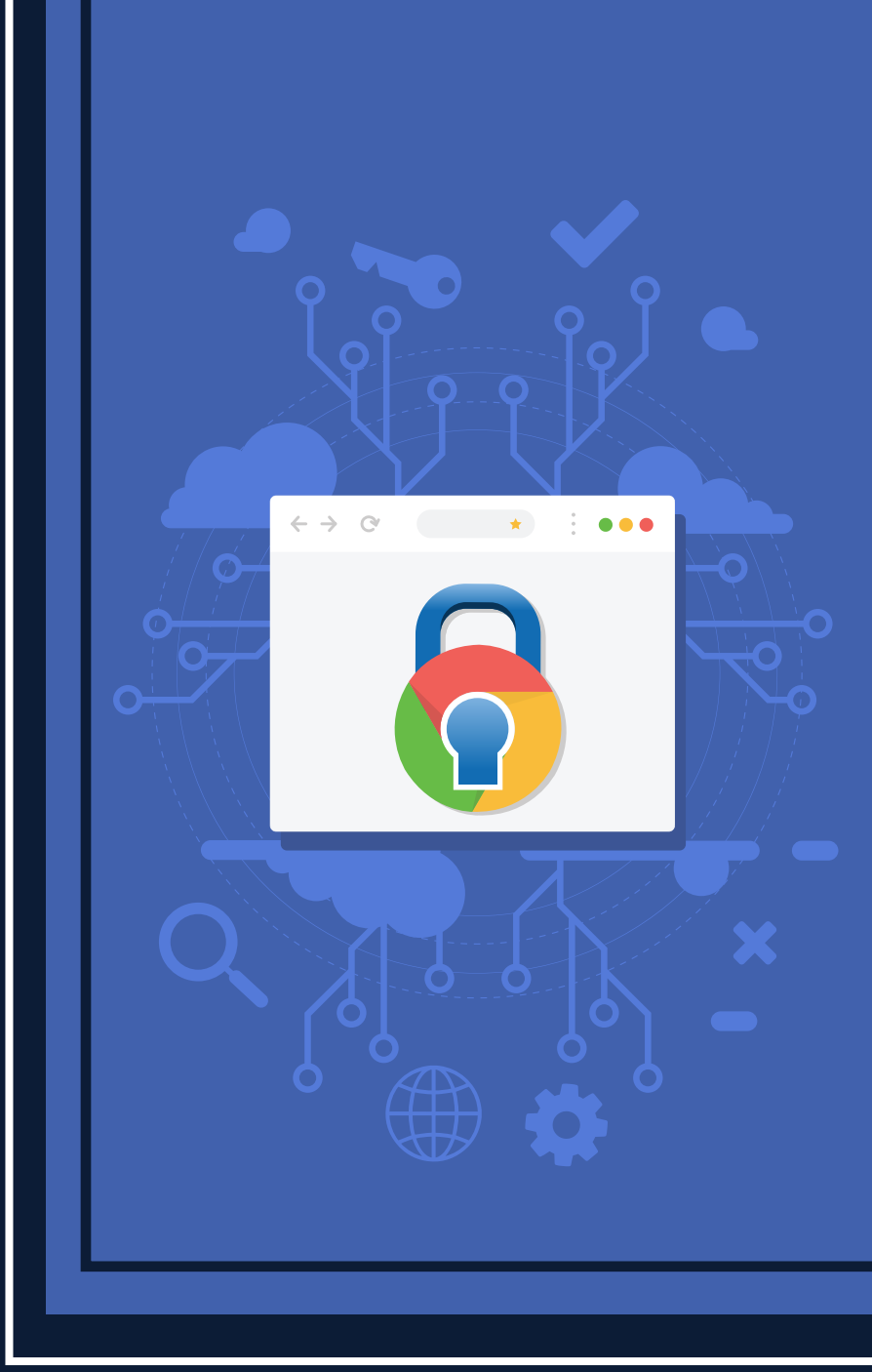
CCN-CERT

# BP/19



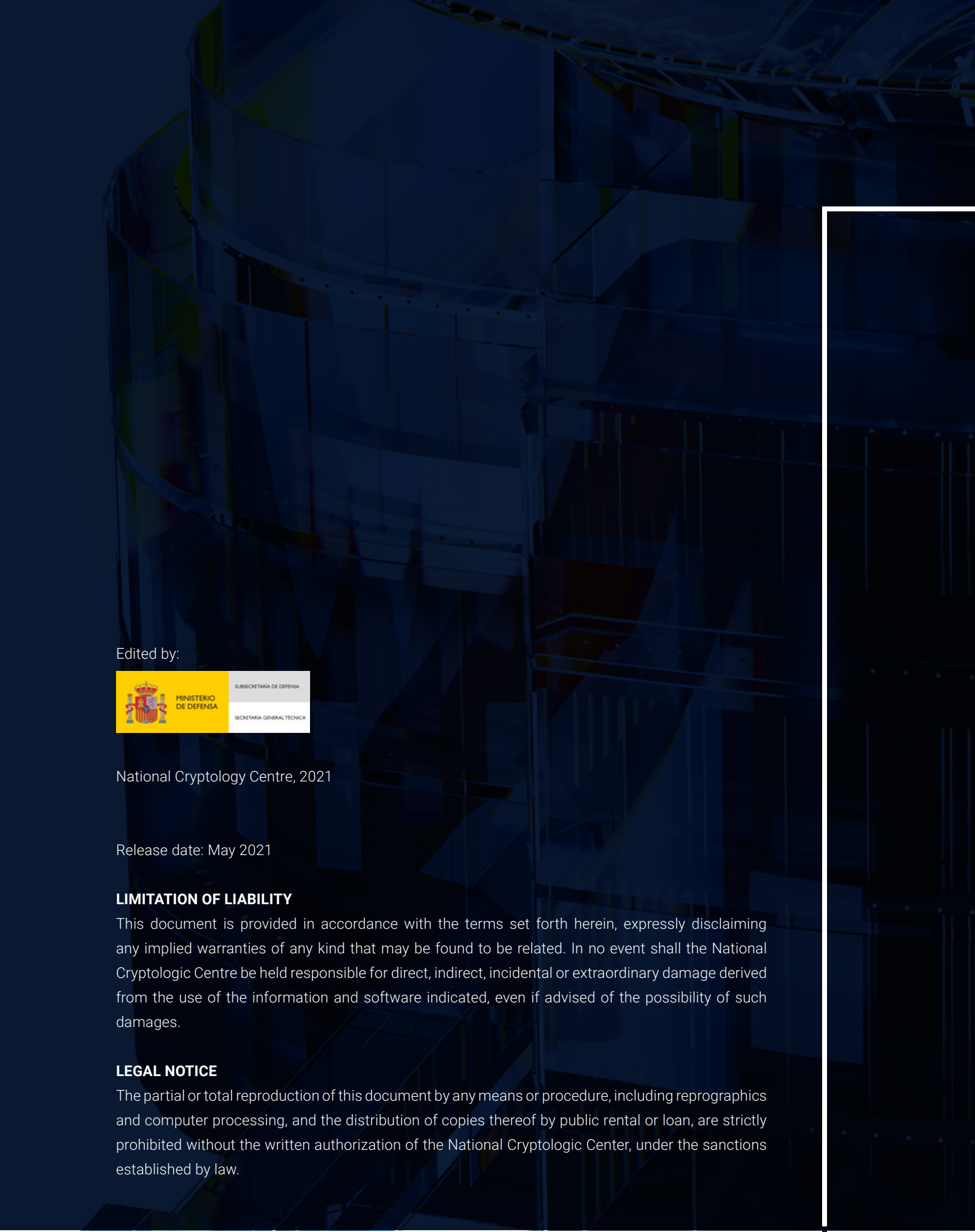
# Google Chrome Security Recommedations

BEST PRACTICES REPORT

MAY **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edited by:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

National Cryptology Centre, 2021

Release date: May 2021

# Index

# 1. About CCN-CERT, National Governmental CERT

**CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN.**

The **CCN-CERT** is the Computer Security Incident Response Team 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 set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

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

Its ultimate aim is **to make cyberspace more secure and reliable**, 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 the Public Sector Legal System, 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-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

# 2. Introduction

**The purpose of this document is to set out the procedures and utilities required to implement and ensure *Google Chrome*'s security.**

For this purpose, a configuration file is provided to implement security measures and thus facilitate the possibility of implementing security.

This document sets out a procedure **for improving security** and **protecting the** *Google Chrome* **browser** to mitigate potential vulnerabilities and risks to which it may be exposed.

For the development of this guide we have used the installer of the program *Google Chrome* **version 89.0.4389** for Windows operating systems.

# 3. Google Chrome web browser

### *Google Chrome* is available for free download from *Google*'s website.

Once the installer is downloaded it requires internet connection for the browser installation. If the computer on which *Google Chrome* is installed does not have internet connection, the full download will need to be performed at the alternative link provided by *Google* to that effect.

In this regard, *Google Chrome* must have the latest security *software* updates installed. For this purpose, it is advisable to determine the update method (e.g. connection to a *WSUS* server, local procedure, automatic update, etc.). In case the latest security-related *software* updates for Chrome are not implemented, it would be considered a **critical security failure**.

# 3.1 Versions

***Google Chrome* browser comes in several versions. The choice of the version to install will depend on the intended use.**

### Chrome (Stable)

This is the **official version**, the one that will be used by the majority of users. This version will always be the most stable version as it undergoes a full battery of tests prior to release. This version receives minor updates every three (3) weeks and major updates every six (6) weeks.


### Chrome Beta

This version is characterized as a **pre-stable version**, where bugs are debugged before the release of the final version. This version receives minor updates every week and major updates every six (6) weeks.


### Chrome Dev

**Pre-beta version and less known as** it is mainly used by **Google developers for** testing major updates. This version is used to complete the most important improvements or new features that will be available in the next version. This version contains bugs, bugs and/or compatibility issues, which makes it an unstable version. This version receives updates once or twice a week because many of its features are still under development.

### Chrome Canary

This version introduces the **latest changes**, new features, new tools and more options, but it **provides some instability** to the browser.

This version is intended to **identify the problems of the new features**, which makes it very unstable. It is automatically generated on Google's servers and changes to the browser code are made daily. Not recommended for use, but it can be downloaded.

### Chrome Enterprise

This version is the same Chrome browser that is used in the stable version. The difference relies in how it is deployed and managed. **IT administrators can download this version** to install the Chrome browser via an MSI installer **and manage their organization's Chrome browsers** via group policies (there are currently over 200 configuration policies).

To find out which version of *Google Chrome* is installed on a device follow the steps below:

Click on ⋮,Click on of the browser. Next, select "**Settings**" and then, in the new window opened in the browser, click "**Chrome Information**" in the left-hand panel. The number of the version installed will be displayed below the name *Google Chrome*, as shown in the following image:

**Description**

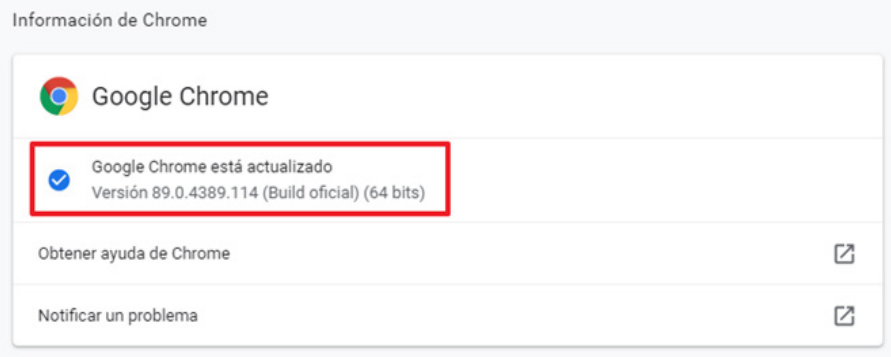



Figure 1

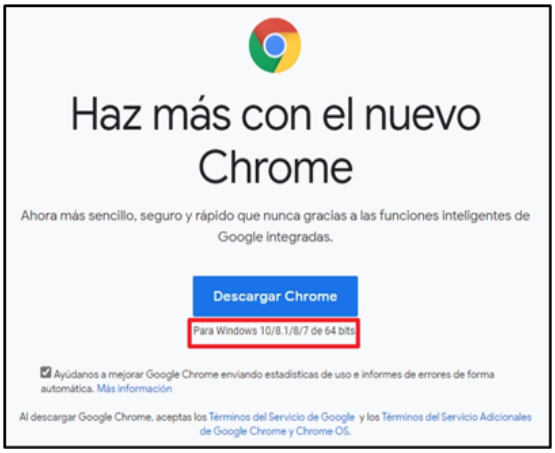
# 3.2 Minimum requirements

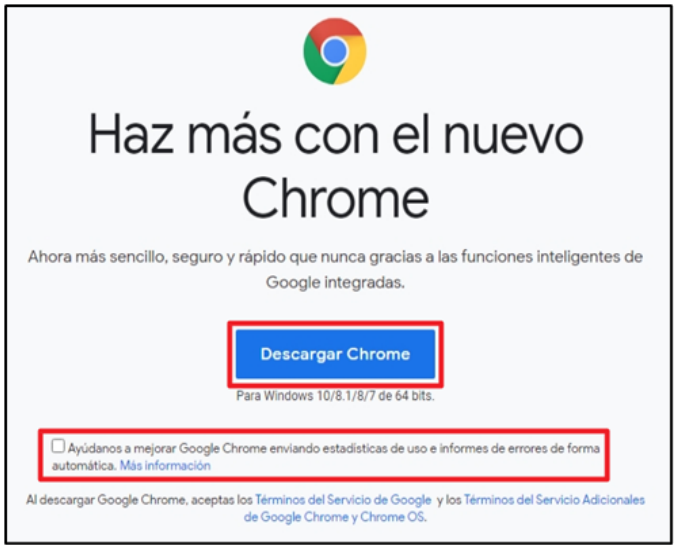
The following are the **minimum system requirements** for implementing the *Google Chrome* program in Windows.

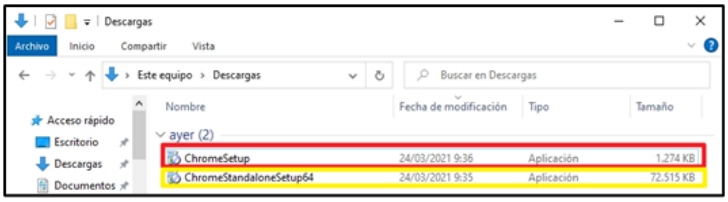
- **Supported Operating Systems** (32-bit and 64-bit versions):
  - **Windows 7**
  - **Windows 8 and Windows 8.1**
  - **Windows 10**
  - **Windows Server 2008 R2**
  - **Windows Server 2012 R2**
  - **Windows Server 2016**
- **Recommended hardware:**
  - **Pentium 4 or a more modern processor that supports SSE2.**

# 3.3 Download

Below is the **process to be followed** for **downloading** the file of the *Google Chrome* browser.

| Step | Description |
|---|---|
| **1.** | To download the program from the official source, please use the following link link:<br><br>**https://www.google.com/chrome/browser/desktop/index.html** |
| **2.** | The download website automatically detects the operating system installed on the computer and its architecture (32 or 64 bits) and adjusts the installation options as shown in the following image:<br><br>  <br><br>Figure 2 |

| Step | Description |
|---|---|
| **3.** | Uncheck the option "*Help us improve Google Chrome by sending usage statistics and bug reports automatically*". Then click on "*Download Chrome*".<br>  <br><br>Figure 3 |
| **4.** | Once the download is finished, the following image will appear in your browser:<br>  <br><br>Figure 4 |

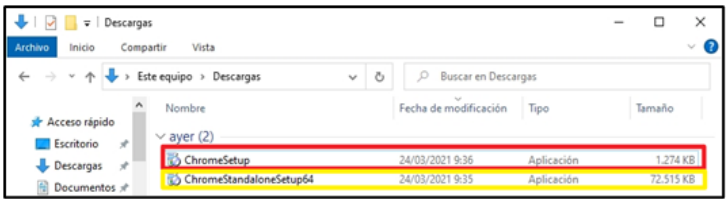
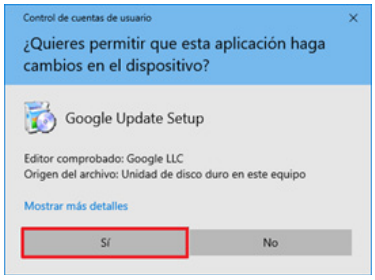
| Step | Description |
|---|---|
| **5.** | The downloaded file will be saved in the location you determined, depending on the configuration set in the browser you are using.<br><br>The red box corresponds to the normal download of the installer. The yellow box corresponds to the download for devices without internet connection.<br><br>  <br><br>Figure 5 |

**Note: There is a version for systems that do not have Internet connection. It can be downloaded from the official link:**

**Link: https://www.google.com/intl/es/chrome/browser/desktop/index.html?standalone=1**

The download process is the same as the normal download, except that in this case **the file to be downloaded is larger** and it will take **longer to download**.

# 3.4 Installation

| Step | Description |
|---|---|
| 1. | Run the downloaded file by double-clicking on it, either the version that requires an internet connection or the offline version.<br>  <br><br>Figure 6 |
| 2. | To start the installation *Google Chrome* needs your authorization. To do so, click "*Yes*" in the following pop-up window.<br>  <br><br>Figure 7 |
| 3. | Once you allow the program to run, it will be installed automatically.<br><br>**Note: *Google Chrome* installation does not allow customization of the installation path.** |

# 3.5 Application of security settings

The "*master_preferences*" file located in "**C:\ProgramFiles\Google\Chrome\Application**" is used to customize the installation of *Chrome* in an enterprise environment. The enterprise version of Chrome allows to customize its installation via the "*master_preferences*" file, and to use administrative templates via Group Policy Object (GPO) on a Windows Server domain controller.

*Google Chrome* has a configuration file called "*Preferences*" where the options selected by the user in this browser are stored. In order to use and apply this file, the browser must be closed. This file is located on the route:

**C:\Users>User>AppData\Local\Google Chrome User Data Default**

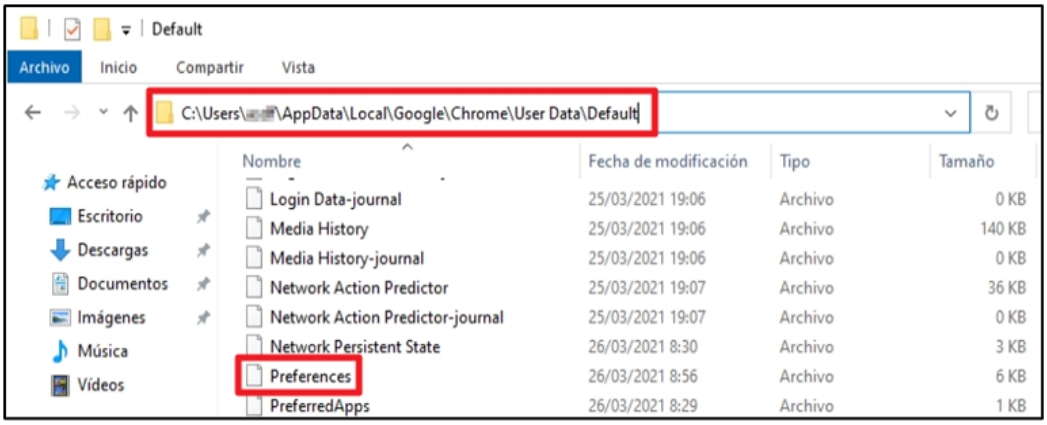



Figure 8

# 3. Google Chrome web browser

To make use of the file supplied with this guide, you will need to replace the file created during the installation of *Google Chrome*. This is done by copying the "**Preferences**" file located in the folder "Scripts" and replacing it in the path above-mentioned.

This file will change the checked and unchecked options with the values of the recommended configurations in section "**3.6. SETTINGS GUIDELINES**" of this guide. The settings for customization of routes, web pages and other options will not be affected. If you wish to customize any of these **custom settings** (such as the home URL, for example) you have to do it manually in the *Google Chrome* browser.

# 3.6 Configuration guidelines

The *Google Chrome* browser has a graphical user interface to edit the **browser options**. To access this interface you must click on the button ⋮, located at the top right of the browser, then select the option "*Settings*" where the configuration options that can be edited by the user.

An alternative method of accessing the configuration interface is to type **chrome://settings/** in the address bar and press the "*Enter*" key.

## 3.6.1 Section Google and you

The *Google Chrome* browser **allows automatic synchronization with Google services**, allowing users, among others, to automatically synchronize various elements such as **bookmarks**, **open tabs**, **passwords**, **plug-ins**, etc. This information is stored in the Google account provided by the user for this purpose.

**To avoid privacy and security problems it is recommended to disable this browser functionality.**

## It is recommended to follow these steps:

Locate the "*Google & You*" section and click on the **Synchronization** part. and **Google services**, as shown in the following image:

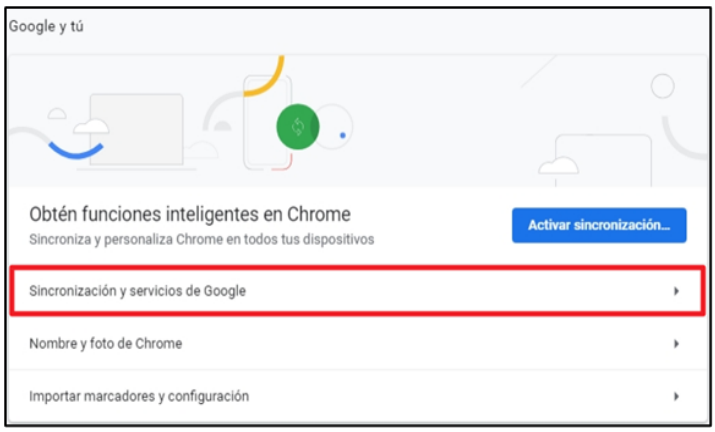



Figure 9

In this section uncheck the options "*Allow Chrome sign-in*", "*Auto-complete searches and URLs*", "*Help improve Chrome features and performance*", "*Improve search and navigation*", "*Improved spell checking*" as shown in the next image:


Figure 10

These changes require a **restart of the browser**, as shown by the notice at the bottom of the screen.

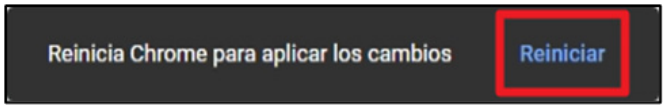



Figure 11

## 3.6.2 Autocomplete section

Because of the way credentials are stored, **it is possible that a malicious attacker could gain access to** user accounts and/or use stored credentials for unwanted logins.

To avoid misuse **it is recommended to disable the following options**:

- In the left panel of the page locate the "*Autocomplete*" section and click on the passwords part, as shown in the picture:

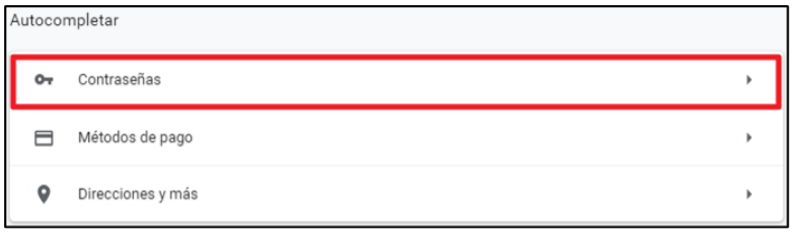



Figure 12

- In this section **uncheck the options** "*Ask if I want to save passwords*" and "*Start session automatically*", as shown below:

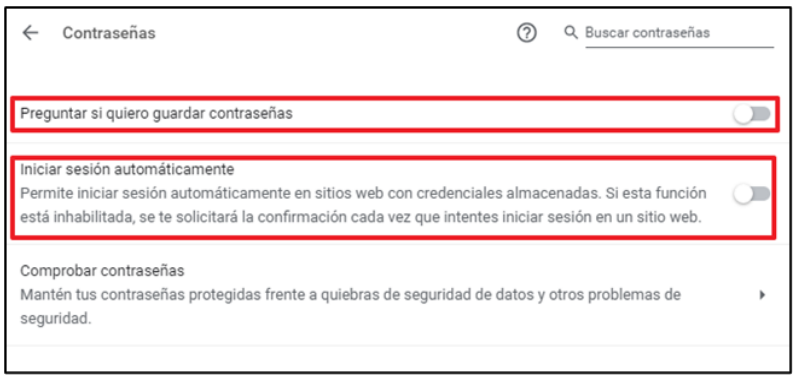



Figure 13

**Payment method** information is an attractive element for attackers looking to make **fraudulent use of it**, and it is **therefore recommended that you do not store this information** in your *Google Chrome* browser to avoid being the target of malicious attacks.

The following steps are recommended:

- In the "*AutoComplete*" section, click on the section "*Payment methods*", as shown in the picture.

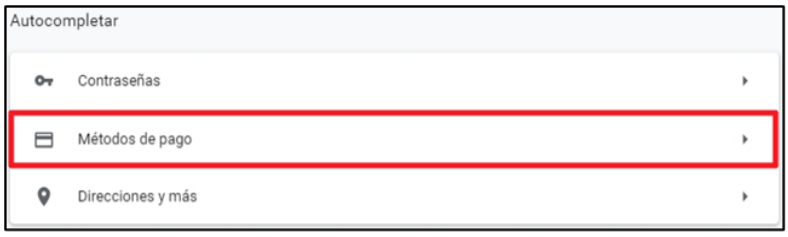



Figure 14

- In this section **uncheck the options** "*Save and auto-complete payment methods*" and "*Allow sites to check if you have payment methods saved*" as indicated in the following image.

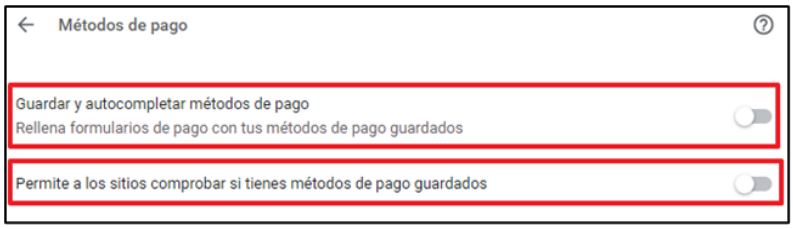



Figure 15

**Payment information is an attractive element for attackers and it is recommended not to have this information stored in the *Google Chrome* browser.**

As in the previous case, the **storage of information**, although not critical, can provide an attacker with relevant information on the user's **movements, actions or other considerations**.

To prevent the use of this information, it is recommended that you **disable** the following option:

- In the "*AutoComplete*" section, click on "*Addresses and more*".


Figure 16

- In this section **uncheck the option** "*Save and autocomplete addresses*", as shown below:

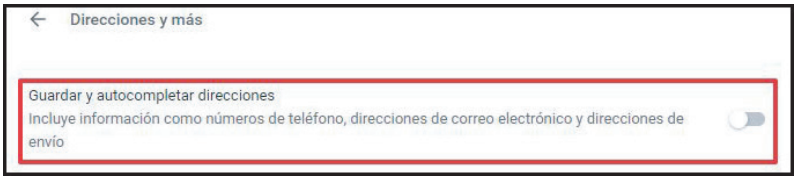



Figure 17

## 3.6.3 Privacy and security section

The configuration of cookies[1] and **background data** delivery is a very important part of security and privacy. A secure configuration of these elements can prevent security breaches and the theft of sensitive information, as an attacker could hide the execution of malicious code through the background traffic in the browser.

To avoid these risks, the following configuration is recommended for the *Google Chrome* browser:

In the "*Privacy and security*" section in the left-hand panel of the page, click on "*Cookies and other site data*", as shown below.

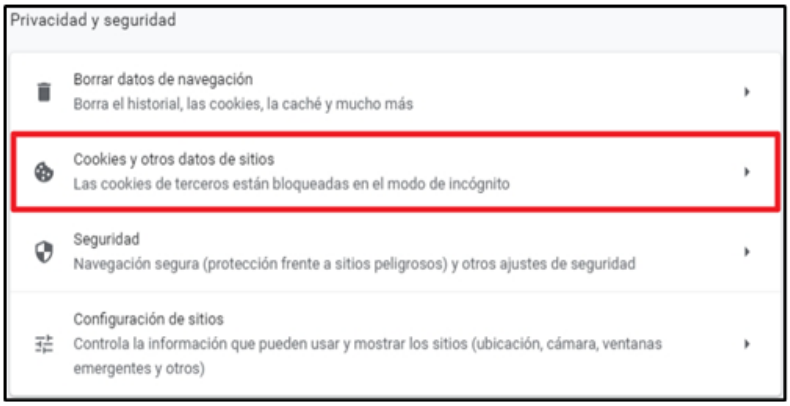



Figure 18

Some configurations should be defined so that when you finish browsing and close the browser, the **files generated by the browser during its execution are deleted**. This favors the loading, on subsequent occasions when visiting the site, of the latest versions of the pages visited, as well as the updated configuration of the website, thus improving the general security of browsing.

**1.** A file generated by a web server that stores browsing data to make the user experience easier with information about your preferences and browsing patterns.

In order to proceed with these settings, go to "*Cookies and other site data*" on the left-hand side of your browser. Once there, **check the following options** as shown in the image:

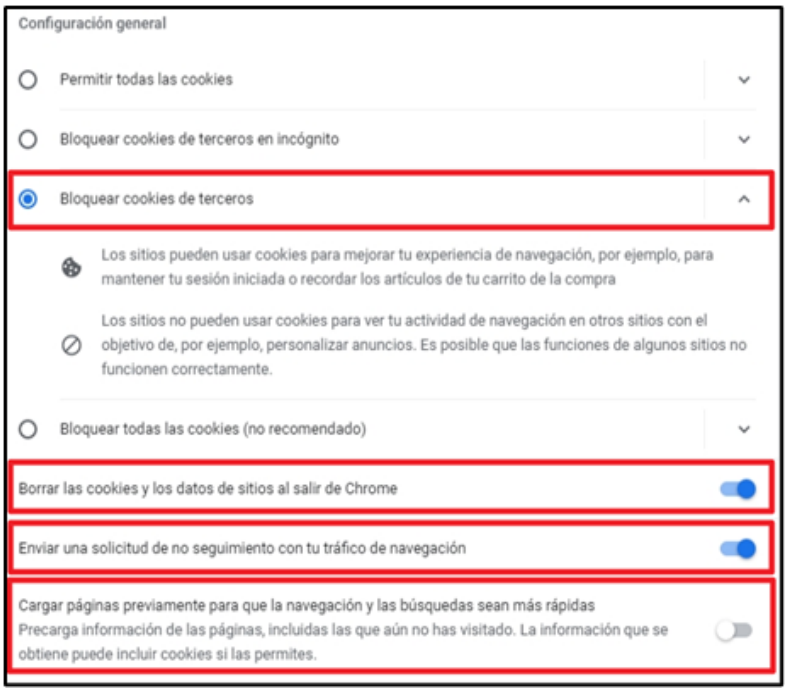



Figure 19

**Note: There are some pages that require third party cookies to function properly. If you find that a page is not working as expected, you may need to enable third party cookies for it to work properly. To do this, you can generate an exception for third party cookies on certain pages to improve your user experience, as shown in the following image.**


Figure 20

In the "*Privacy and security*" section, specifically in the "*Security*" section, it is recommended that you activate the tab "*Enhanced protection*". This protection offered by the *Google Chrome* browser includes, inter alia, the following features:

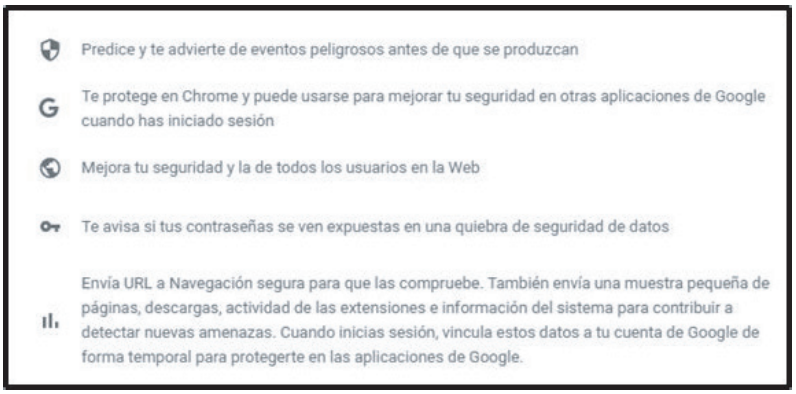



Figure 21

To obtain this protection **you must activate the option** "*Protection improved*" as shown in the following image.

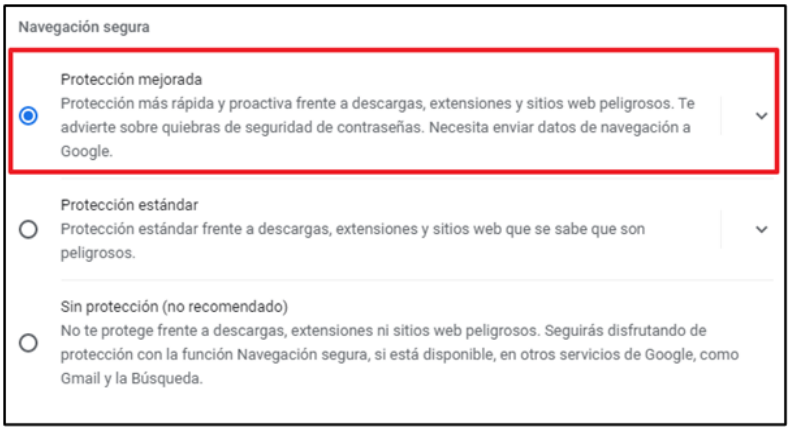



Figure 22

Finally, the "*Use Secure DNS*" functionality is enabled by default. However, by default it makes use of the current service provider's DNS, which can lead to attempts of insecure connections in a website due to service interruption secure against a website due to service interruptions.

It is therefore possible to set up one of the DNS provided by Google and even a customized one if you are in a business environment.


Figure 23

Getting back to the settings in the "*Privacy and security*" section, some aspects should be changed to avoid attacks in minimized windows, windows in the background, and code executions through *JavaScript*, which are normally used to perform malicious attacks.

To limit the above, access "*Configuration of sites*" as shown below:

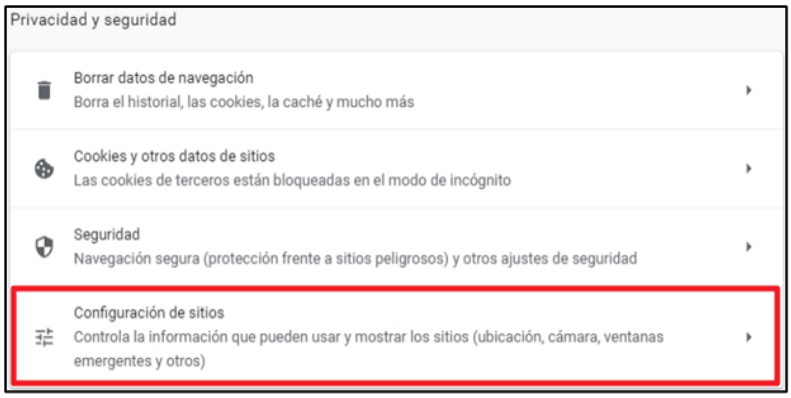



Figure 24

In this section, modify the "*Background synchronization*" aspects so that they do not allow recently closed sites to finish sending and receiving data, as shown in the next image:

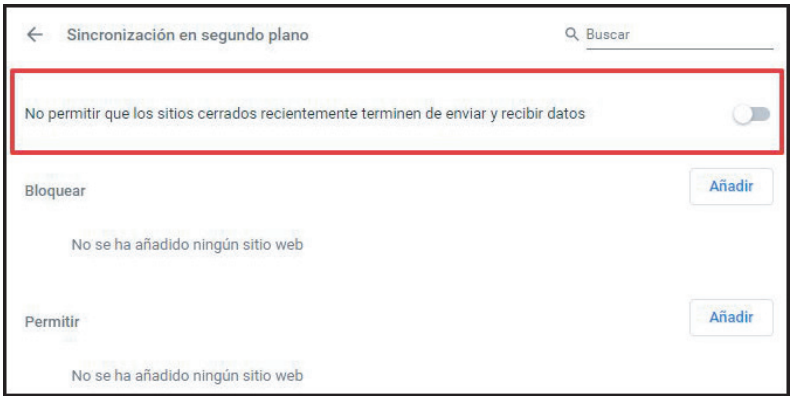



Figure 25

**Note: In most cases, JavaScript should be enabled to obtain full functionality on the web pages visited. However, in some enterprise environments where enhanced levels of security are required, it is recommended to review these settings and block the use of JavaScript to prevent code execution attacks, adding exceptions for those sites that are necessary for the organization.**


Figure 26

To conclude with the settings of the "*Privacy and security*" section, some aspects relating the use of the system's hardware communication elements shall be modified.

This way, privacy settings will suit user needs. By default, the "*Location*", "*Camera*", "*Microphone*" and "*Notifications*" settings will be blocked. Likewise, all the elements included in the "*Additional Permissions*" section will be limited.

This configuration may be modified by adding exceptions to the websites that require the use of these elements.

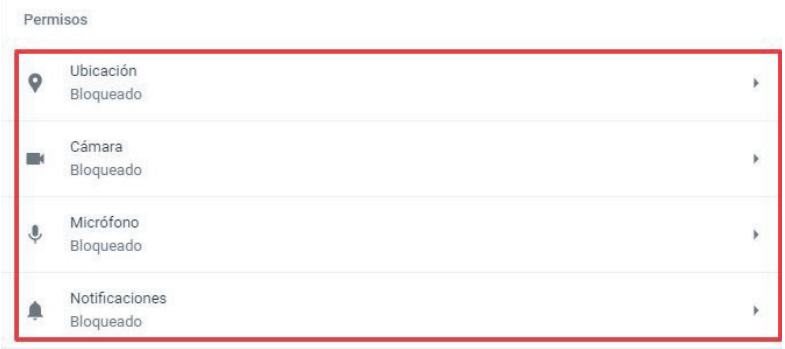



Figure 27

**Note: In addition to this configuration in the general section, "Search engine", it is advisable to regularly review the established configuration, eliminating any unknown search engines. In any case, it is advisable to eliminate those search engines that are not going to be used by the user. to be used.**

## 3.6.4 System section

As discussed in previous sections, the **execution of code in the background** after closing the **Google Chrome** browser is susceptible to malicious attacks, and should be disabled.

- In the "*System*" section, within "*Advanced Settings*" tab in the left panel of the "*Settings*" page, disable the option "*Continue running background applications when Google Chrome is closed*", as shown in the following image.

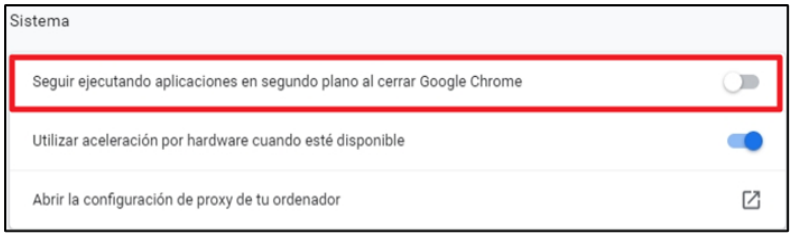



Figure 28

# 4. Checklist

| Criticality | Description |
|---|---|
| **High** | *Google Chrome* must have the latest security-related software updates installed. |
| **High** | In the case of using browser extensions you should check that they are updated to the latest version and come from reliable sources. |
| **Media** | The security preferences required by *Google Chrome* cannot be changed by the user. |
| **Media** | *Google Chrome* is set to update automatically. |
| **Media** | *Google Chrome* is configured to provide warnings when a user switches from a secure (SSL-enabled) page to a non-secure page. |
| **Media** | *Google Chrome* is configured to block pop-up windows. |
| **Media** | *Google Chrome* is configured to not use Google accounts and to not be able to sign in to Google services with an account provided by the user. |
| **Media** | *Google Chrome* is configured not to auto-complete searches and URLs, without sending information to the default search engine. |
| **Media** | *Google Chrome* is configured not to save site passwords. |
| **Media** | *Google Chrome* is configured to not automatically sign in to the sites that store credentials. |
| **Media** | *Google Chrome* is configured not to save or auto-complete methods for payment. |
| **Media** | *Google Chrome* is configured to stop websites from checking whether there are stored payment methods. |
| **Media** | *Google Chrome* is set to block third-party cookies. |
| **Media** | *Google Chrome* is configured not to preload information from pages, even if you have not visited them. This preloading may include cookies if they are permitted. |
| **Media** | *Google Chrome* is configured to stop closed pages from sending and receiving data. |
| **Media** | *Google Chrome* is configured to allow the use of JavaScript. |
| **Media** | *Google Chrome* is configured not to run applications in the background when *Google Chrome* is closed. |

# 5. Decalogue of recommendation

The following are ten (10) security recommendations for the use of *Google Chrome*.

# Security Decalogue for Google Chrome

1. It is recommended to **always use the most current stable version** with the **latest updates**.
2. It is recommended that **the software's security-related functions be reviewed** since it will provide a better defense against certain attacks.
3. If you need to install **plug-ins**, we recommend using **official and /or reliable sources**.
4. It is recommended that you **do not use the password storage available in Google Chrome**, but to **use other applications** that implement a strong encryption system to store passwords more securely.
5. It is recommended to look at **the site's identity button** (a padlock located 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 malicious pages.
6. It is recommended to **always use secure protocols (https)**, even more so when using personal data to secure end-to-end communications.
7. The **use of encryption software** is recommended for sending personal information, as an additional security measure, even with secure protocols such as https.
8. The **use of two-factor authentication** is recommended for online services. This adds an additional layer of security to the accounts as additional verification will be required at login (SMS, phone call, authenticators, etc.).
9. It is recommended that you **delete cookies and block background browsing** to prevent some websites from tracking search patterns and thus safeguard user privacy.
10. It is recommended that you **clear your cache and delete temporary internet files** in order to fix usual problems with websites.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Figure 29. Decalogue of recommendation

# Annex A. Security configuration file

To facilitate the implementation of these security measures on *Google Chrome*, a file with the name "*Preferences*" is attached to the document for the initial configuration of the browser. All these settings can be modified by the user and will be stored in the browser's default folder.

See section "**3.5. APPLICATION OF SECURITY SETTINGS**" to find out how to implement this configuration file within *Google Chrome*.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es