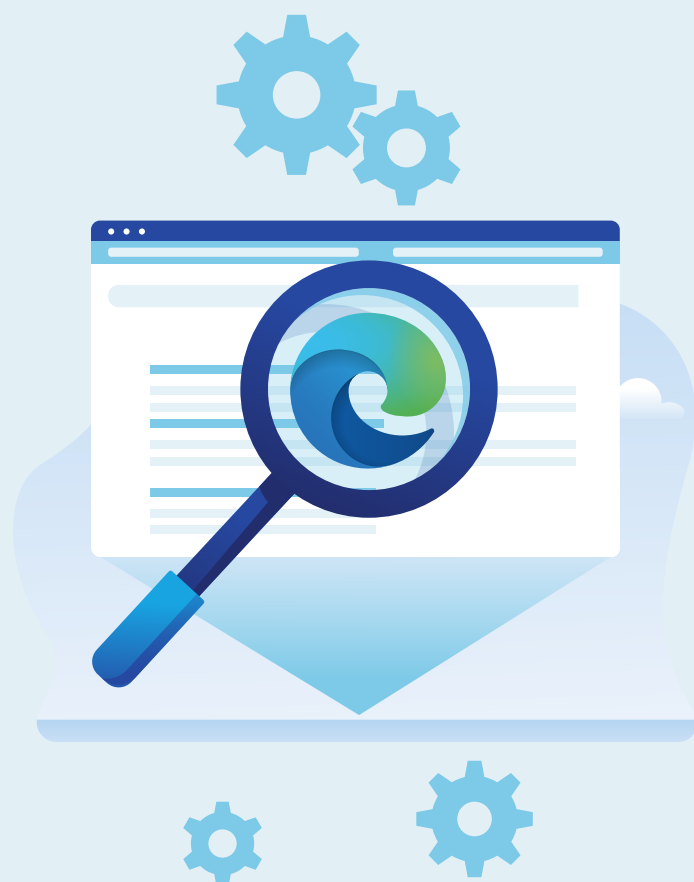


CCN-CERT BP/26



Recomendaciones de seguridad en Microsoft Edge

INFORME DE BUENAS PRÁCTICAS

JUNIO 2022

Edita:



© Centro Criptológico Nacional, 2022

Fecha de edición: junio de 2022

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.

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.

Hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar.

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



Índice

1. Introducción	6
2. Navegador web Microsoft Edge	7
2.1. Versiones	9
2.2. Requisitos mínimos	11
2.3. Descarga	13
2.4. Instalación y configuración inicial	15
2.5. Directrices de configuración	19
2.5.1 Sincronización y ajustes básicos de idioma	19
2.5.2 Sección perfiles	21
2.5.3 Sección privacidad, búsqueda y servicios	24
2.5.4 Sección página de inicio, página principal y nuevas pestañas	31
2.5.5 Sección cookies y permisos del sitio	32
2.5.6 Sección sistema y rendimiento	37
3. Lista de comprobación	38
4. Decálogo de recomendaciones	40

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.

**Microsoft Edge
sustituirá al navegador
Internet Explorer en
los entornos Windows
como navegador
predeterminado.**

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.

2. Navegador web Microsoft Edge

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 le 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:



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.

2. Navegador web Microsoft Edge

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.

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.

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.

Microsoft Edge Business

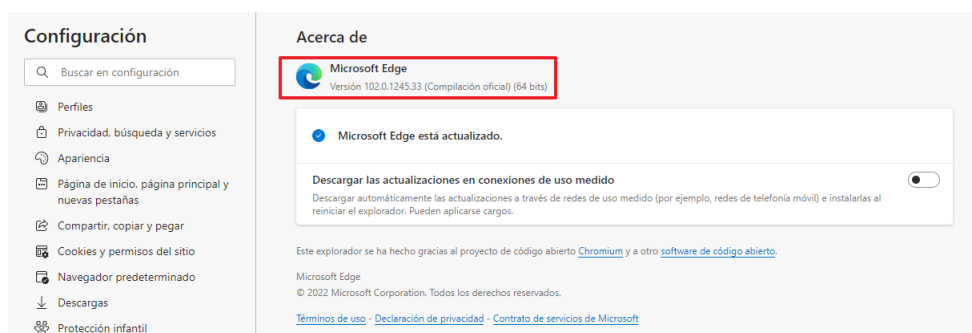


Esta versión es el mismo navegador Microsoft Edge que se utiliza en la versión Stable. La diferencia está en cómo se despliega y se administra. Los administradores de TI pueden descargar esta versión para instalar el navegador Microsoft Edge a través de un instalador **.msi** y administrar los navegadores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

2. Navegador web Microsoft Edge

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:



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

- Windows 7.
- Windows 8.1.
- Windows 10 Professional 1709 y versiones posteriores.
- Windows 10 Home 1709 y versiones posteriores.
- Windows 10 Enterprise 2015 LTSC.
- Windows 10 Enterprise 2016 LTSC.
- Windows 10 Enterprise 2019 LTSC.
- Windows 11 Professional.

2. Navegador web Microsoft Edge



Windows 11 Enterprise.
Windows 11 Home.
Windows Server 2008 R2.
Windows Server 2012.
Windows Server 2012 R2.
Windows Server 2016 (LTSC).
Windows Server 2019 (LTSC).
Windows Server (SAC).
MacOS Sierra 10.2 o superior.
iOS 11 o superior.
Android KitKat4.4 o superior.
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>



Requisitos hardware recomendados:

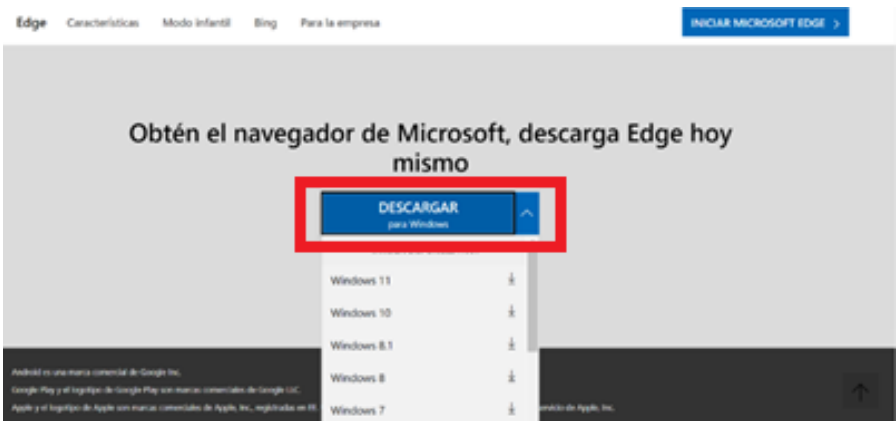
Requisitos mínimos recomendados para el sistema operativo de 64 bits instalado.
Requisitos mínimos recomendados para el sistema operativo de 32 bits instalado.

2.3 Descarga

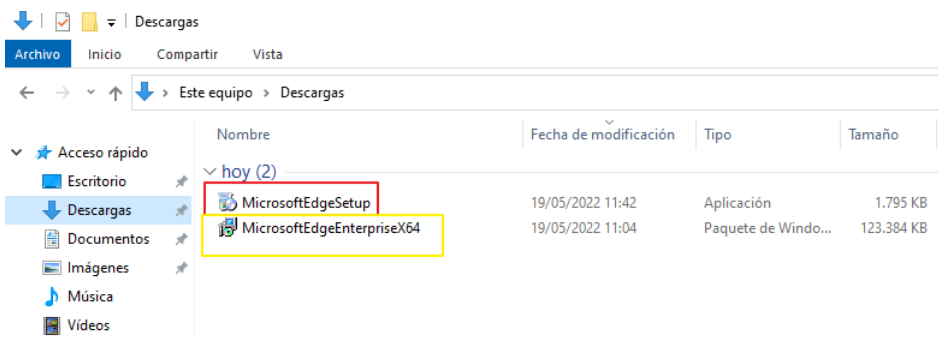
En algunos casos, como por ejemplo en los sistemas operativos Windows 10 en sus versiones Pro y Home, Microsoft Edge este ya se encuentra instalado por defecto e integrado junto al sistema operativo.

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:



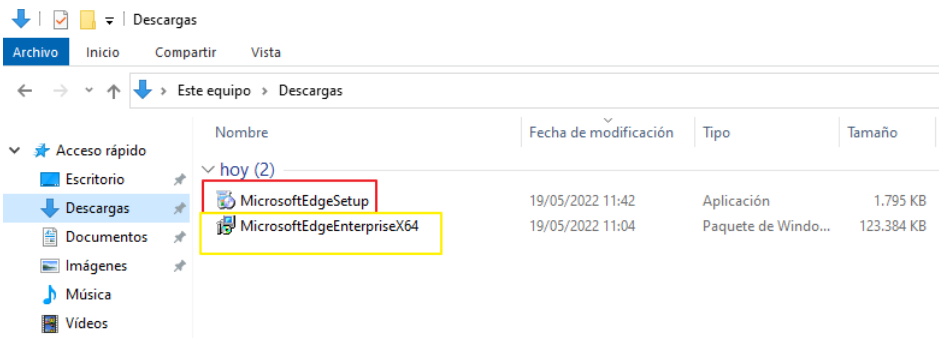
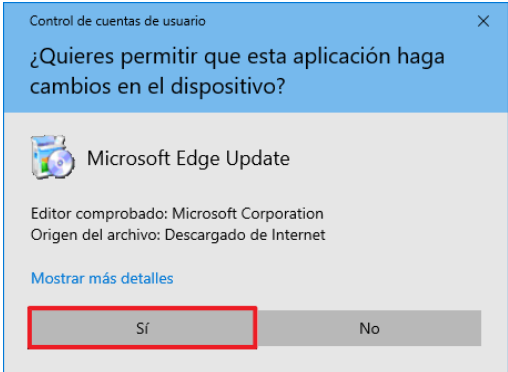
Paso	Descripción
1.	Para la descarga del programa desde la fuente oficial se utilizará el siguiente enlace: https://www.microsoft.com/es-es/edge
2.	Descargue la versión del navegador en función de su sistema operativo.  A screenshot of the Microsoft Edge download page. The page has a header with links for 'Edge', 'Características', 'Modo infantil', 'Bing', and 'Para la empresa', along with a button 'INICIAR MICROSOFT EDGE'. The main heading reads 'Obtén el navegador de Microsoft, descarga Edge hoy mismo'. Below this is a large blue button labeled 'DESCARGAR para Windows', which is highlighted with a red rectangle. Underneath the button is a list of operating systems: Windows 11, Windows 10, Windows 8.1, Windows 8, and Windows 7, each with a download icon. At the bottom, there are small text blocks for Android, Google Play, and Apple.

2. Navegador web Microsoft Edge

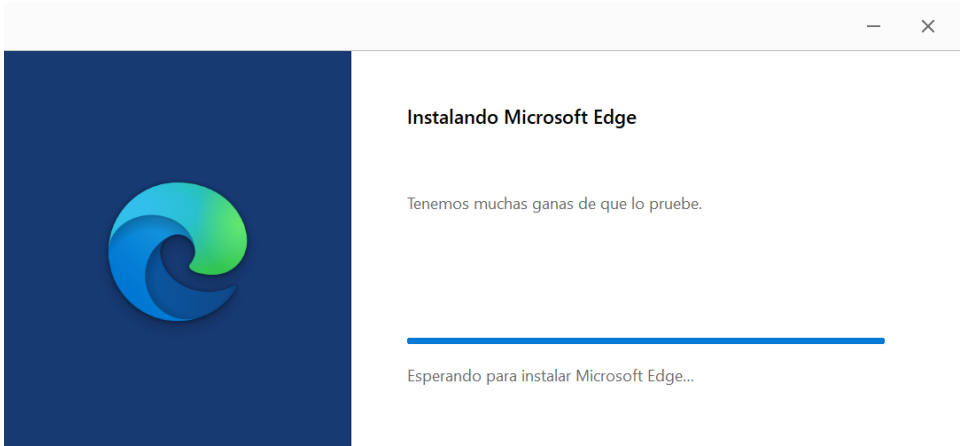
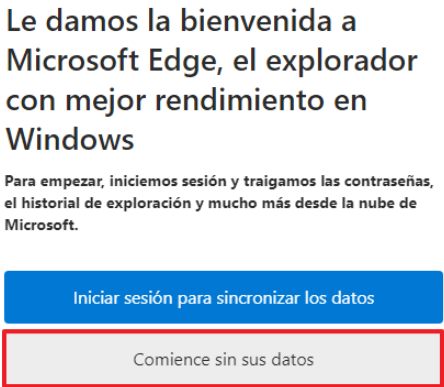
Paso	Descripción
3.	El archivo descargado, aparecerá en la ubicación que se haya determinado, en función de la configuración establecida en el navegador que se esté usando. El recuadro rojo en la imagen corresponde a la descarga normal del instalador que requiere conexión a internet (Utilizado durante 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 de 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. 

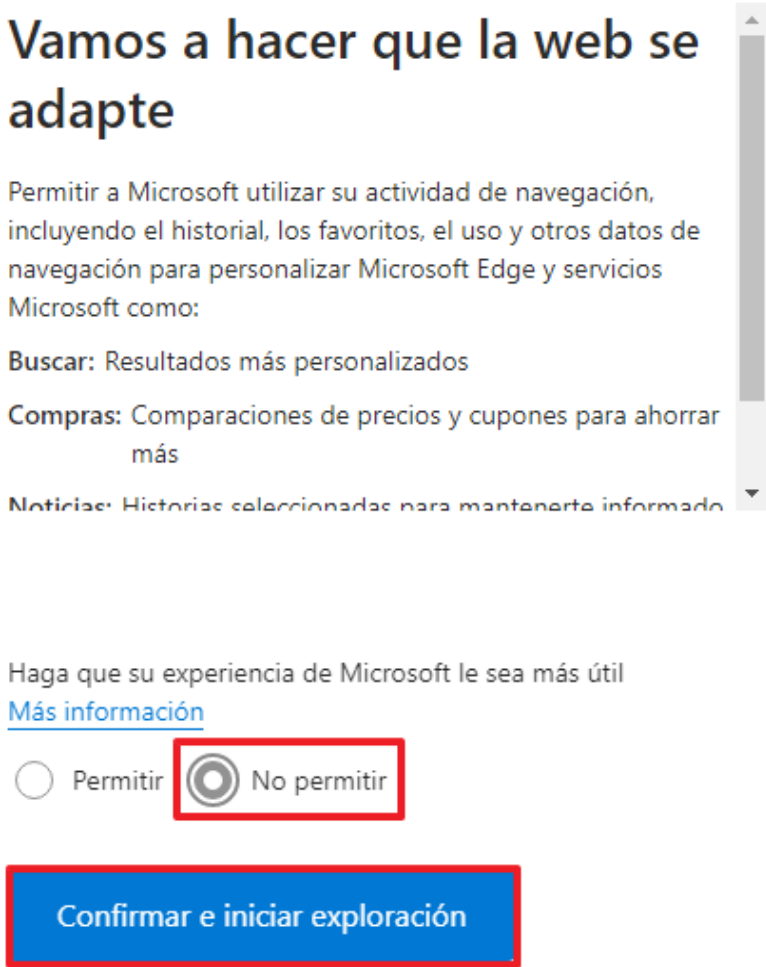
2. Navegador web Microsoft Edge

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". 

2. Navegador web Microsoft Edge

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

2. Navegador web Microsoft Edge

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".  Vamos a hacer que la web se adapte Permitir a Microsoft utilizar su actividad de navegación, incluyendo el historial, los favoritos, el uso y otros datos de navegación para personalizar Microsoft Edge y servicios Microsoft como: Buscar: Resultados más personalizados Compras: Comparaciones de precios y cupones para ahorrar más Noticias: Historias seleccionadas para mantenerte informado Haga que su experiencia de Microsoft le sea más útil Más información ☐ Permitir ☒ No permitir 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

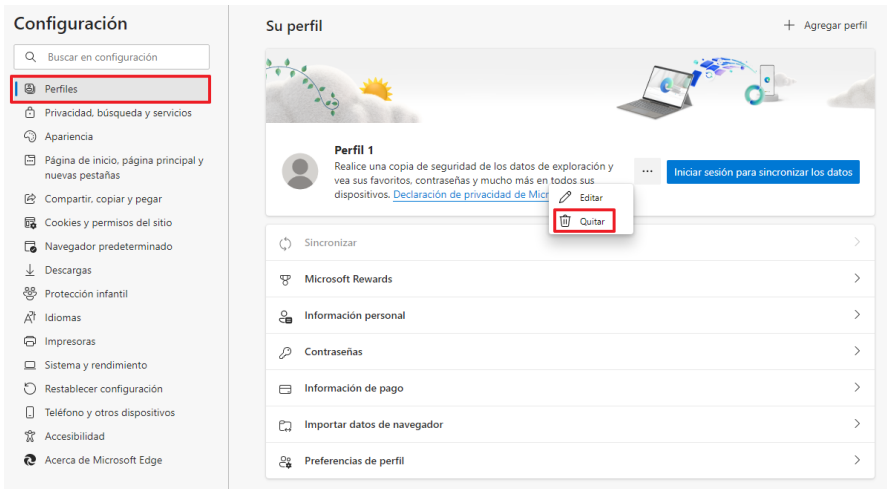
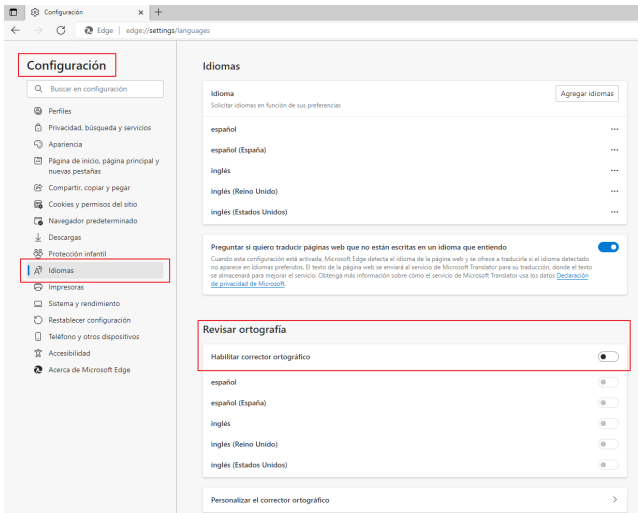
El navegador Microsoft Edge permite la sincronización automática con servicios de Microsoft, permitiendo a los usuarios, entre otros, sincronizar automáticamente varios elementos como favoritos, pestañas abiertas, contraseñas, extensiones, etc.

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:



2. Navegador web Microsoft Edge

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". 

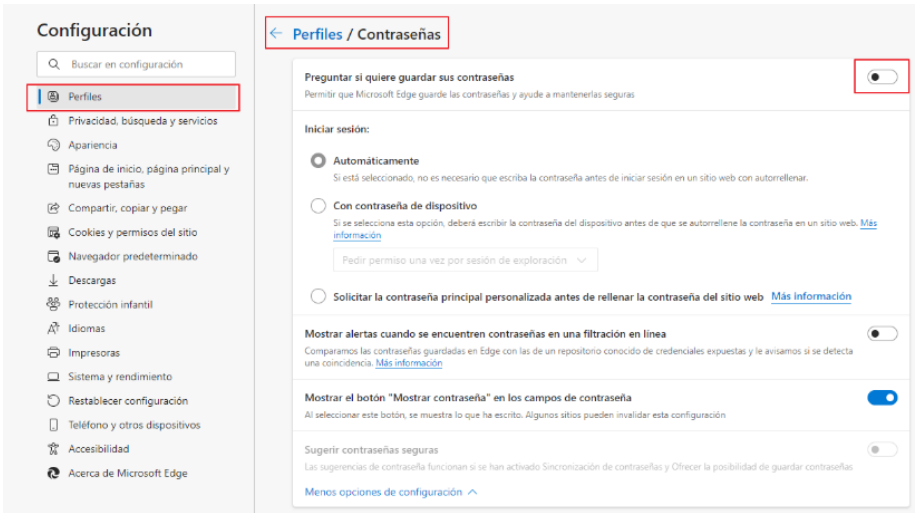
2. Navegador web Microsoft Edge

2.5.2 Sección perfiles

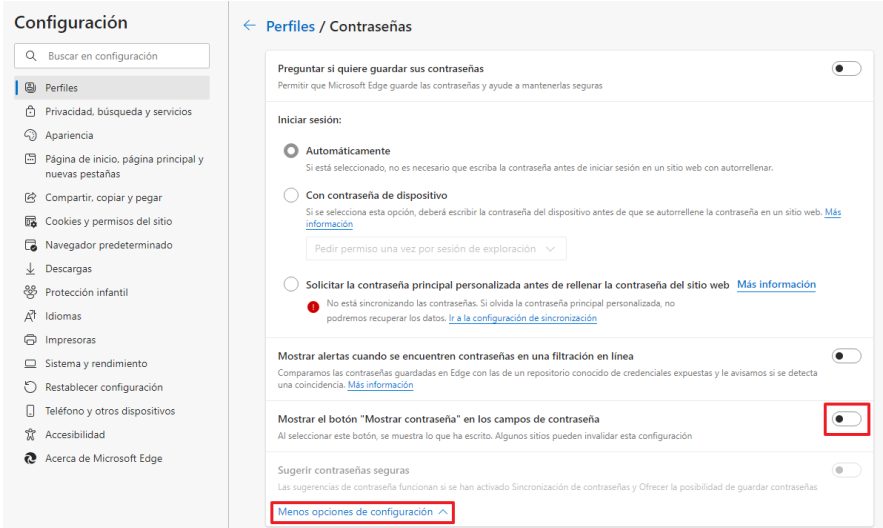
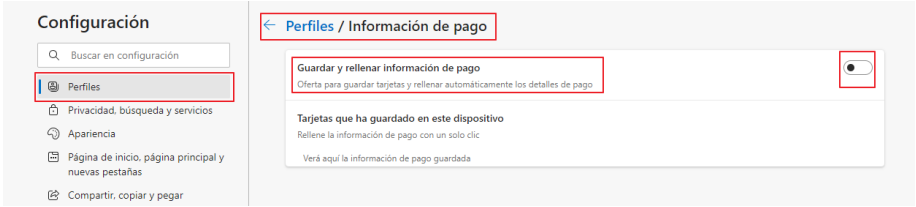
En este apartado, se indicarán los ajustes a tener en cuenta, de manera que los datos almacenados en el navegador no estén expuestos a posibles ataques no deseados así como evitar que directamente se puedan almacenar.

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

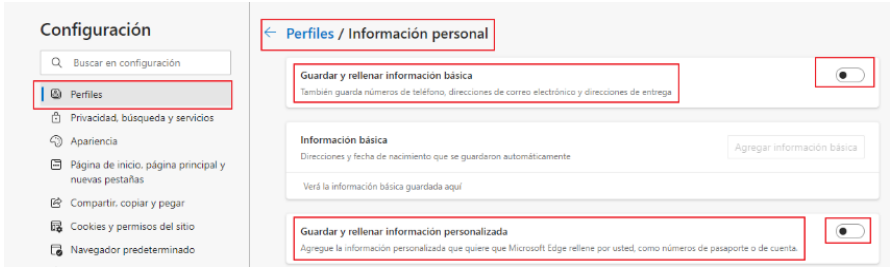


Paso	Descripción
1.	Debido a la forma en la que se almacenan las credenciales, es posible que un atacante malicioso pueda obtener acceso a las cuentas del usuario y/o utilizar las "Credenciales almacenadas" para inicios de sesión no deseados.
2.	Para evitar estos usos indebidos deshabilite la opción "Preguntar si quiere guardar sus contraseñas", en la sección "Perfiles" dentro del apartado "Contraseñas": 

2. Navegador web Microsoft Edge

Paso	Descripción
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".  The screenshot shows the 'Configuración' (Settings) menu on the left with 'Perfiles' selected. The main panel is titled 'Perfiles / Contraseñas'. Under the 'Iniciar sesión:' section, the 'Automáticamente' option is selected. Below this, the toggle for 'Mostrar el botón "Mostrar contraseña" en los campos de contraseña' is turned off, highlighted with a red box. At the bottom of the panel, the 'Menos opciones de configuración' link is also highlighted with a red box.
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) menu on the left with 'Perfiles' selected. The main panel is titled 'Perfiles / Información de pago'. Under the 'Guardar y rellenar información de pago' section, the toggle is turned off, highlighted with a red box. Below this, the 'Tarjetas que ha guardado en este dispositivo' section is visible, showing a list of saved payment methods.

2. Navegador web Microsoft Edge

Paso	Descripción
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": 
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"

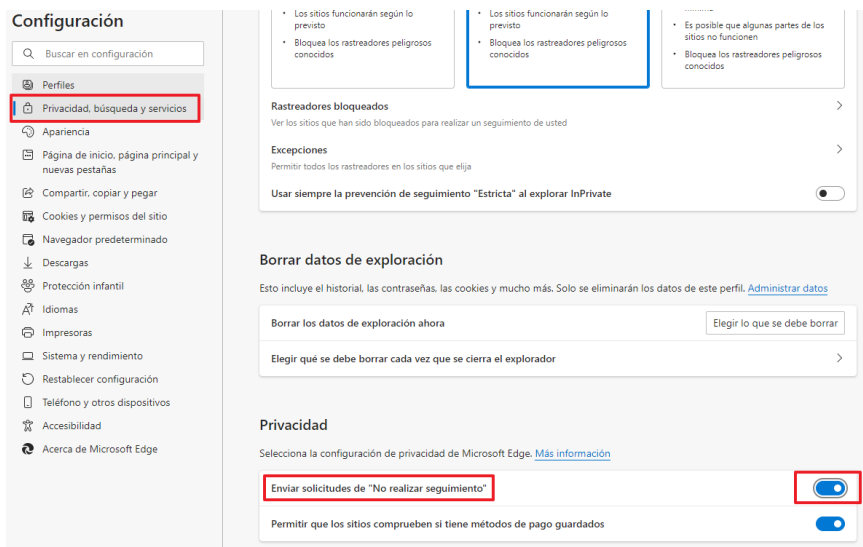
2. Navegador web Microsoft Edge

2.5.3 Sección privacidad, búsqueda y servicios

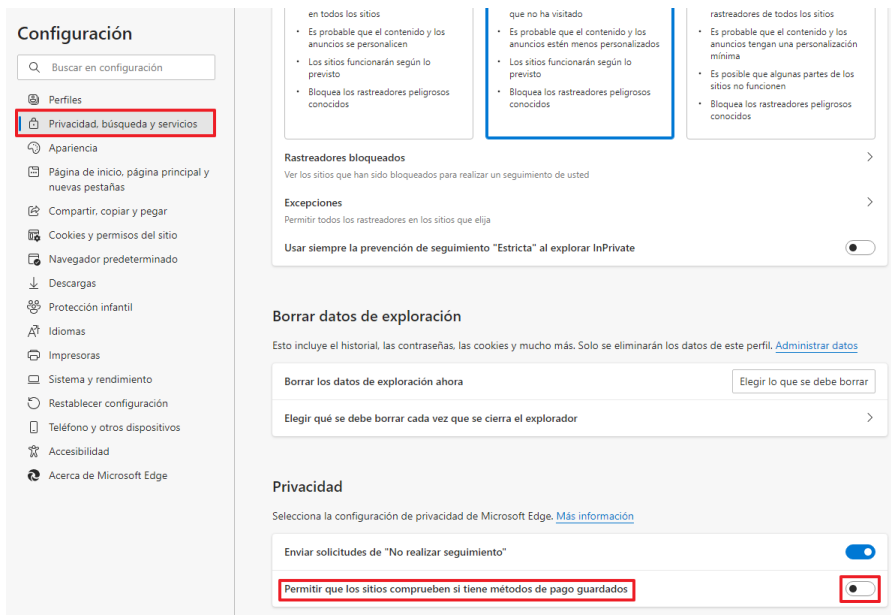
En este apartado, se configurarán las opciones de privacidad, búsqueda y servicios para evitar la obtención de información no deseada y/o requerida así como limitar las funcionalidades de los servicios ofrecidos a través del navegador.



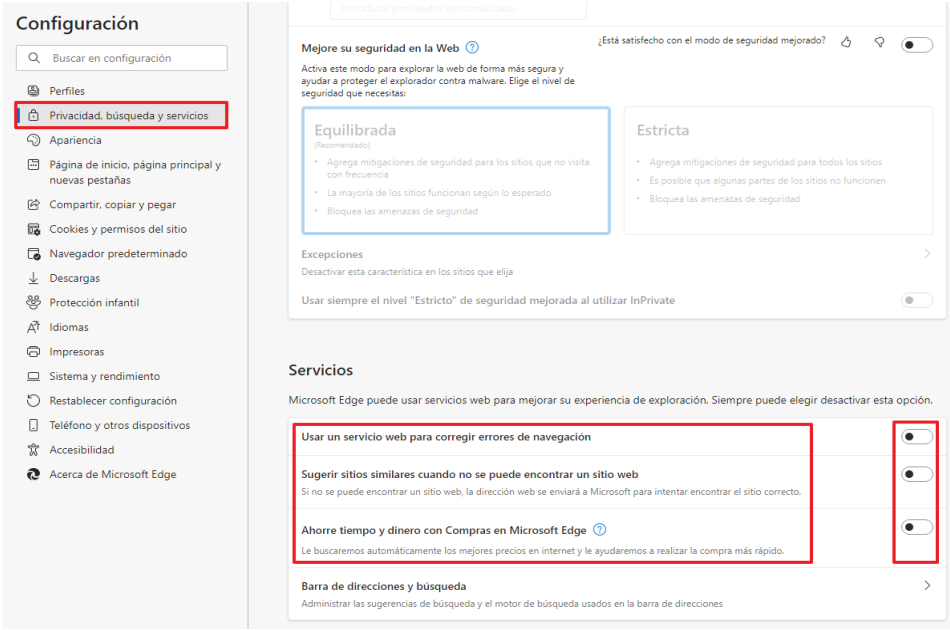
A continuación se describen las configuraciones a configurar:

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.

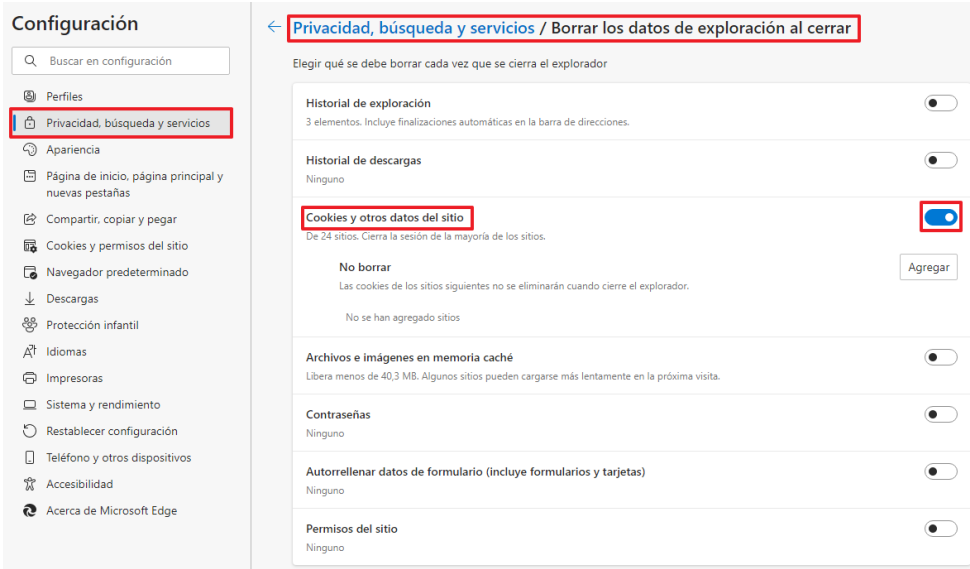
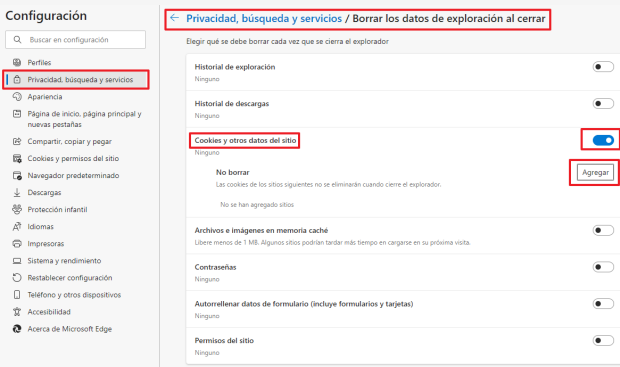
2. Navegador web Microsoft Edge

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 'Privacidad, búsqueda y servicios' (Privacy, search, and services) section selected. Under the 'Rastreadores bloqueados' (Blocked trackers) section, the toggle for 'Permitir que los sitios comprueben si tiene métodos de pago guardados' (Allow sites to check if you have saved payment methods) is turned off. Other settings like 'Rastreadores bloqueados' and 'Excepciones' are also visible.
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 'Privacidad, búsqueda y servicios' (Privacy, search, and services) section selected. Under the 'Datos de diagnóstico opcionales' (Optional diagnostic data) section, the toggle for 'Ayuda a mejorar los productos de Microsoft enviando datos de diagnóstico opcionales sobre el uso del explorador, los sitios web que visitas y los informes de bloqueo' (Help improve Microsoft products by sending optional diagnostic data about your browser usage, the websites you visit, and block reports) is turned off. Under the 'Personalizar su experiencia web' (Personalize your web experience) section, the toggle for 'Mejore su experiencia web al permitir que Microsoft use el historial de exploración de esta cuenta para personalizar la publicidad, la búsqueda, las noticias y otros servicios Microsoft' (Improve your web experience by allowing Microsoft to use your browsing history to personalize ads, search, news, and other Microsoft services) is also turned off.

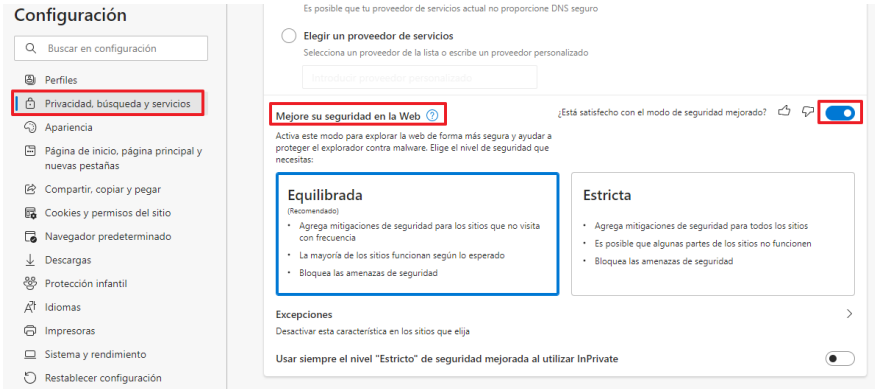
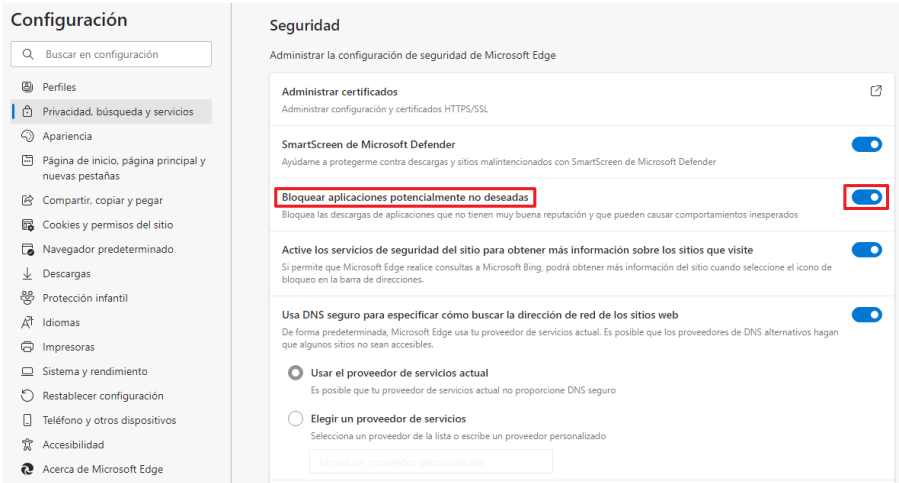
2. Navegador web Microsoft Edge

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.

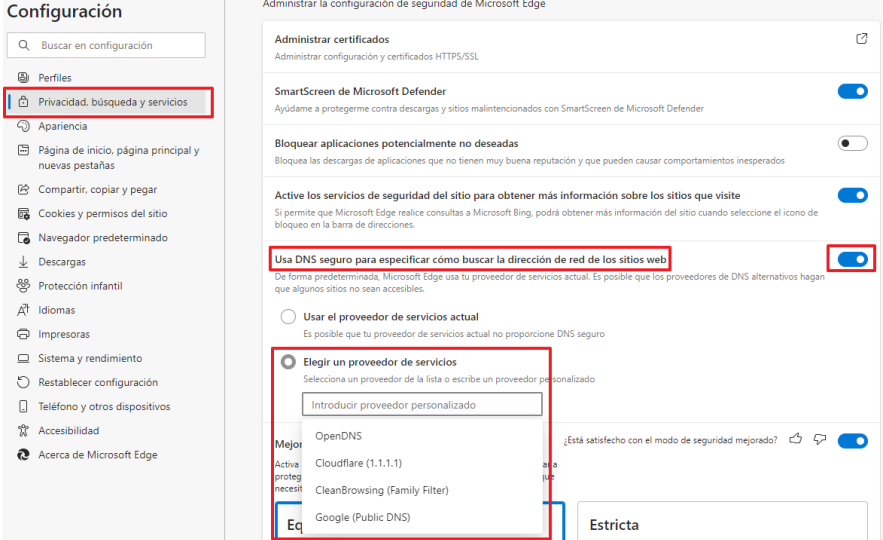
2. Navegador web Microsoft Edge

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:  Configuración ← Privacidad, búsqueda y servicios / Borrar los datos de exploración al cerrar Elegir qué se debe borrar cada vez que se cierra el explorador Historial de exploración 3 elementos. Incluye finalizaciones automáticas en la barra de direcciones. Historial de descargas Ninguno Cookies y otros datos del sitio De 24 sitios. Cierra la sesión de la mayoría de los sitios. No borrar Las cookies de los sitios siguientes no se eliminarán cuando cierre el explorador. Agregar No se han agregado sitios Archivos e imágenes en memoria caché Libera menos de 40,3 MB. Algunos sitios pueden cargarse más lentamente en la próxima visita. Contraseñas Ninguno Autorrellenar datos de formulario (incluye formularios y tarjetas) Ninguno Permisos del sitio Ninguno 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":  Configuración ← Privacidad, búsqueda y servicios / Borrar los datos de exploración al cerrar Elegir qué se debe borrar cada vez que se cierra el explorador Historial de exploración Ninguno Historial de descargas Ninguno Cookies y otros datos del sitio Ninguno No borrar Las cookies de los sitios siguientes no se eliminarán cuando cierre el explorador. Agregar No se han agregado sitios Archivos e imágenes en memoria caché Libere menos de 1 MB. Algunos sitios posiblemente tardarán más tiempo en cargarse en su próxima visita. Contraseñas Ninguno Autorrellenar datos de formulario (incluye formularios y tarjetas) Ninguno Permisos del sitio Ninguno

2. Navegador web Microsoft Edge

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:  The screenshot shows the 'Configuración' (Settings) window with the left sidebar containing 'Privacidad, búsqueda y servicios' highlighted. The main pane shows the 'Mejore su seguridad en la Web' toggle switch turned on. Below it, the 'Equilibrada' (Balanced) security level is selected, with a list of features: 'Agrega mitigaciones de seguridad para los sitios que no visita con frecuencia', 'La mayoría de los sitios funcionan según lo esperado', and 'Bloquea las amenazas de seguridad'. The 'Estricta' (Strict) level is also visible with its own list of features. At the bottom, there is an 'Excepciones' section and a toggle for 'Usar siempre el nivel "Estricto" de seguridad mejorada al utilizar InPrivate'. 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":  The screenshot shows the 'Configuración' (Settings) window with the left sidebar containing 'Privacidad, búsqueda y servicios' highlighted. The main pane shows the 'Seguridad' (Security) section. Under 'Administrar la configuración de seguridad de Microsoft Edge', the 'Bloquear aplicaciones potencialmente no deseadas' toggle switch is turned on. Other visible settings include 'Administrar certificados', 'SmartScreen de Microsoft Defender', 'Active los servicios de seguridad del sitio para obtener más información sobre los sitios que visite', and 'Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web'.

2. Navegador web Microsoft Edge

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.

2. Navegador web Microsoft Edge

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. Navegador web Microsoft Edge

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.



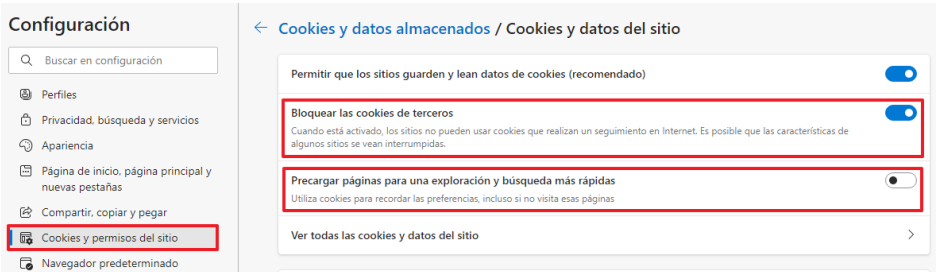
Paso	Descripción
1.	Dentro de la sección “Página de inicio, página principal y nuevas pestañas”, en el apartado “Página de la nueva pestaña”, deshabilite la opción “Carga previa de la página de pestaña nueva para una experiencia más rápida”.

2.5.5 Sección cookies y permisos del sitio

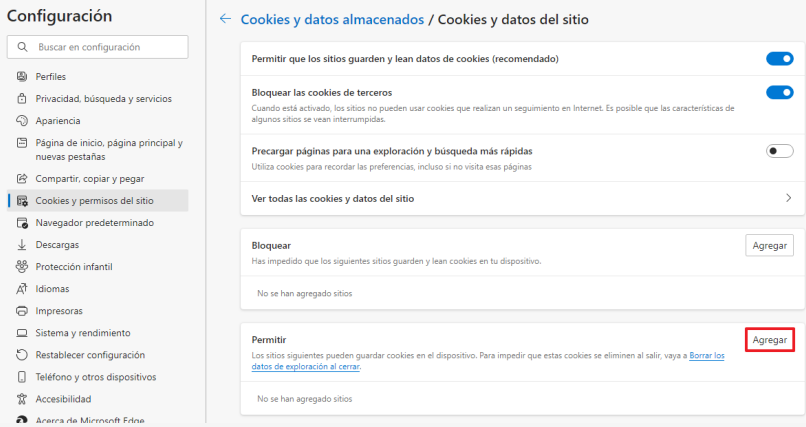
La configuración de las cookies y los envíos de información en segundo plano son una parte muy importante para la seguridad y privacidad. Con una configuración segura de estos elementos se pueden prevenir brechas de seguridad y posibles robos de información sensible, ya que un atacante podría ocultar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

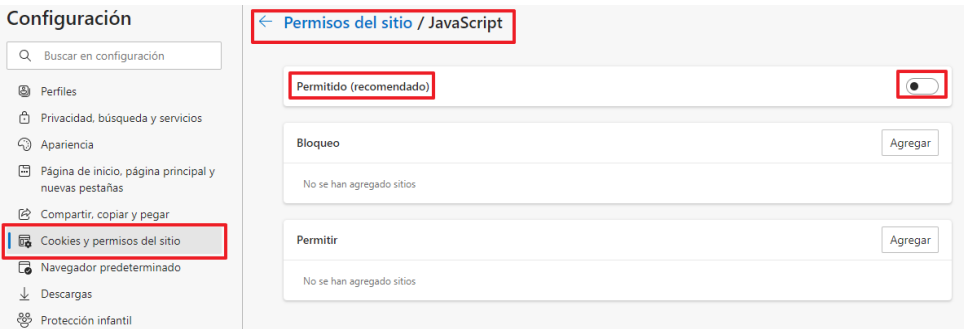
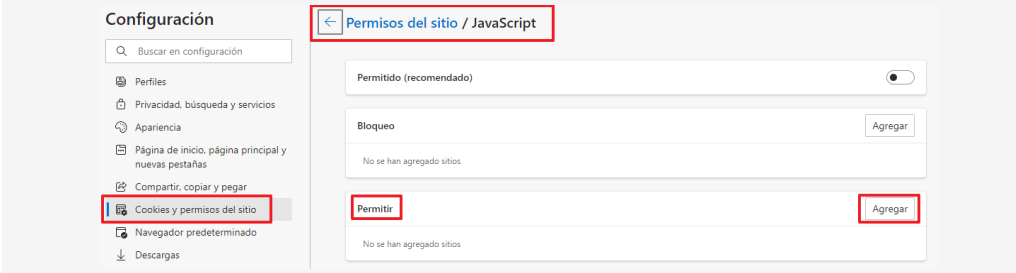
La configuración de las cookies y los envíos de información en segundo plano son una parte muy importante para la seguridad y privacidad.

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.
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: 

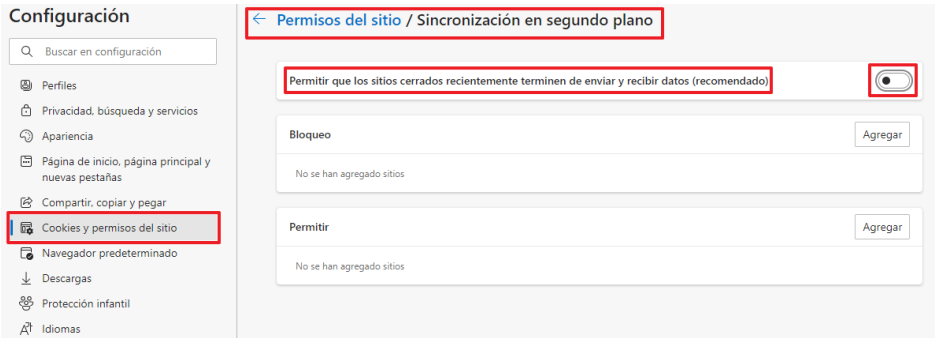
2. Navegador web Microsoft Edge

Paso	Descripción
	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.

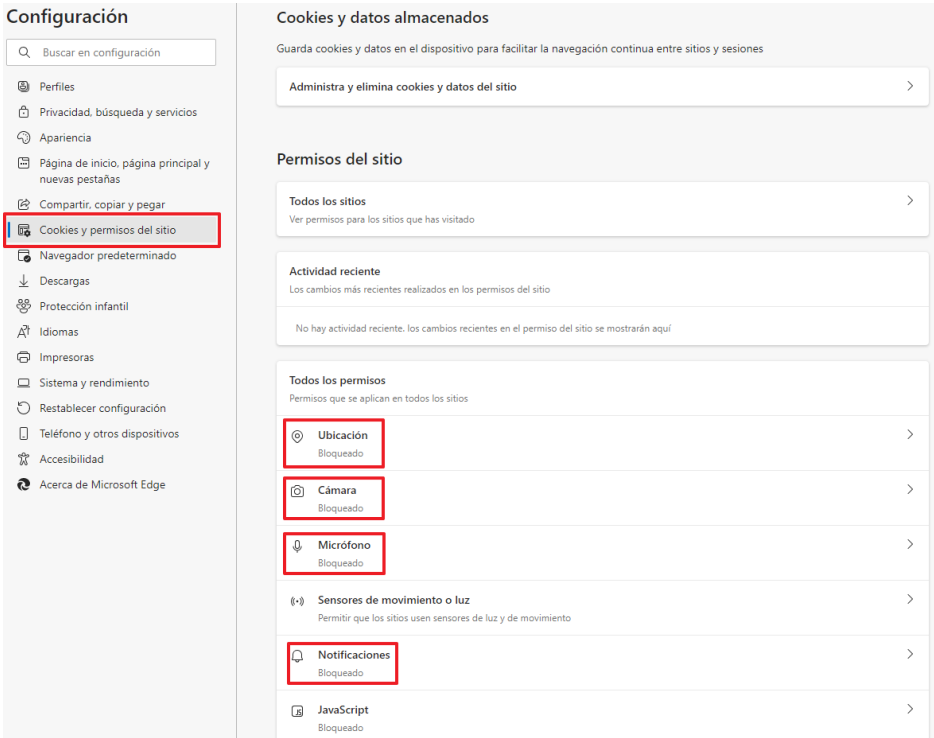
2. Navegador web Microsoft Edge

Paso	Descripción
	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:  The screenshot shows the 'Configuración' (Settings) window. In the left sidebar, 'Cookies y permisos del sitio' (Cookies and site permissions) is highlighted with a red box. The main panel shows 'Permisos del sitio / JavaScript' (Site permissions / JavaScript). Under 'Permitido (recomendado)' (Allowed (recommended)), the toggle switch is turned off, also highlighted with a red box. Below it, the 'Bloqueo' (Block) section has an 'Agregar' (Add) button. The 'Permitir' (Allow) section also has an 'Agregar' button.
4.	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".  This screenshot is similar to the previous one, but with an additional red box around the 'Permitir' (Allow) button in the 'Permisos del sitio / JavaScript' section, indicating where to add exceptions.

2. Navegador web Microsoft Edge

Paso	Descripción
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:  The screenshot shows the 'Configuración' (Settings) menu on the left with 'Cookies y permisos del sitio' highlighted. The main panel shows 'Permisos del sitio / Sincronización en segundo plano'. The toggle for 'Permitir que los sitios cerrados recientemente terminen de enviar y recibir datos (recomendado)' is turned off. Below it are sections for 'Bloqueo' and 'Permitir', both showing 'No se han agregado sitios'.
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”

2. Navegador web Microsoft Edge

Paso	Descripción
	Esta configuración podrá ser modificada, permitiendo su uso o añadiendo excepciones a los sitios web que requieran el uso de estos elementos:  Configuración Buscar en configuración - Perfiles - Privacidad, búsqueda y servicios - Apariencia - Página de inicio, página principal y nuevas pestañas - Compartir, copiar y pegar Cookies y permisos del sitio - Navegador predeterminado - Descargas - Protección infantil - Idiomas - Impresoras - Sistema y rendimiento - Restablecer configuración - Teléfono y otros dispositivos - Accesibilidad - Acerca de Microsoft Edge Cookies y datos almacenados Guarda cookies y datos en el dispositivo para facilitar la navegación continua entre sitios y sesiones Administra y elimina cookies y datos del sitio Permisos del sitio Todos los sitios Ver permisos para los sitios que has visitado Actividad reciente Los cambios más recientes realizados en los permisos del sitio No hay actividad reciente. los cambios recientes en el permiso del sitio se mostrarán aquí Todos los permisos Permisos que se aplican en todos los sitios Ubicación Bloqueado Cámara Bloqueado Microfono Bloqueado Sensores de movimiento o luz Permitir que los sitios usen sensores de luz y de movimiento Notificaciones Bloqueado JavaScript Bloqueado

2. Navegador web Microsoft Edge

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:

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.

3. Lista de comprobación

Criticidad	Descripción
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

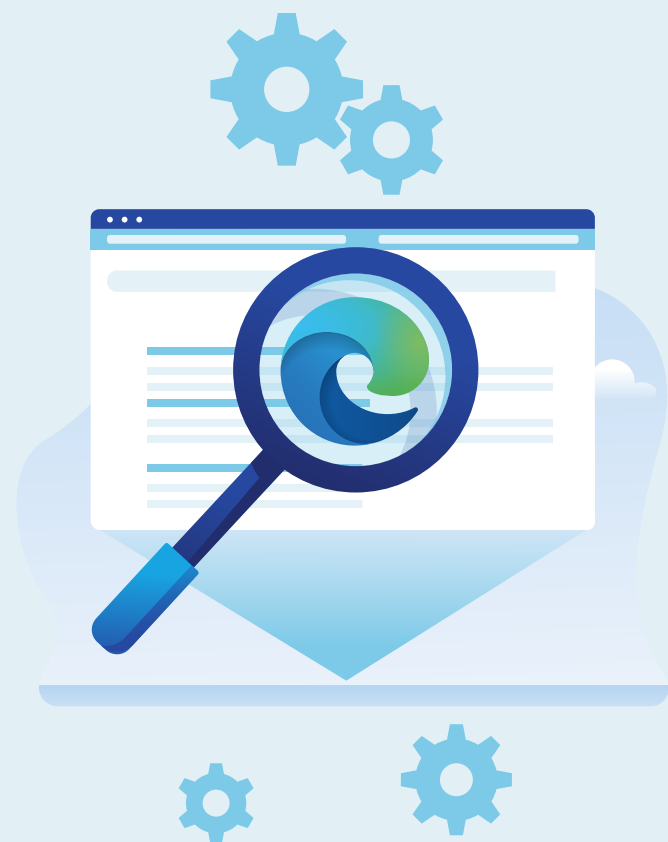
A continuación, se indican diez recomendaciones de seguridad en el uso de Microsoft Edge.



Decálogo de recomendaciones para Microsoft Edge

- 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 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.
- 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, código de verificación, 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.





www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es