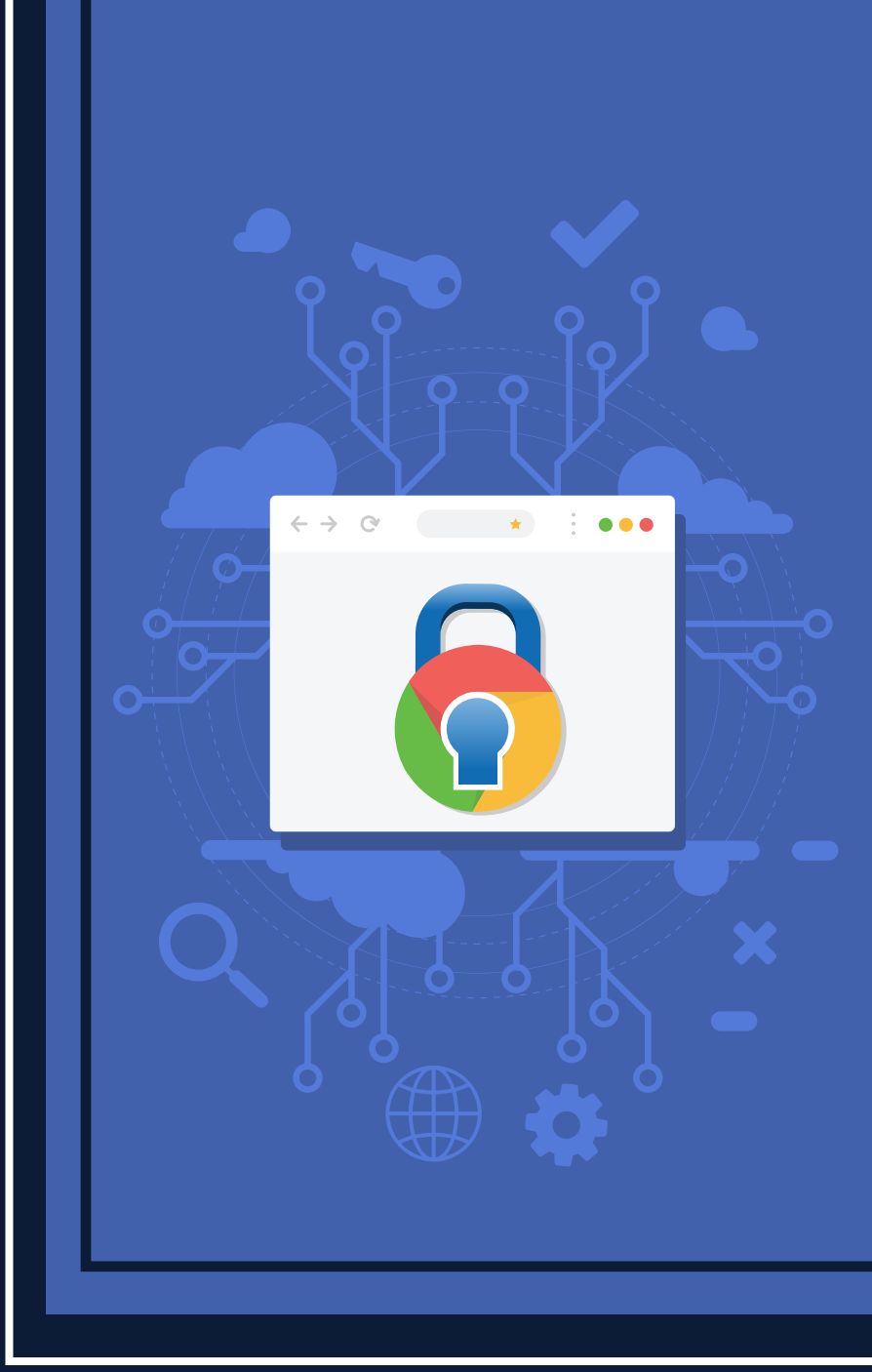
CCN-CERT

BP/19



Recommandations de sécurité dans Google

RAPPORT DE BONNES PRATIQUES

MAI **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Éditer:

Centre National de Cryptologie, 2021

Date de sortie : mai 2021

Index

1. À propos du CCN-CERT, le CERT gouvernemental national

Le CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN.

Le **CCN-CERT** est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national du renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015. du 23 octobre.

Sa mission est donc de **contribuer à l'amélioration de la cybersécurité espagnole**, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux cybermenaces.

Tout cela, dans le but ultime de parvenir à un cyberespace plus sûr et plus fiable, en préservant les informations classifiées (comme indiqué à l'article 4. F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique espagnol, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité, et utiliser et mettre en œuvre des procédures de sécurité.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas d'opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec l'Agence européenne pour la sécurité maritime.

2. Introduction

L'objectif de ce document est d'établir les procédures et les utilitaires nécessaires pour mettre en œuvre et garantir le respect de l'environnement.
la sécurité dans Google Chrome.

À cette fin, un fichier de configuration est fourni pour appliquer le programme les mesures de sécurité et facilitent ainsi la possibilité de mettre en œuvre la sécurité.

Ce document établit une procédure pour **améliorer la sécurité et protéger le navigateur** Google Chrome pour atténuer les vulnérabilités et les risques potentiels auxquels il peut être exposé.

Dans l'élaboration de ce guide, nous avons utilisé l'installateur du programme Google Chrome **version 89.0.4389** pour les systèmes d'exploitation Windows.

3. Le navigateur web Google Chrome

Google Chrome peut être téléchargé gratuitement à partir du site Web de Google.

Le programme d'installation est téléchargé et nécessite une connexion Internet pour le processus d'installation du navigateur. Si l'ordinateur sur lequel Google Chrome est installé ne dispose pas d'une connexion Internet, le téléchargement complet devra être effectué sur le lien alternatif fourni par Google.

À cet égard, Google Chrome doit avoir installé les dernières mises à jour logicielles liées à la sécurité. À cette fin, il est conseillé de déterminer la méthode de mise à jour (par exemple, connexion à un serveur WSUS, procédure locale, mise à jour automatique, etc.) car, si les dernières mises à jour logicielles liées à la sécurité pour Chrome ne sont pas appliquées, cela serait considéré comme un **bug sécurité critique.**

3.1 Versions

Le navigateur Google Chrome existe en plusieurs versions. Choix de la version à installer

Chrome (Stable)

Il s'agit de la **version officielle,** celle que la plupart des utilisateurs utiliseront. Cette version sera toujours la plus stable puisqu'elle subit une batterie complète de tests avant d'être publiée. Cette version reçoit des mises à jour mineures toutes les trois (3) semaines et des mises à jour majeures toutes les six (6) semaines.

Chrome Beta

Cette version se caractérise par le fait qu'il s'agit d'une **version pré-stable**, où les bogues sont débogués avant la publication de la version finale. Cette version reçoit des mises à jour mineures chaque semaine et des mises à jour majeures toutes les six (6) semaines.

Chrome Dev

Version précédente à la bêta et moins connue car elle est principalement utilisée par les **développeurs de Google pour** tester les mises à jour majeures. Dans cette version, les améliorations les plus importantes ou les nouvelles fonctionnalités qui seront disponibles dans la prochaine version sont finalisées. Cette version contient des bogues, des pépins et/ou des problèmes de compatibilité, ce qui en fait une version instable. Cette version est mise à jour une ou deux fois par semaine car de nombreuses fonctionnalités sont encore en cours de développement.

Canari chromé

Cette version **comporte les derniers changements,** de nouvelles fonctionnalités, de nouveaux outils et plus d'options, mais **donne une certaine instabilité** au navigateur.

Cela conduit à une version **destinée à identifier les problèmes liés aux nouvelles fonctionnalités**, ce qui en fait une version très instable. Cette version est automatiquement générée sur les serveurs de Google avec les modifications apportées au code du navigateur pour quotidien. Son utilisation n'est pas recommandée, mais il est possible de le télécharger.

Chrome Enterprise

Esta versión es el mismo navegador Chrome que se utiliza en la versión Cette version est le même navigateur Chrome que celui utilisé dans la version stable. La différence réside dans la manière dont il est déployé et géré. Les **administrateurs informatiques peuvent télécharger cette version** pour installer le navigateur Chrome au moyen d'un programme d'installation MSI **et gérer les navigateurs Chrome de leur organisation** au moyen de stratégies de groupe (il existe actuellement plus de 200 stratégies de configuration).

Pour savoir quelle version de *Google Chrome* est installée sur un appareil:

Cliquez sur le bouton ⋮ situé en haut à droite dans le navigateur. Ensuite, sélectionnez l'option **"Paramètres"** puis, dans la nouvelle fenêtre ouverte dans le navigateur, dans le volet de gauche, cliquez sur l'option **"Informations sur Chrome".** Le numéro de la version installée s'affiche sous le nom de *Google Chrome*,
comme le montre l'image suivante:

Description

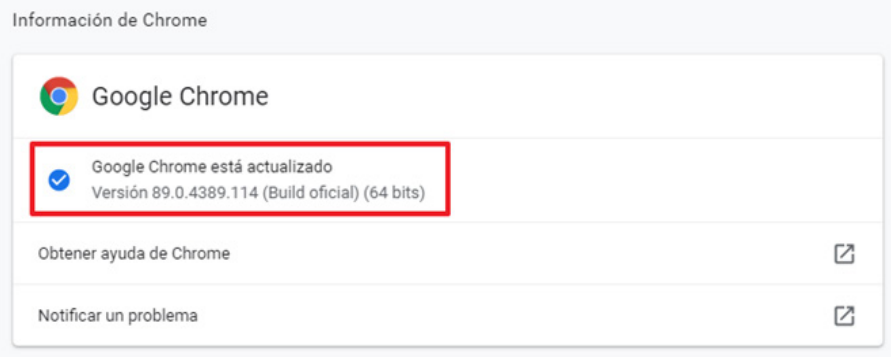


Figure 1

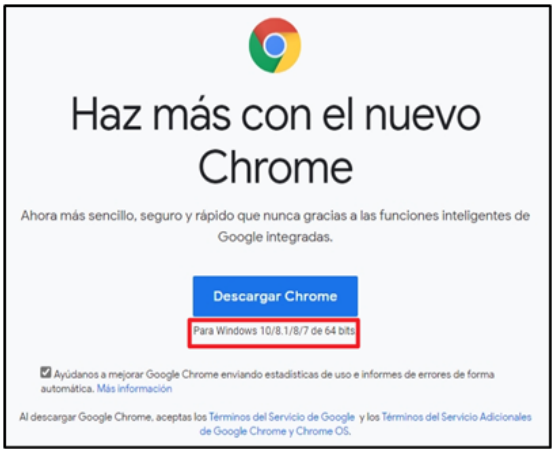
3.2 Exigences minimales

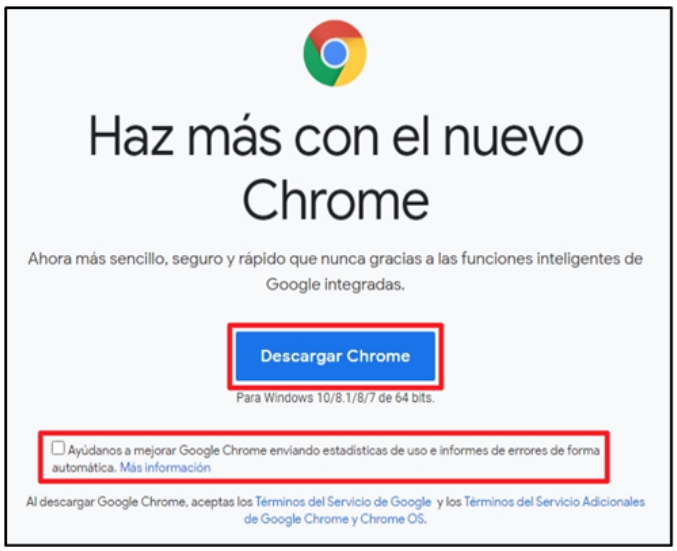
Voici la configuration **minimale requise pour** la mise en œuvre du programme *Google Chrome* dans Windows.

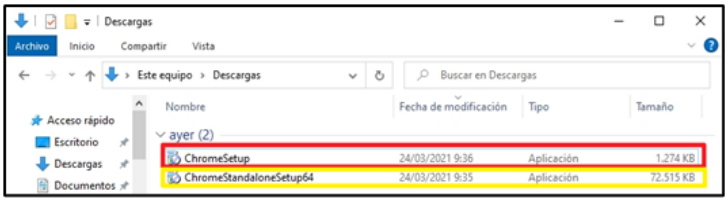
- **Sistemas Operativos soportados** (en versiones de 32-bit y 64-bit):
  - **Windows 7**
  - **Windows 8 y Windows 8.1**
  - **Windows 10**
  - **Windows Server 2008 R2**
  - **Windows Server 2012 R2**
  - **Windows Server 2016**
- **Hardware recomendado:**
  - **Pentium 4 o un procesador más moderno que admita SSE2.**

3.3 Télécharger

Voici la **procédure à suivre** pour **télécharger le fichier** du navigateur *Google Chrome*.

Étape	Description
1.	Pour télécharger le programme depuis la source officielle, veuillez utiliser le lien suivant lien: **https://www.google.com/chrome/browser/desktop/index.html**
2.	Le web download détecte automatiquement le système d'exploitation installé sur l'ordinateur et l'architecture du système d'exploitation (32 ou 64 bits) en adaptant les options d'installation comme le montre l'image suivante:  Figure 2

Étape	Description
3.	Décochez l'option *"Aidez-nous à améliorer Google Chrome en envoyant automatiquement des statistiques d'utilisation et des rapports d'erreur"*. Cliquez ensuite sur le bouton *"Télécharger Chrome"*.  Figure 3
4.	Une fois le téléchargement terminé, l'image suivante apparaîtra dans votre navigateur  Figure 4

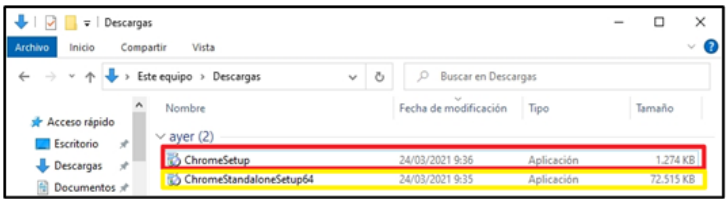
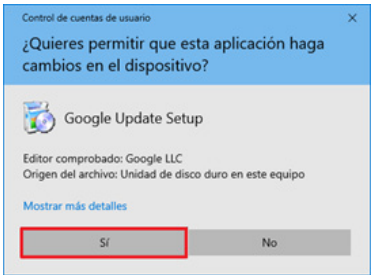
Étape	Description
5.	Le fichier téléchargé apparaîtra à l'endroit que vous avez déterminé, à l'adresse suivante en fonction de la configuration définie dans le navigateur que vous utilisez. La case rouge correspond au téléchargement normal du programme d'installation. La case jaune correspond au téléchargement pour les ordinateurs sans connexion Internet.  Figure 5

Remarque : il existe une version pour les ordinateurs qui ne disposent pas d'une connexion:

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

Le processus de téléchargement est le même que le téléchargement normal, sauf que dans ce cas, **le fichier à télécharger est plus volumineux** et nécessitera.

3.4. Installation

Étape	Description
1.	Exécutez le fichier téléchargé en double-cliquant dessus, qu'il s'agisse de la version nécessitant une connexion Internet ou de la version sans connexion Internet.  Figura 6
2.	Pour commencer l'installation, *Google Chrome* a besoin de votre autorisation. Pour ce faire, cliquez sur *"Oui"* dans la fenêtre pop-up suivante.  Figure 7
3.	Une fois que vous aurez autorisé l'exécution du programme, il sera installé automatiquement.. **Remarque: l'installation de *Google Chrome* ne permet pas de personnaliser le chemin d'installation.**

3.5 Application des paramètres de sécurité

Le fichier *"master_preferences"* situé dans **"C:\ProgramFiles\Google\Chrome\Application"** est utilisé pour personnaliser l'installation de *Chrome* dans un environnement d'entreprise. Si une version d'entreprise de *Chrome* est installée, outre la possibilité de personnaliser l'installation à l'aide du fichier *"master_préférences"*, il est possible d'utiliser des modèles administratifs par le biais de l'édition de la stratégie de groupe (GPO) sur un contrôleur de domaine Windows Server.

Google Chrome possède un fichier de configuration appelé *"Préférences"* dans lequel sont stockées les options sélectionnées par l'utilisateur dans ce navigateur. Pour l'utilisation et l'application de ce fichier, il est nécessaire que le navigateur soit fermé. Ce fichier est situé
situé sur la route:

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

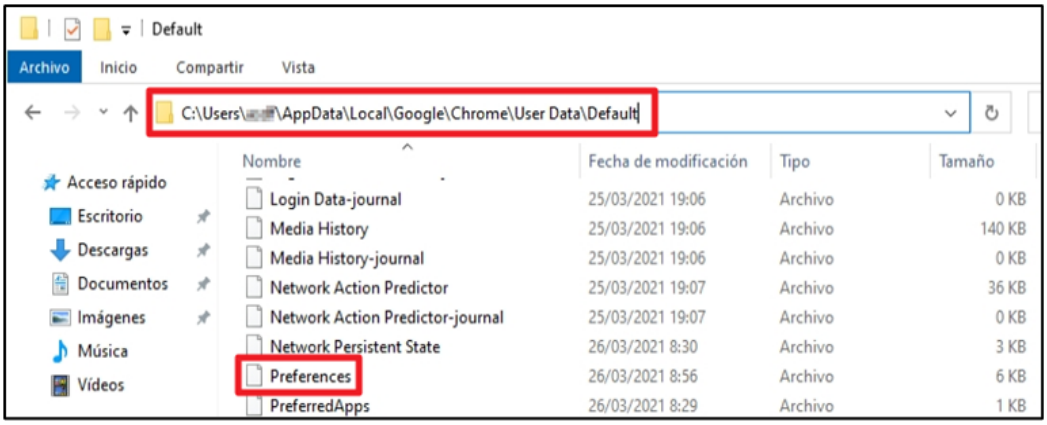


Figure 8

3. Le navigateur web Google

Pour utiliser le fichier fourni avec ce guide, vous devez remplacer le fichier créé lors de l'installation de *Google Chrome*. Pour ce faire, vous devez copier le fichier **"Préférences"** situé dans le dossier de l'utilisateur "Scripts" et remplacez-le par le chemin mentionné ci-dessus.

Ce fichier modifiera les options cochées et non cochées avec les valeurs des paramètres recommandés dans la section **"3.6. LES PARAMÈTRES DE PERSONNALISATION DES ITINÉRAIRES",** des pages Web et d'autres options ne seront pas affectés. Si vous souhaitez personnaliser l'un de ces **paramètres personnalisés** (comme l'URL d'accueil, par exemple) doit être configuré manuellement dans le navigateur *Google Chrome*.

3.6 Directives de configuration

Le navigateur Google Chrome dispose d'une interface utilisateur graphique pour l'édition des options du navigateur. Pour accéder modifier les **options du navigateur**. Pour accéder à cette interface vous devez cliquer sur ⋮ situé en haut à droite du navigateur, puis sélectionnez l'option *"Paramètres"* où les options de configuration qui peuvent être modifiées par l'utilisateur de l'application.

Une autre méthode pour accéder à l'interface de configuration consiste en tapez **chrome://settings/** dans la barre d'adresse et appuyez sur la touche *"Entrée"*.

3.6.1 Google et votre section

Le navigateur Google Chrome permet la **synchronisation automatique avec les services Google**, ce qui permet aux utilisateurs, entre autres, de synchroniser automatiquement divers éléments tels que les **signets**, les **onglets ouverts**, les **mots de passe**, les **plugins**, etc. Ces informations sont stockées dans le compte Google fourni par l'utilisateur à cette fin. effet.

Pour éviter les problèmes la vie privée et la sécurité sont recommande de désactiver cette fonctionnalité du navigateur.

Les étapes suivantes sont recommandées :

- Localisez la section "*Google et vous*" et cliquez sur la partie "Synchronisation".

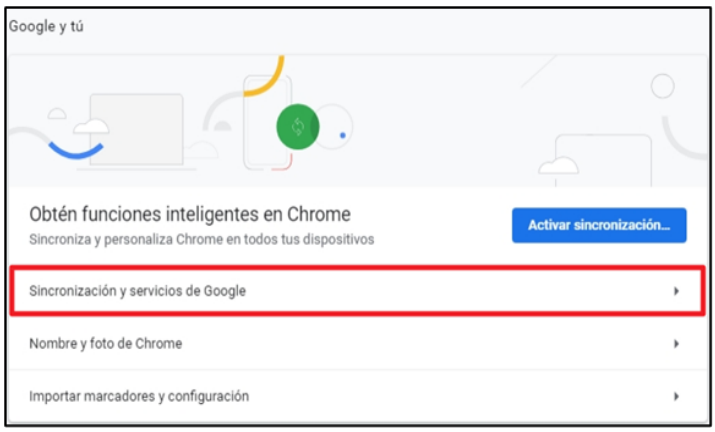


Figure 9

- Dans cette section, décochez les options "*Autoriser la connexion à Chrome*", "*Compléter automatiquement les recherches et les URL*", "*Aider à améliorer les fonctionnalités et les performances de Chrome*", "*Améliorer la recherche et la navigation*", "*Améliorer la vérification orthographique*", comme indiqué dans l'image ci-dessous.

Figure 10

- Ces modifications nécessitent un **redémarrage du navigateur**, comme l'indique l'icône

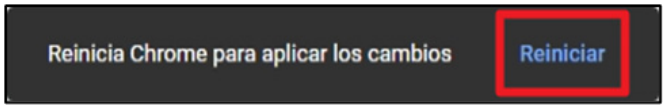


Figure 11

3.6.2 Section saisie automatique

En raison de la manière dont les informations d'identification sont stockées, **il est possible pour un attaquant malveillant d'accéder aux comptes des** utilisateurs et/ou d'utiliser les informations d'identification stockées pour se connecter indésirable.

Pour éviter ces utilisations **les options suivantes**: **il est recommandé de désactiver l'option.**

Dans le volet gauche de la page, localisez la section "*Autocomplete*" et cliquez sur la partie mots de passe, comme indiqué dans l'image:

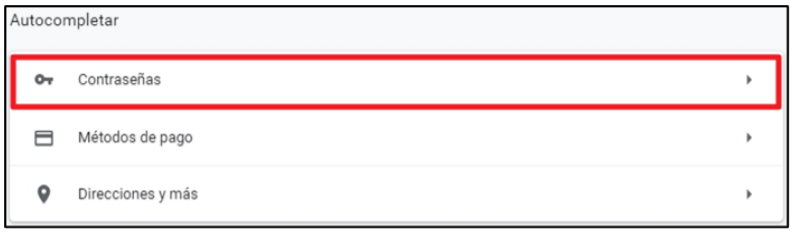


Figure 12

Dans cette section, décochez les options *"Demander si je veux sauvegarder mots de passe"* et *"Commencez session automatiquement"*, comme à l'adresse échantillon a continuation :

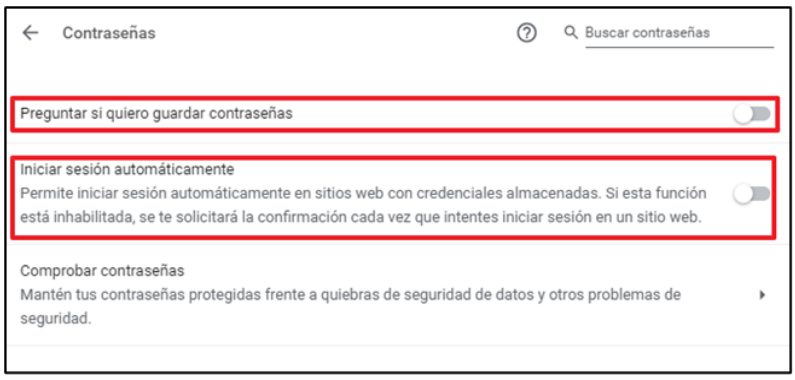


Figure 13

Les informations relatives aux **moyens de paiement** constituent un élément attractif pour les attaquants qui cherchent à **en faire** un **usage frauduleux**. **Il est** donc **recommandé de ne pas stocker ces informations** dans le navigateur Google Chrome afin d'éviter d'être la cible des attaques suivantes les attaques malveillantes.

Les étapes suivantes sont recommandées:

- Dans la section *"Autocomplétion"*, cliquez sur la section *"Méthodes d'autocomplétion paiement"*, comme le montre l'image:

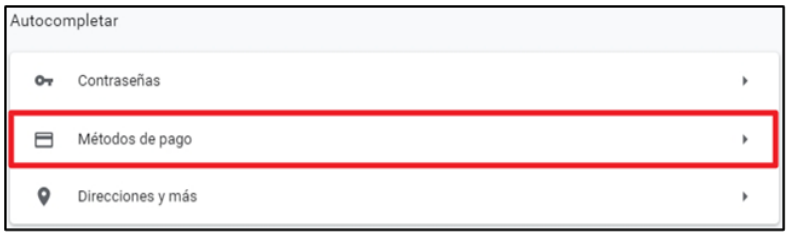


Figure 14

- Dans cette section, **décochez les options** *"Enregistrer et compléter automatiquement les méthodes de paiement"* et *"Autoriser les sites à vérifier si vous avez des méthodes de paiement"*.

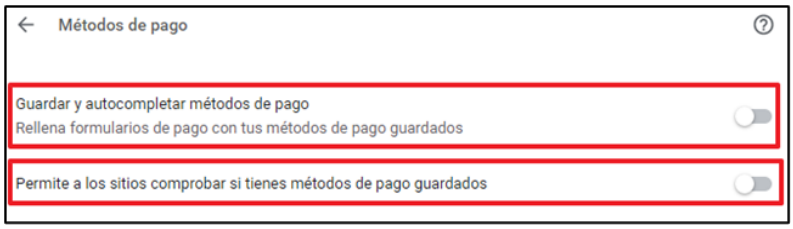


Figure 15

Les informations sur les méthodes de paiement constituent un élément attrayant pour les attaquants.
et il est recommandé de ne pas stocker ces informations dans le navigateur Google

Comme dans le cas précédent, le **stockage d'informations,** bien que non critique, peut fournir à un attaquant des informations pertinentes. sur les **mouvements, les actions ou autres considérations** de l'utilisateur.

Pour empêcher l'utilisation de ces informations, il est recommandé de **désactiver** l'option option suivante:

- Dans la section "*AutoComplete*", cliquez sur la section "*Adresses et plus encore*".

Figura 16

- Dans cette section, **décochez l'option** "Enregistrer et autocompléter les adresses", comme indiqué ci-dessous :

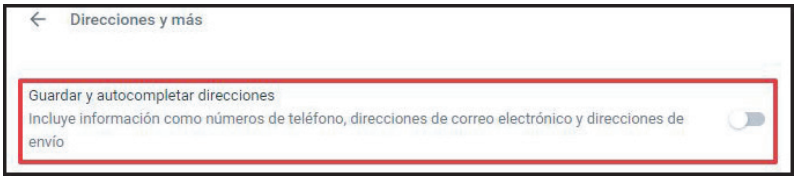


Figura 17

3.6.3 Section vie privée et sécurité

La configuration des cookies1 et de la transmission de **données en arrière-plan** est un élément très important de la sécurité et de la confidentialité. Une configuration sécurisée de ces éléments permet d'éviter les failles de sécurité et le vol éventuel d'informations sensibles, car un attaquant pourrait dissimuler l'exécution d'un code malveillant à l'aide des éléments suivants le trafic de fond du navigateur.

Pour éviter ces risques, la configuration suivante est recommandée pour le navigateur *Google Chrome*:

- Dans la section "*Confidentialité et sécurité*" du panneau gauche de la page, cliquez sur la section "*Cookies et autres données du site*", comme indiqué ci-dessous montré ci-dessous:

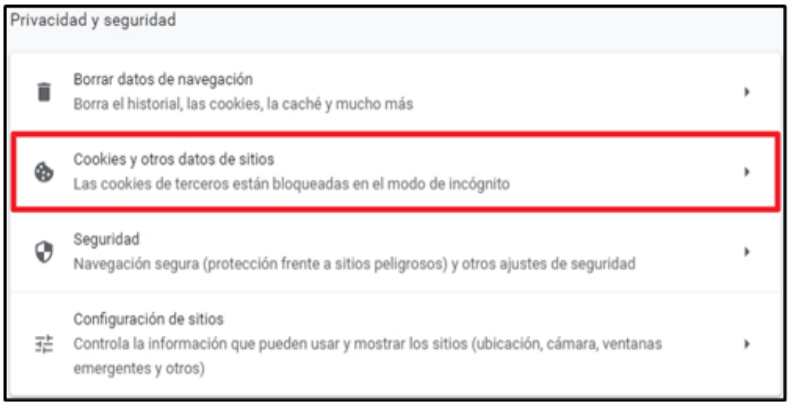


Figure 18

- Certaines configurations doivent être définies de manière à ce que, lorsque vous terminez la navigation et fermez le navigateur, les **fichiers générés par le navigateur pendant son exécution soient supprimés**. Cela favorise le chargement, lors des visites ultérieures du site, des dernières versions des pages visitées, ainsi que la mise à jour de la configuration de l'interface utilisateur site web, améliorant ainsi la sécurité générale de la navigation.

1. Fichier généré par un serveur web qui stocke les données de navigation pour faciliter l'expérience de l'utilisateur avec des informations sur vos préférences et vos habitudes de navigation.

Pour procéder à ces réglages, allez dans la section "Cookies et autres données du site" sur le côté gauche du navigateur. Une fois sur place, **vérifiez les options suivantes** comme indiqué dans l'image:

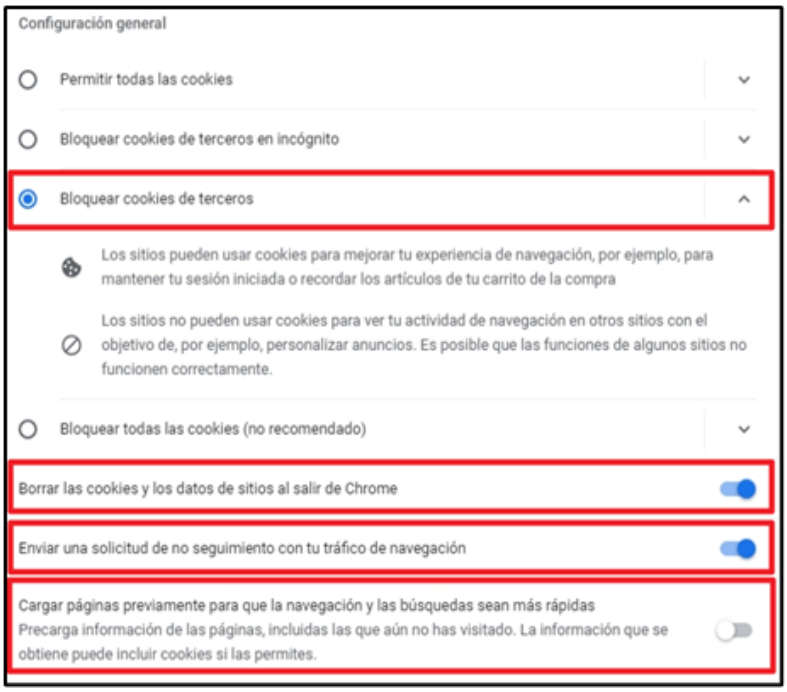


Figure 19

Remarque : certaines pages nécessitent des cookies tiers pour fonctionner correctement. Si vous constatez qu'une page ne fonctionne pas comme prévu, vous devrez peut-être activer les cookies tiers pour qu'elle fonctionne correctement. Pour ce faire, vous pouvez générer une exception pour les cookies tiers sur certaines pages afin d'améliorer leur efficacité comme le montre l'image suivante.

Figure 20

Dans la section "*Confidentialité et sécurité*", plus précisément dans la section "*Sécurité*", il est recommandé d'activer l'onglet intitulé "*Protection renforcée*". Cette protection offerte par le navigateur *Google Chrome* comprend, entre autres, les caractéristiques suivantes :

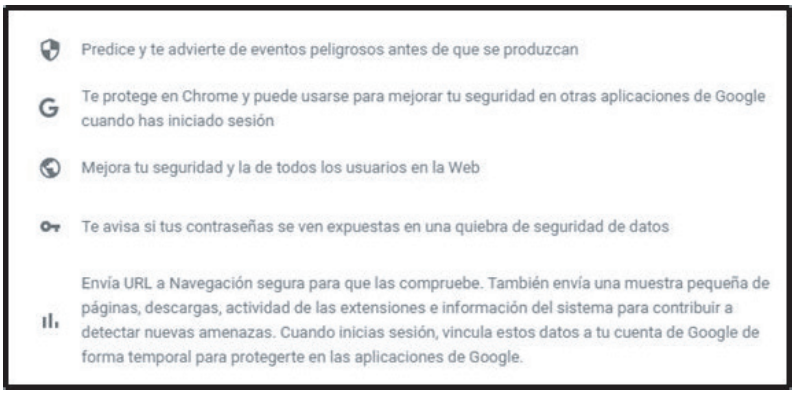


Figure 21

Pour obtenir cette protection, **vous devez activer l'option** "*Protection amélioré*" comme le montre l'image suivante.

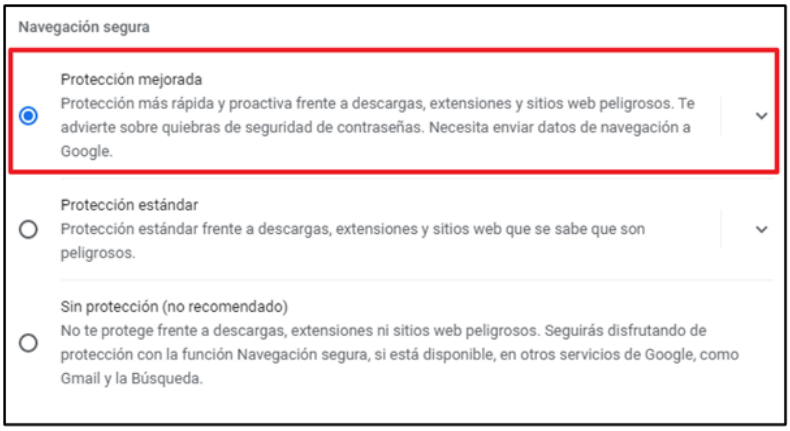


Figure 22

Enfin, la fonction "*Utiliser un DNS sécurisé*" est activée par défaut. Cependant, par défaut, il utilise le DNS du fournisseur des services actuel, ce qui peut conduire à des tentatives de connexion qui ne sont pas conformes à la norme de se protéger contre un site web en raison d'interruptions de service.

Il est donc possible de mettre en place l'un des DNS fournis par Google et même une version personnalisée si vous êtes dans un environnement professionnel.

Figure 23

En continuant avec les paramètres de la section "*Confidentialité et sécurité*", certains aspects devraient être modifiés pour éviter les attaques sur les fenêtres réduites, les fenêtres en arrière-plan et les exécutions de code utilisant *JavaScript*, qui sont normalement utilisées pour effectuer les attaques malveillantes.

Pour limiter ce qui précède, allez dans la section "*Paramètres" des sites*" comme indiqué ci-dessous :

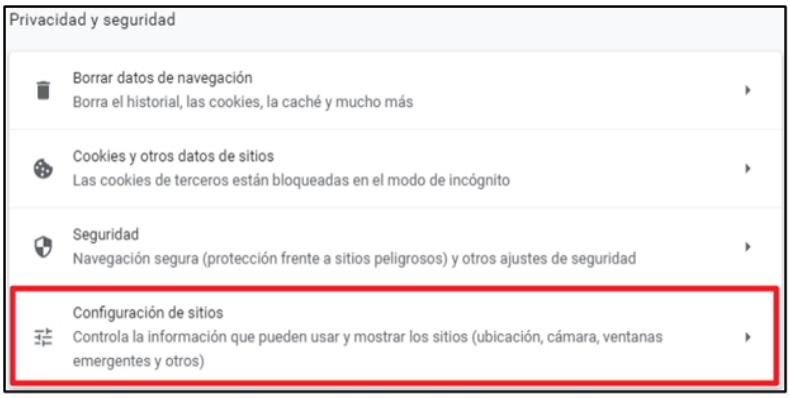


Figure 24

Dans cette section, modifiez les aspects "*Synchronisation en arrière-plan*" de manière à ce qu'ils ne permettent pas aux sites récemment fermés de terminer l'envoi et la réception de données, comme le montre l'image suivante image suivante:

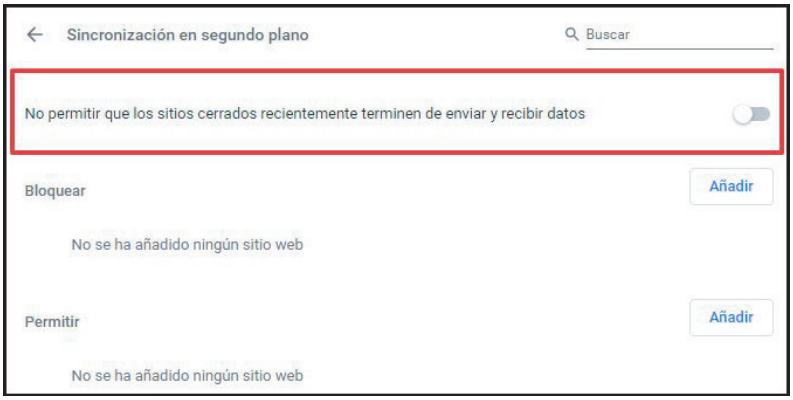


Figure 25

Remarque: dans la plupart des cas, JavaScript doit rester activé pour une fonctionnalité complète des pages Web consultées. Toutefois, dans certains environnements d'entreprise où des niveaux de sécurité accrus sont requis, il est recommandé de revoir ces paramètres et de bloquer l'utilisation de JavaScript pour empêcher les attaques par exécution de code, en ajoutant des exceptions dans les cas suivants les sites qui sont nécessaires à l'organisation.

Figure 26

Pour terminer les réglages de la section "*Confidentialité et sécurité*", il convient de modifier certains aspects liés à l'utilisation des éléments suivants les éléments matériels de communication de l'équipement.

Cela permettra de définir les paramètres de confidentialité en fonction des besoins de l'utilisateur. Par défaut, les paramètres "*Localisation*", "*Caméra*", "*Microphone*" et "*Notifications*" seront bloqués. De même, tous les éléments inclus dans la section "*Permissions seront limités Supplémentaire*".

Cette configuration peut être modifiée en ajoutant des exceptions à l'option les sites web qui nécessitent l'utilisation de ces éléments.

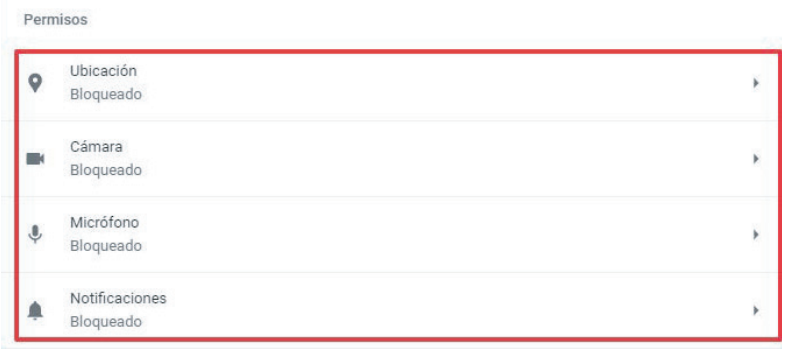


Figure 27

Note: En plus de cette configuration dans la section générale, "Moteur de recherche", il est conseillé de revoir régulièrement la configuration établie, en éliminant tout moteur de recherche inconnu. Dans tous les cas, il est conseillé d'éliminer les moteurs de recherche qui ne seront pas utilisés.

3.6.4 Section système

Comme nous l'avons vu dans les points précédents, l'**exécution de code en arrière-plan** après la fermeture du navigateur Google Chrome est susceptible de faire l'objet d'attaques malveillantes et devrait être handicapés.

- Dans la section "*Système*", sous l'onglet "*Paramètres avancés*" du volet gauche de la page "*Paramètres*", désactivez l'option "*Continuer à exécuter les applications en arrière-plan à la fermeture de Google Chrome*", comme le montre l'image suivante.

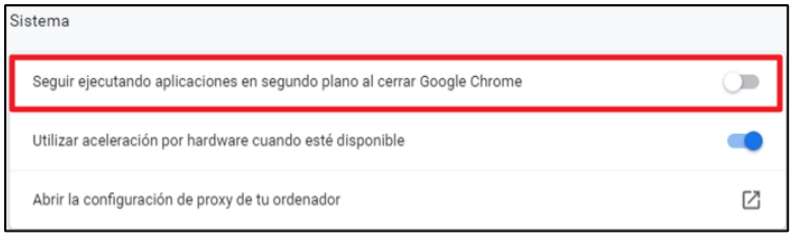


Figure 28

4. Liste de contrôle

Criticité	Description
Haut	Les dernières mises à jour logicielles relatives à la sécurité doivent être installées sur *Google Chrome*.
Haut	En cas d'utilisation d'extensions dans le navigateur, vous devez vérifier que sont mis à jour à la dernière version et proviennent de sources fiables.
Médias	Les préférences de sécurité requises par *Google Chrome* ne peuvent pas être modifiées par l'utilisateur.
Médias	*Google Chrome* est configuré pour se mettre à jour automatiquement.
Médias	*Google Chrome* est configuré de manière à fournir des avertissements lorsqu'une l'utilisateur passe d'une page sécurisée (SSL activé) à une page non sécurisée.
Médias	*Google Chrome* est configuré pour bloquer les fenêtres pop-up.
Médias	*Google Chrome* est configuré pour ne pas utiliser les comptes Google et pour ne pas être en mesure de se connecter aux services Google avec un compte fourni par l'utilisateur.
Médias	*Google Chrome* est configuré pour ne pas compléter automatiquement les recherches et les URL, sans envoyer des informations au navigateur par défaut.
Médias	*Google Chrome* est configuré pour ne pas enregistrer les mots de passe des sites.
Médias	*Google Chrome* est configuré de manière à ne pas vous connecter automatiquement au site Web de la Commission européenne.
Médias	*Google Chrome* est configuré de manière à ne pas enregistrer ou autocompléter les méthodes pour les éléments suivants paiement.
Médias	*Google Chrome* est configuré pour permettre aux sites Web de ne pas rechercher les modes de paiement enregistrés.
Médias	*Google Chrome* est configuré pour bloquer les cookies tiers.
Médias	*Google Chrome* est configuré pour ne pas précharger les informations des pages, même si vous ne les avez pas visitées. Ce préchargement peut inclure des cookies s'ils sont autorisé.
Médias	*Google Chrome* est configuré pour que les pages fermées ne soient pas envoyées. et recevoir des données.
Médias	*Google Chrome* est configuré pour autoriser l'utilisation de JavaScript.
Médias	*Google Chrome* est configuré pour ne pas exécuter les applications en arrière-plan lorsque vous fermez Google Chrome.

5. Décalogue des recommandation

Voici dix (10) recommandations de sécurité pour l'utilisation des produits suivants

Décalogue de sécurité de Google Chrome

1. Il est recommandé de **toujours utiliser la version stable la plus récente** avec la **dernière des mises à jour**.

2. Il est recommandé de **revoir les fonctions de sécurité du logiciel**, étant donné que ce qui permettra de mieux se défendre contre d'éventuelles attaques.

3. Si vous devez **installer des plugins**, il est recommandé d'utiliser les **sources officielles.** et/ou fiable.

4. Il est recommandé de **ne pas utiliser le magasin de mots de passe disponible dans Google Chrome**, mais plutôt d'**utiliser d'autres applications** qui mettent en œuvre un système de gestion des mots de passe.

5. **Il** est recommandé de **regarder le bouton d'identité du site** (un cadenas dans la barre d'adresse, à gauche de celle-ci) pour savoir rapidement et facilement si l**a connexion à la page est cryptée** et, dans certains cas, qui est l'administrateur du site propriétaire. Ces informations aident à la détection des pages malveillantes.

6. Il est recommandé de **toujours utiliser des protocoles sécurisés (https)**, d'autant plus lorsque l'on utilise.

7. **Il** est recommandé d'**utiliser un logiciel de cryptage pour envoyer des informations personnelles**, telles que mesure de sécurité supplémentaire, même avec l'utilisation de protocoles sécurisés tels que https.

8. L'**utilisation d'une authentification à deux facteurs** est recommandée pour l'utilisation des services en ligne. Cela ajoute une couche supplémentaire de sécurité aux comptes car ils seront une vérification supplémentaire est requise lors de la connexion (SMS, appel téléphonique, authentificateurs, etc.).

9. Il est recommandé de **supprimer les cookies et de bloquer la navigation en arrière-plan** afin d'empêcher certains sites Web de suivre les habitudes de recherche et de protéger votre vie privée.

10. Il est recommandé de **vider votre cache et de supprimer les fichiers Internet temporaires** afin de résoudre les problèmes courants des sites web.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Figura 29. Decálogo de recomendaciones

Annexe A. Fichier de configuration de la sécurité

Pour faciliter la mise en œuvre du renforcement de ces mesures de sécurité sur *Google Chrome*, un fichier "*Préférences*" pour la configuration initiale du navigateur est inclus en pièce jointe du document. Toutes ces configurations peuvent être modifiées par l'utilisateur et seront stockées dans l'application

Reportez-vous à la section "**3.5. APPLICATION DES CONFIGURATIONS SAFETY**" pour savoir comment implanter cet archives de configuration dans *Google Chrome*.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es