CCN-CERT

BP/17

Security recommendations of Mozilla Firefox

GOOD PRACTICE REPORT

MAY **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Release date: May 2020

LIMITATION OF RESPONSABILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

Without written authorisation from the National Cryptologic Centre, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or distribute copies of it by means of rental or public lending.

Index

1. About CCN-CERT, National Governmental CERT

The **CCN-CER**T is the Information Security Incident Response Capacity of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are included in the Law 11/2002 regulating the CNI, the RD 421/2004 regulating the CCN and in the RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by the RD 951/2015 of 23 October.

Its mission, therefore, is **to contribute to the improvement of Spanish cybersecurity,** being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively face cyber-threats, including the coordination at state public level of the different existing Incident Response Capabilities or Cybersecurity Operations Centres.

All of this, with the **ultimate aim of achieving a safer and more reliable cyberspace,** preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Legal Regime of the Public Sector, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incident management will be carried out by the CCN-CERT in coordination with the CNPIC.

CCN-CERT is the Information Security Incident Response Capability of the National Cryptologic Centre.

2. Introduction

This document is part of the documentation issued by the National Cryptologic Centre whose objective is to preserve the security of the ICT systems of Public Administrations.

For this purpose, a configuration file is provided to implement security measures on a web browser *software* to facilitate the possibility of implementing security in ICT systems.

For the development of this guide we have used the *Mozilla Firefox* installer in its version 72.0.1 (64bit) for *Windows OS*.

The development of this guide has been done using the Mozilla Firefox installer in its version 72.0.1 (64bit) for Windows OS.

3. Objet

The purpose of this document is to set out the procedures and utilities needed to implement and ensure security in *Mozilla Firefox*.

4. Scope

This document sets out a procedure for improving security and securing *Mozilla Firefox* to mitigate potential vulnerabilities and risks to which it may be exposed.

The users of this guide can improve the security of this application through the configuration files included in its annex.

5. Mozilla Firefox download, installation and configuration

Mozilla Firefox is available for free download from the Mozilla website.

Mozilla Firefox must have the latest security-related *software* updates installed. To do this, determine the update method (e.g. connection to a *WSUS* server, local procedure, automatic update, etc.).

If the latest *Firefox* security-related software updates are not applied, this would be a critical security fault.

Download the browser at: https://www.mozilla.org/en-US/firefox/new/

5.1 Realeses

The Mozilla Firefox desktop software is available for deployment with both the “fast” and the “ESR” versions.

Fast realease: Receives major updates every six weeks and minor updates, such as bug fixes and security fixes, as needed during those six weeks.

Extended Support Release (ESR): On average, it receives major updates every 42 weeks and minor updates, such as bug fixes, security fixes and policy updates, as needed, but at least every six weeks.

In addition to the different update cycles, the ESR currently has access to additional policies that are not available in the fast release.

5.1 Realeses

- Integrated authentication (SPNEGO and NTLM).
- Disable application updates.
- Disable system add-on updates.
- Manage extensions.
- Change the home page.
- Change the Firstrun page.
- Change the update page.
- Show the search bar.
- Change of search engines.
- Filtering of websites.

5.1 Realeses

To find out which version of Firefox you are using:

Paso	Descripción
1.	Click on the menu button ☰ , click on “Help” and select “About Firefox”. Then, the “About Firefox” window will appear. The release number of the installed release will be displayed below the Firefox name, as shown in the image below:
2.	
3.	Alternatively, to see which browser version is installed, you can click on the menu button ☰, *click* on “Help” and select “Troubleshooting information”. This will open a page with the address “about:support” in a new tab. The Firefox version is listed under the **Basic Settings** section **of the application.**

5.2 Minimum requirements

The following are the minimum system requirements necessary to implement Mozilla Firefox on Windows.

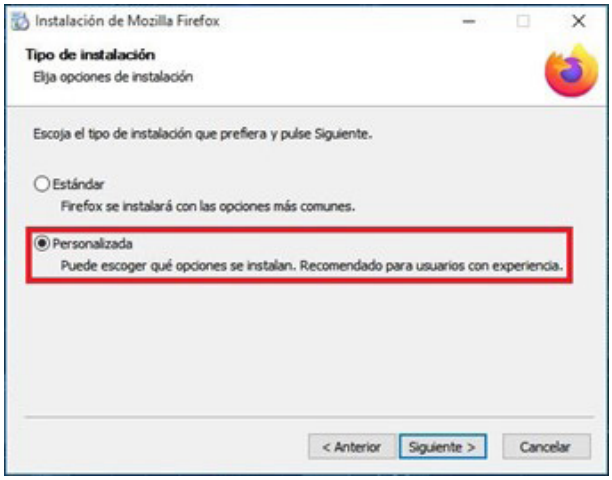
- **Operating System (32-bit and 64-bit)**
  - Windows 7
  - Windows 8
  - Windows 10
- **Recommended hardware**
  - Pentium 4 or a more modern processor supporting SSE2.
  - 512MB RAM / 2GB RAM for the 64-bit version.
  - 200MB of available hard disk space.

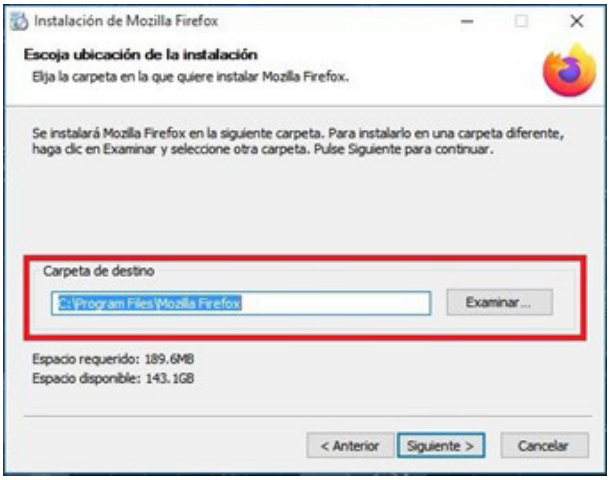
5.3 Location of the installation

The installation paths for *Mozilla Firefox* on a *Windows OS* are described below:

- C:\Program Files Mozilla Firefox is the default installation path for both the 32-bit version (installed on a 32-bit operating system) and the 64-bit version (installed on a 64-bit operating system).
- C:\Program Files(x86)\Mozilla Firefox is the default installation path when installing the 32-bit browser on a 64-bit operating system.

Note: It is possible to customise the path where the programme is installed during the installation process.



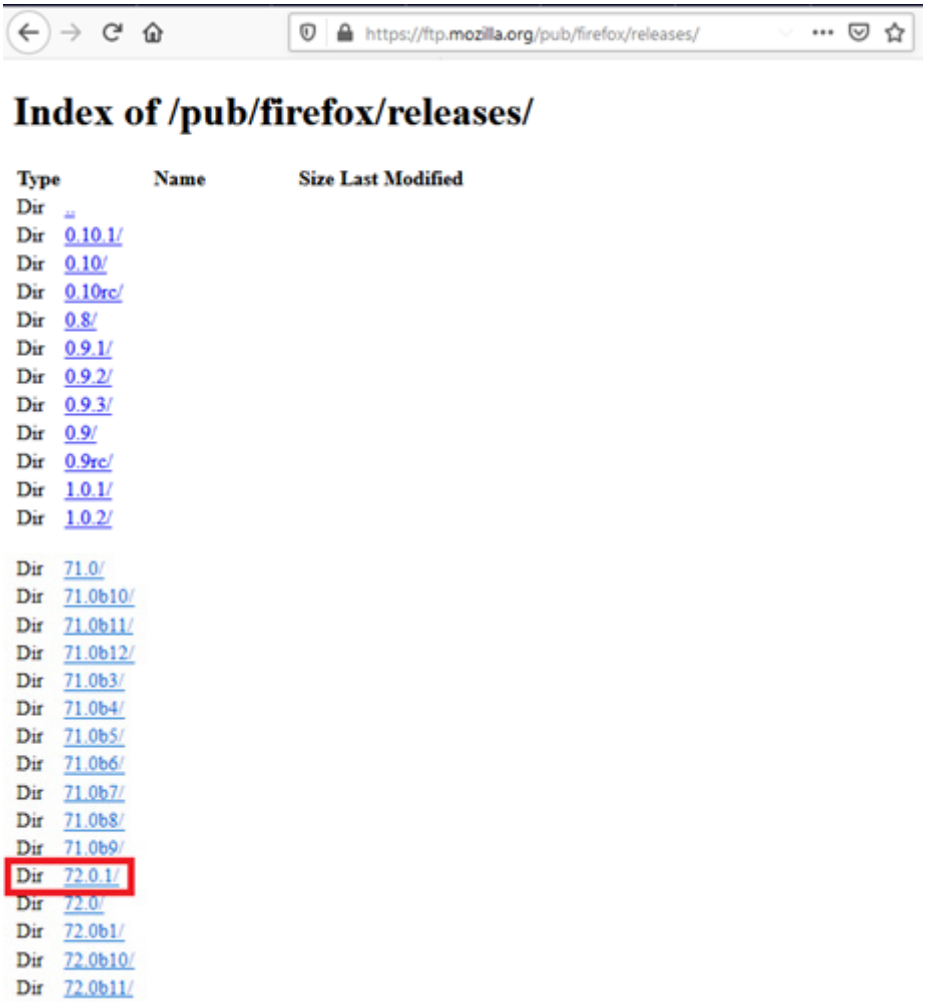


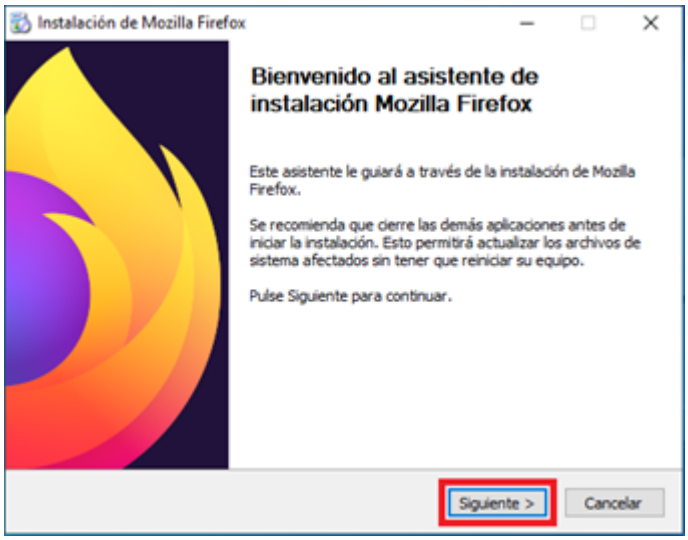
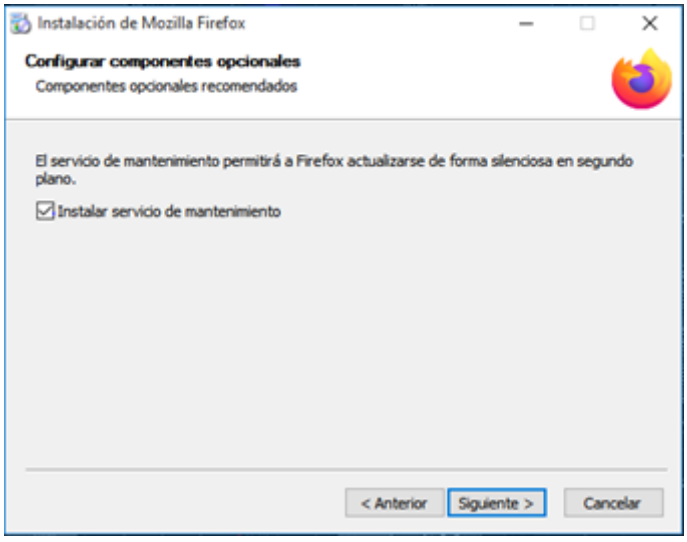
5.4 Mozilla Firefox download and installation

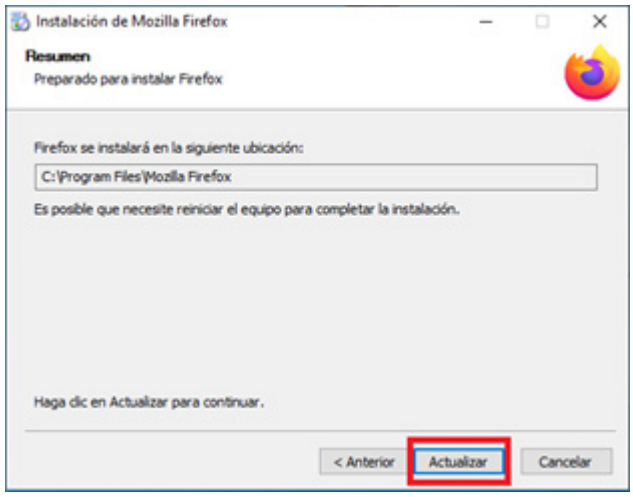
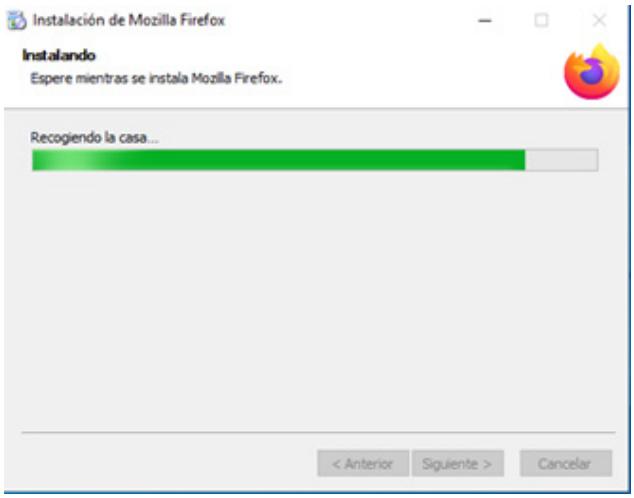
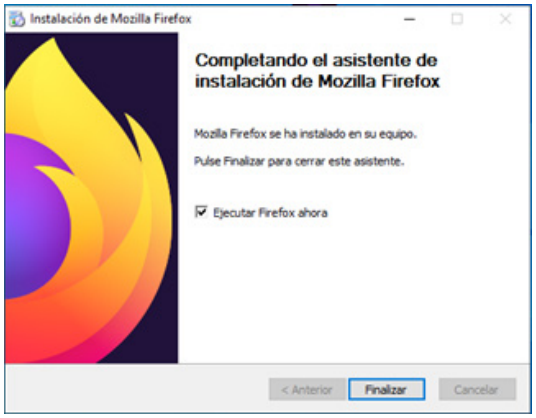
The programme can be downloaded from the following url:

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

Steps	Description
1.	In this window you select the browser to download, the operating system on which this download will be installed and finally you select the language. Then click on the "Download now" button to start downloading the programme. This would be an example for a download of the latest version of the Firefox browser for Windows 64-bit.  **Note: Firefox Enterprise offers MSI installers to help system administrators customize and deploy Firefox in their environments through standard Windows deployment tools, such as applying GPOs in Active Directory or through Microsoft System Center Configuration Manager.** **https://support.mozilla.org/es/kb/personalizacion-de-firefox-con-instaladores-msi#w_msi-installers** An alternative method of downloading the browser is via FTP, at the following URL: **https://ftp.mozilla.org/pub/firefox/releases/**

Steps	Description
2.	The following window will be used as an example for downloading Mozilla Firefox release 72.0.1.  The installation file obtained from the download will be used to install or update the version of Mozilla Firefox on the system where the security and privacy settings are made. To start the installation of the browser, *double-click* on the downloaded file. **Note: To install the program, it is necessary to install it with a user with administrative privileges on the computer where you are installing Firefox.**

Steps	Description
3.	 Then, the browser is installed as shown in the image above. Mozilla Firefox installs by default an optional service called "maintenance service", which allows updates in the background, without having to click OK in the Windows User Account Control dialog. This option can be unchecked when performing the custom installation.  If a reinstallation of Firefox is performed over an existing version, an "Upgrade" button will appear instead of the "Install" button, as shown in the following image:

Steps	Description
3.	 Once the above steps have been completed, click on the install or update button and wait until the process has finished.   Once the installation is complete, the system is restarted and the browser can be used.

5.5 Apply security and privacy settings

The following describes how to add security settings to *Firefox* to keep our information secure.

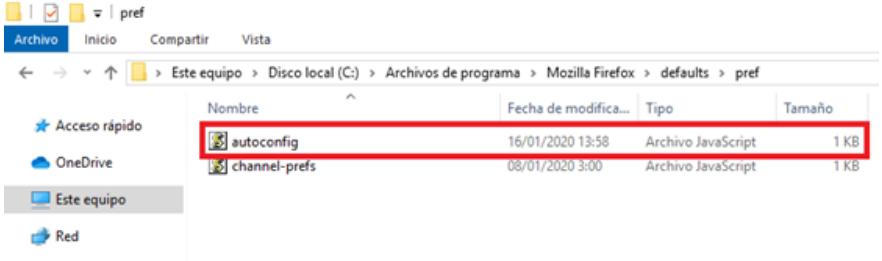
Automatic configuration files can be used to set and lock preferences that are not covered by *Firefox* policies.

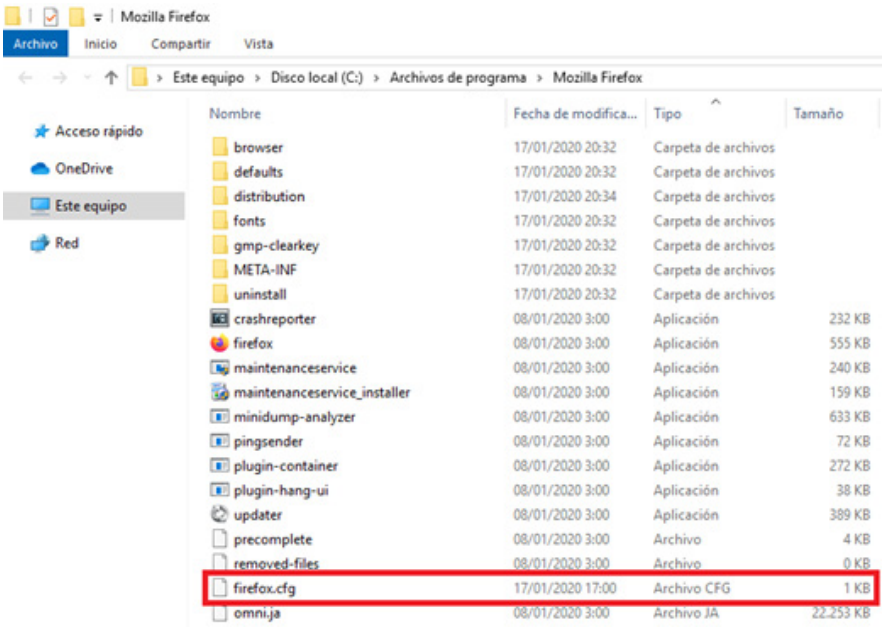
To use the automatic configuration, two files must be placed in the *Firefox* directories.

If the operating system is **Microsoft Windows**, these files will be located in the *Firefox* installation directory.

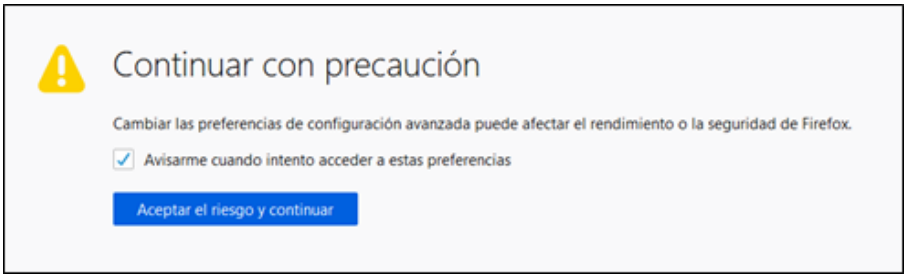
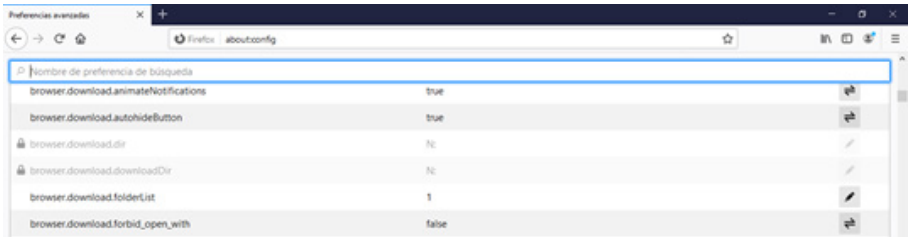
The file **"autoconfig.js"** is located in the directory "/Mozilla Firefox /defaults/pref".

The file **"firefox.cfg"** is located in the firefox installation directory ("/Mozilla Firefox").

Steps	Description
1.	The default installation path is used for a 64-bit Mozilla Firefox installation: The file *"autoconfig.js"* is located in the directory C:\Program Files\Mozilla Firefox\ defaults\pref\. 

Steps	Description
2.	The file "*firefox.cfg*" is located in the directory C: \Program Files\Mozilla Firefox\.  **Note: The configuration files "*autoconfig*.js" and "*firefox.cfg*" are located in the "Scripts" folder of this Good Practices Guide.**

5.6 Values of the directives

Steps	Description
1.	The security modifications implemented by incorporating the "*autoconfig.js*" and "*firefox.cfg*" files in the security hardening process set out in section "5.5 Apply configuration of " are detailed below. In the configuration editor (the *about:config* page) you will find a list of *advanced* Firefox *preferences* to check the values placed in the "*firefox.cfg*" file. To access the advanced preferences, type **about:config** and press Enter in the **address bar.** When you do this, a warning page appears with a notice that modifying these advanced settings may affect the performance or security of Firefox. To continue, **click** on **Accept the risks and continue.** 
2.	At the top of the about:config page, you can use the Search field for quick retrieval of specific preferences. 

Firefox is configured to use a password store with or without a master password.

Firefox can be configured to store passwords for sites visited by the user. These individual passwords are stored in a file and can be protected with a master password.

Password autofill can be enabled when visiting the website. This feature could also be used to autofill a certificate pin, which could compromise information.

The value "**signon.rememberSignons**" must be set to "false" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "signon.rememberSignons" is set and locked to "false".

The form-filling assistance option in Firefox is disabled.

In order to protect privacy and sensitive data, Firefox offers the possibility to configure the programme so that data entered in forms is not saved. This setting mitigates the risk that a web page can obtain previously entered private information.

The value "**browser.formfill.enable**" must be set to "false" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "browser.formfill.enable" is set and locked to "false".

Firefox is configured to auto-complete passwords.

Because of the way credentials are stored it is possible for an attacker to gain access to user accounts.

The value **"signon. autofillForms"** must be set to "false" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "signon. autofillForms" is set and locked to "false".

The security preferences required by Firefox cannot be changed by the user.

Locking the configuration prevents users from accessing “about:config” and modifying the security settings set by the system administrator.

Check:

Type “about:config” in the browser window and verify that the values placed in the “firefox.cfg” file are marked as locked.

Firefox automatically updates add-ons and plugins.

Setting this value to “false” disables any communication to an additional server to check for new add-on versions. Automatic updates from untrusted sites put the browser at risk to an attacker and may override security settings.

If installation of browser add-ons is required, it is recommended to set the value to “true” to avoid losing the latest security fixes for these add-ons. It should be ensured that the installation of these add-ons and their security fixes are from trusted sources.

The value “extensions.update.enabled” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “extensions.update.enabled” is set and locked to “false”.

Firefox is configured to update itself automatically.

Allowing software updates from untrusted sites may introduce values that invalidate a secure browser installation with the known risk.

If this option is enabled, "true", check the default settings containing the URLs defined for automatic updates, and only allow the default URLs.

If the values of "app.update.url", "app.update.url.details" and "app.update.url.manual" have been modified, they shall be restored to their default values.

With the value "app.update.enabled" set to "true", in the "firefox.cfg" file, you have to perform the steps indicated in check.

Check:

Type "about:config" in the browser window. Verify that the preference name "app.update.enabled" is set and locked to "true".

Verify that the reference values "app.update.url", "app.update.url.details" and "app.update.url.manual" contain a url pointing to a trusted internal server or to the default "Mozilla.com" or "Mozilla.org" configuration.

Note: To disable updates over the internet, set these values as indicated below, in the "firefox.cfg" file:

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

Firefox automatically checks for the current version of installed search plugins.

Updates must be controlled and installed from authorised and trusted servers. This configuration overrides other configurations that may direct the application to access external URLs.

The value “browser.search.update” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “browser.search.update” is set and locked to “false”.

Firefox is configured to ask which certificate to present to a website when a certificate is required.

When a website requests a certificate for user authentication, Firefox must be configured to allow the user to choose which certificate to present. The user will be denied access if certificate management is not configured.

The value “security.default_personal_cert” must be set to “Ask Every Time” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “security.default_personal_cert” is set and locked to “Ask Every Time”.

Sending background information to Mozilla must be disabled.

No technical or other information should be sent from our system to Mozilla.

The value “datareporting.policy.dataSubmissionEnabled” must be set to “false” in the “firefox.cfg” file.

The value “datareporting.healthreport.service.enabled” must be set to “false” in the “firefox.cfg” file.

The value “datareporting.healthreport.uploadEnabled” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about: config” in the browser window. Verify that the preference names “datareporting.policy.dataSubmissionEnabled”, “datareporting.healthreport.service.enabled” and “datareporting.healthreport.uploadEnabled” are set and locked to “false”.

Installation of extensions must be disabled.

The installation of extensions must be disabled. A browser extension is a programme that is installed on the browser that adds new functionality to the browser. An add-on interacts with a web page and usually with an external third-party application (Flash, Adobe Reader), an extension interacts with the browser itself.

Extensions are not embedded in web pages and must be downloaded and installed to work. Extensions allow browsers to bypass restrictions that apply to web pages.

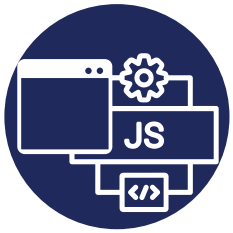
If a browser is configured to allow unrestricted use of the extension, add-ons can be loaded and installed from malicious sources and used in the browser.

The value "xpinstall.enabled" must be set to "false" in the "firefox.cfg" file.

Check:

Type "about: config" in the browser window. Verify that the preference name "xpinstall.enabled" is set and locked to "false".

Firefox is configured to allow JavaScript to bring up (bring to front) or bring down (send to back) windows.



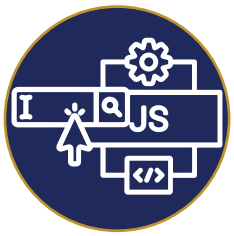
JavaScript can make changes to the appearance of the browser. Allowing a website to use JavaScript to bring browser windows to the front and/or send them to the back can hide an attack. Browser windows cannot be set as active via JavaScript.

The value “dom.disable_window_flip” must be set to “true” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “dom.disable_window_flip” is set and locked to “true”.

Firefox is configured to allow JavaScript to change the text in the status bar.



JavaScript can make changes to the appearance of the browser. This action can help hide an attack that takes place in a minimised window. Web page authors can disable many functions related to the opening of a pop-up window.

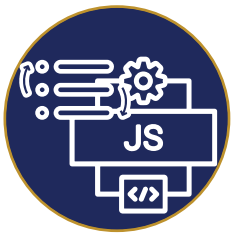
Setting this preference to “true” overrides the web author’s setting and ensures that the status bar is enabled and present in any pop-up window. This setting prevents the status bar from being hidden in any browser window.

The value “dom.disable_window_open_feature.status” must be set to “true” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “dom.disable_window_open_feature.status” is set and locked to “true”.

Firefox is configured to allow JavaScript to disable or override context menus.



A context menu (also known as a pop-up menu) is often used in a graphical user interface (GUI). This menu appears after user interaction (e.g. a right mouse click). A context menu offers a limited set of options available in the current state or context of the operating system or application.

A website can execute JavaScript to make changes to these context menus, which can help hide an attack. This preference should be set to "false" so that web pages cannot make changes to the context menu.

The value "dom.event.contextmenu.enabled" must be set to "false" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "dom.event.contextmenu.enabled" is set and locked to "false".

Firefox is not configured to display a prompt message to a user before downloading and opening different types of files.

New file types cannot be added directly to the list of add-ons or helper applications. Files with these extensions will not be able to use Firefox directly, but will use external applications to open the files.

External applications are configured after a download action of a file type not stored in the browser has been established. At this point, you select the action to perform, external application assignment to open the file or the option to save the file to download. Once the option is selected, and as long as the Do this automatically for files like this from now on option is checked, this will be done automatically for future downloads of the same file type.

This action generates an entry for that file type in the list of add-ons and thus will allow this file type to be opened automatically in the future.

This setting may be a security issue. New file types should not be able to be added directly to the add-on list of the application to avoid possible malicious use.

The value "plugin.disable_full_full_page_plugin_for_types" must be set to "true" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "plugin.disable_full_full_page_plugin_for_types" is set and locked to "true".

Firefox has the ActiveX controls plug-in installed.

When an ActiveX control is referenced in an HTML document, MS Windows checks if the control already resides on the client machine. If not, the control can be downloaded from a remote website. This provides an automated delivery method for mobile code.

ActiveX control and plug-in support must not be present or enabled.

Check:

Type “about:plugins” in the browser window. Check that there are no ActiveX plug-ins. If not, remove or uninstall.

The network shell protocol is enabled in Firefox.

Although current versions of Firefox have this setting disabled by default, using this option can be dangerous. This would allow the browser to access the Windows shell.

The value “network.protocol-handler.external.shell” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “network.protocol-handler.external.shell” is set and locked to “false”.

Firefox is not configured to provide warnings when a user switches from a secure (SSL-enabled) page to a non-secure page.

Users may not be aware that they are switching from a previous secure page to a current insecure page.

The value “security.warn_leaving_secure” must be set to “true” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “security.warn_leaving_secure” is set and locked to “true”.

Firefox is not configured to block pop-up windows.

Pop-ups can be used to launch an attack inside a new browser window with altered settings. This setting blocks pop-up windows created while the page is loading.

The value " dom.disable_window_open_feature.status" must be set to "true" in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "dom.disable_window_open_feature.status" is set and locked to "true".

Firefox is configured to allow JavaScript to move or resize windows.

JavaScript can make changes to the appearance of the browser. This activity can help hide an attack that takes place in a minimised background window. Browser settings should be set to prevent scripts on visited websites from moving and resizing browser windows.

The value “dom.disable_window_flip” must be set to “true” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “dom.disable_window_flip” is set and locked to “true”.

Firefox must be configured to allow TLS only.

The use of secure protocols with versions older than TLS 1.1 puts security at risk. The older SSL 2.0, SSL 3.0 and TLS 1.0 contain a number of security flaws that can put the browser at risk. These protocols should be disabled depending on the needs of the network infrastructure.

It is recommended to set "security.tls.version.min" with the value "2" for the use of TSL 1.1 protocol as the minimum value.

t is recommended to set "security.tls.version.max" with the value "3" for the use of the TLS 1.2 protocol as the maximum value.

These values should appear in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window and check the following preferred names:

- "security.tls.version.min" set to "2".
- "security.tls.version.max" set to "3".

Firefox automatically executes or downloads MIME types that are not allowed for automatic download.

The default action, for file types for which an add-on is installed, is to automatically download and execute the file using the associated add-on. Firefox allows you to change the specified download action so that the file is opened with a selected external application or saved to disk.

View the list of installed browser plugins and related MIME types by entering “about:plugins” in the address bar. When you click on a link to download a file, the MIME type determines what action Firefox will take.

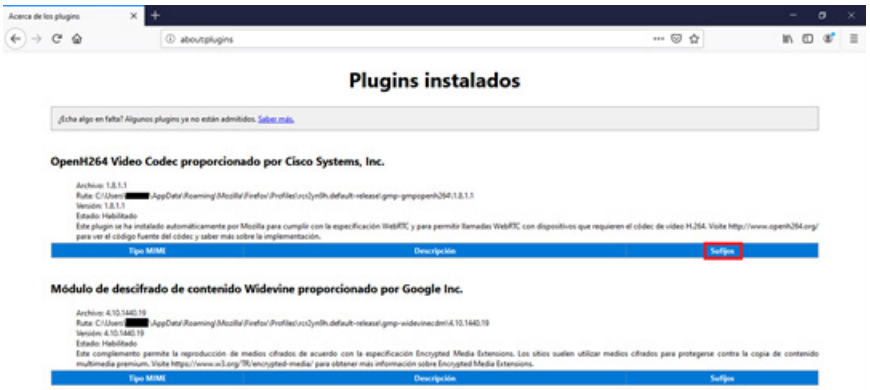
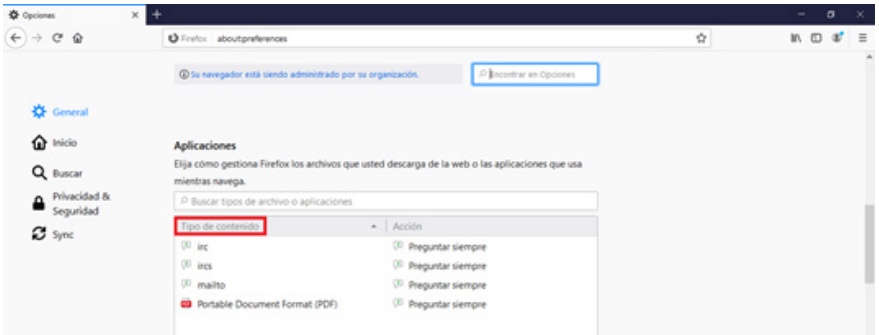
You may already have a plug-in installed that will automatically handle the download, such as Windows Media Player or QuickTime. Other times, you may see a dialog box asking if you want to save the file or open it with a specific application.

When you tell Firefox to open or save the file and also check the option “Do this automatically for files like this from now on”, an entry for that file type appears in the Firefox Applications pane.

Check:

Use Option A or B to check if the following extensions appear in the browser settings: HTA, JSE, JS, MOCHA, SHS, VBE, VBS, SCT, WSC. By default, most of these extensions will not appear in the Firefox list.

5.6 Values of the directives

Option	Description
A.	Under “about:plugins”, Installed plug-in, inspect the entries in the Suffix column. You should not find the extensions mentioned in this column. If you find one, check that it is not associated with an application that executes code. There are applications such as Notepad.exe, which do not execute code, but may be associated with the extensions mentioned. Remove any unauthorised extensions from the list. 
B.	Click on the menu button ☰ , click on “Options” and look for the extensions mentioned in the column “Content type” under “Applications”. It is recommended that the extensions mentioned above, show in the column “Action” the options “Save file” or “Always ask”. Another option is that it is associated with an application that does not execute code (e.g. Notepad). If any of the above-mentioned extensions are found in the “Action” column associated with an application that can execute the code, then it is recommended to remove it from the list. 

Firefox is not configured to use the Windows certificate store

As of Firefox 49, a new option has been included that allows Firefox to trust the root authorities in the Windows certificate store. This means that certificates can be deployed through Group Policy as normal and Firefox will trust the same root authorities that Internet Explorer trusts.

This function is disabled by default.

To enable this setting, you must create a new entry, with the value "security.enterprise_roots.enabled" set to "true", in the "firefox.cfg" file.

Check:

Type "about:config" in the browser window. Verify that the preference name "security.enterprise_roots.enabled" is set and locked to the option set.

Firefox is configured to allow autocomplete.

To protect our information, Firefox offers the ability to configure itself so that data entered into forms is not saved. This mitigates the risk of a website obtaining private information from this saved information.

The value “browser.formfill.enable” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “browser.formfill.enable” is set and locked to “false”.

Firefox is configured to display our real IP while browsing

Disabling the WebRTC (Web Real-Time Communication) protocol can significantly improve privacy. This protocol hides several rather serious privacy issues, issues that can be omitted, for example, filtering the real IP address when surfing through a VPN.

However, disabling this protocol may cause some applications and web tools that rely on it to stop working. Applications such as WhatsApp Web would stop working.

There are websites that show whether the browser is leaking personal information through this protocol.

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

The value “media.peerconnection.enabled” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “media.peerconnection.enabled” is set and locked to “false”.

Delete files generated during browsing when closing the browser.

Some configurations must be defined so that when browsing ends and the browser is closed, the files generated by the browser during its operation are deleted.

This encourages the loading, the next time the site is visited, of the latest versions of the pages visited, as well as the configuration for the website, thus improving the overall security of navigation.

To perform this operation, the following properties must be defined in the configuration file:

- 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

In organisations where browsing history must be retained, the preference “privacy.clearOnShutdown.history” should be set to allow browsing history to be remembered, with the value set to “false” so that the history is not deleted when the browser is closed.

5.6 Values of the directives

Check:

Type "about:config" in the browser window. Verify that the following preference names are set and locked to "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

Disable the Firefox account synchronisation feature.

Firefox Account formerly known as Firefox Sync is a built-in browser feature that allows users to automatically synchronise various items such as bookmarks, open tabs, passwords and add-ons.

If you do not want to use the synchronisation and installation of everything configured in a Firefox account and thus avoid privacy and security issues, you should disable this browser feature.

The value “identity.fxaccounts.enabled” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about: config” in the browser window. Verify that the preference name “identity.fxaccounts.enabled” is set and locked to “false”.

Disable Pocket in Firefox.

Pocket is a functionality that allows users to save any type of web content for later viewing.

For organisations that prefer to enable Pocket functionality, the preference “extensions.pocket.enabled” should be set to “true”.

The value “extensions.pocket.enabled” must be set to “false” in the “firefox.cfg” file.

Check:

Type “about:config” in the browser window. Verify that the preference name “extensions.pocket.enabled” is set and locked to “false”.

6. Checklist (assessment)

Criticality	Assesment
High	Mozilla Firefox must have the latest security-related software updates installed.
Media	Mozilla Firefox est configuré pour utiliser un coffre-fort de mots de passe avec ou sans mot de passe principal.
Media	Mozilla Firefox is configured to use a password store with or without a master password.
Media	Mozilla Firefox's form filling support is disabled.
Media	Mozilla Firefox is set to autofill passwords
Media	The security preferences required by Mozilla Firefox cannot be changed by the user.
Media	Mozilla Firefox automatically updates add-ons and plugins
Media	Mozilla Firefox is set to update automatically
Media	Mozilla Firefox automatically checks for updated versions of installed search plugins
Media	Mozilla Firefox is configured to ask which certificate to present to a website when a certificate is required.
Media	Sending background information to Mozilla Firefox must be disabled.
Media	Installation of extensions must be disabled.
Media	Mozilla Firefox is configured to allow JavaScript to bring up (bring to front) or bring down (send to back) windows.
Media	Mozilla Firefox is configured to allow JavaScript to change the text in the status bar.
Media	Mozilla Firefox is configured to allow JavaScript to disable or override context menus.

6. Checklist (assessment)

Criticality	Assesment
Media	Mozilla Firefox is not configured to display a prompt message to a user before downloading and opening different types of files.
Media	Mozilla Firefox has the ActiveX controls plug-in installed.
Media	Network shell protocol enabled in Mozilla Firefox
Media	Mozilla Firefox is not configured to provide warnings when a user switches from a secure (SSL-enabled) page to a non-secure page.
Media	Mozilla Firefox is not configured to block pop-ups
Media	Mozilla Firefox is configured to allow JavaScript to move or resize windows.
Media	Mozilla Firefox must be configured to allow TLS only.
Media	Mozilla Firefox automatically executes or downloads MIME types that are not allowed for automatic download.
Media	Mozilla Firefox is not configured to use the Windows certificate store.
Media	Mozilla Firefox is configured to allow autocomplete.
Media	Mozilla Firefox is configured to show our real ip while browsing.

7. Decalogue of recommendations

The following are ten (10) security recommendations for *Mozilla Firefox*

Security Decalogue for Mozilla Firefox

1. Always use the latest version of Mozilla Firefox.
2. In case of installing add-ons, it is recommended to check that they are installed from trusted sources.
3. It is advisable to review any security-related features of the software, as they provide further defence against attacks.
4. It is recommended to not store passwords by default and instead use other applications that implement strong encryption to securely store your passwords.
5. It is recommended to look at the site's identity button (a padlock in the address bar to the left of the address bar) to quickly and easily find out if the connection to the page is encrypted and, in some cases, who is the owner. This information helps in the detection of harmful pages.
6. It is recommended to always use https, especially when using personal data to secure end-to-end communications.
7. The use of PGP software to send encrypted personal information is recommended as an additional security measure, even if secure protocols such as https are used.
8. The use of two-factor authentication is recommended when using online services. By configuring the service to send a PIN code to the mobile phone. This adds an additional layer of security to accounts.
9. It is recommended to delete cookies to prevent some websites from tracking your search patterns and to safeguard your privacy.
10. It is recommended to clear the cache and delete temporary Internet files to solve common problems with websites.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Annex A. Security configuration files

To facilitate the implementation of the security enforcement on Mozilla Firefox, a folder containing the files necessary to keep information secure on a computer is included in this document.

The files included in the **"Scripts"** folder are listed below.

- autoconfig.js
- firefox.cfg

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es