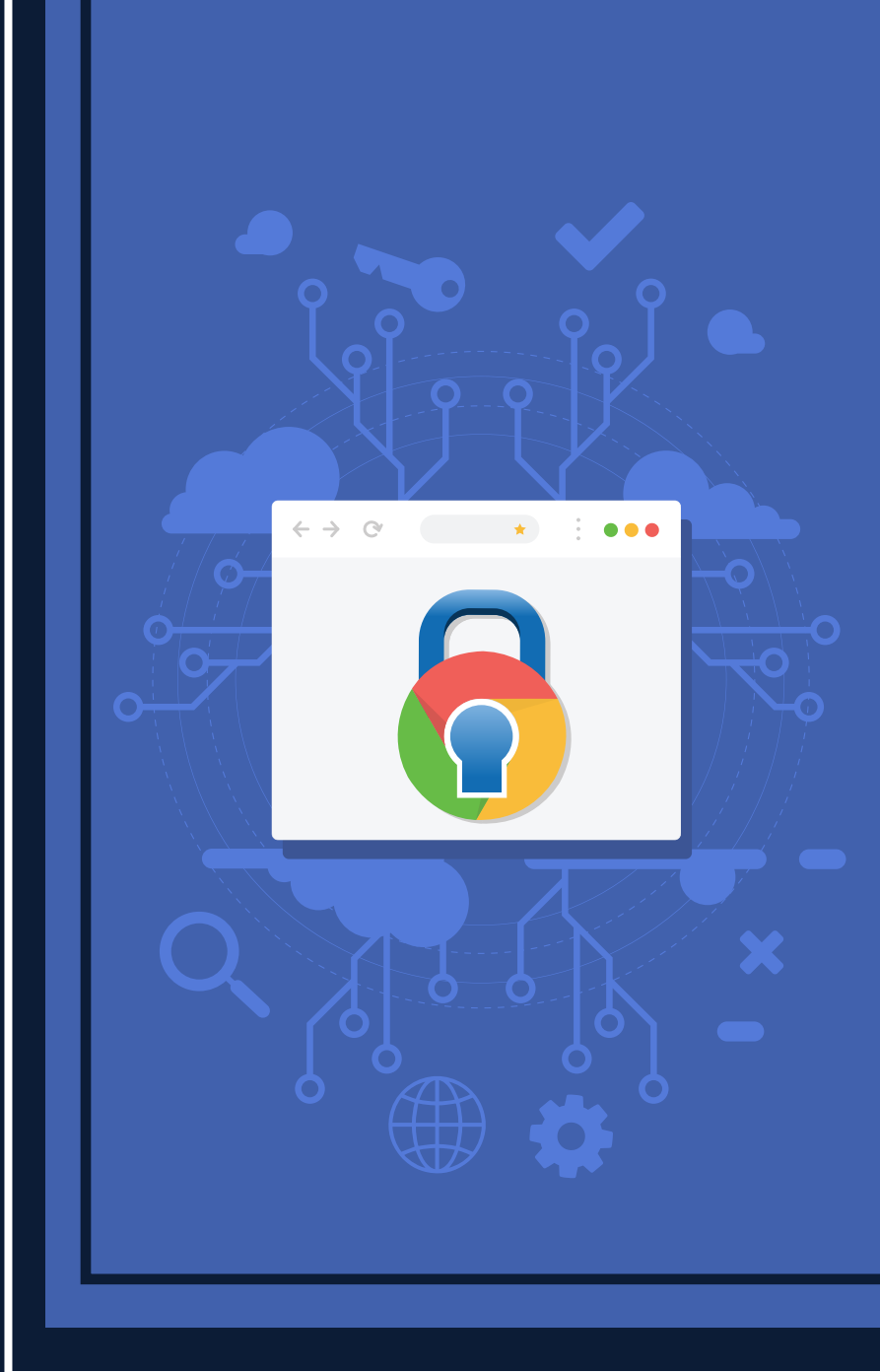


CCN-CERT BP/19



Recomendaciones de seguridad en Google Chrome

INFORME DE BUENAS PRÁCTICAS

MAYO 2021

Edita:



Centro Criptológico Nacional, 2021

Fecha de edición: mayo de 2021

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional	4
2. Introducción	5
3. Navegador web Google Chrome	6
3.1 Versiones	7
3.2 Requisitos mínimos	8
3.3 Descarga	10
3.4 Instalación	11
3.5 Aplicación de configuraciones de seguridad	14
3.6 Directrices de configuración	15
3.6.1 Sección Google y tú	17
3.6.2 Sección autocompletar	17
3.6.3 Sección privacidad y seguridad	19
3.6.4 Sección sistema	21
4. Lista de comprobación	25
5. Decálogo de recomendaciones	26
Anexo A. Archivo de configuración de seguridad	28

1. Sobre CCN-CERT, CERT Gubernamental Nacional

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

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

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

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

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

2. Introducción

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

Para ello, se proporciona un archivo de configuración para aplicar medidas de seguridad y así facilitar la posibilidad de implementar seguridad.

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

En el desarrollo de esta guía se ha utilizado el instalador del programa *Google Chrome* en su **versión 89.0.4389** para sistemas operativos Windows.

3. Navegador web Google Chrome

***Google Chrome* está disponible para su descarga de manera gratuita desde la página web de Google.**

El instalador se descarga y necesita tener conexión a internet para el proceso de instalación del navegador. Si el equipo en el que se instalara *Google Chrome* no tiene conexión a internet se necesitará realizar la descarga completa en el enlace alternativo proporcionado por *Google* a tal efecto.

En este sentido, *Google Chrome* debe tener instaladas las últimas actualizaciones de *software* relacionadas con la seguridad. Para ello, se aconseja determinar el método de actualización (por ejemplo, conexión a un servidor *WSUS*, procedimiento local, actualización automática, etc.) ya que, si no se aplican las últimas actualizaciones de *software* relacionadas con la seguridad de Chrome, esto se consideraría un **fallo crítico de seguridad**.

3.1 Versiones

El navegador *Google Chrome* dispone de varias versiones. La elección de la versión a instalar dependerá del uso que se vaya a dar.



Chrome (Estable)

Es la **versión oficial**, aquella que utilizarán la mayoría de los usuarios. Esta versión siempre será la más estable dado que antes de su publicación es sometida a una completa batería de pruebas. Esta versión recibe actualizaciones menores cada tres (3) semanas y actualizaciones mayores cada seis (6) semanas.



Chrome Beta

Esta versión se caracteriza por ser una **versión previa a la estable**, donde se depuran los fallos antes de la publicación de la versión final. Dicha versión recibe actualizaciones menores todas las semanas y actualizaciones mayores cada seis (6) semanas.



Chrome Dev

Versión anterior a la beta y menos conocida ya que se utiliza principalmente por los **desarrolladores de Google** para las pruebas de las actualizaciones mayores. En esta versión se finalizan las mejoras o nuevas funciones más importantes que estarán disponibles en la siguiente versión. Esta versión contiene errores, fallos y/o problemas de compatibilidad, lo que la convierte en una versión inestable. Esta versión recibe actualizaciones una o dos veces por semana debido a que muchas de sus funcionalidades están aún en fase de desarrollo.

3. Navegador web Google Chrome



Chrome Canary

Esta versión **cuenta con los últimos cambios**, las nuevas funcionalidades, nuevas herramientas y más opciones, pero **otorgando cierta inestabilidad** al navegador.

Esto lleva a una versión **destinada a identificar los problemas de las nuevas características**, lo que la convierte en una versión muy inestable. Esta versión se genera automáticamente en los servidores de Google con los cambios realizados en el código del navegador a diario. No se recomienda su uso, pero se puede descargar.



Chrome Empresarial

Esta versión es el mismo navegador Chrome que se utiliza en la versión estable. La diferencia está en cómo se despliega y se administra. Los **administradores de TI pueden descargar esta versión** para instalar el navegador Chrome a través de un instalador MSI **y administrar los navegadores Chrome de su organización** mediante las políticas de grupo (actualmente existen más de 200 políticas).

Para conocer la versión de *Google Chrome* instalada en un dispositivo siga los siguientes pasos:

Haga clic sobre el botón , ubicado en la parte superior derecha del navegador. A continuación, seleccione la opción "**Configuración**" y posteriormente en la siguiente ventana, en la parte inferior izquierda, pinche izquierda "**Información de Chrome**". El número de la versión instalada se mostrará debajo del nombre de *Google Chrome*, tal y como se muestra en la siguiente imagen:

Descripción

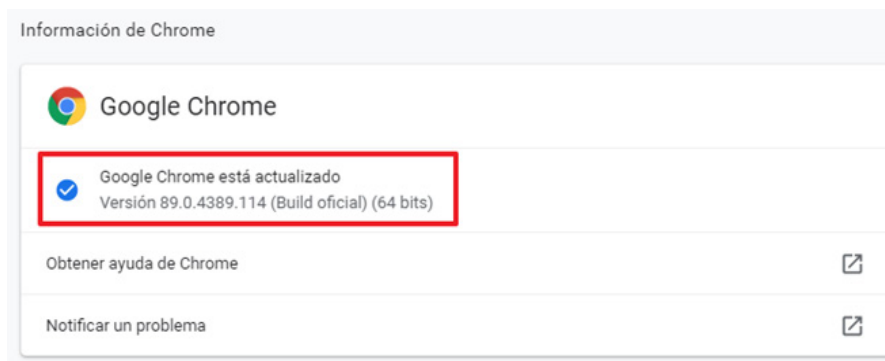
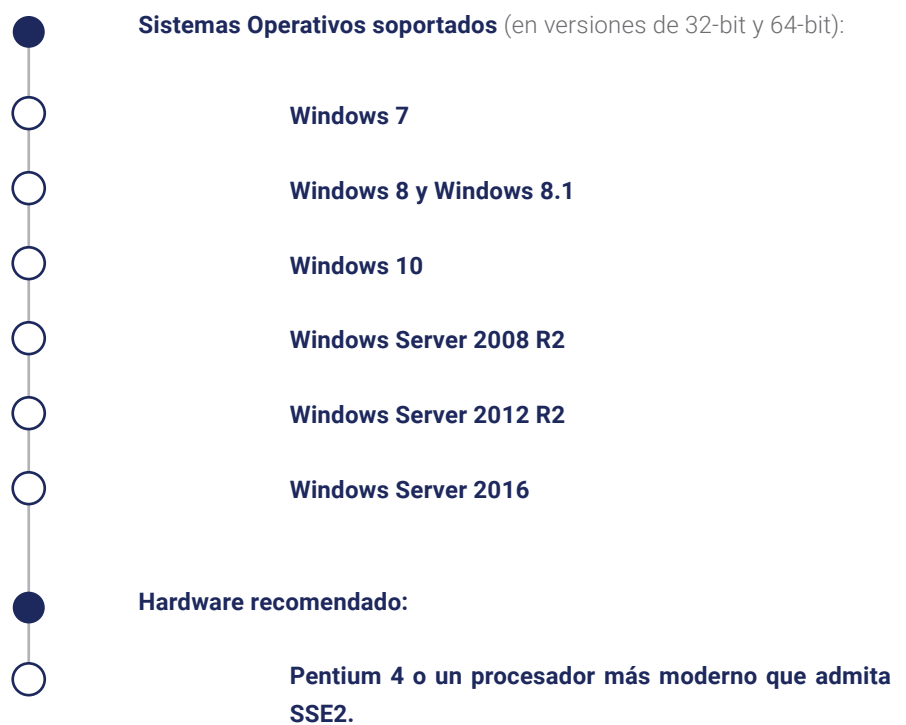


Figura 1

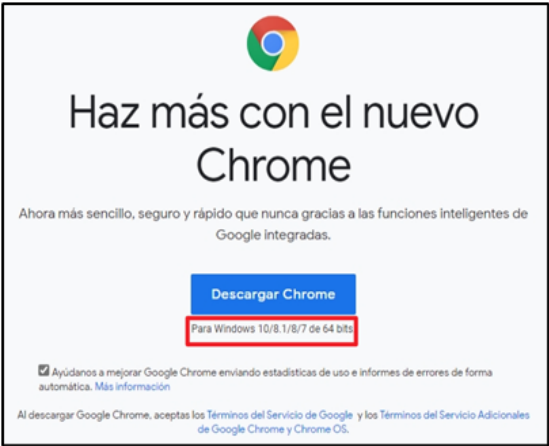
3.2 Requisitos mínimos

A continuación, se detallan los requisitos mínimos necesarios del sistema para realizar la implementación del programa *Google Chrome* en Windows.

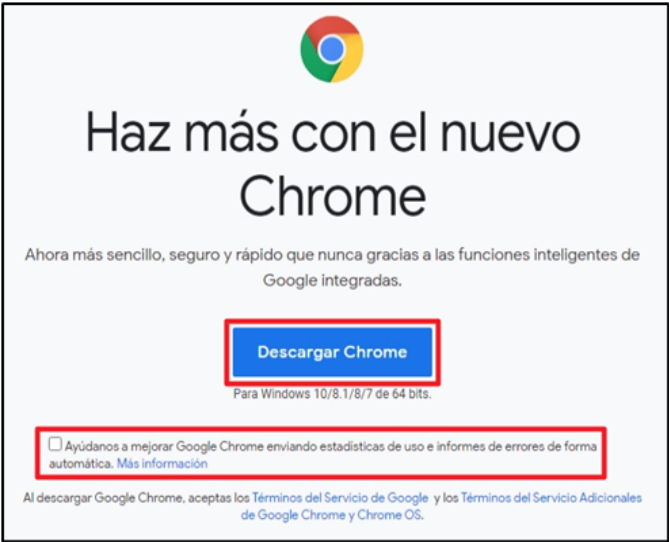


3.3 Descarga

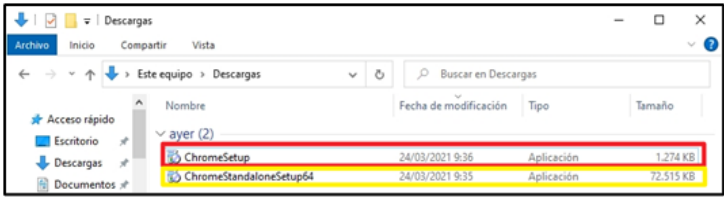
A continuación, se detallan los **requisitos mínimos necesarios** del sistema para realizar la implementación del programa *Google Chrome* en **Windows**.

Paso	Descripción
1.	Para la descarga del programa desde la fuente oficial se utilizará el siguiente enlace: https://www.google.com/chrome/browser/desktop/index.html
2.	La web de descarga detecta automáticamente el sistema operativo instalado en el equipo y la arquitectura de dicho sistema operativo (32 o 64 bits) adecuando las opciones de instalación tal y como se muestra en la siguiente imagen:  Figura 2

3. Navegador web Google Chrome

Paso	Descripción
3.	Desmarque la opción “Ayúdanos a mejorar Google Chrome enviando estadísticas de uso e informes de errores de forma automática”. Posteriormente, pulse sobre el botón “Descargar Chrome”.  Figura 3
4.	Una vez acabada la descarga aparecerá la siguiente imagen en su navegador:  Figura 4

3. Navegador web Google Chrome

Paso	Descripción
5.	El archivo descargado aparecerá en la ubicación que se haya determinado en pasos anteriores. El recuadro rojo corresponde a la descarga normal del instalador. El recuadro amarillo corresponde a la descarga para equipos sin conexión a internet.  Figura 5

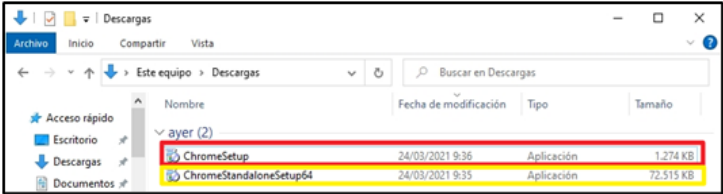
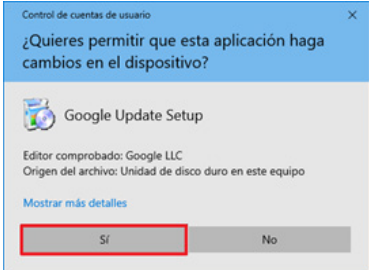
Nota: Existe una versión para equipos que no disponen de conexión a internet. Se puede acceder a su descarga desde el enlace oficial:



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

El proceso de descarga es el mismo que el de la descarga normal, salvo que en este caso **el archivo a descargar es de mayor tamaño** y llevará **más tiempo su descarga**.

3.4 Instalación

Paso	Descripción
1.	Ejecute el archivo descargado haciendo doble clic sobre él, ya sea la versión que necesita conexión a internet o la versión sin conexión a internet.  Figura 6
2.	Para comenzar con la instalación <i>Google Chrome</i> necesita de su autorización. Para ello, pulse “Sí” en la siguiente ventana emergente.  Figura 7
3.	Una vez permita la ejecución del programa se instalará automáticamente. Nota: La instalación de <i>Google Chrome</i> no permite la personalización de la ruta de instalación.

3. Navegador web Google Chrome

3.5 Aplicación de configuraciones de seguridad

El archivo "*master_preferences*" ubicado en "**C:\ProgramFiles\Google\Chrome\Application**" sirve para personalizar la instalación de *Chrome* en entorno empresarial. Si se instala una versión *Chrome* empresarial, además de poder personalizar la instalación mediante el archivo "*master_preferences*", se pueden utilizar plantillas administrativas a través de la edición de directivas de grupo (GPO) en un controlador de dominio Windows Server.

Google Chrome dispone de un fichero de configuración llamado "*Preferences*" donde se almacenan las opciones seleccionadas por el usuario en este navegador. Este fichero se encuentra ubicado en la ruta:

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

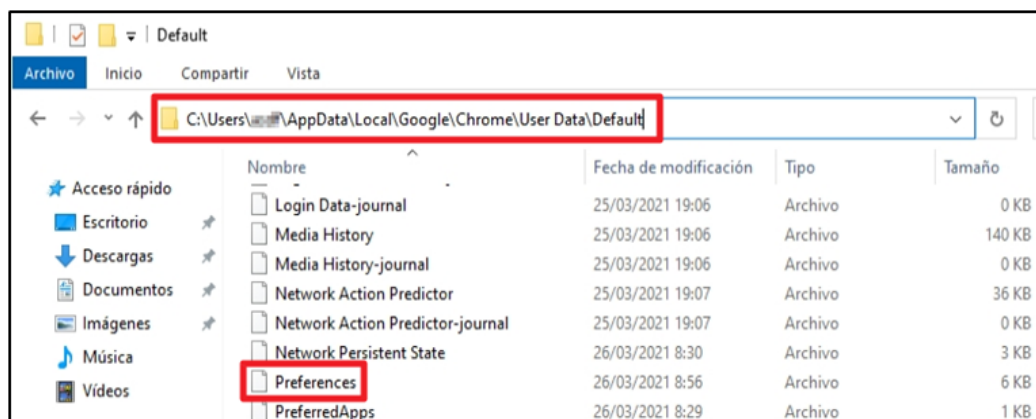


Figura 8

3. Navegador web Google Chrome

Para hacer uso del archivo suministrado junto a esta guía, deberá reemplazar el fichero creado durante la instalación de *Google Chrome*. Para esto se deberá copiar el fichero "**Preferences**" dentro de la carpeta "Scripts" y sustituirlo en la ruta citada anteriormente.

Este fichero cambiará las opciones marcadas y desmarcadas con los valores de las configuraciones recomendadas en el apartado "**3.6. DIRECTRICES DE CONFIGURACIÓN**" de esta guía. Las configuraciones de personalización de rutas, de páginas web y otro tipo de opciones no se verán afectadas. Si se desea personalizar alguna de estas **configuraciones personalizadas** (como la URL de inicio, por ejemplo) se deberán configurar manualmente en el navegador *Google Chrome*.

3.6 Directrices de configuración

El navegador *Google Chrome* dispone de una interfaz gráfica para la edición de las **opciones del navegador**. Para acceder a esta interfaz se debe hacer clic sobre el botón , ubicado en la parte superior derecha del navegador, y a continuación, seleccionar la opción “Configuración” donde aparecerán las opciones de configuración editables por el usuario.

Un método alternativo para acceder a la interfaz de configuración es escribir **chrome://settings/** en la barra de direcciones y pulsar la tecla “Enter”.

3.6.1 Sección Google y tú

El navegador *Google Chrome* permite la **sincronización automática con servicios de Google**, permitiendo a los usuarios, entre otros, sincronizar automáticamente varios elementos como **marcadores**, **pestañas abiertas**, **contraseñas**, **complementos**, etc. Esta información se almacena en la cuenta de Google proporcionada por el usuario a tal efecto.



Para evitar problemas de privacidad y seguridad se recomienda deshabilitar esta funcionalidad del navegador.

3. Navegador web Google Chrome

Se recomienda seguir los siguientes pasos:

Localice la sección de “Google y tú” y se hace clic en la parte de **Sincronización y servicios de Google**, tal y como aparece en la siguiente imagen:

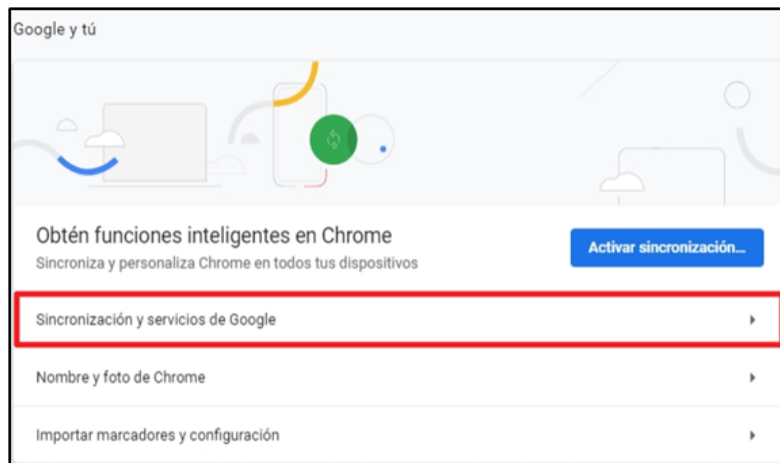


Figura 9

En este apartado desmarque las opciones “Permitir el inicio de sesión en Chrome” y “Autocompletar búsquedas y URLs”, tal y como se muestra en la siguiente imagen:

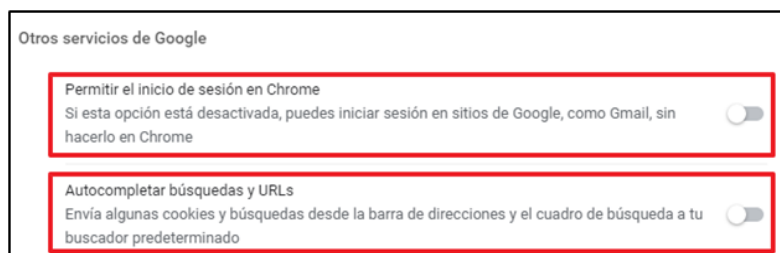


Figura 10

Estos cambios requieren el **reinicio del navegador**, tal y como muestra el aviso en la parte inferior de la pantalla.

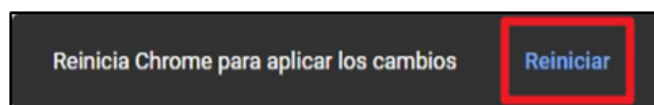


Figura 11

3. Navegador web Google Chrome

3.6.2 Sección autocompletar

Debido a la forma en la que se almacenan las credenciales, **es posible que un atacante malicioso pueda obtener acceso a las cuentas** del usuario y/o utilizar las credenciales almacenadas para inicios de sesión no deseados.

Para evitar estos usos indebidos **se recomienda deshabilitar las siguientes opciones:**

En la sección “Google y tú” localice la sección de “Autocompletar” y haga clic en la parte de contraseñas, tal y como muestra la imagen:



Figura 12

En este apartado **desmarque las opciones** “Preguntar si quiero guardar contraseñas” e “iniciar sesión automáticamente”, como se muestra a continuación:

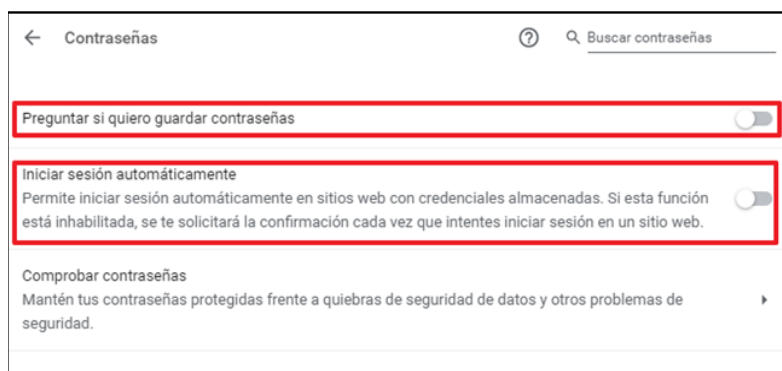


Figura 13

3. Navegador web Google Chrome

La información referente a los **medios de pago** es un elemento atractivo para los atacantes buscando hacer un **uso fraudulento de la misma** y, por ello, **se recomienda no tener almacenada esta información** en el navegador Google Chrome para evitar ser objeto de ataques maliciosos.

Se recomienda realizar los siguientes pasos:

- Dentro de la sección “Autocompletar”, haga clic en el apartado de métodos de pago, como se muestra en la imagen.

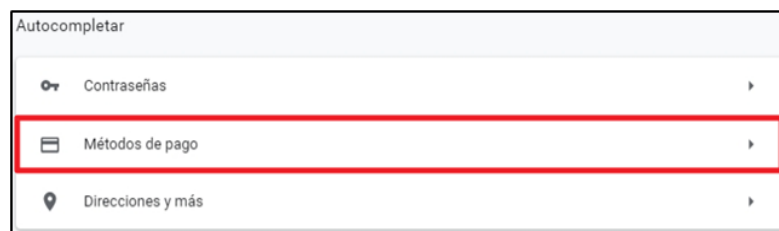


Figura 14

- En este apartado **desmarque las opciones** “Guardar y autocompletar métodos de pago” y “Permitir a los sitios comprobar si tienes métodos de pago guardados” siguiendo de referencia la siguiente imagen.

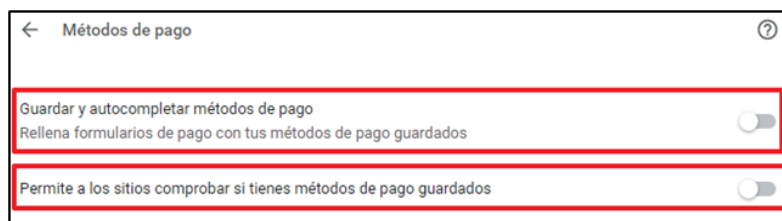


Figura 15

La información referente a los medios de pago es un elemento atractivo para los atacantes y se recomienda no tener almacenada esta información en el navegador Google Chrome.

3. Navegador web Google Chrome

3.6.3 Sección privacidad y seguridad

La configuración de las cookies¹ y los envíos de **información en segundo plano** son una parte muy importante para la seguridad y privacidad. Con una configuración segura de estos elementos se pueden prevenir brechas de seguridad y posibles robos de información sensible, ya que un atacante podría ocultar la ejecución de código malicioso mediante el tráfico en segundo plano del navegador.

Para evitar estos riesgos, se recomienda la siguiente configuración para el navegador *Google Chrome*:

En la sección de “Privacidad y seguridad”, en el panel izquierdo de la página, haga clic en el apartado “Cookies y otros datos de sitios”, tal y como se muestra a continuación:



Figura 16

Se deben definir algunas configuraciones para que cuando se termine de navegar, y se proceda al cierre del navegador, **se eliminen los archivos generados por el navegador durante su ejecución**. Esto favorece la carga, en siguientes ocasiones cuando se visite el sitio, de las últimas versiones de las páginas visitadas, así como la configuración actualizada para el sitio web mejorando así la seguridad general de la navegación.

¹. Archivo generado por un servidor web y que guarda datos de la navegación para hacer que la experiencia del usuario sea más sencilla con información sobre sus preferencias y pautas de navegación.

3. Navegador web Google Chrome

Para poder proceder a estas configuraciones acceda al apartado “Cookies y otros datos de sitios” en la sección izquierda del navegador. Una vez allí, **marque las siguientes opciones** tal y como aparece en la imagen:

- » **Bloquear cookies de terceros en incognito.**
- » **Borrar las cookies de terceros.**
- » **Borrar las cookies y los datos de sitios al salir de Google Chrome.**
- » **Enviar una solicitud de no seguimiento con tu tráfico de navegación.**

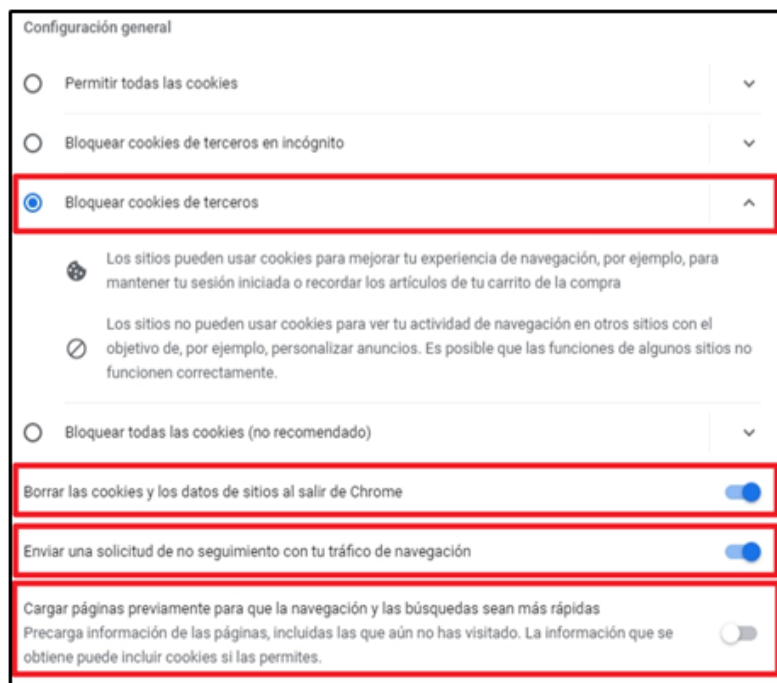


Figura 17

Nota: Hay algunas páginas que necesitan cookies de terceros para su correcto funcionamiento. Si se detecta que una página no funciona como se espera, es posible que se necesite habilitar las cookies de terceros para su correcto funcionamiento. Una vez se concluya el uso de la web que necesita las cookies de terceros, habrá que volver a habilitar el bloqueo estas cookies.

3. Navegador web Google Chrome

Dentro de la sección “*Privacidad y seguridad*”, concretamente en el apartado “*Seguridad*” se recomienda activar la pestaña llamada “*Protección mejorada*”. Esta protección que ofrece el navegador Google Chrome incluye, entre otros, las siguientes características:

- » **Predicción y aviso de eventos peligrosos antes de que ocurran.**
- » **Protección al usar Google Chrome y permite mejorar la seguridad al usar otras aplicaciones de Google cuando se haya iniciado sesión.**
- » **Mejora la seguridad y la del resto de usuarios en internet.**
- » **Avisa si las contraseñas guardadas se ven expuestas en una brecha de seguridad de datos.**
- » **Envía las URL al modo de Navegación segura para que se comprueben.**
- » **Envía cierta información de la navegación para contribuir a detectar nuevas amenazas.**

Para obtener esta protección **deberá activar la opción** “*Protección mejorada*” tal y como se muestra en la siguiente imagen.

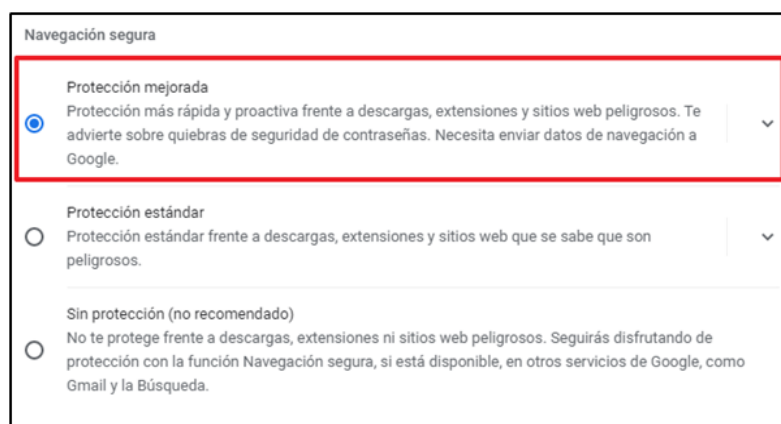


Figura 18

3. Navegador web Google Chrome

Para terminar las configuraciones dentro del apartado de “*Privacidad y seguridad*”, se deberán cambiar algunos aspectos para evitar ataques en ventanas minimizadas, ventanas en segundo plano, y ejecuciones de código mediante *JavaScript*, que normalmente se utilizan para realizar ataques maliciosos.

Para limitar lo indicado anteriormente, acceda al apartado “*Configuración de sitios*” tal y como se muestra a continuación:

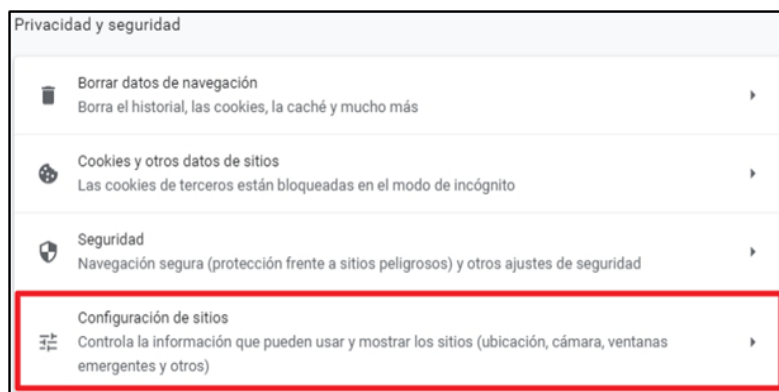


Figura 19

En este apartado modifique los aspectos referentes a “*Sincronización en segundo plano*” y “*JavaScript*”, de tal modo que bloqueen o no permitan dichas funcionalidades, tal y como aparece en la siguiente imagen:

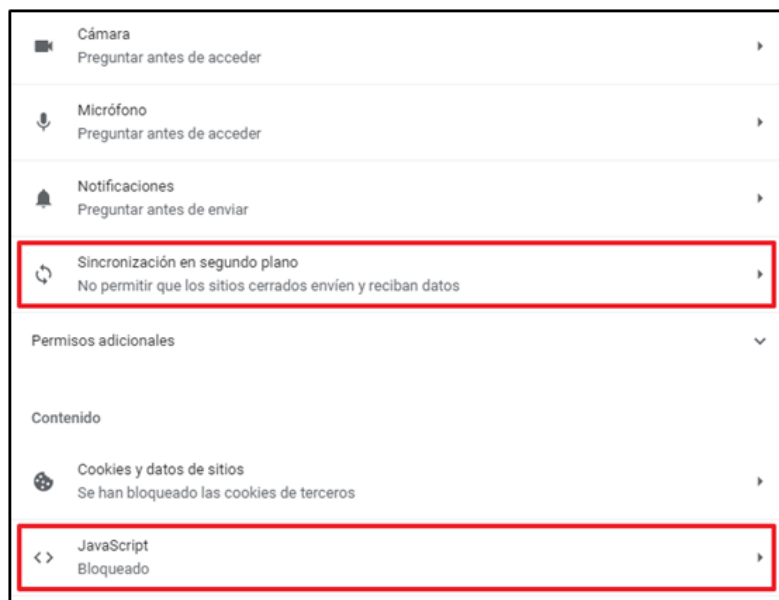


Figura 20

3. Navegador web Google Chrome

Nota: Hay algunas páginas que necesitan JavaScript para su correcto funcionamiento. Si se detecta que una página no funciona correctamente, es posible que necesite habilitar JavaScript para su correcto funcionamiento. Si necesita tener activado el uso del JavaScript, se recomienda la instalación de la última versión de Java, con las últimas actualizaciones de seguridad. Se puede acceder a esta descarga en el siguiente enlace:



Enlace: <http://www.java.com/es/download/manual.jsp>

3.6.4 Sección sistema

Como ya se ha comentado en puntos anteriores, la **ejecución de código en segundo plano** después del cierre del navegador *Google Chrome*, es susceptible de uso para ataques maliciosos y deben ser deshabilitados.



En la sección de "Sistema", dentro de la pestaña "Configuración avanzada" en el panel izquierdo de la página de "Configuración", deshabilite la opción "Seguir ejecutando las aplicaciones en segundo plano al cerrar Google Chrome", como se muestra en la siguiente imagen.

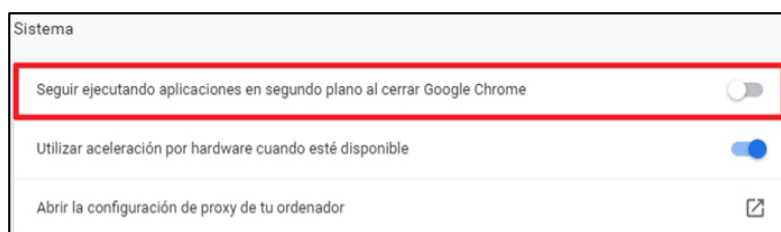


Figura 21

4. Lista de comprobación

Criticidad	Descripción
Alta	<i>Google Chrome</i> debe tener instaladas las últimas actualizaciones de software relacionadas con la seguridad.
Media	Las preferencias de seguridad requeridas por <i>Google Chrome</i> pueden ser cambiadas por el usuario.
Media	<i>Google Chrome</i> está configurado para actualizarse de forma automática.
Media	<i>Google Chrome</i> no está configurado para proporcionar advertencias cuando un usuario cambia de una página segura (habilitada para SSL) a una página no segura.
Media	<i>Google Chrome</i> está configurado para bloquear ventanas emergentes.
Media	<i>Google Chrome</i> está configurado para utilizar cuentas de Google y poder iniciar sesión en los servicios de Google con una cuenta proporcionada por el usuario.
Media	<i>Google Chrome</i> está configurado para autocompletar búsquedas y URLs, enviando información al buscador predeterminado.
Media	<i>Google Chrome</i> está configurado para preguntar si se quieren guardar las contraseñas de los sitios.
Media	<i>Google Chrome</i> está configurado para iniciar sesión automáticamente en las webs que tiene las credenciales almacenadas.
Media	<i>Google Chrome</i> está configurado para guardar y autocompletar métodos de pago, rellenando los formularios automáticamente con estos datos.
Media	<i>Google Chrome</i> está configurado para permitir que los sitios web comprueben si hay métodos de pago guardados.
Media	<i>Google Chrome</i> está configurado para bloquear las cookies de terceros solo cuando se navega en modo incógnito.
Media	<i>Google Chrome</i> está configurado para precargar información de las páginas, incluso sin haberlas visitado. Esta precarga puede incluir cookies si están permitidas.
Media	<i>Google Chrome</i> está configurado para permitir que las páginas cerradas terminen de enviar y recibir datos.
Media	<i>Google Chrome</i> está configurado para permitir el uso de JavaScript.
Media	<i>Google Chrome</i> está configurado para seguir ejecutando aplicaciones en segundo plano al cerrar <i>Google Chrome</i> .

5. Decálogo de recomendaciones

A continuación, se indican diez (10) recomendaciones de seguridad en el uso de *Google Chrome*.



Decálogo de seguridad para Google Chrome

1

Se recomienda **utilizar siempre la versión estable más actual** y con las **últimas actualizaciones**.

2

Se recomienda la **revisión de las funciones relativas a la seguridad del software**, dado que proporcionará una mejor defensa contra posibles ataques.

3

Si se necesita **instalar complementos**, se recomienda la utilización de **fuentes oficiales** y/o confiables.

4

Se recomienda **no usar el almacén de contraseñas disponible en Google Chrome**, en su lugar se recomienda el **uso de otras aplicaciones** que implementen un sistema de cifrado robusto, para guardar las contraseñas de forma más segura.

5

Se recomienda **observar el botón de identidad del sitio** (un candado que se encuentra en la barra de direcciones, a la izquierda de esta) para descubrir de forma rápida y sencilla si **la conexión a la página está cifrada** y, en algunos casos, quién es el propietario. Esta información ayuda a la detección de páginas maliciosas.

6

Se recomienda **utilizar siempre protocolos seguros (https)**, más aún cuando se utilicen datos personales para asegurar las comunicaciones de extremo a extremo.

7

Se recomienda el **uso de software de cifrado para enviar información personal**, como medida de seguridad adicional, incluso con la utilización protocolos seguros tales como https.

8

Se recomienda el **uso del doble factor de autenticación** para el uso de servicios online. Esto añade una capa adicional de seguridad a las cuentas debido a que será necesario una verificación adicional en el inicio de sesión (SMS, llamada telefónica, autenticadores, etc.).

9

Se recomienda **borrar las cookies y bloquear la navegación en segundo plano** para evitar que algunos sitios web rastreen patrones de búsqueda y así salvaguardar la privacidad del usuario.

10

Se recomienda **limpiar la caché y eliminar los archivos temporales de internet** para solucionar problemas habituales con los sitios web.



Figura 22. Decálogo de recomendaciones

Anexo A.

Archivo de configuración de seguridad

Para facilitar la aplicación del refuerzo de estas medidas de seguridad sobre *Google Chrome*, se incluye adjunto al documento un archivo “*Preferences*” para la configuración inicial del navegador. Todas estas configuraciones son modificables por el usuario y se almacenarán en la carpeta por defecto del navegador.

Acuda al apartado “**3.5. APLICACIÓN DE CONFIGURACIONES DE SEGURIDAD**” para conocer cómo implantar este archivo de configuración dentro de *Google Chrome*.



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es