

Guía de Seguridad CCN-CERT BP/26

Informe de buenas prácticas

BP/26 Recomendaciones de seguridad en Microsoft Edge



JUNIO 2022



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022

Fecha de Edición: junio de 2022

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

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.

cpage.mpr.gob.es

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

junio de 2022

Esperanza Casteleiro Llamazares
Secretaria de Estado
Directora del Centro Criptológico Nacional

INDICE

1. INTRODUCCIÓN	5
2. NAVEGADOR WEB MICROSOFT EDGE	5
2.1 VERSIONES	6
2.2 REQUISITOS MÍNIMOS	9
2.3 DESCARGA.....	10
2.4 INSTALACIÓN Y CONFIGURACIÓN INICIAL.....	11
2.5 DIRECTRICES DE CONFIGURACIÓN	15
2.5.1 SINCRONIZACIÓN Y AJUSTES BÁSICOS DE IDIOMA	15
2.5.2 SECCIÓN PERFILES.....	17
2.5.3 SECCIÓN PRIVACIDAD, BUSQUEDA Y SERVICIOS.....	19
2.5.4 SECCIÓN PÁGINA DE INICIO, PÁGINA PRINCIPAL Y NUEVAS PESTAÑAS	26
2.5.5 SECCIÓN COOKIES Y PERMISOS DEL SITIO	26
2.5.6 SECCIÓN SISTEMA Y RENDIMIENTO	30
3. LISTA DE COMPROBACIÓN.....	31
4. DECÁLOGO DE RECOMENDACIONES	32

1. INTRODUCCIÓN

El propósito de este documento consiste en establecer los procedimientos y utilidades necesarias para implementar y garantizar la seguridad en Microsoft Edge, frente a los riesgos a los que este pueda estar expuesto.

Para ello, se proporciona una serie de pasos e instrucciones que permitan la configuración adecuada del navegador de forma manual. Así mismo se proporciona un archivo de configuración para aplicar medidas de seguridad y así facilitar la posibilidad de implementar seguridad.

En el desarrollo de esta guía se ha utilizado el instalador del programa **Microsoft Edge Stable** en su **Versión 102.0.1245.33 (Compilación oficial 64 bits)** para sistemas operativos Windows. Esta configuración también es válida para la versión Microsoft Edge Business.

Independientemente de la versión elegida, versión Stable o versión Business de Microsoft Edge, ambas corresponden con la misma compilación, con la única diferencia de que la versión Business no necesita conexión a internet para su instalación.

2. NAVEGADOR WEB MICROSOFT EDGE

Microsoft Edge inicialmente fue compilado con los motores **EdgeHTML** y **Chakra** propios de Microsoft. En 2019, Microsoft Edge pasó a ser reconstruido como un navegador basado en **Chromium**, utilizando los motores **Blink** y **V8**. Estos motores, aportan mayor seguridad y mejor apariencia.

Microsoft Edge sustituirá al navegador Internet Explorer en los entornos Windows como navegador predeterminado a partir de la distribución 1709 de Windows 10 y en su nuevo sistema operativo Windows 11.

Nota: Es posible obtener información adicional sobre la finalización del soporte en Internet Explorer 11 y la sustitución por Microsoft Edge a través del siguiente enlace:

<https://blogs.windows.com/windowsexperience/2021/05/19/the-future-of-internet-explorer-on-windows-10-is-in-microsoft-edge/>

Microsoft Edge está disponible para su descarga de manera gratuita desde la página web de Microsoft. De igual modo este viene desplegado por defecto en los sistemas operativos Windows 10 y Windows 11 sin necesidad de descarga.

Para descargar el instalador se necesita tener conexión a internet, al igual que para el proceso de instalación del navegador. Si el equipo en el que se instala Microsoft Edge no tiene conexión a internet, se necesitará realizar la descarga completa del navegador a través de la versión **“Business”** de este, por medio del enlace alternativo proporcionado por Microsoft a tal efecto.

Nota: La descarga del navegador se realizará más adelante, concretamente en el punto **“2.3 DESCARGA”**. No obstante se procede a indicar a continuación un enlace de descarga del propio fabricante sobre la versión Business de este, dado que la guía está basada en la versión Stable del navegador:

<https://www.microsoft.com/es-es/edge/business/download>

También se puede instalar y actualizar el navegador Microsoft Edge desde la herramienta **“Windows Update”** del sistema operativo Windows, manualmente descargando la última versión desde la web de Microsoft o desde el propio panel de configuración de Microsoft Edge.

En este sentido, Microsoft Edge debe tener instaladas las últimas actualizaciones de software relacionadas con la seguridad. Si no se aplican las últimas actualizaciones de software relacionadas con la seguridad de Microsoft Edge, esto se consideraría un **fallo crítico de seguridad**.

2.1 VERSIONES

Microsoft Edge ofrece una cadencia de ciclo de lanzamiento principal de cuatro (4) semanas, pero la duración efectiva del soporte asistido para una versión de canal estable es de aproximadamente doce (12) semanas.

Nota: Puede obtener información adicional sobre el ciclo de vida del producto a través del siguiente enlace: <https://docs.microsoft.com/es-es/deployedge/microsoft-edge-support-lifecycle>

Las actualizaciones de seguridad y las actualizaciones de mantenimiento solo están disponibles en la versión más reciente de la versión “**Stable**” y la última versión del canal “**Beta**”. Si usa versiones anteriores de Microsoft Edge, es probable que se pierda las últimas actualizaciones de calidad y seguridad.

A continuación, se resumen las diferentes versiones existentes para Microsoft Edge:

- a) **Microsoft Edge:** El canal estable está diseñado para una amplia implementación en la organización y es el canal en el que la mayoría de los usuarios deberían estar. Es la más extendida de las versiones y es el resultado de la estabilización del conjunto de funciones disponibles, en la versión anterior del Canal Beta. Las nuevas características se envían aproximadamente cada 4 semanas. Las actualizaciones de seguridad y calidad se envían según sea necesario.



- b) **Microsoft Edge BETA:** El Canal Beta está destinado a la implementación de pruebas en producción para un conjunto representativo de usuarios. Este canal brinda una gran oportunidad para validar que las configuraciones o necesidades funcionan como se espera en un entorno. Si encuentra un problema, es posible solucionarlo antes de que se publique el lanzamiento en el canal estable. Al igual que la versión de Microsoft Edge las nuevas características se envían aproximadamente cada 4 semanas. Las actualizaciones de seguridad y calidad se envían según sea necesario.



- c) **Microsoft Edge DEV:** El canal DEV está destinado para ayudar a planificar y desarrollar las actualizaciones más recientes de Microsoft Edge, pero con mayor calidad que el canal Canary. Este canal sirve para echar un vistazo anticipado a las novedades y prepararse para la próxima versión Beta.



- d) **Microsoft Edge Canary:** El canal Canary se actualiza a diario y es el más vanguardista de todos los canales. Si se desea acceder a las características más recientes, aparecerán aquí primero.

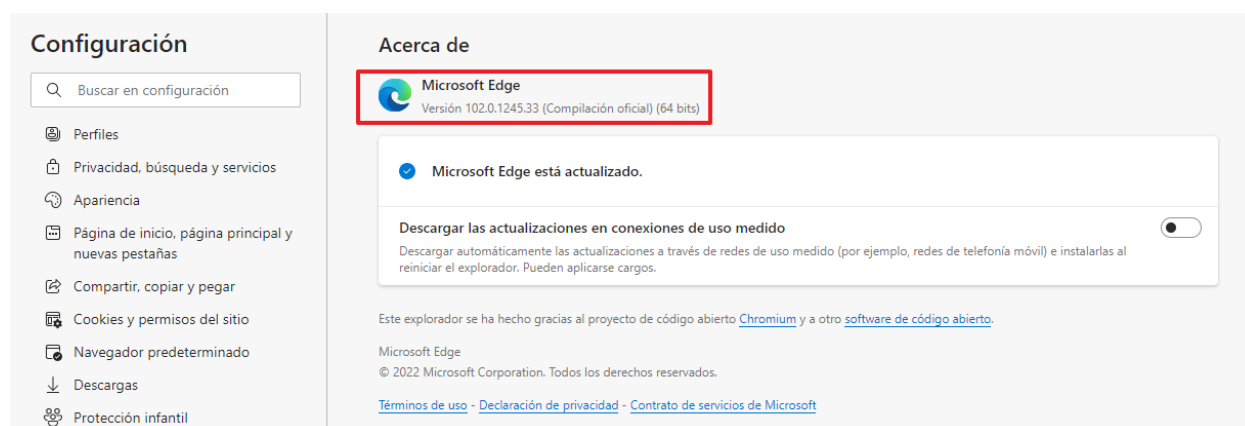


- e) **Microsoft Edge Business:** Esta versión es el mismo navegador Microsoft Edge que se utiliza en la versión Stable. La diferencia está en cómo se despliega y se administra. Los administradores de TI pueden descargar esta versión para instalar el navegador Microsoft Edge a través de un instalador **.msi** y administrar los navegadores de su organización mediante las políticas de grupo.



Para conocer la versión de Microsoft Edge instalada en un dispositivo, realice los siguientes pasos:

Inicie Microsoft Edge, y haga clic sobre el botón **...** ubicado en la parte superior derecha del navegador. A continuación, haga clic sobre **“Configuración”** en el panel que se desplegará. Posteriormente, sitúese en la sección **“Acerca de Microsoft Edge”**. El número de la versión instalada se mostrará debajo del nombre de Microsoft Edge, tal y como se muestra en la siguiente imagen:



2.2 REQUISITOS MÍNIMOS

A continuación, se detallan los requisitos mínimos necesarios del sistema para realizar la implementación del programa Microsoft Edge:

a) Sistemas operativos soportados (En versiones de 32-bit y 64 bit)

- i. Windows 7
- ii. Windows 8.1
- iii. Windows 10 Professional 1709 y versiones posteriores
- iv. Windows 10 Home 1709 y versiones posteriores
- v. Windows 10 Enterprise 2015 LTSC
- vi. Windows 10 Enterprise 2016 LTSC
- vii. Windows 10 Enterprise 2019 LTSC
- viii. Windows 11 Professional
- ix. Windows 11 Enterprise
- x. Windows 11 Home
- xi. Windows Server 2008 R2
- xii. Windows Server 2012
- xiii. Windows Server 2012 R2
- xiv. Windows Server 2016 (LTSC)
- xv. Windows Server 2019 (LTSC)
- xvi. Windows Server (SAC)
- xvii. MacOS Sierra 10.2 o superior
- xviii. iOS 11 o superior
- xix. Android KitKat4.4 o superior
- xx. Linux (Ubuntu, Debian, Fedora y openSUSE)

Nota: Puede consultar información adicional sobre los sistemas operativos compatibles a través del siguiente enlace oficial del fabricante: <https://docs.microsoft.com/es-es/deployedge/microsoft-edge-supported-operating-systems>

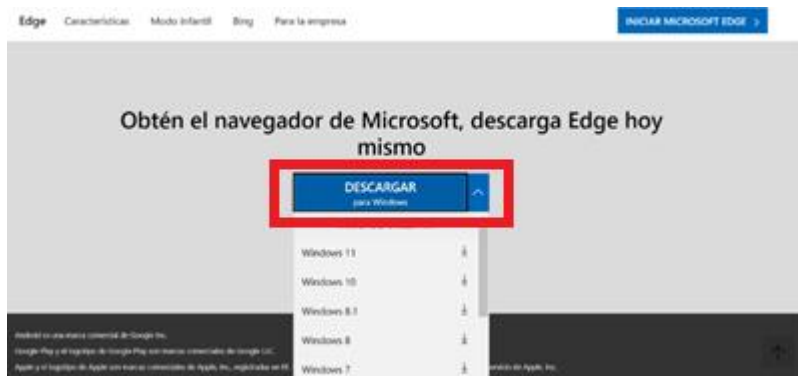
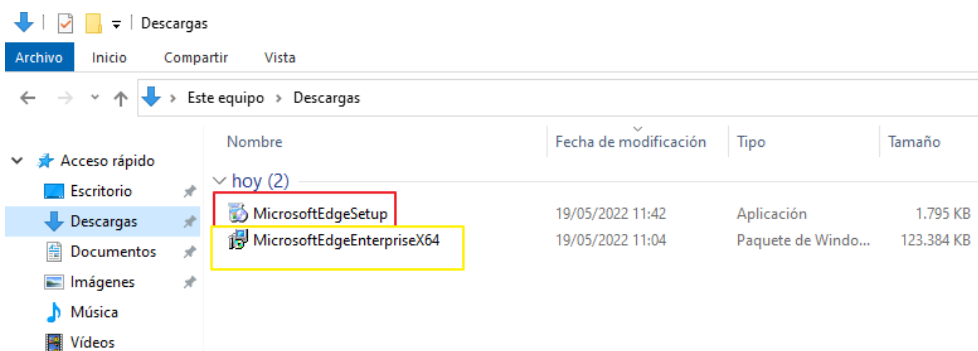
b) Requisitos hardware recomendados:

- i. Requisitos mínimos recomendados para el sistema operativo de 64 bits instalado.
- ii. Requisitos mínimos recomendados para el sistema operativo de 32 bits instalado.

2.3 DESCARGA

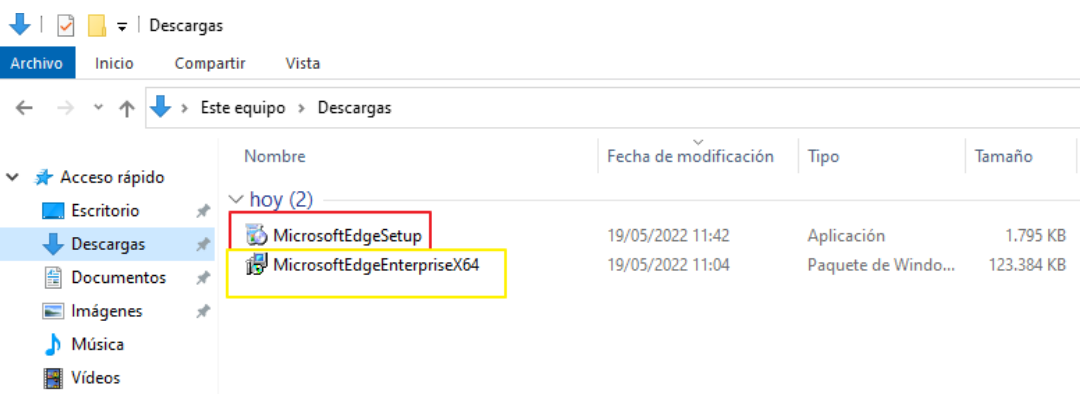
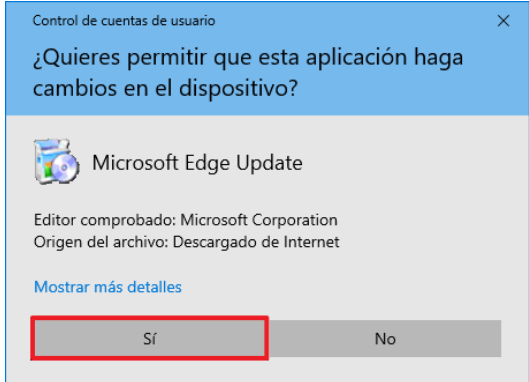
En algunos casos, como por ejemplo en los sistemas operativos Windows 10 en sus versiones Pro y Home, Microsoft Edge este ya se encuentra instalado por defecto e integrado junto al sistema operativo.

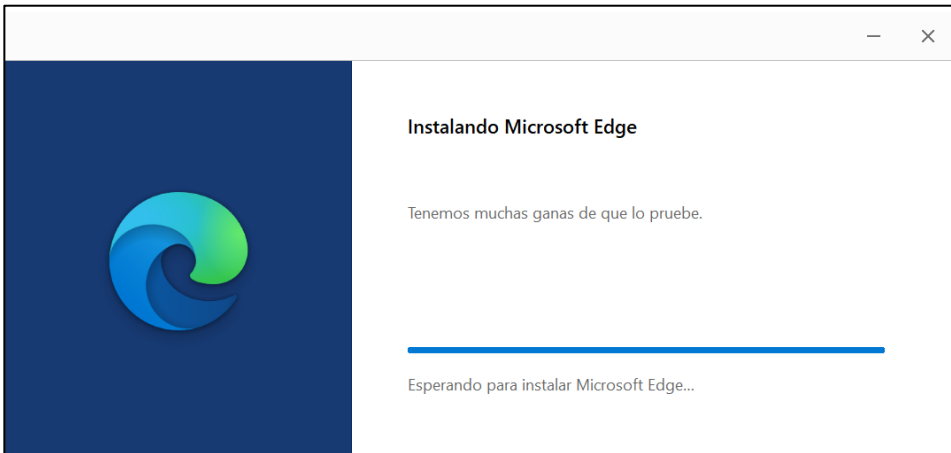
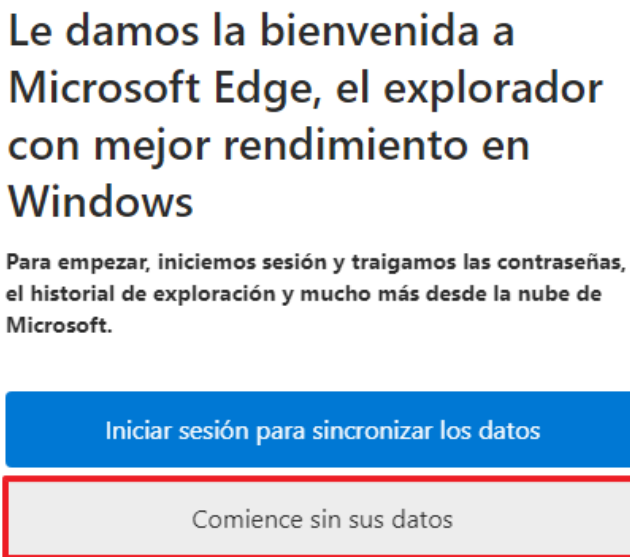
A continuación, se detalla el proceso a seguir para realizar la descarga del navegador Microsoft Edge, en equipos que no lo tengan instalado por defecto y sea requerido su instalación:

Paso	Descripción
1.	Para la descarga del programa desde la fuente oficial se utilizará el siguiente enlace: – https://www.microsoft.com/es-es/edge
2.	Descargue la versión del navegador en función de su sistema operativo. 
3.	El archivo descargado, aparecerá en la ubicación que se haya determinado, en función de la configuración establecida en el navegador que se esté usando. El recuadro rojo en la imagen corresponde a la descarga normal del instalador que requiere conexión a internet (Utilizado durante la guía). El recuadro amarillo en la imagen corresponde a la descarga para equipos sin conexión a Internet, en la que Microsoft Edge ofrece la solución Business para instalaciones offline. 

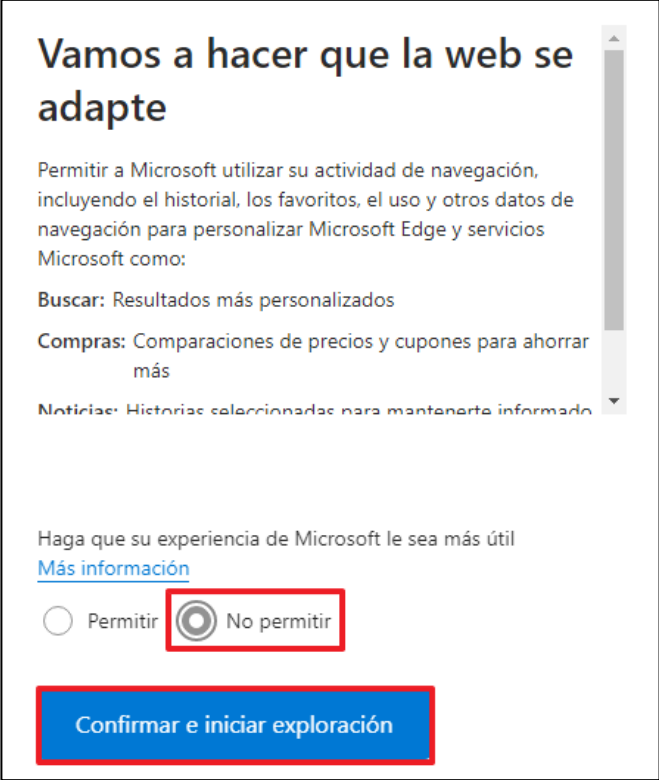
2.4 INSTALACIÓN Y CONFIGURACIÓN INICIAL

Para realizar la instalación de Microsoft Edge realice los siguientes pasos:

Paso	Descripción
1.	Ejecute el archivo descargado haciendo doble clic sobre él, ya sea en la versión que necesita conexión a internet (Utilizada durante esta guía) o la versión sin conexión a internet. 
2.	Para comenzar con la instalación de Microsoft Edge, se requiere la elevación de privilegios. Para ello, se debe pulsar en la opción “Sí” en la ventana emergente (“Control de cuentas de usuario”) o introducir el usuario con privilegios para instalar si así lo requiere. 

Paso	Descripción
3.	Una vez se permita la ejecución, se descargará e instalará automáticamente. 
4.	Tras finalizar la instalación, en el primer inicio, aparecerá una ventana de bienvenida donde se han de realizar configuraciones previas de seguridad.
5.	En la primera ventana de configuración de Microsoft Edge marque la opción “Comience sin sus datos”. 

Paso	Descripción
6.	En la segunda venta de configuración de Microsoft Edge maque la opción “Continuar sin estos datos”. Podemos ayudarle a importar sus datos de exploración de Google Si usa un explorador de Google con la sincronización activada, podemos ayudarle a importar sus marcadores, historial y mucho más desde Google para que esté listo para usar Microsoft Edge. Administrar Iniciar sesión en Google para continuar Continuar sin estos datos
7.	En la siguiente pantalla, configure el acceso a los datos de exploración recientes. Marque la opción “No permitir” para restringir dicho acceso y pulse sobre “Confirmar y continuar”. Tenga siempre acceso a los datos de exploración recientes. Incorpore periódicamente sus datos de exploración para estar siempre al día. Puede administrar sus preferencias en cualquier momento en Configuración Administrar ☐ Permitir ☒ No permitir Confirmar y continuar

Paso	Descripción
8.	Por último, en la configuración de la adaptación web marque la opción “No permitir” para impedir que Microsoft utilice la información de navegación. Pulse sobre “Confirmar e iniciar exploración”. 
9.	Posterior a dichas configuraciones se abrirán varias ventanas de exploración y una de ellas orientada a la personalización estética del navegador. Puede ignorarlas y continuar con el siguiente apartado.

2.5 DIRECTRICES DE CONFIGURACIÓN

El navegador Microsoft Edge dispone de una interfaz gráfica para la edición de sus opciones de uso y de seguridad.

Para acceder la interfaz de configuración se debe iniciar Microsoft Edge y hacer clic sobre el botón , ubicado en la parte superior derecha del navegador. A continuación, se debe seleccionar la sección **“Configuración”** donde aparecerán las opciones de configuración editables por el usuario.

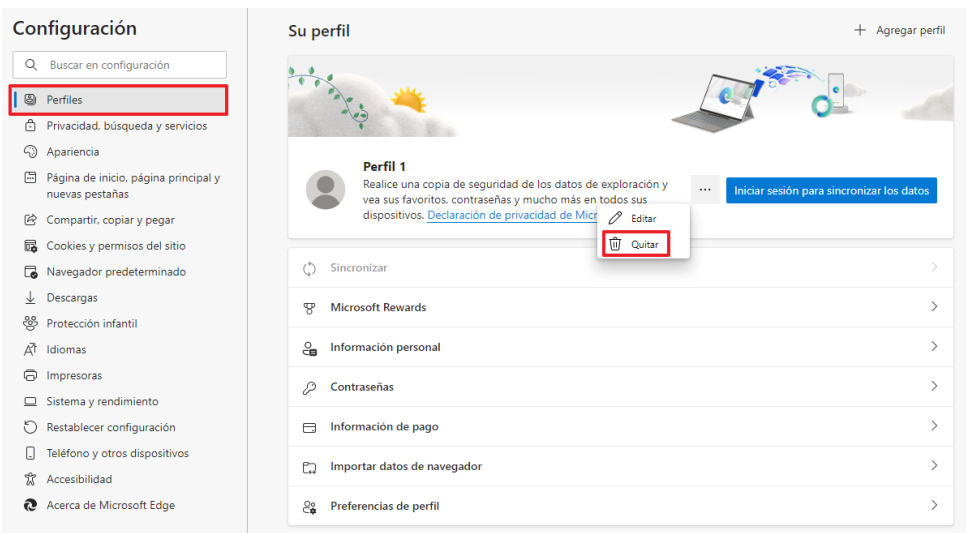
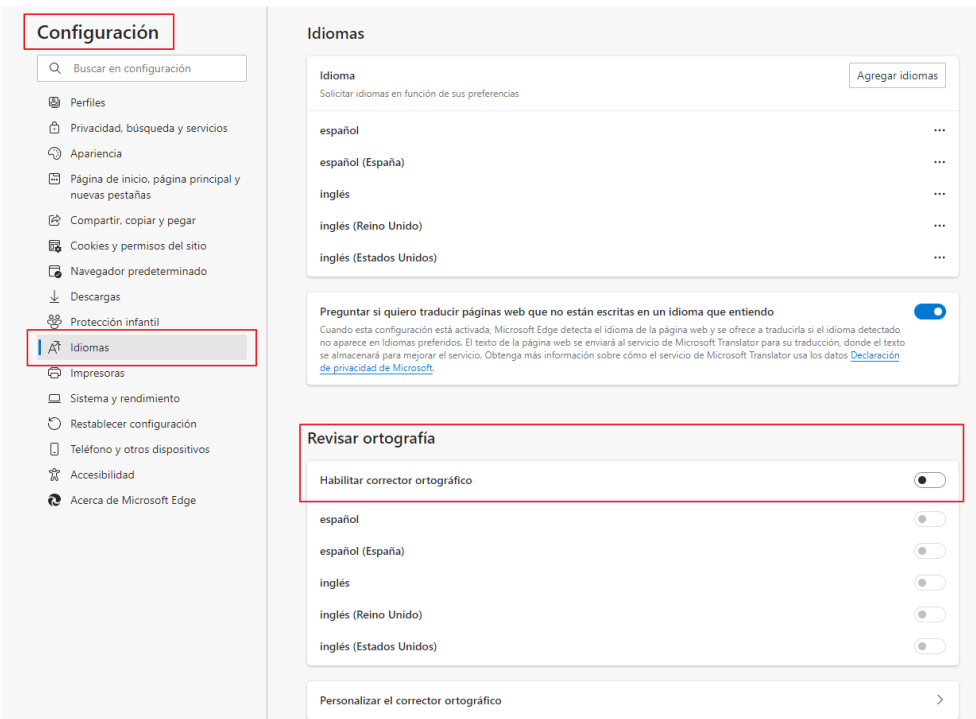
Un método alternativo para acceder a la interfaz de configuración es escribir **“edge://settings/profiles”** en la barra de direcciones.

2.5.1 SINCRONIZACIÓN Y AJUSTES BÁSICOS DE IDIOMA

El navegador Microsoft Edge permite la sincronización automática con servicios de Microsoft, permitiendo a los usuarios, entre otros, sincronizar automáticamente varios elementos como favoritos, pestañas abiertas, contraseñas, extensiones, etc.

Esta información se almacena en la cuenta de Microsoft proporcionada por el usuario a tal efecto. Cabe destacar, que para evitar problemas de privacidad y seguridad se recomienda deshabilitar dicha funcionalidad del explorador.

Una vez el navegador se encuentre instalado, siga los siguientes pasos para realizar el ajuste básico de idioma y deshabilitar el corrector ortográfico, con la finalidad de que no se recopilen datos del usuario mediante estos métodos:

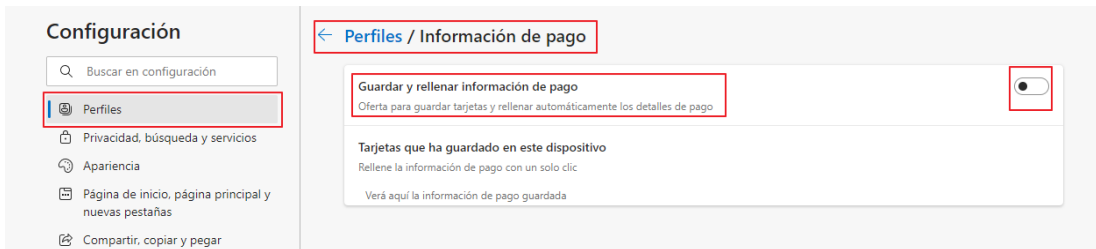
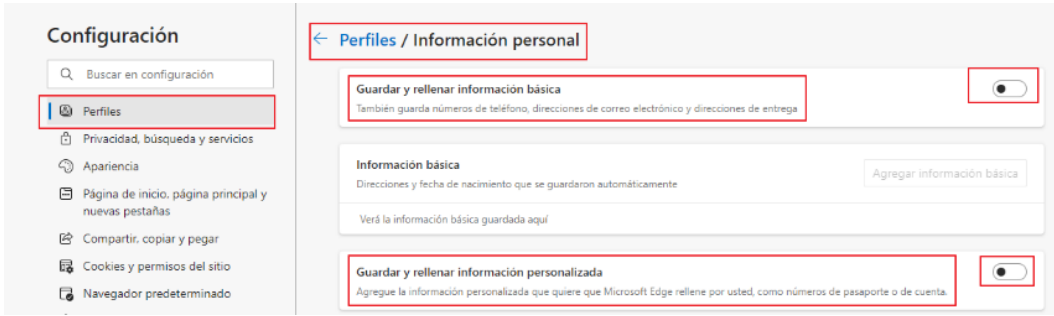
Paso	Descripción
1.	En la sección “Perfiles”, y siempre que sea posible, <u>se recomienda</u> la eliminación de cualquier cuenta sincronizada para evitar la revelación y/o obtención de la información recopilada. Esto no es impedimento con la existencia de perfiles que permitan diferenciar el uso que se realiza con el navegador. 
2.	En el menú “Configuración”, dentro de la sección “Idiomas”, acceda al apartado “Revisar ortografía”. Deshabilite la opción “Habilitar corrector ortográfico”. 

2.5.2 SECCIÓN PERFILES

En este apartado, se indicarán los ajustes a tener en cuenta, de manera que los datos almacenados en el navegador no estén expuestos a posibles ataques no deseados así como evitar que directamente se puedan almacenar.

A continuación, se describe cada uno de los pasos a seguir para la adecuada configuración de este apartado:

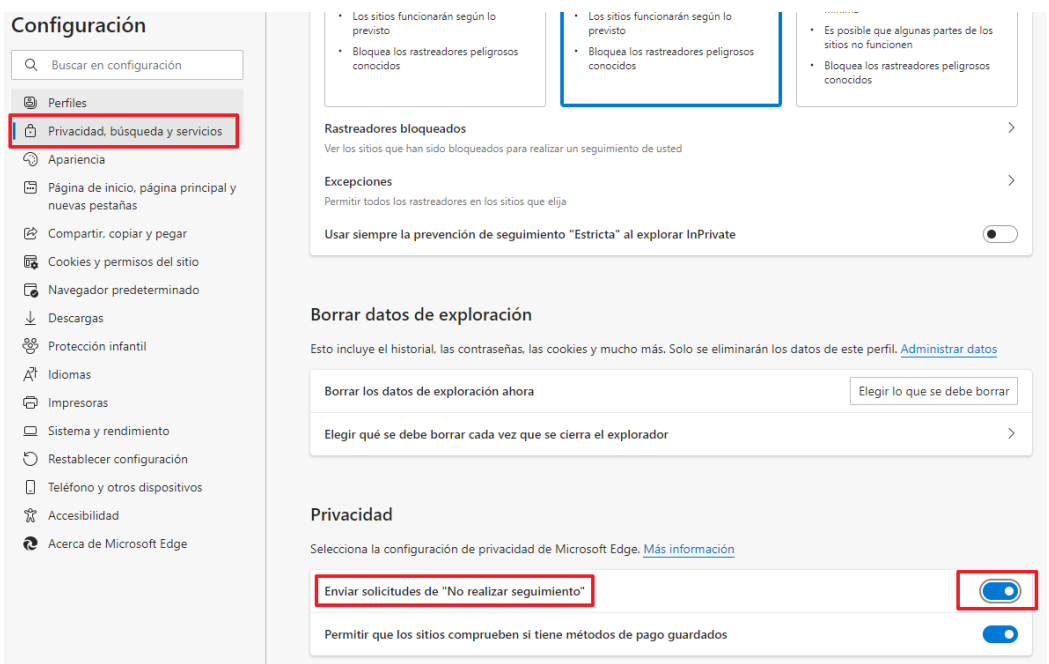
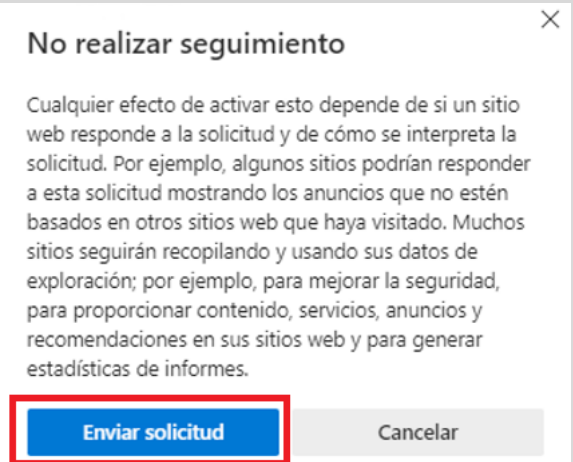
Paso	Descripción
1.	Debido a la forma en la que se almacenan las credenciales, es posible que un atacante malicioso pueda obtener acceso a las cuentas del usuario y/o utilizar las “Credenciales almacenadas” para inicios de sesión no deseados.
2.	Para evitar estos usos indebidos deshabilite la opción “Preguntar si quiere guardar sus contraseñas” , en la sección “Perfiles” dentro del apartado “Contraseñas” :
3.	A continuación pulse sobre la opción “Mas opciones de configuración” y deshabilite la opción “Mostrar el botón “Mostrar contraseña” en los campos de contraseña” .

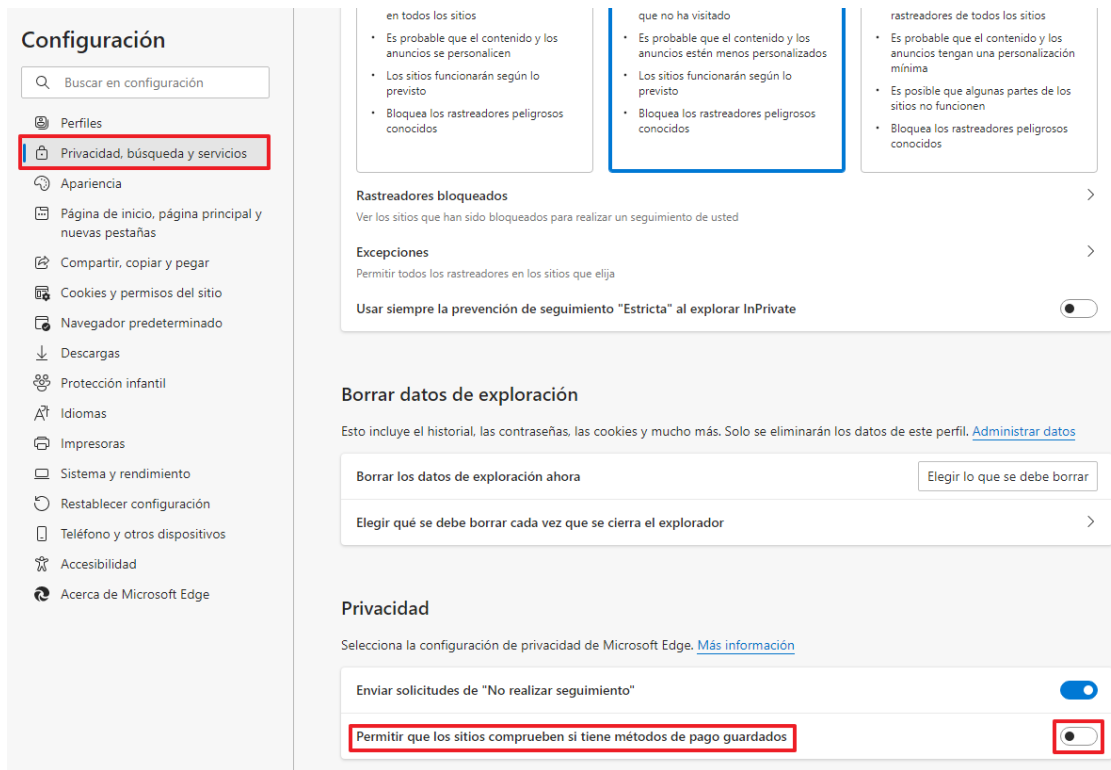
Paso	Descripción
4.	La información referente a los “Métodos de pago” es un elemento atractivo para los atacantes buscando hacer un uso fraudulento de la misma y, por ello, se recomienda no tener almacenada esta información en el navegador Microsoft Edge para evitar ser objeto de ataques maliciosos.
5.	Deshabilite la opción “Guardar y rellenar información de pago”, como indica la siguiente imagen, dentro de la sección “Perfiles” en el apartado “Información de pago”:  The screenshot shows the 'Configuración' (Settings) window with 'Perfiles' selected in the left sidebar. The main pane is titled 'Perfiles / Información de pago'. Under the heading 'Guardar y rellenar información de pago', there is a toggle switch that is currently turned off. Below this, there is a section for 'Tarjetas que ha guardado en este dispositivo'.
6.	Al igual que en el caso anterior, el almacenamiento de información, aun no siendo crítico, puede ofrecer a un atacante información relevante sobre los movimientos, acciones u otras consideraciones del usuario.
7.	Para evitar el uso de esta información, deshabilite las siguientes opciones: – “Guardar y rellenar información básica”. – “Guardar y rellenar información personalizada”. Estas se encuentran dentro de la sección “Perfiles”, en el apartado “Información personal”:  The screenshot shows the 'Configuración' (Settings) window with 'Perfiles' selected in the left sidebar. The main pane is titled 'Perfiles / Información personal'. There are two toggle switches turned off: 'Guardar y rellenar información básica' and 'Guardar y rellenar información personalizada'.
8.	Adicional a la configuración indicada anteriormente citada, dentro de la sección perfiles deberán deshabilitarse las siguientes opciones dentro de cada uno de los apartados indicados: – Apartado “Microsoft Rewards”: • Deshabilite “Gane Microsoft Rewards en Microsoft Edge” – Apartado “Preferencia de perfil”: • Deshabilite “Permitir el inicio de sesión único para sitios profesionales o educativos que usen este perfil”

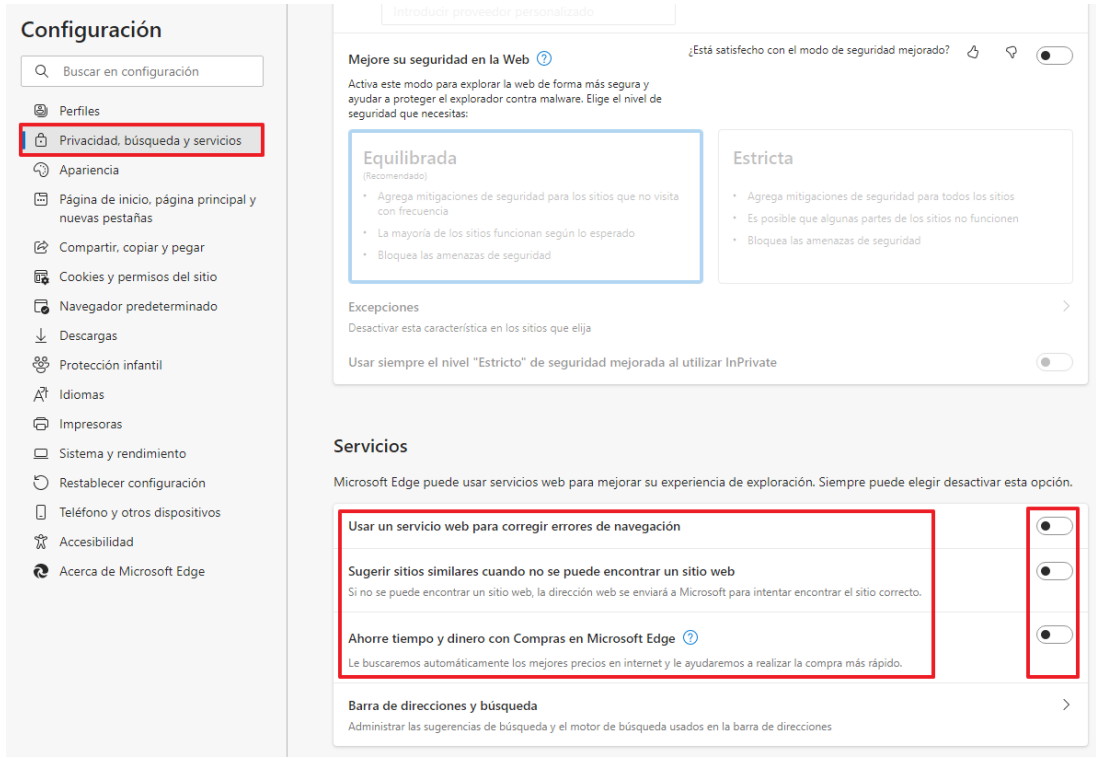
2.5.3 SECCIÓN PRIVACIDAD, BÚSQUEDA Y SERVICIOS

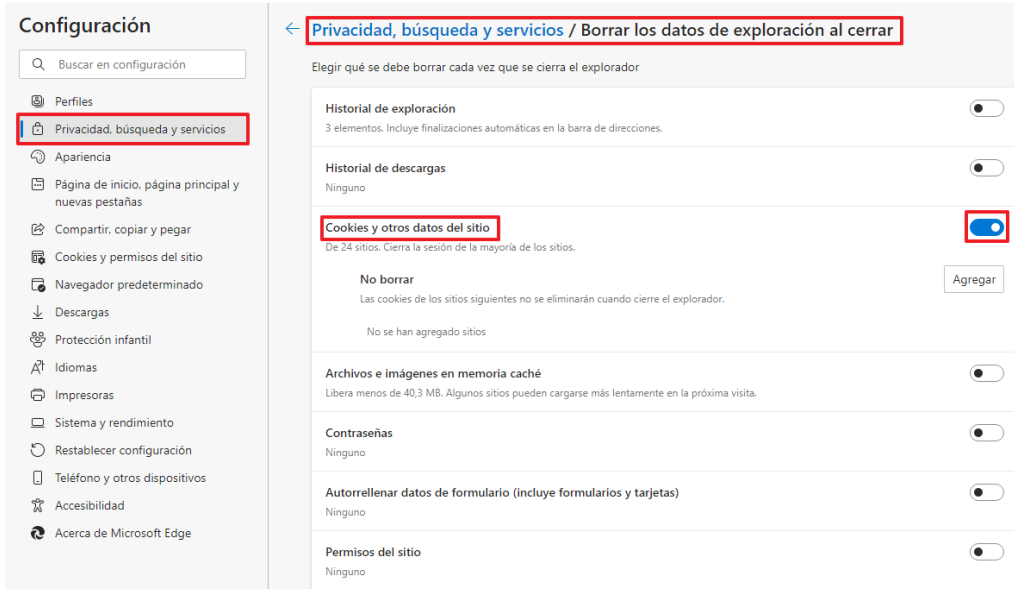
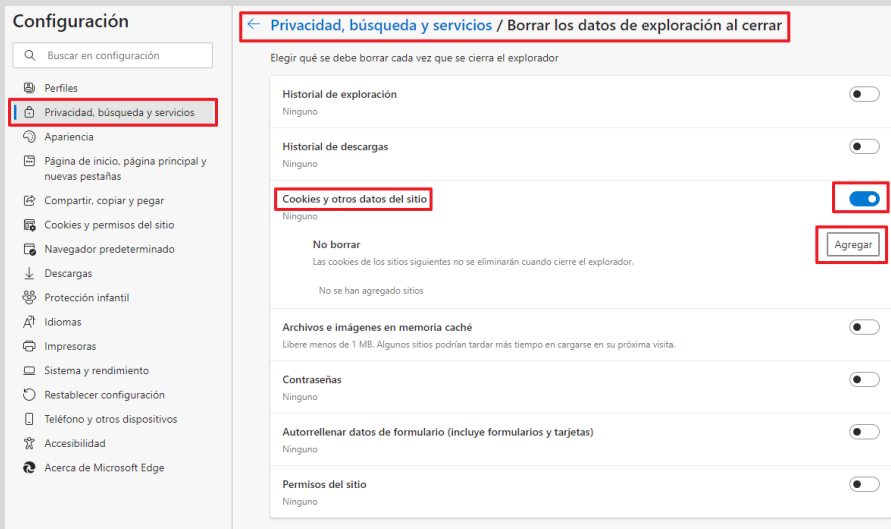
En este apartado, se configurarán las opciones de privacidad, búsqueda y servicios para evitar la obtención de información no deseada y/o requerida así como limitar las funcionalidades de los servicios ofrecidos a través del navegador.

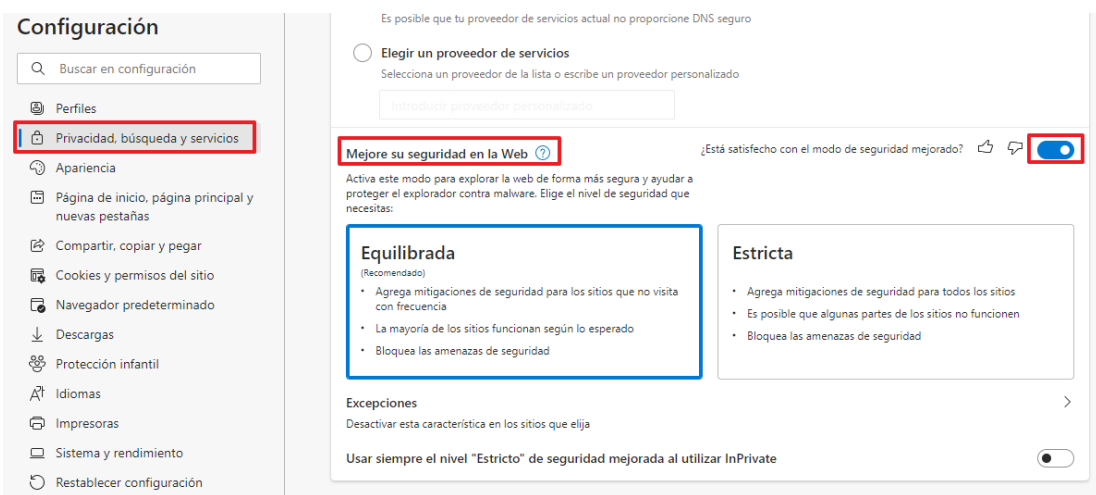
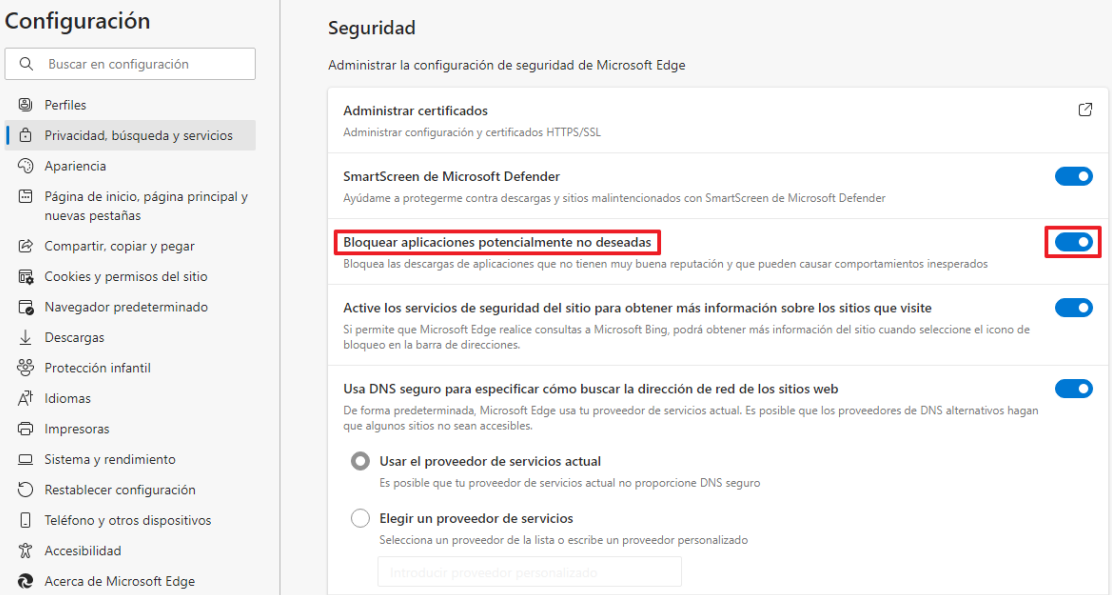
A continuación se describen las configuraciones a configurar:

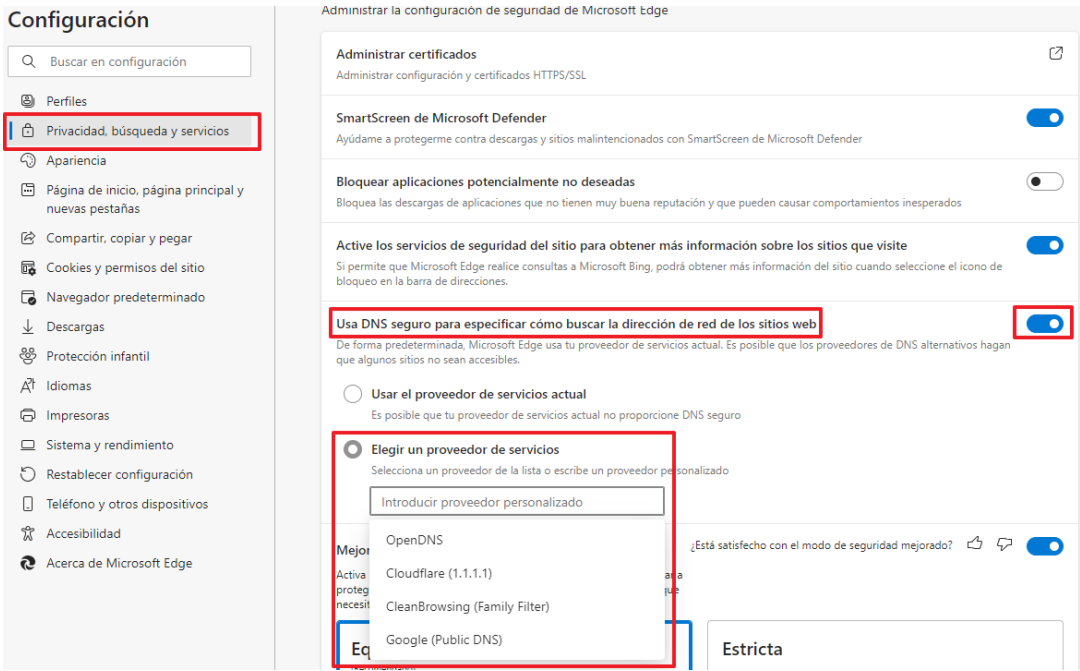
Paso	Descripción
1.	En la propia sección “Privacidad, búsqueda y servicios”, en el apartado “Privacidad”, deshabilite la opción “Enviar solicitudes de “no realizar seguimiento””, tal y como se muestra en la siguiente imagen:  Nota: Cuando se active esta opción, aparecerá un cuadro de diálogo, pulse “Enviar solicitud” para continuar. 

Paso	Descripción
2.	En el mismo apartado deshabilite la opción “Permitir que los sitios comprueben si tiene métodos de pago guardados”.  The screenshot shows the 'Configuración' (Settings) window with the left sidebar containing various categories. 'Privacidad, búsqueda y servicios' is selected and highlighted with a red box. The main content area shows three columns of tracking protection settings. The 'Rastreadores bloqueados' section is expanded, showing 'Excepciones' and a toggle for 'Usar siempre la prevención de seguimiento "Estricta" al explorar InPrivate'. Below this, the 'Borrar datos de exploración' section is visible. The 'Privacidad' section is also shown, with a toggle for 'Permitir que los sitios comprueben si tiene métodos de pago guardados' turned off and highlighted with a red box.
3.	A continuación, en los apartados “Datos de diagnóstico opcionales” y “Personalizar su experiencia web” asegúrese que sendas opciones aparecen deshabilitadas tal y como se muestra en la siguiente imagen:  The screenshot shows the 'Configuración' (Settings) window with the left sidebar. 'Privacidad, búsqueda y servicios' is selected and highlighted with a red box. The main content area shows the 'Datos de diagnóstico opcionales' section, which has a toggle switch turned off and highlighted with a red box. Below this, the 'Personalizar su experiencia web' section is visible, which also has a toggle switch turned off and highlighted with a red box.

Paso	Descripción
4.	Siguiendo en la sección “Privacidad, búsqueda y servicios”, en el apartado “Servicios” se deshabilitarán las siguientes opciones relacionadas con funcionalidades de servicios web, ofrecidos por Microsoft Edge, tal y como muestra la siguiente imagen: 
5.	A continuación, se deberán definir algunas configuraciones que definan el comportamiento del navegador cuando se finaliza el uso de este de modo que se eliminen los ficheros generados por el navegador durante su ejecución. Esto favorece la carga de las últimas versiones de las páginas visitadas, así como la configuración actualizada para el sitio web, en las siguientes ocasiones que se visite el sitio, mejorando la seguridad general de la navegación.

Paso	Descripción
6.	Para ello, dentro de la sección “Privacidad, búsqueda y servicios”, en el apartado “Borrar los datos de exploración al cerrar” habilite la opción “Cookies y otros datos del sitio” como se muestra en las siguiente imagen:  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 o agregarla como excepción. Para ello, se puede generar una excepción de cookies de terceros sobre ciertas páginas para mejorar su experiencia de uso, agregando el sitio, tal y como se aprecia en la siguiente imagen, pulsando sobre el botón “Agregar”: 

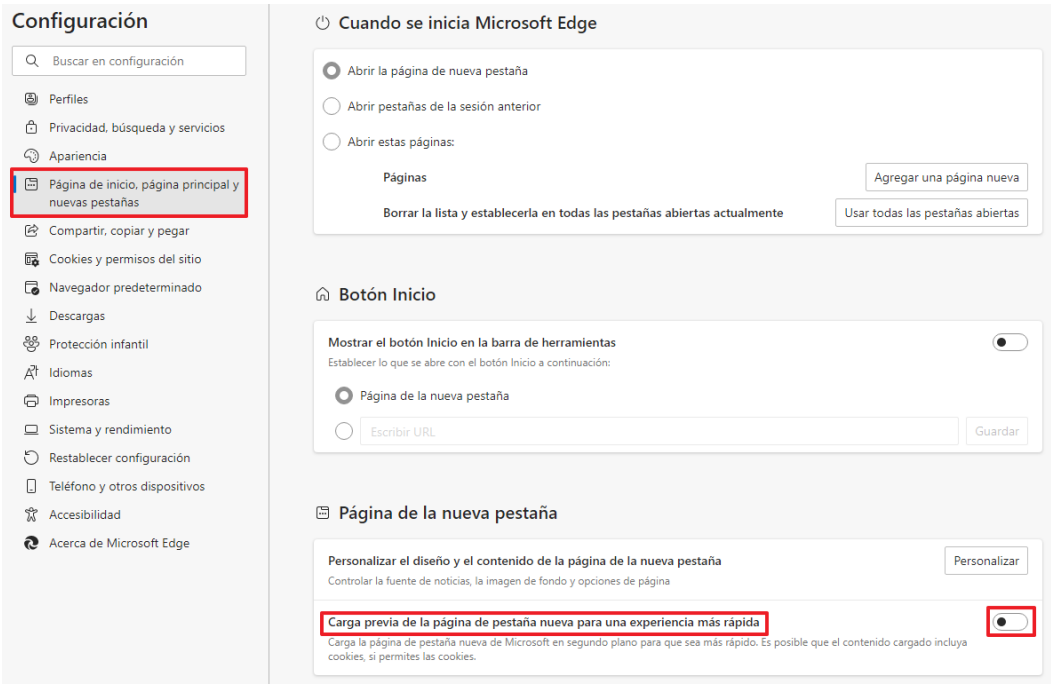
Paso	Descripción
7.	Siguiendo en los ajustes de la sección “Privacidad, búsqueda y servicios”, habilite la opción “Mejore su seguridad en la web” en el apartado “Seguridad”. Para obtener esta protección, se debe hacer clic sobre el texto “Mejore su seguridad en la Web” o habilitar la opción desde el botón lateral, tal y como se observa en la siguiente imagen:  Esta protección que ofrece el navegador Microsoft Edge incluye, entre otras, las siguientes características: – Agrega mitigaciones de seguridad para los sitios que no visita con frecuencia. – La mayoría de los sitios funcionan según lo esperado. – Bloquea las amenazas de seguridad.
8.	Dentro del mismo apartado habilite la opción “Bloquear aplicaciones potencialmente no deseadas”: 

Paso	Descripción
9.	La funcionalidad “Usar DNS seguro”, viene activa de forma predeterminada. Sin embargo, por defecto se hace uso del DNS del proveedor del servicio actual, lo que puede provocar el intento de conexiones no seguras contra un sitio web debido a interrupciones del servicio. Por ello, es posible establecer uno de los DNS facilitados por el navegador o incluso uno personalizado si se encuentra en un entorno empresarial: 
10.	A continuación asegúrese que las opciones “SmartScreen de Microsoft Defender” y “Active los servicios de seguridad del sitio para obtener mas información sobre los sitios web que visite” se encuentra habilitados. En caso contrario habilite ambas opciones.

Paso	Descripción
11.	Por último, relacionado con las configuraciones orientadas a la prevención del seguimiento y la mejora de la seguridad web, es posible establecer una configuración mas restrictiva estableciendo sendas configuraciones con la configuración “Estricta”. Esta configuración es mas segura pero puede provocar que ciertos sitios web dejen de funcionar según se espera. Por ello, en caso de habilitar dicha configuración es posible establecer excepciones para aquellos sitios web que así lo requieran. Prevención de seguimiento ⓘ Los sitios web usan rastreadores para recopilar información acerca de su exploración. Los sitios web pueden usar esta información para mejorar los sitios y mostrar contenido como anuncios personalizados. Algunos rastreadores recopilan y envían su información a sitios que no ha visitado. Prevención de seguimiento ⓘ Básica - Permite la mayoría de los rastreadores en todos los sitios - Es probable que el contenido y los anuncios se personalicen - Los sitios funcionarán según lo previsto - Bloquea los rastreadores peligrosos conocidos Equilibrada (Recomendado) - Bloquea los rastreadores de los sitios que no ha visitado - Es probable que el contenido y los anuncios estén menos personalizados - Los sitios funcionarán según lo previsto - Bloquea los rastreadores peligrosos conocidos Estricta - Bloquea la mayoría de los rastreadores de todos los sitios - Es probable que el contenido y los anuncios tengan una personalización mínima - Es posible que algunas partes de los sitios no funcionen - Bloquea los rastreadores peligrosos conocidos Mejore su seguridad en la Web ⓘ ¿Está satisfecho con el modo de seguridad mejorado? ⓘ ⓘ ⓘ Activa este modo para explorar la web de forma más segura y ayudar a proteger el explorador contra malware. Elige el nivel de seguridad que necesitas: Equilibrada (Recomendado) - Agrega mitigaciones de seguridad para los sitios que no visita con frecuencia - La mayoría de los sitios funcionan según lo esperado - Bloquea las amenazas de seguridad Estricta - Agrega mitigaciones de seguridad para todos los sitios - Es posible que algunas partes de los sitios no funcionen - Bloquea las amenazas de seguridad Excepciones ⓘ Desactivar esta característica en los sitios que elija Usar siempre el nivel "Estricto" de seguridad mejorada al utilizar InPrivate ⓘ

2.5.4 SECCIÓN PÁGINA DE INICIO, PÁGINA PRINCIPAL Y NUEVAS PESTAÑAS

Tal y como se verá también en apartados posteriores, los envíos de información en segundo plano son una parte muy importante para la seguridad y privacidad para evitar la ejecución de código malicioso.

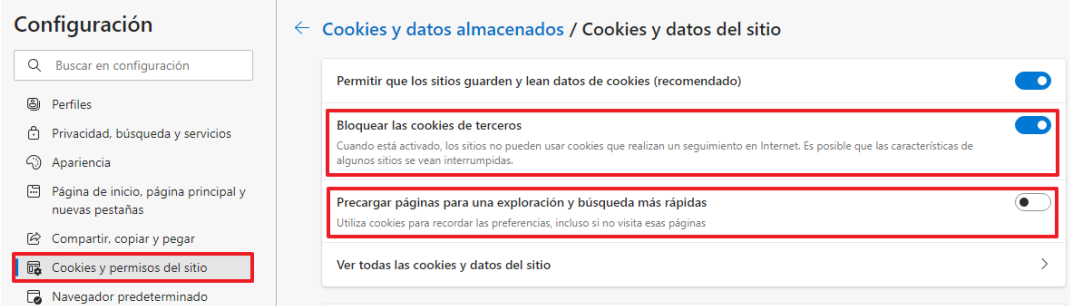
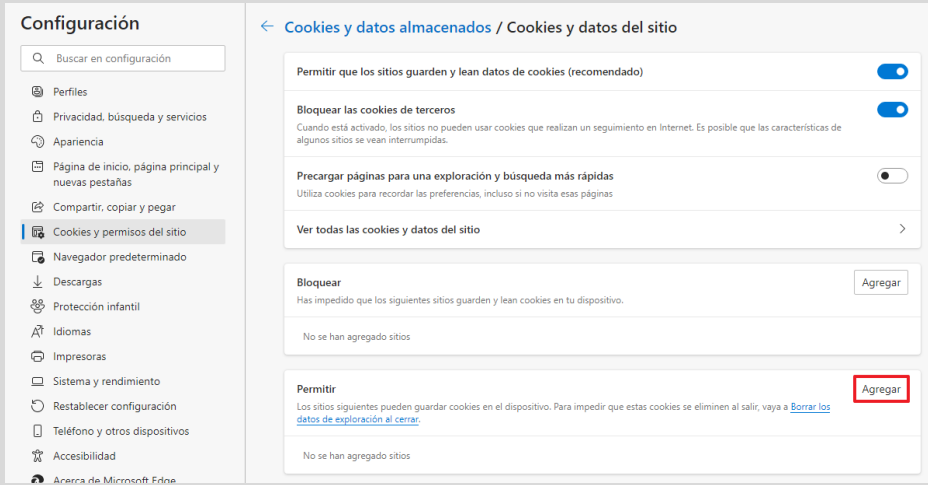
Paso	Descripción
1.	Dentro de la sección “Página de inicio, página principal y nuevas pestañas”, en el apartado “Página de la nueva pestaña”, deshabilite la opción “Carga previa de la página de pestaña nueva para una experiencia más rápida”. 

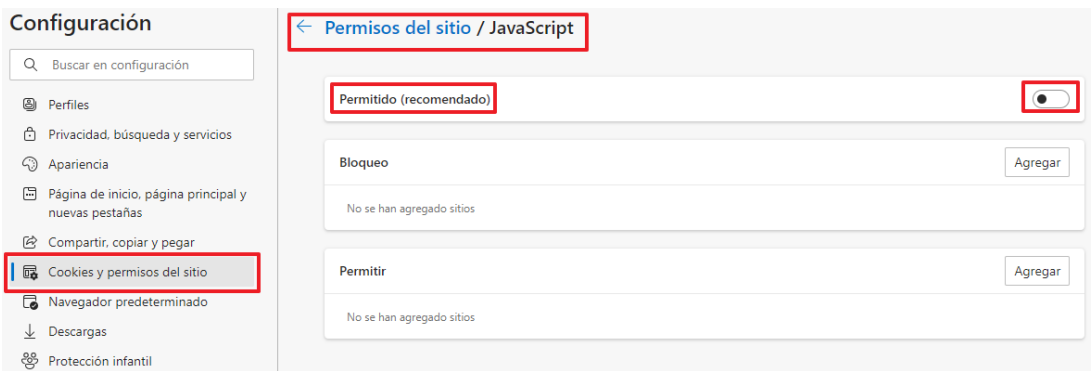
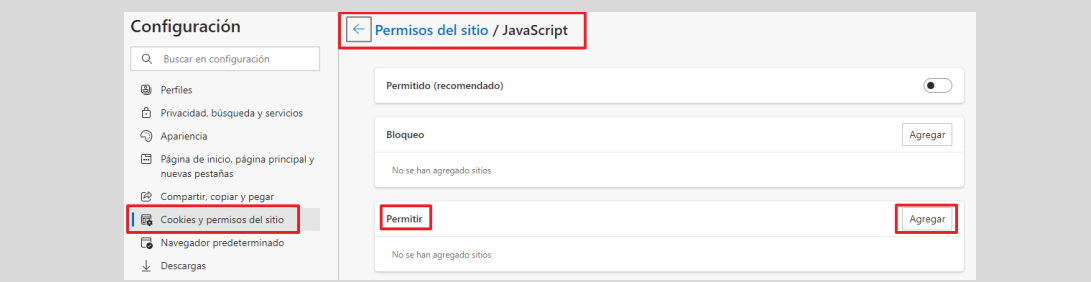
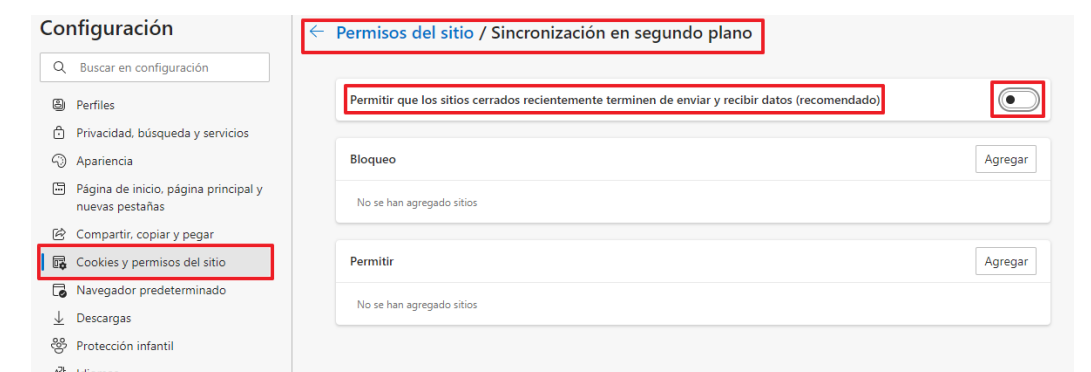
2.5.5 SECCIÓN COOKIES Y PERMISOS DEL SITIO

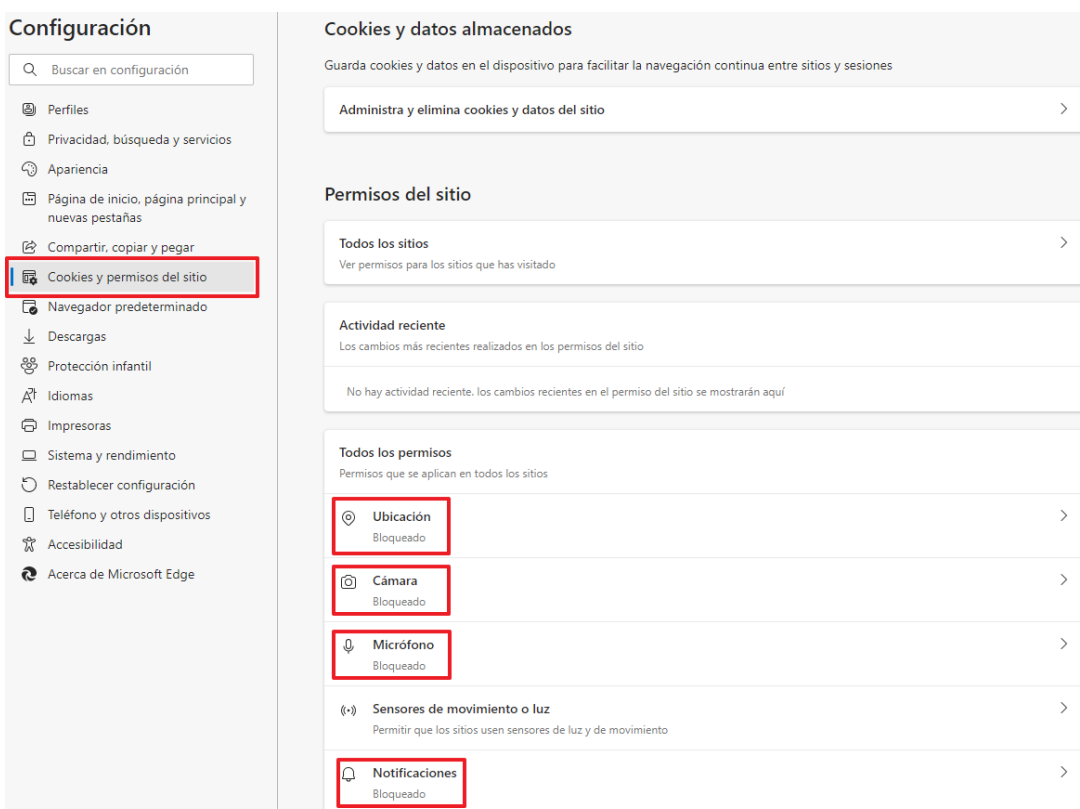
La configuración de las cookies y los envíos de información en segundo plano son una parte muy importante para la seguridad y privacidad. Con una configuración segura de estos elementos se pueden prevenir brechas de seguridad y posibles robos de información sensible, ya que un atacante podría ocultar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

Para evitar estos riesgos, se recomienda realizar la siguiente configuración en el navegador Microsoft Edge:

Paso	Descripción
1.	A continuación se modificarán los aspectos que impiden el almacenamiento y el bloqueo de ciertas cookies para evitar el almacenamiento de información no necesario, así como el bloqueo de información en segundo plano.

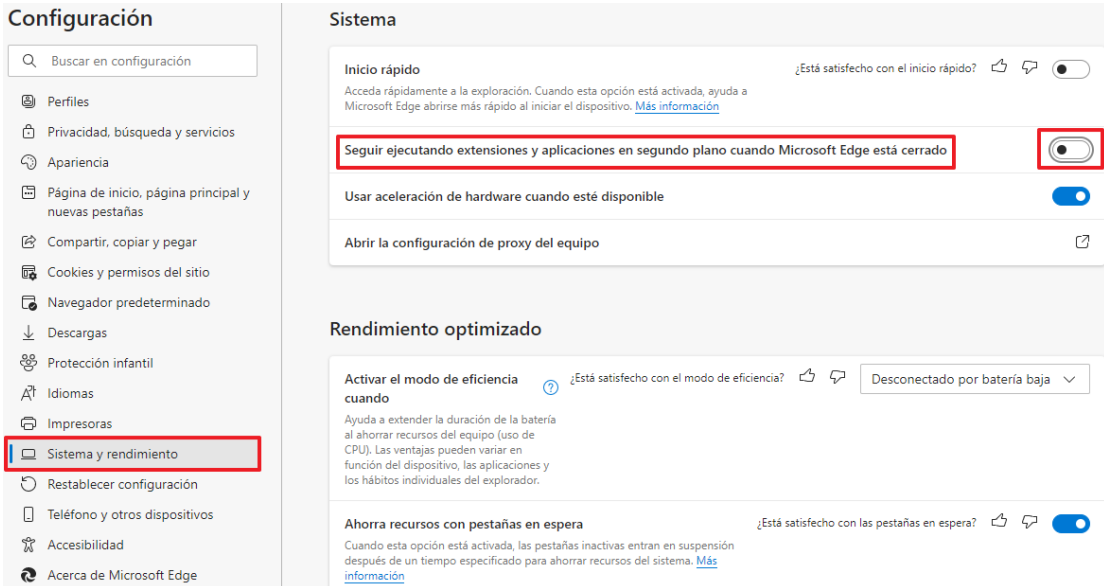
Paso	Descripción
2.	En la configuración de Edge, diríjase a la sección de “Cookies y permisos del sitio”, y después al apartado “Administra y elimina cookies y datos del sitio”. Una vez allí, habilite la opción “Bloquear las cookies de terceros” y deshabilite la opción “Precargar páginas para una exploración y búsqueda más rápida”, como se muestra en la siguiente imagen:  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. Para ello, puede generar una excepción de cookies de terceros sobre ciertas páginas para mejorar su experiencia de uso, tal y como se aprecia en la siguiente imagen. 
3.	Continuando con las configuraciones, 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.

Paso	Descripción
4.	Para limitar y evitar lo indicado anteriormente, se debe acceder a la sección “Cookies y permisos del sitio”, dentro del apartado “JavaScript”. Una vez dentro de JavaScript, <u>se recomienda deshabilitar</u> la opción “Permitido (recomendado)” como se muestra en la siguiente imagen:  Nota: En la mayoría de los casos, JavaScript deberá mantenerse habilitado para disponer de una funcionalidad completa en las páginas web que se visitan. Sin embargo, en algunos entornos empresariales donde se requieran niveles de seguridad mejorados, se recomienda revisar esta configuración y bloquear el uso de JavaScript para evitar ataques de ejecución de código, añadiendo solamente las excepciones en aquellos sitios que sean necesarios para la organización, agregándolos en el apartado de “Permitir”. 
5.	Posteriormente en el mismo apartado, denominado “Cookies y permisos del sitio”, se deshabilitarán los aspectos referentes a la “Sincronización en segundo plano”, del tal modo que no permita que los sitios cerrados recientemente puedan realizar ejecuciones de forma no deseada. Deshabilite la opción “Permitir que los sitios cerrados recientemente terminen de enviar y recibir datos” como aparece en la siguiente imagen: 

Paso	Descripción
6.	Para terminar las configuraciones dentro del apartado de “Cookies y permisos del sitio” , se deberán cambiar algunos aspectos relativos al uso de elementos de comunicación hardware del equipo. Esto permitirá establecer una configuración de privacidad adecuándose a las necesidades del usuario.
7.	Se deberán establecer en estado “Bloqueado” los siguientes elementos: – “Ubicación” – “Cámara” – “Micrófono” – “Notificaciones” – “Descargas automáticas” – “Dispositivos USB” – “Puertos serie” – “Edición de archivos” – “Portapapeles” – “Controladores de pago” – “Realidad virtual” – “Realidad aumentada” Esta configuración podrá ser modificada, permitiendo su uso o añadiendo excepciones a los sitios web que requieran el uso de estos elementos: 

2.5.6 SECCIÓN SISTEMA Y RENDIMIENTO

Como ya se ha comentado en puntos anteriores, la ejecución de código en segundo plano después del cierre del navegador Microsoft Edge es susceptible de uso para ataques maliciosos y debe ser deshabilitada, para ello, se han de realizar los siguientes pasos:

Paso	Descripción
1.	En la sección “Sistema y rendimiento”, en el apartado “Sistema”, deshabilite la opción “Seguir ejecutando extensiones y aplicaciones en segundo plano cuando Microsoft Edge está cerrado”, tal y como se muestra en la siguiente imagen:  The screenshot shows the Windows Settings application. On the left, the 'Configuración' (Settings) menu is visible, with 'Sistema y rendimiento' (System and performance) highlighted with a red box. The main area shows the 'Sistema' (System) settings. Under the 'Inicio rápido' (Fast startup) section, the option 'Seguir ejecutando extensiones y aplicaciones en segundo plano cuando Microsoft Edge está cerrado' (Continue running extensions and applications in the background when Microsoft Edge is closed) is highlighted with a red box. The toggle switch for this option is also highlighted with a red box and is currently turned off. Other options visible include 'Usar aceleración de hardware cuando esté disponible' (Use hardware acceleration when available) which is turned on, and 'Abrir la configuración de proxy del equipo' (Open your proxy settings).

3. LISTA DE COMPROBACIÓN

Criticidad	Descripción
Alta	Microsoft Edge debe tener instaladas las últimas actualizaciones de software relacionadas con la seguridad, aplicándolas mediante instalación manual de la última versión disponible para su descarga, la herramienta de actualización automática de Microsoft Edge, o la herramienta Windows Update del sistema operativo Windows.
Alta	En el caso de que se usen extensiones en el navegador, deberá asegurarse de que estén actualizadas y provengan de fuentes confiables
Media	Cuando un usuario cambia de una página segura (habilitada para SSL) a una página no segura, Microsoft Edge está configurado para notificar al usuario.
Media	Microsoft Edge está configurado para bloquear ventanas emergentes.
Media	Se pueden utilizar cuentas de Microsoft y e iniciar sesión para sincronizar los datos en Microsoft Edge, con una cuenta proporcionada por el usuario.
Media	Microsoft Edge está configurado para no autocompletar búsquedas y URLs, sin enviar información al buscador predeterminado.
Media	Microsoft Edge está configurado para no guardar las contraseñas de los sitios.
Media	Microsoft Edge está configurado para no iniciar sesión automáticamente en las webs que tiene las credenciales almacenadas.
Media	Microsoft Edge está configurado para no guardar ni autocompletar métodos de pago.
Media	Microsoft Edge está configurado para permitir que los sitios web no comprueben si hay métodos de pago guardados.
Media	Microsoft Edge está configurado para bloquear las cookies de terceros.
Media	Microsoft Edge está configurado para no precargar información de las páginas.
Media	Microsoft Edge está configurado para permitir que las páginas cerradas no envíen y reciban datos.
Media	Microsoft Edge está configurado para no permitir el uso de JavaScript, excepto que se añada alguna excepción.
Media	Microsoft Edge está configurado para no ejecutar aplicaciones en segundo plano al cerrar el navegador.

4. DECÁLOGO DE RECOMENDACIONES

A continuación, se indican diez recomendaciones de seguridad en el uso de Microsoft Edge.

- a) Se recomienda utilizar siempre la versión estable más actual y con las últimas actualizaciones.
- b) Se recomienda la **revisión de las funciones relativas a la seguridad del software**, dado que proporcionará una mejor defensa contra posibles ataques.
- c) Si se necesita **instalar complementos**, se recomienda la utilización de **fuentes oficiales y/o confiables**.
- d) Se recomienda **no usar el almacén de contraseñas disponible en Microsoft Edge**. 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.
- e) 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.
- f) Se recomienda **utilizar siempre protocolos seguros (https)**, más aún cuando se utilicen datos personales para asegurar las comunicaciones de extremo a extremo.
- g) 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.
- h) 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, código de verificación, etc.).
- i) 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.
- j) Se recomienda **limpiar la caché y eliminar los archivos temporales de internet** para solucionar problemas habituales con los sitios web.

