Firefox

Contenido

Introducción

El presente articulo es un derivado actualizado y ampliado del existente en el blog Mi mar conceptual (http://mimarconceptual.blogspot.com/2011/06/darknet-firefox.html) (en la clearnet).

```
Nota: Ese blog no tiene ninguna relación (conocida) con esta comunidad.
```

Para llegar hasta aquí, ya has configurado Firefox, es decir, has conseguido que tu navegador pueda entrar y navegar por esta red. Ahora bien, navegar por I2P no es en si 100% seguro, si no se toman mas medidas para mejorar nuestra seguridad.

Es por esto que te invitamos a conocer los objetivos de esta guia:

- en primer termino, configurar firefox correctamente para navegar en modo hibrido, o sea, paralelamente en varias redes
- mejorar sustancialmente la seguridad al navegar
- ampliar sus capacidades
- descubrir sus puntos débiles
- modificar nuestro comportamiento de navegación, concentrándose cada mas en nuestra seguridad
- generar el interés por buscar formas de optimizar nuestro navegador

Firefox es probablemente el navegador mas popular después de IE (que viene de fabricación en todas las maquinas con windows), aunque cifras mas recientes sugieren que Chrome ya se encontraría en segundo lugar por delante de Mozilla-Firefox. Lo importante es entender, que todo usuario que usa el navegador de fuente abierta, no esta 100% seguro, ni libre del espionaje.

Lamentablemente Firefox viene con una serie de configuraciones por defecto, que permiten a los sitios que visitamos, como así a los gobiernos y en primer termino a empresas como Google poder monitorizar nuestro comportamiento en la red.

```
Consejo: Windows, Mac OSX y los sistemas Unix/Linux privativos violan TODOS tus derechos a la privacidad.
TAILs es una distribución LINUX especialmente desarrollada para protegernos de tales intensiones.
```

PASO 1- Instalar Firefox y Tor

Ubuntu

- Instalar firefox, tor, polipo. Polipo nos ayudara a cargar mas rápidamente las paginas, ya que las guarda en cache.

```
$ sudo apt-get install tor polipo firefox
```

- Luego hay que editar polipo

```
$ sudo gedit /etc/polipo/config
```

- Hay que descomentar las siguientes líneas:

```
socksParentProxy = “localhost:9150˝
socksProxyType = socks5
```

- Guardamos y cerramos el archivo. Luego ejecutamos lo siguiente para que los servicios tor y polipo comiencen de forma automática:

```
$ sudo service tor restart
$ sudo service polipo restart
```

Windows

Si usas Windows, Linux o Mac OSX, puedes descargarte el "Tor Browser Bundle" (https://www.torproject.org/projects/torbrowser.html.en). Este es un paquete portable (que no necesita instalación), con Firefox, Tor, Polipo y Vidalia ya listos para ser ejecutado.

Mac OSX

Ademas del "Tor Browser Bundle" (https://www.torproject.org/projects/torbrowser.html.en), también se pueden instalar las aplicaciones de forma separada.

- Se debe descargar e instalar "Firefox" (https://www.mozilla.org/). A continuación se recomienda descargar e instalar "MacPorts" (https://www.MacPorts.org/) (algo asi como APT de Linux), para ejecutar:

```
$ sudo port selfupdate
$ sudo port install tor lingon privoxy polipo
```

Lingon es un GUI para configurar procesos que se podrán ejecutar como demonios en el sistema y que ayudara a configurar TOR e i2p en este sentido y se inicien automáticamente con el inicio de OSX.

- Luego hay que editar polipo

```
$ sudo cp /opt/local/etc/polipo/config.sample /opt/local/etc/polipo/config
$ sudo nano /opt/local/etc/polipo/config
```

- Hay que descomentar las siguientes líneas:

```
socksParentProxy = “localhost:9150˝
socksProxyType = socks5
```

- Guardamos y cerramos el archivo. Luego ejecutamos lo siguiente para que los servicios tor y polipo comiencen de forma automática:

```
$ sudo /op/local/bin/tor
$ sudo /opt/local/bin/polipo
```

PASO 2 - Instalar I2P

Ubuntu

Se necesita tener java instalado. Últimamente I2P también dispone de paquetes para debian y distribuciones derivadas. Estos son los pasos a seguir:

```
$ sudo apt-add-repository ppa:i2p-maintainers/i2p
$ sudo apt-get update
$ sudo apt-get install i2p
```

Otra opción es descargar el paquete directamente desde la pagina del proyecto y ejecutar:

```
$ java -jar i2pinstall_x.x.jar
```

Para ejecutar la red I2P, hay que ejecutar como usuario la siguiente orden:

```
$ i2prouter start
```

Esta orden se puede agregar a *Mis programas de inicio* para que se inicie de forma automática.

Windows

Se necesita tener *Java* instalado. Se descarga el instalador gráfico de I2P (Será algo así como "Graphical installer: i2pinstall_x.x.x.exe"), desde la pagina del Proyecto I2P (https://www.i2p2.de/download.html) o de su espejo en i2p (http://www.i2p2.i2p/download.html), y ejecutamos el archivo exe. Seguimos todas las instrucciones y listo. Para iniciar la red I2P hay que pulsar en "Start I2P".

Mac OSX

Se necesita tener *Java*. A continuación se debe descargar e instalar I2P (https://www.i2p2.de/download.html). Para instalar i2pinstall_x.x.jar existen dos caminos. Gráficamente al pulsar dos veces sobre el paquete que se descargo.

La segunda forma, es idéntica a la de Linux:

```
$ java -jar i2pinstall_x.x.jar
```

Para ejecutar I2P, se puede usar el ejecutable desde el directorio donde se instalo:

```
$ ./i2prouter start
```

O se puede buscar en el menú *Launchpad* el ejecutable *I2P Start*.

Con la ayuda de Lingon se puede ejecutar automáticamente I2P en cada inicio de sesión de OSX.

PASO 3 - Instalar Privoxy

Bueno, ya tenemos dos redes Darknet: la I2P por un lado y la red Tor por otro. Sin embargo, ahora mismo no podemos usar las dos a la vez. Tendríamos que estar cambiando de configuración constantemente, y eso podría llevarnos a errores y es peligroso para la seguridad.

Aquí es donde entra en escena Privoxy.

Privoxy va a permitir organizar las conexiones, en función de si es un sitio .i2p, un .onion, o la WWW.

Ubuntu

Para instalar privoxy:

```
$ sudo apt-get install privoxy
```

Editamos

```
$ sudo gedit /etc/privoxy/config
```

Hay que buscar la siguiente línea:

```
listen-address 127.0.0.1:8118
```

La substituimos por:

```
listen-address 127.0.0.1:8112
```

Al final de todo del archivo, añadimos lo siguiente:

```
forward / 127.0.0.1:8123
forward .i2p localhost:4444
forward 192.168.*.*/     .
forward 10.*.*.*/        .
forward 127.*.*.*/       .
```

Las ultimas 3 lineas nos permiten acceder a las direcciones locales sin necesidad de proxy alguno.

Guardar y cerrar el archivo. Y ahora se puede ejecutar Privoxy:

```
$ sudo service privoxy restart
```

Windows

Descargamos la última versión de Privoxy (http://www.privoxy.org). Lo instalamos y buscamos el archivo de configuración config.txt para editarlo. En el archivo se busca la siguiente línea:

```
listen-address 127.0.0.1:8118
```

La substituimos por:

```
listen-address 127.0.0.1:8112
```

Al final de todo del archivo, añadimos lo siguiente:

```
forward / localhost:8118 (P.D. También puede que sea 8123, depende de la versión)
forward .i2p localhost:4444
```

Y ahora se puede proceder a ejecutar privoxy.

Mac OSX

Se edita privoxy desde la linea de comandos

```
$ sudo nano /opt/local/etc/privoxy/config
```

Se cambia:

```
listen-address 127.0.0.1:8118
```

Y se substituye por:

```
listen-address 127.0.0.1:8112
```

Al final de todo del archivo, se añade lo siguiente:

```
forward / localhost:8123
forward .i2p localhost:4444
```

Y ahora se puede proceder a volver a ejecutar privoxy:

```
$ sudo /opt/local/sbin/privoxy /opt/local/etc/privoxy/config
```

Windows, Ubuntu y Mac OSX

Con las dos últimas líneas al archivo de configuración de privoxy le decimos que cuando una dirección sea ".onion" o la WWW, redirija al puerto 8123 en Ubuntu y al puerto 8118 en Windows (la red Tor), y cuando sea ".i2p" redirija al puerto 4444 (la red I2P).

PASO 4 - Configurar Firefox

Ubuntu, Windows y Mac OSX

1. Privoxy

Para que Firefox utilice Privoxy, debemos ir a "Options > Advanced > Network > Settings" (o su equivalente en español). Activamos "Manual proxy configuration".

A continuacion se realizan los siguientes cambios:

```
"HTTP"  > "localhost" > "8112"
"SSL"   > "localhost" > "8112"
"FTP"   > "localhost" > "8112"
"Socks" > "localhost" > "9150"
```

2. Que información debe recordar/actualizar firefox?

Ya que estamos en "Options", vamos a "Options > Privacy". Activamos la opción "Use custom settings for history". Y dentro desactivamos "Accept third-party cookies" y "Remember search and form history". Ahora vamos a "Options > Advanced > Update" y desactivamos las actualizaciones de "Add-ons" (Extensiones) y "Search Engines".

Ya podemos guardar y cerrar las opciones.

3. Desactivar el Spyware en about:config

Ahora hay que desactivar varias opciones "peligrosas", pero que no son accesibles de la forma habitual. En especial hay que desactivar el filtrado de Malware de Firefox. En realidad, el filtrado de Firefox es Spyware, ya que funciona enviando a G00gle todas las páginas que visitamos, para que Google nos diga si son buenas o malas. De hecho, esa es una importante fuente de ingresos para Mozilla en la actualidad. Obviamente lo último que queremos es a G00gle fisgando todo lo que visitamos, así que eso hay que desactivarlo.

a. desactivar "safebrowsing"

Escribimos en la barra de direcciones de Firefox "*about:config*". Prometemos ser buenos y buscamos "*safebrowsing*". Todas las opciones que comienzan con "*browser.safebrowsing*" hay que dejarlas, o bien en "false", o bien en "0", o bien vacías. De esa forma habremos desactivado totalmente el sistema de filtrado de G00gle (Claro, que quien tenga confianza ciega en G00gle, no tiene porque hacer esto).

b. evitar envío de información de rastreo vía headers

Sin salir de about:config, buscamos "*network.http.sendRefererHeader*" y lo ponemos en "0". Buscamos "*network.prefetch-next*" y lo ponemos en "false". Buscamos "*layout.css.visited_links_enable*" y lo ponemos en "false". Buscamos

"geo.enabled" y lo ponemos en "false". Buscamos "browser.geolocation.warning.infoURL" y "geo.wifi.uri" y lo ponemos vacío.

4. Algunas extensiones útiles

Ya para terminar, hay que instalar las siguientes extensiones:

```
Ghostery, UAControl
```

- *Ghostery*: no permite controlar que información cedemos a Internet. Nos da absoluto control de qué scripts y pluguins se ejecutan, y de qué redirecciones permitimos.
- *UAcontrol*: sirve para enmascarar nuestro navegador. En "Addons>UAControl", nos aparecerá un recuadro blanco donde al lado pone "Default for sites not listed:". Pulsamos *Edit* y ponemos *Custom*, y en el recuadro de al lado:

```
Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
```

Y se da a "OK" y "OK". A partir de ahora todas las páginas que visitemos verán que nuestro navegador es un Firefox estadísticamente de lo más corriente, y además bajo Windows, aunque en realidad usemos Linux. Esto hace mucho más difícil que nos identifiquen por cuestiones relacionadas con nuestro navegador concreto.

Mas extensiones se pueden encontrar en la pagina dedicada a **Extensiones y about:config de Firefox optimizados**

5. Desactivar referencias a G00gle

En opciones, hay que desactivar "G00gle search".

Ahora, Firefox usará tor para acceder a Internet de forma anónima. Si la dirección termina en ".onion", privoxy redirige a Tor. Si la dirección termina en ".i2p", privoxy redirige a I2P. En teoría, las extensiones instaladas hacen que la navegación por las onion e I2P sea perfectamente anónima.

Mas detalles referentes a extensiones y configuraciones las puedes hallar en **Firefox en detalle**

FELICIDADES, AHORA YA PUEDES NAVEGAR DE FORMA ANÓNIMA POR

INTERNET

PASO 5 - Testar y finalizar

Pulsando control + / se puede ver la barra de addons en Firefox, algo necesario para algunas de las extensiones que hemos instalado.

Para testar tu conexión y ver que no hay problemas, dos enlaces:

- TorProject.org (https://check.torproject.org/) nos dice simplemente si estamos usando Tor
- JAP (http://what-is-my-ip-address.anonymous-proxy-servers.net/) tiene un magnífico test de anonimato, que nos sacará a la luz cualquier cosa que tengamos mal configurada.

En fin, es una entrada muy larga, y con tantas operaciones es posible que algo falle. Si hay algún problema, no dudes en preguntar en los foros.

Comentarios Finales

Como medida de seguridad añadida, y como en la darknet uno se puede encontrar cosas muy desagradables, recomiendo desactivar las imágenes para quien quiera explorar páginas nuevas. En Firefox se hace: "Editar > Preferencias > Contenido" y desactivar la opción "Cargar imágenes automáticamente".

Firefox ha entrado en una dinámica de hacer actualizaciones mayores (con cambio del primer número), y con el Firefox 6 no puedo asegurar que esta configuración sea segura. Por si acaso, también he modificado las siguientes opciones en *about:config*:

```
''toolkit.telemetry.server''     ->   dejar vacío
''urlclassifier.gethashtables''  ->   dejar vacío
```

En cuanto a los addons, se han instalado todos en un Firefox nuevo, desde cero, y parece que funcionan perfectamente. Se ha realizado la prueba de anonimato y me ha dado los mismos buenos resultados que con Firefox 4/5/6. Pero una vez más, se insiste en que no se sabe que nivel de spyware podría haber incluido Mozilla en sus ejecutables precompilados. No olvidar, que en las próximas versiones eventualmente NO se podrá deshabilitar JavaScript.

Otras medidas de seguridad que no deben olvidarse:

Es importante usar un navegador que no tenga DNS leaks, fugas de DNS (en Ingles en TorProject (https://trac.torproject.org/projects/tor/wiki/doc/Preventing_Tor_DNS_Leaks)), y por el momento la mejor opción es usar Mozilla Firefox o un derivado como Iceweasel, Torbrowser o Seamonkey, e ir a about:config y cambiar network.dns.disablePrefetch a true, verdadero. Aunque dooble (http://dooble.sf.net) se ha ido imponiendo como una excelente alternativa basada en webkit, sin JavaScript (o desactivado) y una serie de herramientas que ayudan a proteger la privacidad.

Y por ultimo, el OUTPROXY

Cuando se instala I2P por defecto está configurado para usar un outproxy, pero este puede ser cambiado por otro (p.e. exitproxy.i2p (http://exitproxy.i2p), meeh.i2p (http://meeh.i2p/?p=services&sp=other)). Debemos darnos cuenta que siempre que usamos un outproxy el dueño de ese servicio puede esnifar nuestros datos, lo cual no es posible si navegamos sólo dentro de I2P.

```
Por otra parte, no podemos olvidar que una vez,
los paquetes salen del outproxy muy probablemente serán
investigados y/o recolectados por ISPs, empresas y/o
gobiernos (y sus agencias).
```

Especial: FoxyProxy

Este complemento o extensión nos permite hacer una gran parte de las mismas tareas que realiza privoxy de forma un poco mas fácil, con el agregado de poder definir perfiles, que permitan agregar filtros personalizados para grupos de sitios webs o sitios específicos. Ademas, permite tener tantos filtros, como sean necesarios, y poder usar diferentes proxies paralelos como: Tor, I2P, Freenet, Namecoin, JAP, etc...

Instalación, configuración y puesta en marcha

La instalación se debe hacer via el centro de complementos de firefox (Herramientas > Complementos > Obtener complementos). Es tan facil como buscarlo bajo el termino «foxyproxy» e instalándolo con solo presionar el botón «instalar».

A continuación, firefox se debe reiniciar. Una vez reinicializado aparecerá un icono en la parte inferior derecha (de lo contrario se puede ir directamente vía el menú Herramientas > Complementos > Extensiones > foxyproxy > Preferencias) y con el botón derecho del ratón sobre el, escoger «Opciones» para poder configurar los

diferentes proxies.

I2P, Namecoin, Tor

Para poder acceder a I2P, una vez instalado y ejecutado, foxyproxy nos ayudara de forma optima. A continuación se abren las opciones de foxyproxy, se presiona el botón «Añadir nuevo Proxy» en la parte derecha de la ventana. A continuación se va a la pestaña «General» para asignarle un nombre, como p.e. «I2P».

En la pestaña «Detalles» se configurara lo siguiente:

```
--------------------------------------------------------------------------------------------------------------
--------------------------------
| General | Detalles | Patrones |
-----------           ----------------------------
| Host or IP Address | 127.0.0.1 | Puerto | 4444 |
-------------------------------------------------
--------------------------------------------------------------------------------------------------------------
```

En la pestaña «Patrones» se configura como mínimo lo siguiente:

```
--------------------------------------------------------------------------------------------------------------
--------------------------------
| General | Detalles | Patrones |
----------------------           ----------------------------
| X No usar el proxy para direcciones IP internas         |
-------------------------------------------------------------
| Añadir | Editar | Copiar | Borrar | Ayuda | Referencias |
-------------------------------------------------------------
| Importar | Exportar |
-------------------------------------------------------------
| H | Nombre | Patron  | Lista
-------------------------------------------------------------
| X |  I2P   | *.i2p/* | Blanca(*)
-------------------------------------------------------------
(*) Todas las direcciones terminadas en i2p, serán filtradas por el proxy i2p
--------------------------------------------------------------------------------------------------------------
```

Y al presionar «Aceptar» ya se puede navegar por las paginas clearnet e i2p de forma paralela.

Ahora se va a configurar foxyproxy para permitir navegar en y a través de la red TOR. Se vuelve a añadir una nueva regla proxy y se le asigna el nombre, p.e. «TOR» en la pestaña «General».

En la pestaña «Detalles» se configurara lo siguiente:

```
--------------------------------------------------------------------------------------------------------------
--------------------------------
| General | Detalles | Patrones |
-----------           ----------------------------
| Host or IP Address | 127.0.0.1 | Puerto | 9050 |
-------------------------------------------------
| X Proxy SOCKS?  |  0 SOCKSV4/4a  |  X SOCKS V5 |
```

```
-----------------------------------------------
```

En la pestaña «Patrones» se configura como mínimo lo siguiente:

```
--------------------------------
| General | Detalles | Patrones |
----------------------          ---------------------------
| X No usar el proxy para direcciones IP internas         |
-----------------------------------------------------------
| Añadir | Editar | Copiar | Borrar | Ayuda | Referencias |
-----------------------------------------------------------
| Importar | Exportar |
-----------------------------------------------------------
| H | Nombre | Patron  | Lista
-----------------------------------------------------------
| X |  I2P   | *.i2p/* | Negra(*)
| X |  TOR   | *.*     | Blanca(*)
-----------------------------------------------------------
(*) Todas las direcciones terminadas en i2p, NO serán filtradas por el proxy tor,
y todas las demás direcciones serán filtradas aquí.
```

Y tan pronto se presiona a «Aceptar» se estará listo para poder usar TOR, I2P y clearnet de forma paralela.

Nota: para agregar mas proxies, se debe tomar en cuenta el modificar los proxies existentes, especialmente el de TOR, para que las reglas de filtrado no entren en conflicto entre si.

A continuación se agregara una excepción a la regla de filtrado «TOR» para permitir navegar por las paginas con extensión «.null» que se pueden navegar gracias al proyecto OpenNic (http://www.opennicproject.org)

```
| X |  NULL   | *.null/* | Negra
```

Y ahora se podra navegar por todas estas paginas sin usar TOR.

A continuación se proveen algunas ideas y recomendaciones de addons para firefox, que nos ayudaran a cuidar de nuestra privacidad.

En adición, se debe considerar usar Sandfox para ejecutar Firefox dentro de uno.

Colección de Plugins / Extensiones

- Adblock Plus (https://addons.mozilla.org/en-us/firefox/addon/adblock-plus) - Un bloqueador de publicidad (también se encuentra para Chromium) - **Nota:**

En las Preferencias de Filtrado -> Suscripciones de Filtros -> Desactivar *Permitir alguna publicidad no intrusiva*
    - Fanboy Adblock List (https://www.fanboy.co.nz/)
    - Fanboy Tracking List (https://www.fanboy.co.nz/)
    - Fanboy Annoyance Blocklist (https://www.fanboy.co.nz/)
- HTTPS-Everywhere (https://www.eff.org/https-everywhere) - Cifra las comunicaciones con muchos sitios en Internet - **Nota:** Si se esta usando el SSL Observatory se debe desactivar la opcion *Informar al observatorio sobre tu actual ISP*
- Noscript (https://addons.mozilla.org/en-US/firefox/addon/noscript/) - Desactiva JavaScript, Java, Flash excepto en aquellos sitios de tu lista blanca (White-List). Ademas provee un anti-XSS y un anti-Clickjacking
- RequestPolicy (https://addons.mozilla.org/en-US/firefox/addon/requestpolicy/) - Evita las llamadas o solicitudes de información que realizan los sitios
- RefControl (https://addons.mozilla.org/en-US/firefox/addon/refcontrol/) - Controla la información básica que se envía vía HTTP Referer
- FoxyProxy (https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/) - Administración avanzada de Proxy
- Better Privacy (https://addons.mozilla.org/en-us/firefox/addon/betterprivacy/) - Borra o administra las galletas de información (cookies), LSOs y cookies Flash
- Cookie Monster (https://addons.mozilla.org/en-us/firefox/addon/cookie-monster/) - Administración de Cookies por sitio o nivel básico de dominio
- User Agent Switcher (https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher) - Administrador de agentes de usuario del Navegador
    - UserAgent Switcher List (http://techpatterns.com/forums /about304.html) - espejo local: i2p link (http://salt.i2p /useragentswitcher.xml) tor link (http://salted7fpnlaguiq.onion /useragentswitcher.xml)
- WebPG (https://addons.mozilla.org/en-us/firefox/addon/webpg-firefox/) - Provee funciones relativas a GnuPG/GPG/PGP
- Bloody Vikings (https://addons.mozilla.org/en-US/firefox/addon/bloody-vikings/) - Crea direcciones de correo al vuelo, para formularios

Preferencias de Firefox

```
"General" -> "Cuando firefox se ejecuta" -> "Mostrar una pagina en blanco"
"General" -> "Guardar archivos en la carpeta" : "Descargas"
"Contenido" -> activar : "Bloquear ventanas emergentes"
"Contenido" -> desactivar : "Activar JavaScript" [opcional - La extensión NoScript lo bloqueara de todas
"Aplicaciones" -> escoger : "Ademas preguntar" para cada aplicación - si no es posible : escoger :
 "Previsualizar en Firefox/Nightly"
"Privacidad" -> "Tracking" -> activar : "Avisar a los sitios que no se quiere ser seguido"
"Privacidad" -> "Historico" -> "Firefox will : "Use configuraciones personalizada para histórico"
"Privacidad" -> "Historico" -> desactivar : "Siempre usar modo de navegación privada"
"Privacidad" -> "Historico" -> desactivar : "Recordar mi histórico de navegación y descargas"
"Privacidad" -> "Historico" -> desactivar : "Recordar histórico de búsquedas y formularios"
"Privacidad" -> "Historico" -> desactivar : "Aceptar galletas (cookies) de terceras partes"
```

```
"Privacidad" -> "Historico" -> activar : "Limpiar histórico cuando cierre Firefox/Nightly"
"Privacidad" -> "Historico" -> "Configuraciones" : activar todos los deseados
"Privacidad" -> "Barra de navegación" -> "Sugerencias cuando use la barra de navegación:" -> escoger : "N
"Seguridad" -> activar : "Avisarme cuando los sitios intenten instalar extensiones"
"Avanzado" -> "General" -> "Sistema por defecto" -> desactivar : "Enviar reportes de errores"
"Avanzado" -> "General" -> "Sistema por defecto" -> desactivar : "Enviar datos de rendimiento"
"Avanzado" -> "Actualización" -> activar : "Automáticamente instalar actualizaciones"
"Avanzado" -> "Actualización" -> activar : "Avisarme cuando se desactive cualquiera de las extensiones"
"Avanzado" -> "Actualización" -> activar : "Automáticamente actualizar extensiones de búsqueda"
"Avanzado" -> "Cifrado" -> "certificados" -> "cuando algún servidor solicite mi certificado personal" ->
 "preguntarme cada vez"
```

about:config

about:config es una característica de las aplicaciones de Mozilla que despliega la lista de configuraciones (conocido como preferencias) que se pueden leer desde los archivos prefs.js y user.js, y desde las configuraciones básicas de las aplicaciones. Muchas de esas preferencias no están presente en el menú de las opciones o preferencias.

Las siguientes configuraciones son completamente opcionales. Elegir lo que se desee modificar. Algunas de estas opciones pueden romper o impedir su normal funcionamiento esperado.

- En Firefox y en la Suite Mozilla/SeaMonkey, tipear **about:config** en la barra de navegación (barra de direcciones) y presiona la tecla Enter para desplegar la lista de preferencias

```
---desactivar cache de navegación:
browser.cache.disk.enable:false
browser.cache.disk_cache_ssl:false
browser.cache.offline.enable:false
browser.cache.memory.enable:false
browser.cache.disk.capacity:0
browser.cache.disk.smart_size.enabled:false
browser.cache.disk.smart_size.first_run:false
browser.cache.offline.capacity:0
dom.storage.default_quota:0
dom.storage.enabled:false
dom.indexedDB.enabled:false
dom.battery.enabled:false

---desactivar histórico & localización
browser.search.suggest.enabled:false
browser.sessionstore.resume_from_crash:false
geo.enabled:false

---otras características varias:
keyword.enabled:false
network.dns.disablePrefetch:true
network.dns.disablePrefetchFromHTTPS:true
dom.disable_window_open_feature.menubar:true
dom.disable_window_open_feature.personalbar:true
dom.disable_window_open_feature.scrollbars:true
dom.disable_window_open_feature.toolbar:true
browser.identity.ssl_domain_display:1
```

```
browser.urlbar.autocomplete.enabled:false
browser.urlbar.trimURL:false
privacy.sanitize.sanitizeOnShutdown:true
network.http.sendSecureXSiteReferrer:false
network.http.spdy.enabled:false ---> usar http en vez del espia google
plugins.click_to_play:true ---> ademas activa cada submenu desplegable bajo las "preferencias" -> "conten
security.enable_tls_session_tickets:false ---> desactiva el seguimiento https
security.ssl.enable_false_start:true ---> desactiva el seguimiento https
extensions.blocklist.enabled:false ---> desactiva la opcion en Mozilla para bloquear/desactivar remotamen
webgl.disabled:true ---> desactiva WebGL (http://security.stackexchange.com/questions/13799/is-webgl-a-se
```

Impresión de huellas dactilares (Fingerprinting) del navegador

A continuación se presentan algunas ideas para ayudar a prevenir dejar huellas dactilares mientras se navega con Firefox. Estas crean una identidad falsa de tu navegador a través de la información en los encabezados HTTP que se envían a los sitios. Para hacer estos cambios, se va a about:config y se escoge "nueva"->"cadena" y se pulsa intro para ingresar lo siguiente:

```
Variable:                                Valor:

general.useragent.override               Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0
general.appname.override                 Netscape
general.appversion.override              5.0 (Windows)
general.oscpu.override                   Windows NT 6.1
general.platform.override                Win32
general.productSub.override              20100101
general.buildID.override                 0
general.useragent.vendor                 [ingresar variable - pero se deja en blanco]
general.useragent.vendorSub              [ingresar variable - pero se deja en blanco]
intl.accept_languages                    en-us,en;q=0.5
network.http.accept.default              text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
network.http.accept-encoding             gzip, deflate
```

Tema(s) relacionado(s)

- Firefox_GnuPG
- IE
- Navegadores_Web
- Guia del Proyecto i2p2.i2p con imagenes (http://vekw35szhzysfq7cwsly37coegsnb4rrsggy5k4wtasa6c34gy5a.b32.i2p/es/about/browser-config)

Categorías: Seguridad | Aplicaciones

- Esta página fue modificada por última vez el 23 jun 2015, a las 18:47.