CCN-CERT

BP/17

Recomendaciones de seguridad de Mozilla Firefox

INFORME DE BUENAS PRÁCTICAS

JUNIO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

Fecha de Edición: mayo de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

Este documento forma parte de la documentación emitida por el Centro Criptológico Nacional cuyo objetivo es el de preservar la seguridad de los sistemas TIC de las Administraciones Públicas.

Para ello, se proporciona un archivo de configuración para aplicar medidas de seguridad sobre un *software* de navegación web y así facilitar la posibilidad de implementar seguridad en los sistemas TIC.

Para el desarrollo de esta guía se ha utilizado el instalador del programa *Mozilla Firefox* en su versión 72.0.1 (64bit) para *S.O. Windows*.

El desarrollo de esta guía se ha utilizado el instalador del programa Mozilla Firefox en su versión 72.0.1 (64bit) para S.O. Windows.

3. Objeto

El propósito de este documento consiste en establecer los procedimientos y utilidades necesarias para implementar y garantizar la seguridad en *Mozilla Firefox*.

4. Alcance

Este documento establece un procedimiento para mejorar la seguridad y proteger *Mozilla Firefox* para mitigar las posibles vulnerabilidades y los riesgos frente a los que pudiera estar expuesto.

Los usuarios de esta guía pueden mejorar la seguridad de esta aplicación a través de los archivos de configuración que se incluyen en su anexo.

5. Descarga, instalación y configuración de mozilla firefox

El programa Mozilla Firefox está disponible para descargar de manera gratuita desde la página web de Mozilla.

Mozilla Firefox debe tener instaladas las últimas actualizaciones de software relacionadas con la seguridad. Para ello, determine el método de actualización (por ejemplo, conexión a un servidor *WSUS*, procedimiento local, actualización automática, etc.).

Si no se aplican las últimas actualizaciones de *software* relacionadas con la seguridad de *Firefox*, este sería un fallo crítico de seguridad.

Descarga el navegador en: https://www.mozilla.org/es-ES/firefox/new/

5.1 Versiones

El software de escritorio Mozilla Firefox está disponible para su implementación tanto con la versión "rápida" como con la versión "ESR".

Versión rápida: Recibe actualizaciones importantes cada seis semanas y actualizaciones menores, como correcciones de errores y correcciones de seguridad, según sea necesario durante esas seis semanas.

Versión de soporte extendido (ESR): De media, recibe actualizaciones importantes cada 42 semanas y actualizaciones menores, como correcciones de errores, correcciones de seguridad y actualizaciones de políticas, según sea necesario, pero al menos cada seis semanas.

Además de los diferentes ciclos de actualización, la ESR actualmente tiene acceso a políticas adicionales que no están disponibles en la versión rápida.

5.1 Versiones

- Autenticación integrada (SPNEGO y NTLM).
- Deshabilitar las actualizaciones de la aplicación.
- Deshabilitar las actualizaciones de complementos del sistema.
- Administrar extensiones.
- Cambiar la página de inicio.
- Cambiar la página de Firstrun.
- Cambiar la página de actualización.
- Mostrar la barra de búsqueda.
- Cambio de motores de búsqueda.
- Filtrado de sitios web.

5.1 Versiones

Para saber la versión de Firefox que se está utilizando:

Paso	Descripción
1.	Se debe hacer clic en el botón menú ☰ se hará clic en “Ayuda” y se selecciona “Acerca de Firefox”. A continuación, aparecerá la ventana “Acerca de Firefox”. El número de la versión instalada se mostrará debajo del nombre de Firefox, tal como se muestra en la siguiente imagen:
2.	
3.	Como alternativa, para ver la versión de navegador que está instalado, se puede hacer clic en el botón de menú ☰, se hace clic en “Ayuda” y se selecciona “Información para solucionar problemas”. Se abrirá una página con la dirección “about:support” en una pestaña nueva. La versión de Firefox aparece bajo la sección Configuración básica de la aplicación.

5.2 Requisitos mínimos

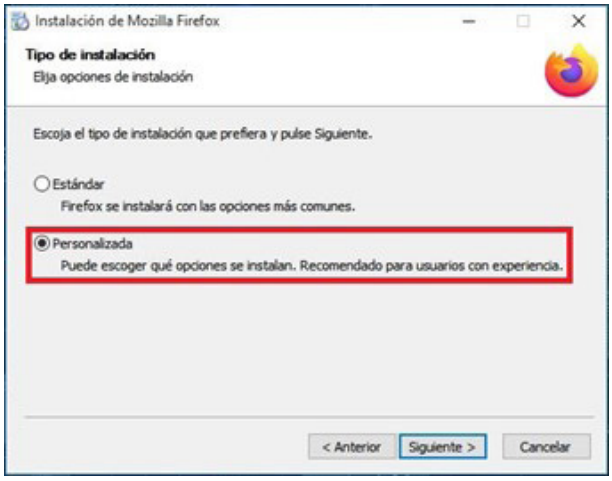
A continuación, se detallan los requisitos mínimos necesarios del sistema para realizar la implementación del programa Mozilla Firefox en Windows.

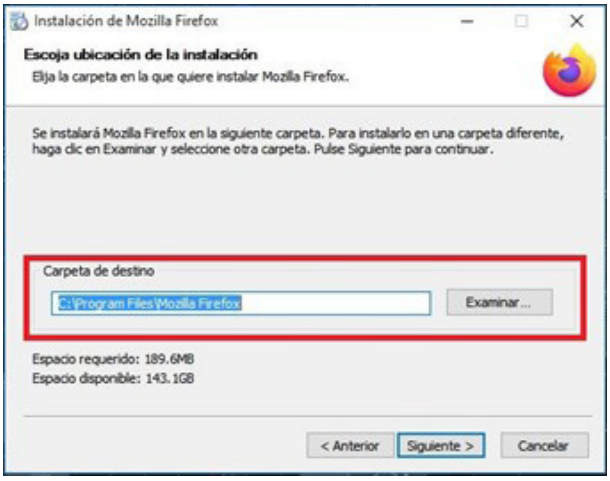
- **Sistema Operativo (32-bit y 64-bit)**
  - Windows 7
  - Windows 8
  - Windows 10
- **Hardware recomendado**
  - Pentium 4 o un procesador más moderno que admita SSE2.
  - 512MB de RAM / 2GB de RAM para la versión de 64-bit.
  - 200MB de espacio disponible en el disco duro.

5.3 Ubicación de la instalación

Como alternativa, para ver la versión de navegador que está instalado, se puede hacer clic en el botón de menú , se hace clic en "Ayuda" y se selecciona "Información para solucionar problemas". Se abrirá una página con la dirección "about:support" en una pestaña nueva. La versión de Firefox aparece bajo la sección **Configuración básica de la aplicación**

- C:\Archivos de programa\Mozilla Firefox\ es la ruta de instalación por defecto, tanto para la versión de 32-bits (instalado en un sistema operativo de 32 bits) como para la versión de 64 bits (instalado en un sistema operativo de 64 bits).
- C:\Archivos de programa(x86)\Mozilla Firefox\ es la ruta de instalación por defecto, cuando se instala el navegador de 32-bits en un sistema operativo de 64 bits.





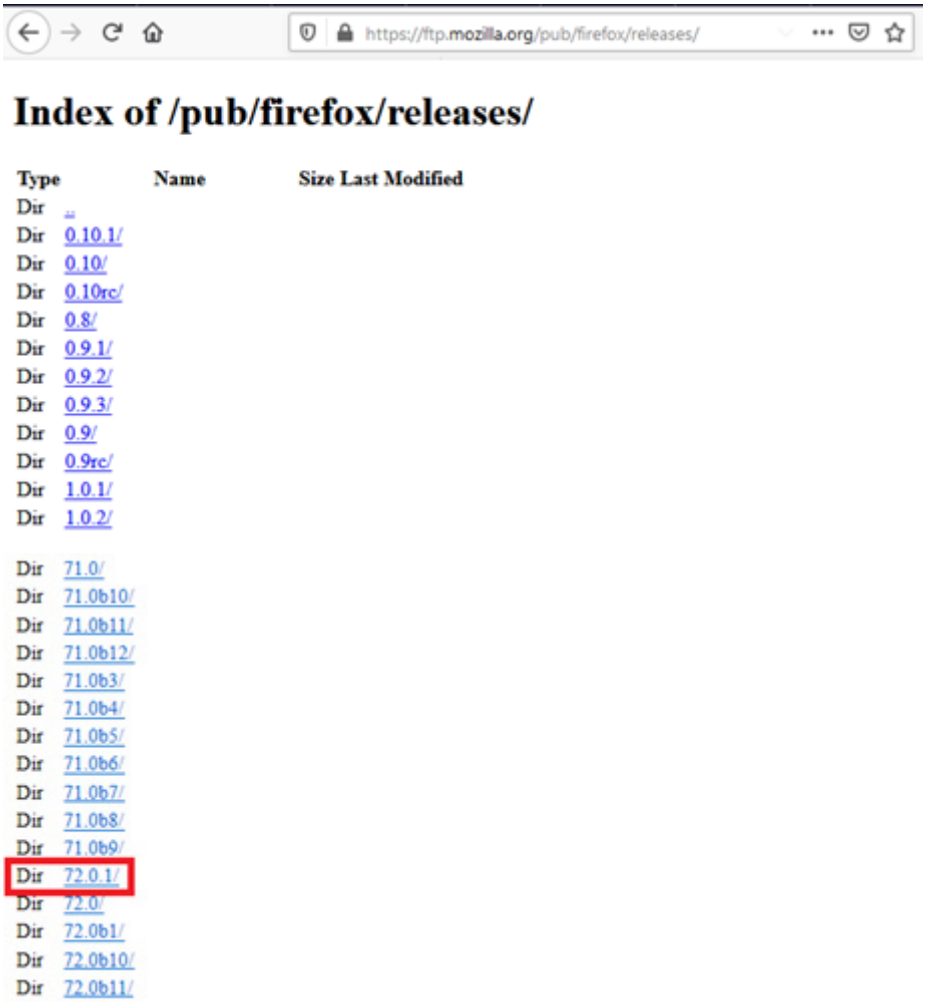
Nota: Es posible personalizar la ruta donde se realiza la instalación del programa durante el proceso de instalación.

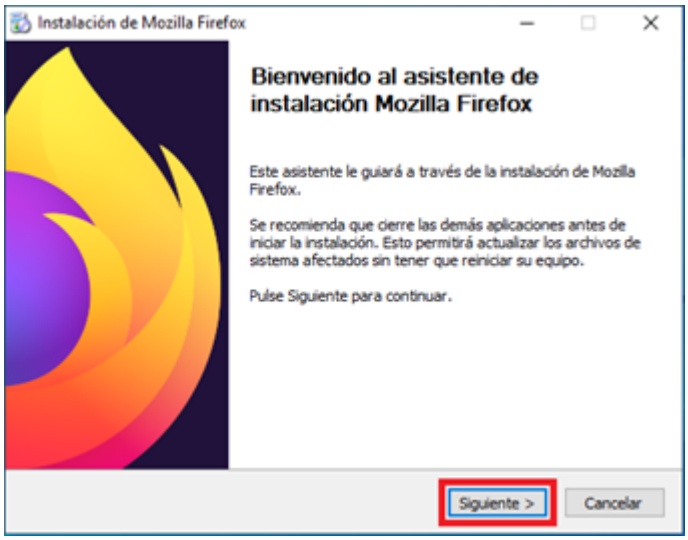
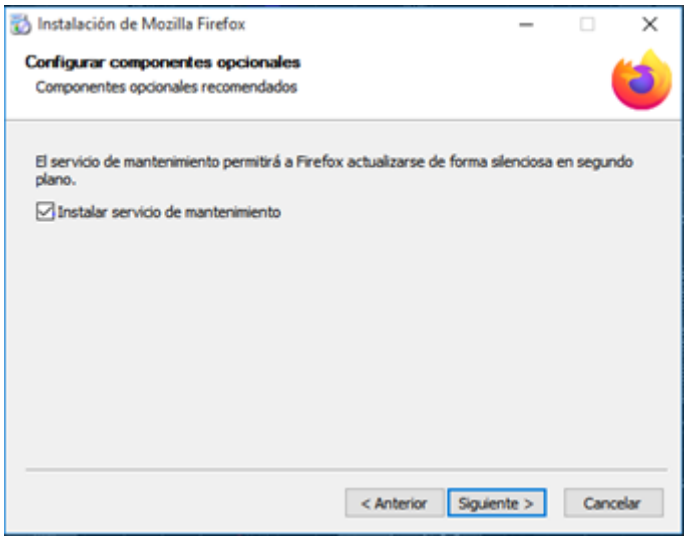
5.4. Descarga e instalación de Mozilla Firefox

Es posible realizar la descarga del programa mediante la siguiente url:

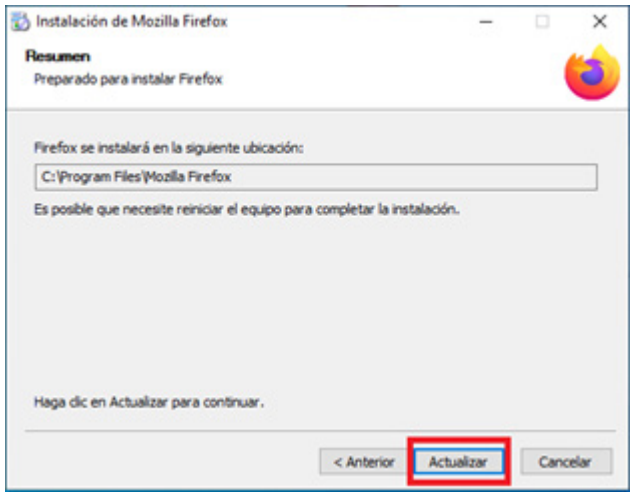
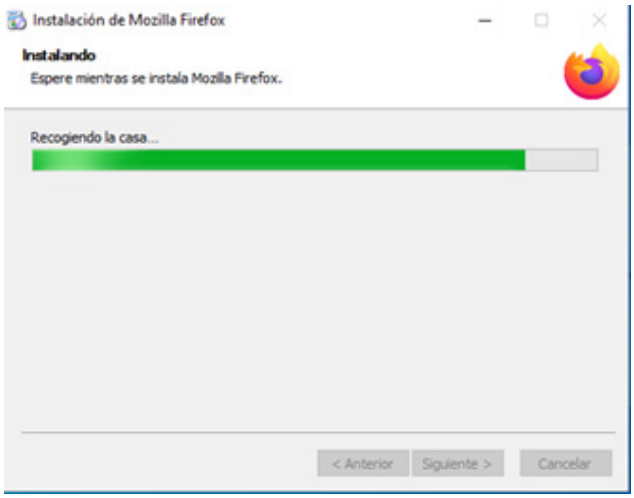
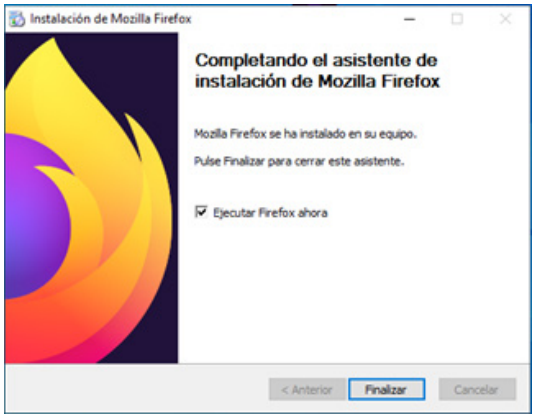
https://www.mozilla.org/es-ES/firefox/all/#product-desktop-release

Paso	Descripción
1.	En esta ventana se selecciona el navegador a descargar, el sistema operativo en el cual se instalará esta descarga y por último se selecciona el idioma. A continuación, se pulsará el botón "Descargar ahora" para iniciar la descarga del programa.  **Nota: Firefox Enterprise ofrece instaladores MSI para ayudar a los administradores de sistemas a personalizar e implementar Firefox en sus entornos a través de herramientas de implementación estándar de Windows, como pueden ser la aplicación de GPOs en Active Directory o mediante Microsoft System Center Configuration Manager.** **https://support.mozilla.org/es/kb/personalizacion-de-firefox-con-instaladores-msi#w_msi-installers** **Otro método alternativo para la descarga del navegador es mediante FTP, en la siguiente URL:** **https://ftp.mozilla.org/pub/firefox/releases/**

Paso	Descripción
2.	La siguiente ventana se utilizará como ejemplo la descarga de Mozilla Firefox en su versión 72.0.1.  El archivo de instalación que se obtiene de la descarga será utilizado para instalar o actualizar la versión de Mozilla Firefox en el sistema donde se realice la configuración de seguridad y privacidad. Para iniciar la instalación del navegador se realizará doble *clic* sobre el archivo descargado. **Nota: Para la instalación del programa es necesario realizarlo con un usuario con privilegios administrativos en el equipo donde está instalando Firefox.**

Paso	Descripción
3.	 A continuación, se procede a la instalación del navegador como se indica en la imagen anterior. Mozilla Firefox instala por defecto un servicio opcional llamado "servicio de mantenimiento", que permite actualizaciones en segundo plano, sin que tengas que hacer clic en Aceptar en el diálogo de Control de cuenta de usuario de Windows. Esta opción se puede desmarcar al realizar la instalación personalizada.  Si se realiza una reinstalación del Firefox sobre una versión existente, aparecerá un botón de "Actualizar" en lugar del botón de "Instalar", como se observa en la siguiente imagen:

5.4 Descarga e instalación de Mozilla Firefox

Paso	Descripción
3.	 Una vez realizados los pasos anteriores, se deberá hacer clic sobre el botón de instalar o actualizar y esperar hasta que el proceso haya terminado.   Una vez finalizada la instalación, se reinicia el sistema y ya se puede utilizar el navegador.

5.5 Aplicar configuración de seguridad y privacidad

A continuación, se describe cómo añadir las configuraciones de seguridad a Firefox para mantener nuestra información segura.

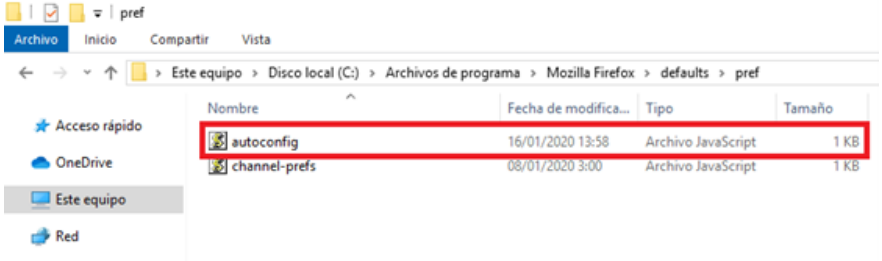
Los archivos de configuración automática se pueden usar para establecer y bloquear preferencias que no están cubiertas por las políticas de *Firefox*.

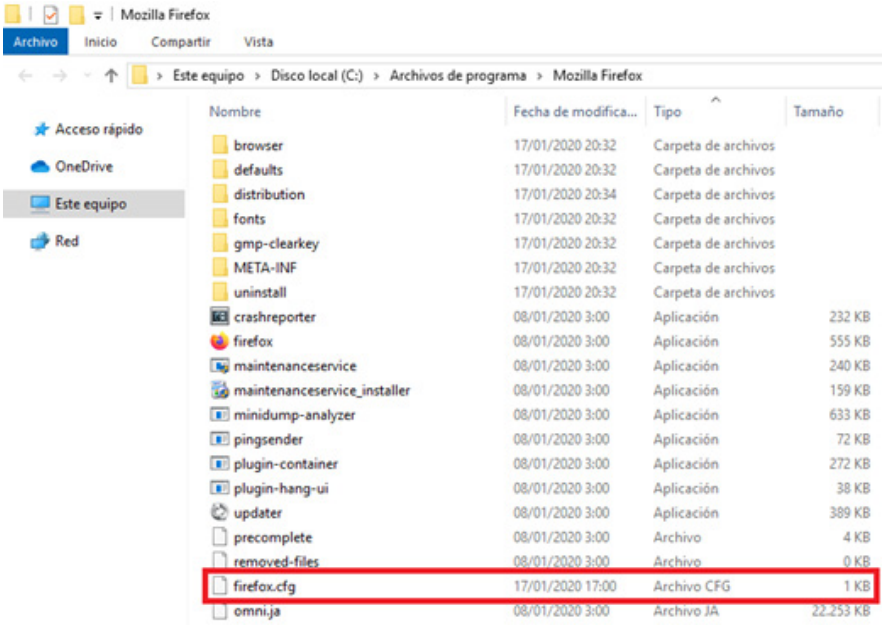
Para usar la configuración automática, se deben colocar dos archivos en los directorios de *Firefox*.

Si el sistema operativo es **Microsoft Windows**, estos ficheros se ubicarán en el directorio de instalación de *Firefox*.

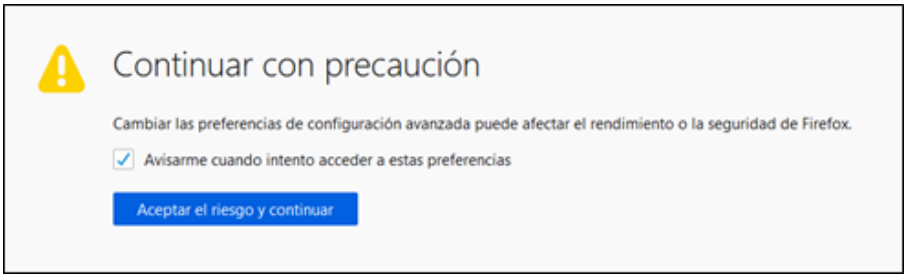
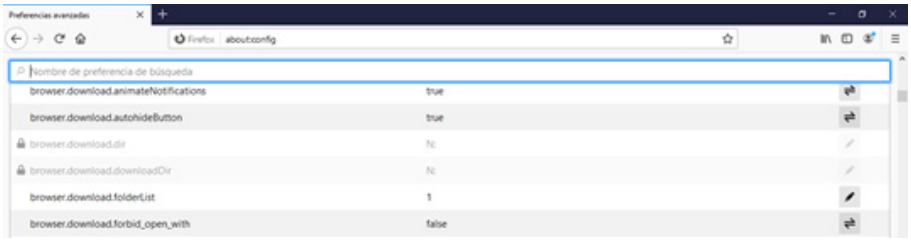
El archivo ***"autoconfig.js"*** se ubica en el directorio "/Mozilla Firefox/defaults/pref".

El archivo ***"firefox.cfg"*** se ubica en el directorio de instalación de firefox ("/Mozilla Firefox\)".

Paso	Descripción
1.	Se utiliza la ruta de instalación por defecto para una instalación de Mozilla Firefox de 64-bit: El archivo "*autoconfig.js*" se ubica en el directorio C:\Archivos de programa\Mozilla Firefox\defaults\pref\. 

Paso	Descripción
2.	El archivo *"firefox.cfg"* se ubica en el directorio C:\Archivos de programa\Mozilla Firefox\.  **Nota: Los ficheros de configuración "*autoconfig.js*" y "*firefox.cfg*" se encuentran ubicados en la carpeta "Scripts" de la presente guía de buenas prácticas.**

5.6 Valores de las directivas

Paso	Descripción
1.	A continuación, se detallan las modificaciones de seguridad aplicadas mediante la incorporación de los archivos *"autoconfig.js"* y *"firefox.cfg"* en el proceso de refuerzo de seguridad establecido en el punto **"5.5 Aplicar configuración de ".** En el editor de configuración (la página *about:config*) se encuentra una lista con las preferencias avanzadas de Firefox para verificar los valores colocados en el archivo *"firefox.cfg"*. Para acceder a las preferencias avanzadas se deberá escribir **about:config** y pulsar Enter en la *barra de direcciones*. Al realizar esta acción, aparece una página de advertencia con un aviso sobre la modificación de estas configuraciones avanzadas puede afectar al rendimiento o a la seguridad de Firefox. Para continuar, se debe hacer clic en **Aceptar los riesgos y continuar.** 
2.	En la parte superior de la página about:config, se puede usar el campo "Buscar" para la rápida obtención de las preferencias específicas 

Firefox está configurado para usar un almacén de contraseñas con o sin contraseña maestra.

Firefox se puede configurar para almacenar las contraseñas de los sitios visitados por el usuario. Estas contraseñas individuales se almacenan en un archivo y se pueden proteger con una contraseña maestra.

El rellenado automático de la contraseña se puede habilitar cuando se visita el sitio web. Esta característica también se podría usar para autocompletar el pin de un certificado, lo que podría comprometer la información.

El valor **"signon.rememberSignons"** debe estar establecido en "false" en el archivo "firefox.cfg"

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "signon.rememberSignons" esté configurado y bloqueado en "false".

La opción de asistencia para rellenar formularios en Firefox está desactivada.

Con el fin de proteger la privacidad y los datos sensibles, Firefox ofrece la posibilidad de configurar el programa para que los datos introducidos en formularios no se guarden. Esta configuración, mitiga el riesgo de que una página web pueda obtener información privada introducida previamente.

El valor **"browser.formfill.enable"** debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "browser.formfill.enable" esté configurado y bloqueado en "false".

Firefox está configurado para autocompletar contraseñas.

Debido a la forma en la que se almacenan las credenciales es posible para un atacante obtener acceso a las cuentas del usuario.

El valor **"signon.autofillForms"** debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "signon.autofillForms" esté configurado y bloqueado en "false".

Las preferencias de seguridad requeridas por Firefox no pueden ser cambiadas por el usuario.

El bloqueo de la configuración impide que los usuarios accedan a “about:config” y modifiquen la configuración de seguridad establecida por el administrador del sistema.

Comprobación:

Escribir “about:config” en la ventana del navegador y verificar que los valores colocados en el archivo “firefox.cfg” estén marcados como bloqueado.

Firefox actualiza automáticamente los add-ons y plugins.

Establecer este valor como “false” deshabilita cualquier comunicación a un servidor adicional para la búsqueda de nuevas versiones de complementos. Las actualizaciones automáticas desde sitios no confiables ponen en riesgo el navegador ante un atacante, pudiendo anular la configuración de seguridad.

Si se necesita la instalación de complementos en el navegador, se recomienda establecer el valor en “true” para evitar la pérdida de las últimas correcciones de seguridad de estos complementos. Se debe asegurar que la instalación de estos complementos y sus correcciones de seguridad se realizan desde fuentes fiables.

El valor “extensions.update.enabled” debe estar establecido en “false” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “extensions.update.enabled” esté configurado y bloqueado en “false”.

Firefox está configurado para actualizarse de forma automática.

Permitir actualizaciones de software de sitios que no son de confianza puede introducir valores que invaliden una instalación segura del navegador con el conocido riesgo.

Si esta opción está habilitada, "true", se deberán comprobar las configuraciones predeterminadas que contienen las direcciones URL definidas para las actualizaciones automáticas, y solo permitir las URL por defecto.

Si los valores de "app.update.url", "app.update.url.details" y "app.update.url.manual" han sido modificados, se deberán restaurar a sus valores por defecto.

Con el valor "app.update.enabled" establecido como "true", en el archivo "firefox.cfg", hay que realizar los pasos indicados en comprobación.

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "app.update.enabled" esté configurado y bloqueado en la opción "true".

Verificar que los valores de referencia "app.update.url", "app.update.url.details" y "app.update.url.manual" contienen una url que apunta a un servidor interno de confianza o a la configuración predeterminada de "Mozilla.com" o "Mozilla.org".

Nota: Para deshabilitar las actualizaciones a través de internet, establecer estos valores como se indica a continuación, en el archivo "firefox.cfg":

```
lockPref("app.update.enabled", false);
lockPref("app.update.url", "");
```

Firefox comprueba automáticamente la versión actualizada de los plugins de búsqueda instalados.

Las actualizaciones se deben controlar e instalar desde servidores autorizados y de confianza. Esta configuración invalida otras configuraciones que pueden dirigir la aplicación para tener acceso a direcciones URL externas.

El valor "browser.search.update" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "browser.search.update" esté configurado y bloqueado en "false".

Firefox está configurado para preguntar qué certificado presentar a un sitio web cuando se requiere un certificado.

Cuando un sitio web solicita un certificado para la autenticación de usuario, Firefox debe configurarse para que el usuario elija qué certificado presentar. Se denegará el acceso al usuario si no se configura la administración de certificados.

El valor "security.default_personal_cert" debe estar establecido en "Ask Every Time" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "security.default_personal_cert" esté configurado y bloqueado en "Ask Every Time".

El envío de información en segundo plano a Mozilla debe estar deshabilitado.

No se debe enviar información técnica ni de otro tipo desde nuestro sistema a Mozilla.

El valor "datareporting.policy.dataSubmissionEnabled" debe estar establecido en "false" en el archivo "firefox.cfg".

El valor "datareporting.healthreport.service.enabled" debe estar establecido en "false" en el archivo "firefox.cfg".

El valor "datareporting.healthreport.uploadEnabled" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about: config" en la ventana del navegador. Verificar que los nombres de preferencia "datareporting.policy.dataSubmissionEnabled", "datareporting.healthreport.service.enabled" y "datareporting.healthreport.uploadEnabled" estén configurados y bloqueados en "false".

La instalación de extensiones debe estar deshabilitada.

La instalación de extensiones debe estar deshabilitada. Una extensión de navegador es un programa que se instala en el navegador que le agrega nuevas funcionalidades. Un complemento interactúa con una página web y, por lo general, con una aplicación externa de terceros (Flash, Adobe Reader), una extensión interactúa con el propio navegador.

Las extensiones no están incrustadas en las páginas web y se deben descargar e instalar para que funcionen. Las extensiones permiten a los navegadores evitar restricciones que se aplican a las páginas web.

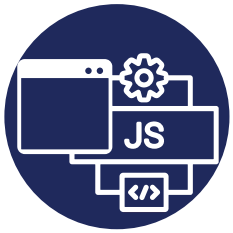
Si un navegador está configurado para permitir el uso sin restricciones de la extensión, los complementos pueden cargarse e instalarse desde fuentes maliciosas y utilizarse en el navegador.

El valor “xpinstall.enabled” debe estar establecido en “false” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about: config” en la ventana del navegador. Verificar que el nombre de preferencia “xpinstall.enabled” esté configurado y bloqueado en “false”.

Firefox está configurado para permitir que JavaScript suba (traer al frente) o baje (enviar al fondo) ventanas.



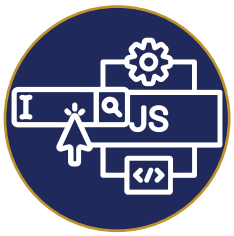
JavaScript puede realizar cambios en la apariencia del navegador. Permitir que un sitio web use JavaScript para traer al frente y/o enviar al fondo las ventanas del navegador, puede ocultar un ataque. Las ventanas del navegador no pueden configurarse como activas a través de JavaScript.

El valor “dom.disable_window_flip” debe estar establecido en “true” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “dom.disable_window_flip” esté configurado y bloqueado en “true”.

Firefox está configurado para permitir que JavaScript cambie el texto de la barra de estado.



JavaScript puede hacer cambios en la apariencia del navegador. Esta acción puede ayudar a ocultar un ataque que tenga lugar en una ventana minimizada. Los autores de páginas web pueden deshabilitar muchas funciones relativas a la apertura de una ventana emergente.

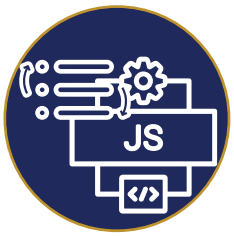
Si se establece esta preferencia como "true", anulará la configuración del autor de la web y garantiza que la barra de estado esté habilitada y presente en cualquier ventana emergente. Esta configuración evita que se oculte la barra de estado en cualquier ventana del navegador.

El valor "dom.disable_window_open_feature.status" debe estar establecido en "true" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "dom.disable_window_open_feature.status" esté configurado y bloqueado en "true".

Firefox está configurado para permitir que JavaScript deshabilite o reemplace los menús contextuales.



Un menú contextual (también conocido como menú emergente) a menudo se utiliza en una interfaz gráfica de usuario (GUI). Este menú aparece tras la interacción del usuario (por ejemplo, un clic derecho del ratón). Un menú contextual ofrece un conjunto limitado de opciones disponibles en el estado actual o contexto del sistema operativo o aplicación.

Un sitio web puede ejecutar JavaScript para realizar cambios en estos menús contextuales, pudiendo así ayudar a ocultar un ataque. Se debe establecer esta preferencia en "false" para que las páginas web no puedan hacer cambios en el menú contextual.

El valor "dom.event.contextmenu.enabled" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "dom.event.contextmenu.enabled" esté configurado y bloqueado en "false".

Firefox no está configurado para mostrar a un usuario, un mensaje de solicitud, antes de descargar y abrir los distintos tipos de archivos.

No se pueden agregar nuevos tipos de archivos directamente a la lista de complementos o aplicaciones auxiliares. Los archivos con estas extensiones no podrán usar Firefox directamente, sino que se utilizarán aplicaciones externas para abrir los archivos.

Las aplicaciones externas se configuran después de que se haya establecido una acción de descarga de un tipo de fichero no almacenado en el navegador. En este momento, se selecciona la acción a realizar, asignación de aplicación externa para la apertura del fichero o la opción de guardar el fichero a descargar. Una vez se selecciona la opción, y siempre que se marque la opción de Hacer esto automáticamente para archivos como este a partir de ahora, esta se realizará automáticamente para futuras descargas del mismo tipo de fichero.

Esta acción genera una entrada para ese tipo de archivo en la lista de complementos y así permitirá que este tipo de archivo se abra automáticamente en el futuro.

Esta configuración puede ser un problema de seguridad. Los nuevos tipos de archivos no se deben de poder agregar directamente a la lista de complementos de la aplicación para evitar posibles usos malintencionados.

El valor “plugin.disable_full_page_plugin_for_types” debe estar establecido en “true” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “plugin.disable_full_page_plugin_for_types” esté configurado y bloqueado en “true”.

Firefox tiene instalado el plug-in para controles ActiveX.

Cuando se hace referencia a un control ActiveX en un documento HTML, MS Windows verifica si el control ya reside en la máquina del cliente. De lo contrario, el control se puede descargar desde un sitio web remoto. Esto proporciona un método de entrega automatizado para el código móvil.

El control ActiveX y el soporte de complementos, no deben estar presentes ni habilitados

Comprobación:

Escribir “about:plugins” en la ventana del navegador. Verificar que no hay plug-in de ActiveX. En caso contrario eliminar o desinstalar.

El protocolo de shell de red está habilitado en Firefox.

Aunque las versiones actuales de Firefox tienen este valor deshabilitado de forma predeterminada, el uso de esta opción puede suponer un peligro. Esto permitiría al navegador acceder a la shell de Windows.

El valor "network.protocol-handler.external.shell" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "network.protocol-handler.external.shell" esté configurado y bloqueado en "false".

Firefox no está configurado para proporcionar advertencias cuando un usuario cambia de una página segura (habilitada para SSL) a una página no segura.

Es posible que los usuarios no sepan que están cambiando de una página segura anterior a una página insegura actual.

El valor “security.warn_leaving_secure” debe estar establecido en “true” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “security.warn_leaving_secure” esté configurado y bloqueado en “true”.

Firefox no está configurado para bloquear ventanas emergentes.

Las ventanas emergentes se pueden usar para lanzar un ataque dentro de una nueva ventana del navegador con configuraciones alteradas. Esta configuración bloquea las ventanas emergentes creadas mientras se carga la página.

El valor "dom.disable_window_open_feature.status" debe estar establecido en "true" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "dom.disable_window_open_feature.status" esté configurado y bloqueado en "true".

Firefox está configurado para permitir que JavaScript mueva o cambie el tamaño de las ventanas.

JavaScript puede realizar cambios en la apariencia del navegador. Esta actividad puede ayudar a ocultar un ataque que tiene lugar en una ventana de fondo minimizada. Se debe establecer la configuración del navegador para evitar que las secuencias de comandos en los sitios web visitados muevan y cambien el tamaño de las ventanas del navegador.

El valor “dom.disable_window_flip” debe estar establecido en “true” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “dom.disable_window_flip” esté configurado y bloqueado en “true”.

Firefox debe estar configurado para permitir solo TLS.

El uso de protocolos seguros con versiones anteriores a TLS 1.1 pone en riesgo la seguridad. Los antiguos SSL 2.0, SSL 3.0 y TLS 1.0 contienen una serie de fallos de seguridad que pueden poner en riesgo el navegador. Se deben deshabilitar estos protocolos en función de las necesidades de la infraestructura de red.

Se recomienda establecer "security.tls.version.min" con el valor "2" para el uso del protocolo TSL 1.1 como valor mínimo.

Se recomienda establecer "security.tls.version.max" con el valor "3" para el uso del protocolo TLS 1.2 como valor máximo.

Estos valores deben aparecer en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador y verificar los siguientes nombres de preferencia:

- "security.tls.version.min" configurado como "2".
- "security.tls.version.max" configurado como "3".

Firefox ejecuta o descarga automáticamente tipos MIME que no están autorizados para la descarga automática.

La acción predeterminada, para los tipos de archivo para los que está instalado un complemento, es descargar y ejecutar automáticamente el archivo utilizando el complemento asociado. Firefox permite cambiar la acción de descarga especificada para que el archivo se abra con una aplicación externa seleccionada o se guarde en disco.

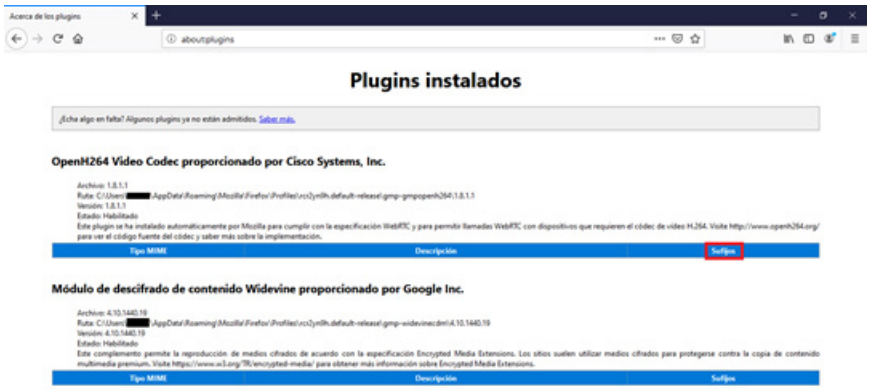
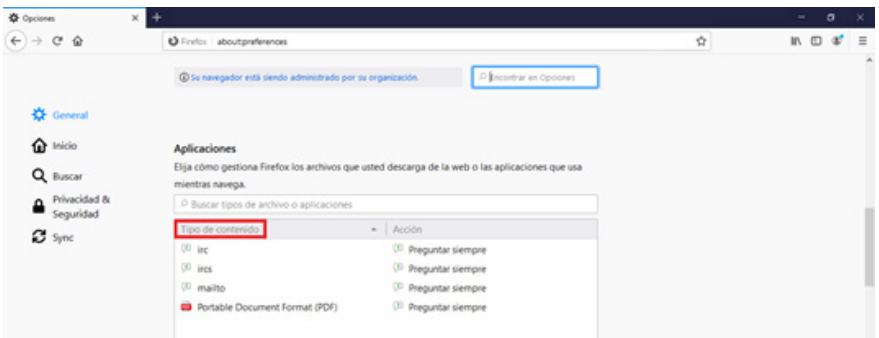
Vea la lista de plugins de navegador instalados y tipos MIME relacionados introduciendo "about:plugins" en la barra de direcciones. Al hacer clic en un vínculo para descargar un archivo, el tipo MIME determina qué acción tomará Firefox.

Es posible que ya tenga un plugin instalado que manejará automáticamente la descarga, como Windows Media Player o QuickTime. Otras veces, es posible que vea un cuadro de diálogo que le pregunta si desea guardar el archivo o abrirlo con una aplicación específica.

Cuando se indica que en Firefox abra o guarde el archivo y también marque la opción "Hacer esto automáticamente para archivos como este a partir de ahora", aparece una entrada para ese tipo de archivo en el panel Aplicaciones de Firefox.

Comprobación:

Utilice la Opción A o B para comprobar si las siguientes extensiones aparecen en la configuración del navegador: HTA, JSE, JS, MOCHA, SHS, VBE, VBS, SCT, WSC. De forma predeterminada, la mayoría de estas extensiones no aparecerán en la lista de Firefox.

Opción	Descripción
A.	En “about:plugins”, Installed plug-in, se debe inspeccionar las entradas en la columna Sufijos. En esta columna no se deben encontrar las extensiones mencionadas. Si se encuentra alguna, se debe comprobar que no está asociada a una aplicación que ejecuta código. Hay aplicaciones como Notepad.exe, que no ejecutan código, pero pueden estar asociadas con las extensiones mencionadas. Eliminar cualquier extensión no autorizada de la lista. 
B.	Haga *clic* en el botón menú ☰, haga *clic* en “Opciones” y se buscan las extensiones mencionadas en la columna “Tipo de contenido” dentro de “Aplicaciones”. Se recomienda que las extensiones mencionadas, muestren en la columna “Acción” las opciones “Guardar archivo” o “Preguntar siempre”. Otra opción es que esté asociada a una aplicación que no ejecuta código (por ejemplo, el Bloc de notas). Si se encuentra alguna de las extensiones antes mencionadas, en la columna “Acción” está asociada a una aplicación que puede ejecutar el código, entonces se recomienda eliminar esta misma de la lista. 

Firefox no está configurado para usar el almacén de certificados de Windows

A partir de Firefox 49, se ha incluido una nueva opción que permite a Firefox confiar en las autoridades raíz en el almacén de certificados de Windows. Esto significa que los certificados se pueden implementar a través de la política de grupo de forma normal y Firefox confiará en las mismas autoridades raíz en las que confía Internet Explorer.

Esta función está desactivada de forma predeterminada.

Para habilitar esta configuración, debe crear una nueva entrada, con el valor "security.enterprise_roots.enabled" establecida en "true", en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "security.enterprise_roots.enabled" esté configurado y bloqueado en la opción establecida.

Firefox está configurado para permitir la función de autocompletar.

Para proteger nuestra información, Firefox ofrece la capacidad de configurarse de modo que los datos ingresados en los formularios no se guarden. Esto mitiga el riesgo de que un sitio web obtenga información privada a partir de esta información guardada.

El valor “browser.formfill.enable” debe estar establecido en “false” en el archivo “firefox.cfg”.

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que el nombre de preferencia “browser.formfill.enable” esté configurado y bloqueado en “false”.

Firefox está configurado para mostrar nuestra IP real mientras se navega

Desactivar el protocolo WebRTC (Web Real-Time Communication) permite mejorar notablemente la privacidad. Este protocolo esconde varios problemas de privacidad bastante graves, problemas que pueden omitir, por ejemplo, filtrar la dirección IP real cuando se está navegando a través de una VPN.

Sin embargo, desactivar este protocolo puede hacer que algunas aplicaciones y herramientas web que dependen de él dejen de funcionar. Aplicaciones como WhatsApp Web dejarían de funcionar.

Existen webs que muestran si el navegador está filtrando información personal a través de este protocolo.

- https://ipleak.net/
- https://browserleaks.com/

El valor "media.peerconnection.enabled" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "media.peerconnection.enabled" esté configurado y bloqueado en "false".

Eliminar los archivos generados durante la navegación al cerrar el navegador.

Se deben definir algunas configuraciones para que cuando se acabe la navegación y se proceda al cierre del navegador se eliminen los ficheros generados por el navegador durante su funcionamiento.

Esto favorece la carga, la próxima vez que se visite el sitio, de las últimas versiones de las páginas visitadas, así como la configuración para el sitio web mejorando así la seguridad general de la navegación.

Para realizar esta operación se deberá definir en el fichero de configuración las siguientes propiedades:

- privacy.sanitize.sanitizeOnShutdown
- privacy.clearOnShutdown.cache
- privacy.clearOnShutdown.cookies
- privacy.clearOnShutdown.downloads
- privacy.clearOnShutdown.formdata
- privacy.clearOnShutdown.history
- privacy.clearOnShutdown.offlineApps
- privacy.clearOnShutdown.openWindows
- privacy.clearOnShutdown.sessions
- privacy.clearOnShutdown.siteSettingsite

En las organizaciones que se deba conservar el historial de navegación se deberá definir la preferencia “privacy.clearOnShutdown.history” para permitir el recuerdo del historial de navegación, colocando el valor en “false” para que el historial no sea eliminado al cerrar el navegador.

5.6 Valores de las directivas

Comprobación:

Escribir “about:config” en la ventana del navegador. Verificar que los siguientes nombres de preferencias están configurados y bloqueados en “true”:

- privacy.sanitize.sanitizeOnShutdown
- privacy.clearOnShutdown.cache
- privacy.clearOnShutdown.cookies
- privacy.clearOnShutdown.downloads
- privacy.clearOnShutdown.formdata
- privacy.clearOnShutdown.history
- privacy.clearOnShutdown.offlineApps
- privacy.clearOnShutdown.openWindows
- privacy.clearOnShutdown.sessions
- privacy.clearOnShutdown.siteSettingsite

Desactivar la función de sincronización de la cuenta de Firefox.

Firefox Account anteriormente conocido como Firefox Sync es una función incorporada del navegador que permite a los usuarios sincronizar automáticamente varios elementos como marcadores, pestañas abiertas, contraseñas y complementos.

Si no deseamos utilizar la sincronización e instalación de todo lo que esté configurado en una cuenta de Firefox y así evitar problemas de privacidad y seguridad, se debe deshabilitar esta función del navegador.

El valor " identity.fxaccounts.enabled" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about: config" en la ventana del navegador. Verificar que el nombre de preferencia "identity.fxaccounts.enabled" esté configurado y bloqueado en "false".

Deshabilitar Pocket en Firefox

Pocket es una funcionalidad que permite a los usuarios guardar cualquier tipo de contenido web para poder visualizarlo posteriormente.

En las organizaciones que prefieran habilitar la funcionalidad Pocket se deberá definir la preferencia "extensions.pocket.enabled" con el valor "true"

El valor "extensions.pocket.enabled" debe estar establecido en "false" en el archivo "firefox.cfg".

Comprobación:

Escribir "about:config" en la ventana del navegador. Verificar que el nombre de preferencia "extensions.pocket.enabled" esté configurado y bloqueado en "false".

6. Lista de comprobación (assessment)

Criticidad	Descripción
Alta	Mozilla Firefox actualiza automáticamente los add-ons y plugins
Alta	Mozilla Firefox está configurado para actualizarse de forma automática
Media	Mozilla Firefox comprueba automáticamente la versión actualizada de los plugins de búsqueda instalados
Media	Mozilla Firefox está configurado para preguntar qué certificado presentar a un sitio web cuando se requiere un certificado
Media	El envío de información de fondo a Mozilla Firefox debe estar desactivado
Media	La instalación de extensiones debe estar deshabilitada
Media	Mozilla Firefox está configurado para permitir que JavaScript suba (traer al frente) o baje (enviar al fondo) ventanas.
Media	Mozilla Firefox está configurado para permitir que JavaScript cambie el texto de la barra de estado.
Media	Mozilla Firefox está configurado para permitir que JavaScript deshabilite o reemplace los menús contextuales.
Media	Mozilla Firefox no está configurado para mostrar a un usuario, un mensaje de solicitud, antes de descargar y abrir los distintos tipos de archivos
Media	Mozilla Firefox tiene instalado el plug-in para controles ActiveX
Media	El protocolo de shell de red está habilitado en Mozilla Firefox
Media	Mozilla Firefox no está configurado para proporcionar advertencias cuando un usuario cambia de una página segura (habilitada para SSL) a una página no segura

6. Lista de comprobación (assessment)

Criticidad	Descripción
Media	Mozilla Firefox no está configurado para bloquear ventanas emergentes
Media	Mozilla Firefox está configurado para permitir que JavaScript mueva o cambie el tamaño de las ventanas
Media	Mozilla Firefox debe estar configurado para permitir solo TLS
Media	Mozilla Firefox ejecuta o descarga automáticamente tipos MIME que no están autorizados para la descarga automática.
Media	Mozilla Firefox no está configurado para usar el almacén de certificados de Windows
Media	Mozilla Firefox está configurado para permitir la función de autocompletar.
Media	Mozilla Firefox está configurado para mostrar nuestra ip real mientras se navega.

7. Decálogo de recomendaciones

A continuación, se indican diez (10) recomendaciones de seguridad para *Mozilla Firefox*

Decálogo de seguridad para Mozilla Firefox

1. Utilizar siempre la versión más actualizada de Mozilla Firefox.
2. En caso de instalar complementos, se recomienda comprobar que se realiza desde fuentes confiables.
3. Se aconseja revisar cualquier función relativa a la seguridad del software, puesto que proporciona una mayor defensa contra los ataques.
4. Se recomienda no almacenar contraseñas de forma predeterminada y en su lugar utilizar otras aplicaciones que implementen un sistema de cifrado robusto, para guardar, de forma segura, nuestras contraseñas.
5. Se recomienda observar el botón de identidad del sitio (un candado que se encuentra en la barra de direcciones, a la izquierda de la barra de direcciones) para descubrir de forma rápida y sencilla si la conexión a la página está encriptada y, en algunos casos, quién es el propietario. Esta información ayuda a la detección de páginas maliciosas.
6. Se recomienda utilizar siempre https, sobre todo cuando se utilicen datos personales para asegurar las comunicaciones de extremo a extremo.
7. Se recomienda el uso de software PGP para enviar información personal cifrada, como medida de seguridad adicional, incluso si se utilizan protocolos seguros como https.
8. Se recomienda el uso de la autenticación de doble factor cuando se utilicen servicios online. Al configurar el servicio para que envíe al móvil un código PIN. Esto añade una capa adicional de seguridad a las cuentas.
9. Se recomienda borrar las cookies para evitar que algunos sitios web rastreen patrones de búsqueda y así salvaguardar nuestra privacidad.
10. Se recomienda Limpiar la caché y eliminar los archivos temporales de Internet para solucionar problemas habituales con los sitios web.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Anexo A. Archivo de configuración de seguridad

Para facilitar la aplicación del refuerzo de seguridad sobre Mozilla Firefox, se incluyen al presente documento una carpeta la cual contiene los archivos necesarios para mantener la información segura en un equipo.

A continuación, se detallan los archivos incluidos en la carpeta **"Scripts".**

- autoconfig.js
- firefox.cfg

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es