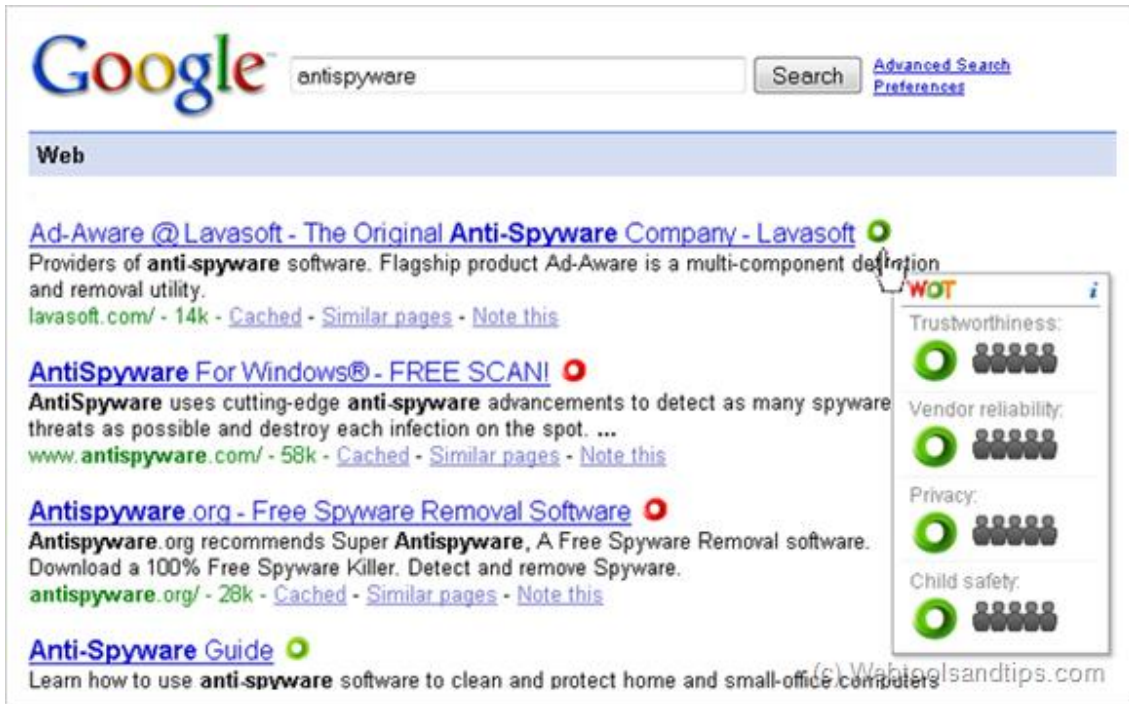
Se trata de un plugin que permite la ejecución de script únicamente de aquellos sitios de confianza que has indicado en su configuración, como puede ser la web de tu banco o la tienda online donde siempre compras. Para llevar a cabo este filtrado se hace uso de listas blancas, donde le podemos ir indicando nuestros sitios de confianza.

### 2.- BetterPrivacy

Este plugin nos permitirá gestionar un tipo especial de cookies denominadas súper cookies o **LSO Cookies**, un tipo de cookies que representa un riesgo mayor que las tradicionales ya que se tratan de elementos que proporcionan sitios como Google, YouTube o Ebay, entre otros muchos, y que se caracterizan por no expirar y ser difíciles de eliminar, cosa que se simplifica de gran forma al empezar a utilizar este complemento.



## 3.- WOT



WOT es un complemento que nos indica de forma visual, al estilo de los semáforos, si una web es fiable o no. Este plugin funciona añadiendo al lado de cada resultado de las búsquedas un icono, que dependiendo del color indicará si es seguro visitarlo o si por el contrario es mejor no entrar en él.

## 4.- Ghostery



Esta extensión bloquea el tráfico de rastreo que se va generando a medida que navegamos por Internet. De esta manera evitamos que recojan y traten terceras personas esa información sin nuestro consentimiento.

## Mejorar la seguridad en Internet Explorer

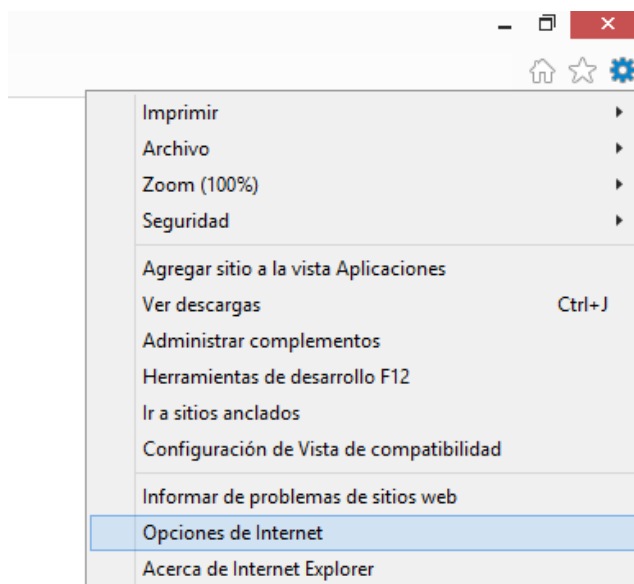
Internet Explorer sigue siendo uno de los navegadores más utilizados en la actualidad, sino el que más, en gran medida debido a que viene instalado con el sistema operativo Windows en todas sus versiones. Actualmente se encuentra por la versión 11, una versión donde se ha mejorado muchos aspectos de seguridad respecto a versiones anteriores.



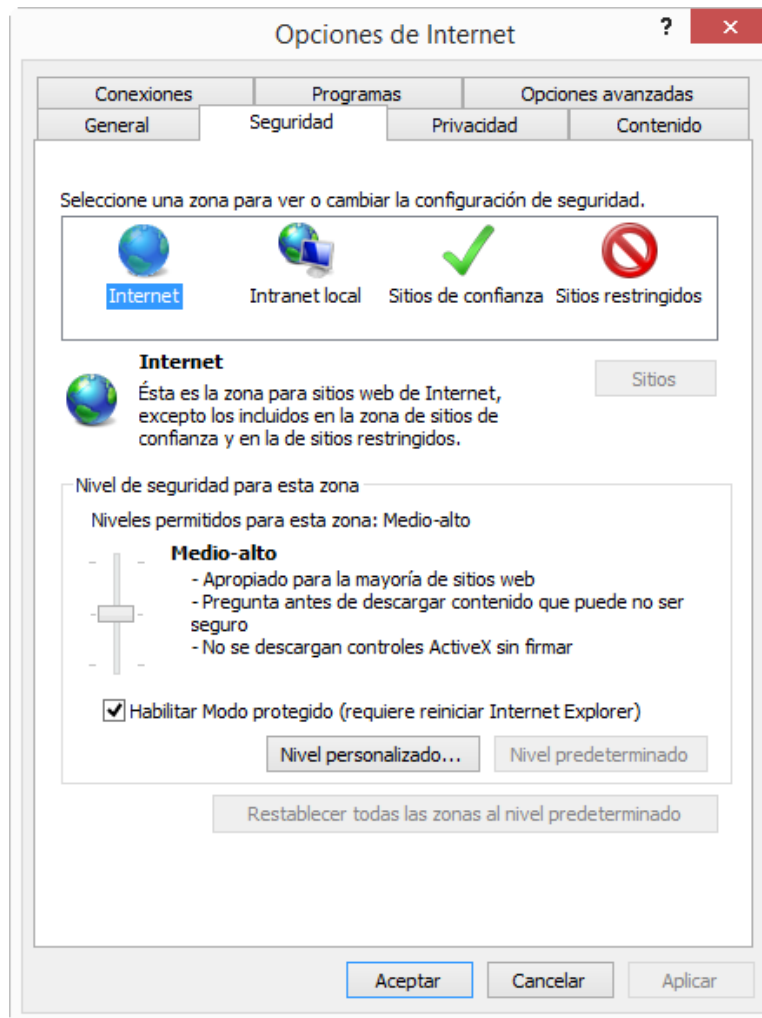
Algunas de las principales características de seguridad que ofrece Internet Explorer son:

- **Filtros SmartScreen**, que nos ayudan a protegernos de ataques de suplantación de identidad.
- **Administrador de complementos**, que le permite deshabilitar o habilitar los complementos del explorador web y eliminar los controles ActiveX no deseados.
- **Filtro de scripts (XSS)**, que evitan ataques de sitios fraudulentos con los que podrían robar información valiosa.
- **Conexión segura SSL de 128 bits para usar sitios webs seguros.**

Si queremos cambiar aspectos de la seguridad de nuestro navegador Internet Explorer, lo que debemos hacer es pulsar sobre el botón "**Herramientas**" y luego en "**Opciones de Internet**".



Luego pulsaríamos sobre la pestaña "**Seguridad**".



Ahí podemos cambiar el nivel de seguridad que queremos utilizar. Cuanto más alto sea, mayor seguridad tendremos a la hora de navegar por la red. Si lo que queremos es cambiar valores de configuración de seguridad específicos, haz clic en 'Nivel personalizado'. Cambia los valores como desees y haz clic en 'Aceptar' cuando hayas terminado.

Internet Explorer también ofrece la posibilidad de añadir plugins para mejorar la seguridad de su navegador, pero es una característica que no está tan desarrollada como en los otros casos anteriores vistos. Entre los que nos podemos encontrar están:

#### 1.- [EasyList Standard](#)

Se trata de un sistema de protección basado en la popular suscripción EasyList par Adblock Plus.

#### 2.- [Lista de protección de rastreo PrivacyChoice](#)

Se trata de una extensión que bloquea a todas aquellas empresas que realizan algún tipo de rastreo y que no se encuentran bajo la supervisión de la Network Advertising Initiative (NAI).

Esta lista está formada por más de 300 redes y plataformas publicitarias y se actualiza periódicamente para ofrecer una mayor seguridad al usuario.

### 3.- TRUSTe



La lista de protección de rastreo TRUSTed permite que únicamente se muestren los anuncios, relevantes y destinados al usuario de aquellas empresas que desarrollen prácticas de privacidad respetuosas con el cliente.

Con todo lo explicado en este documento os hemos enseñado como proteger un poco más tu navegador. Ahora sólo falta que lo pongas en práctica.