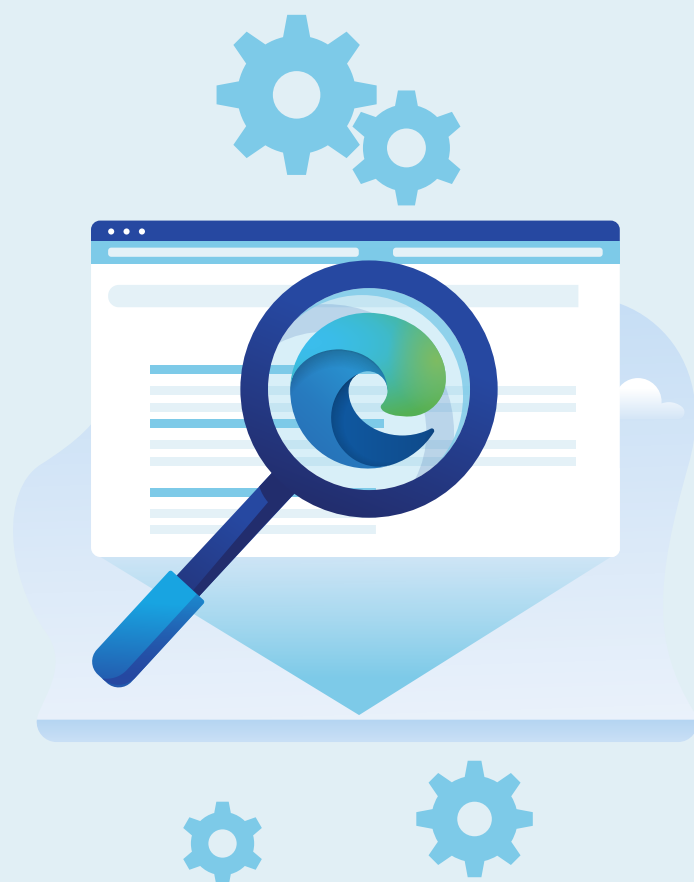


CCN-CERT
BP/26



Microsoft Edge security recommendations

BEST PRACTICE REPORT

JUNE 2022

ccn-cert
centro criptológico nacional

CCN
centro criptológico nacional

Edit:



CENTRO CRIPTOLÓGICO NACIONAL
cn=CENTRO CRIPTOLÓGICO NACIONAL,
2.5.4.97=VATES-528001551, ou=CENTRO
CRIPTOLÓGICO NACIONAL, o=CENTRO
CRIPTOLÓGICO NACIONAL, v=2022.09.23 01:05:55 +0200

© National Cryptologic Centre, 2022

Date of issue: June 2022

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained herein, expressly rejecting any type of implicit guarantee that may be related to it. Under no circumstances can the National Cryptologic Centre be held responsible for direct, indirect, fortuitous or extraordinary damage derived from the use of the information and software indicated, even when warned of such a possibility.

LEGAL NOTICE

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the penalties established by law.

Foreword

In an increasingly complex and globalised world, in which information and communication technologies (ICTs) play an extremely important role, we must be aware that the proper management of cybersecurity is a collective challenge that we must necessarily face. It is necessary to ensure the protection of our country's economic, technological and political capacity, especially when the proliferation of targeted attacks and the theft of sensitive information is an undeniable reality.

It is therefore essential to keep abreast of the threats and vulnerabilities associated with the use of new technologies. Knowledge of the risks that loom over cyberspace must serve to implement with guarantees the measures, both procedural and technical and organisational, that allow for a safe and reliable environment.

Law 11/2002, of 6 May, regulating the National Intelligence Centre (CNI), entrusts the National Intelligence Centre with the exercise of functions relating to the security of information technologies and the protection of classified information, while at the same time conferring on its Secretary of State Director the responsibility of directing the National Cryptologic Centre (CCN).

Based on the CNI's knowledge and experience of threats and vulnerabilities in terms of emerging risks, the Centre carries out, through the National Cryptologic Centre, regulated by Royal Decree 421/2004 of 12 March, various activities directly related to ICT security, aimed at training expert personnel, the use of appropriate security technologies and the application of security policies and procedures.

We must be aware that the proper management of cybersecurity is a collective challenge that we must necessarily face.

Precisely, this series of CCN-STIC documents is a clear reflection of the work that this body carries out in terms of security implementation, enabling the application of policies and procedures, as the guides have been drawn up with a clear objective: to improve the degree of cybersecurity of organisations, aware of the importance of establishing a reference framework in this area to support government staff in carrying out the difficult task of providing security for the ICT systems under their responsibility.

With this series of documents, the National Cryptologic Centre, in compliance with its tasks and with what is reflected in Royal Decree 3/2010 regulating the National Security Scheme in the field of electronic administration, contributes to improving Spanish cybersecurity and maintaining the infrastructures and information systems of all public administrations with optimal levels of security. The aim is to generate confidence and guarantees in the use of these technologies, protecting the confidentiality of data and guaranteeing its authenticity, integrity and availability.

June 2022

Esperanza Casteleiro Llamazares

Secretary of State

Director of the National Cryptologic Centre



Index

1. Introduction	6
2. Microsoft Edge web browser	7
2.1. Versions	9
2.2. Minimum requirements	11
2.3. Download	13
2.4. Installation and initial configuration	15
2.5. Configuration guidelines	19
2.5.1 Synchronisation and basic language settings	19
2.5.2 Profile section	21
2.5.3 Privacy, search and services section	24
2.5.4 Section home page, main page and new tabs	31
2.5.5 Cookies and site permissions section	32
2.5.6 System and performance section	37
3. Checklist	38
4. Decalogue of recommendations	40

1. Introduction

The purpose of this document is to set out the procedures and utilities needed to implement and secure Microsoft Edge against the risks to which it may be exposed.

For this purpose, a series of steps and instructions are provided to enable the browser to be configured manually. A configuration file is also provided to apply security measures and thus facilitate the possibility of implementing security.

In the development of this guide, the **Microsoft Edge Stable** program installer in **Version 102.0.1245.33 (Official 64-bit version)** for Windows operating systems was used. This configuration is also valid for the Microsoft Edge Business version.

Regardless of which version you choose, Stable or Business version of Microsoft Edge, both correspond to the same build, with the only difference being that the Business version does not require an internet connection for installation.



2. Microsoft Edge web browser

Microsoft Edge was initially built with Microsoft's own **EdgeHTML** and **Chakra** engines. In 2019, Microsoft Edge was rebuilt as a Chromium-based browser, using the **Blink** and **V8** engines. These engines provide better security and a better look and feel.

Microsoft Edge will replace the Internet Explorer browser in Windows environments as the default browser starting with the 1709 distribution of Windows 10 and in the new Windows 11 operating system.

Microsoft Edge will replace the Internet Explorer browser in Windows environments as the default browser.

NOTE : Additional information about the end of support for Internet Explorer 11 and the replacement by Microsoft Edge is available via the following link:



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

Microsoft Edge is available for free download from the Microsoft website. It is also deployed by default on Windows 10 and Windows 11 operating systems with no download required.

2. Microsoft Edge web browser

An internet connection is required to download the installer, as for the browser installation process. If the computer on which Microsoft Edge is installed does not have an internet connection, you will need to download the full browser via the **“Business”** version of the browser, using the alternative link provided by Microsoft for this purpose.

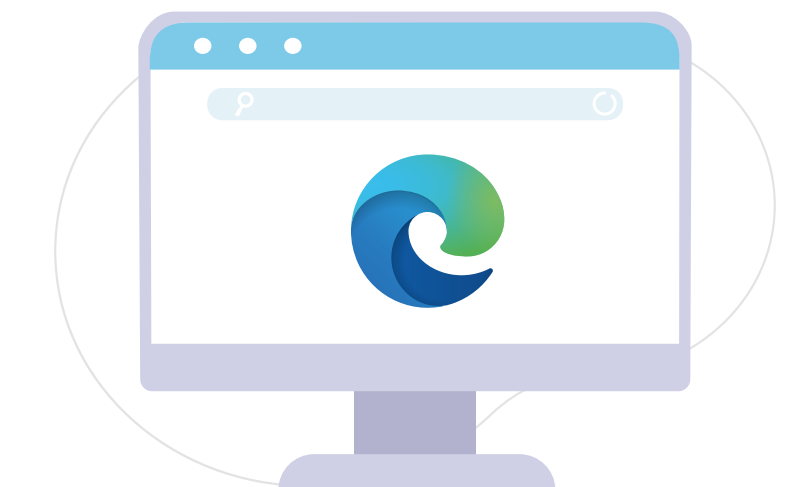
NOTE: The downloading of the browser will be carried out later on, more specifically in the point “2.3 DOWNLOAD”. However, a download link from the manufacturer of the Business version of the browser is provided below, as this guide is based on the stable version of the browser:



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

You can also install and update the Microsoft Edge browser from the **Windows Update** tool of the Windows operating system, manually by downloading the latest version from the Microsoft website or from the Microsoft Edge settings panel itself.

In this regard, Microsoft Edge must have the latest security-related software updates installed. If the latest security-related software updates for Microsoft Edge are not applied, this would be considered a **critical security flaw**.



2. Microsoft Edge web browser

2.1 Versions

Microsoft Edge offers a major release cycle cadence of four (4) weeks, but the effective duration of supported support for a stable channel release is approximately twelve (12) weeks.

NOTE: Additional information on the product lifecycle can be found at the following link:



<https://docs.microsoft.com/es-es/deployedge/microsoft-edge-support-lifecycle>

Security updates and maintenance updates are only available in the latest version of the **“Stable”** version and the latest version of the **“Beta”** channel. If you are using older versions of Microsoft Edge, you are likely to miss out on the latest quality and security updates.

The following is a summary of the different versions of Microsoft Edge:



Microsoft Edge

The Stable Channel is designed for wide deployment in the organisation and is the channel that most users should be on. It is the most widespread of the releases and is the result of the stabilisation of the feature set available in the previous version of the Beta Channel. New features are shipped approximately every 4 weeks. Security and quality updates are shipped as needed.

2. Microsoft Edge web browser

Microsoft Edge BETA



The Beta Channel is intended for production testing deployment to a representative set of users. This channel provides a great opportunity to validate that configurations or requirements work as expected in an environment. If a problem is found, it is possible to fix it before the release is published in the stable channel. Like the Microsoft Edge release new features are shipped approximately every 4 weeks. Security and quality updates are shipped as needed.

Microsoft Edge DEV



The DEV channel is intended to help plan and develop the latest updates to Microsoft Edge, but at a higher quality than the Canary channel. This channel is used to get an early look at what's new and prepare for the next Beta release.

Microsoft Edge Canary



The Canary channel is updated daily and is the most cutting-edge of all channels. If you want to access the latest features, they will appear here first.

Microsoft Edge Business

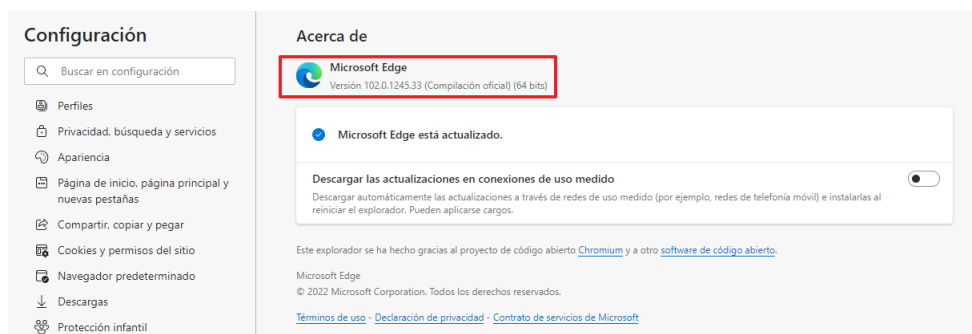


This version is the same Microsoft Edge browser that is used in the stable version. The difference is in how it is deployed and managed. IT administrators can download this version to install the Microsoft Edge browser through an .msi installer and manage their organisation's browsers through group policies.

2. Microsoft Edge web browser

To find out which version of Microsoft Edge is installed on a device, follow the steps below:

Start Microsoft Edge, and click on the  button at the top right of the browser. Then click on **“Settings”** in the panel that appears. Then go to the **“About Microsoft Edge”** section. The version number of the installed version will be displayed below the name of Microsoft Edge, as shown in the image below:



2.2 Minimum requirements

The following are the minimum system requirements necessary to implement Microsoft Edge:



Supported operating systems (32-bit and 64-bit versions).

- Windows 7
- Windows 8.1
- Windows 10 Professional 1709 and later
- Windows 10 Home 1709 and later
- Windows 10 Enterprise 2015 LTSC
- Windows 10 Enterprise 2016 LTSC
- Windows 10 Enterprise 2019 LTSC
- Windows 11 Professional

2. Microsoft Edge web browser

	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 or higher
	iOS 11 or higher
	Android KitKat4.4 or higher
	Linux (Ubuntu, Debian, Fedora and openSUSE)

NOTE: Additional information on supported operating systems is available via the following official manufacturer's link:



<https://docs.microsoft.com/es-es/deployedge/microsoft-edge-supported-operating-systems>



Recommended hardware requirements:



Recommended minimum requirements for the installed 64-bit operating system.



Recommended minimum requirements for the installed 32-bit operating system.

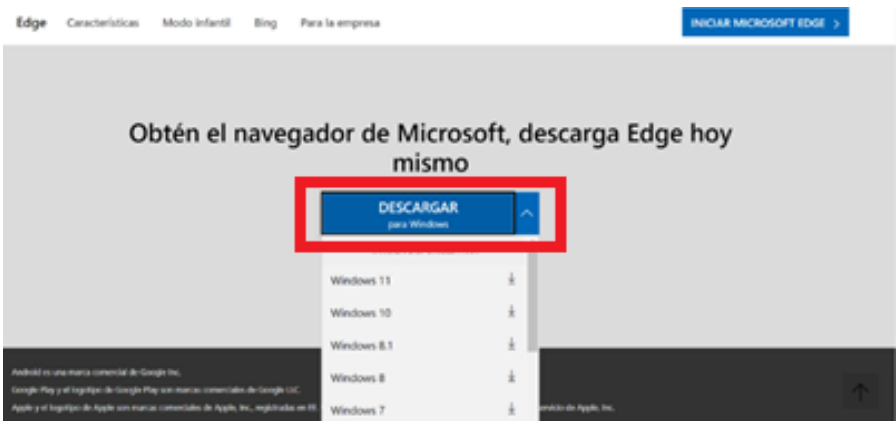
2. Microsoft Edge web browser

2.3 Download

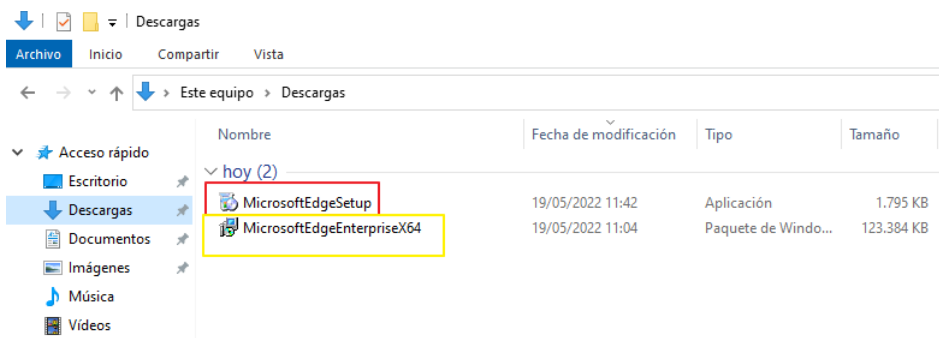
In some cases, for example in the Windows 10 Pro and Home operating systems, Microsoft Edge is already installed by default and integrated with the operating system.

The following is the process to follow to download the Microsoft Edge browser on computers that do not have it installed by default and require it to be installed:



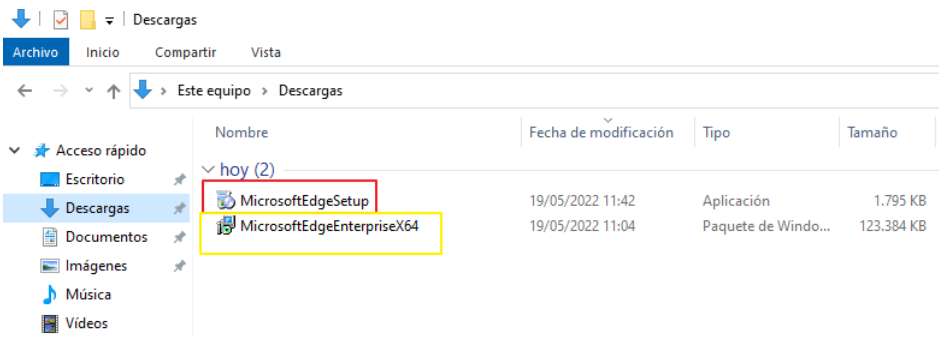
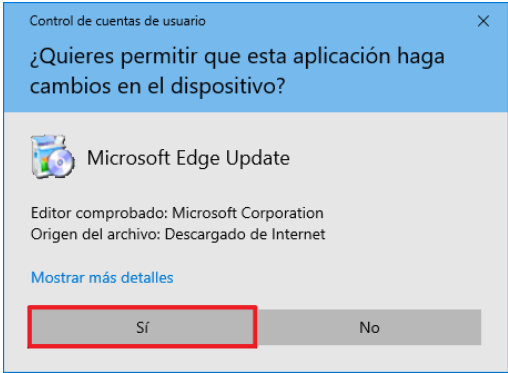
Passage	Description
1.	To download the programme from the official source, please use the following link: https://www.microsoft.com/es-es/edge
2.	Download the browser version according to your operating system.  A screenshot of the Microsoft Edge download page in Spanish. The page has a header with links for 'Edge', 'Características', 'Modo infantil', 'Bing', and 'Para la empresa', along with a button 'INICIAR MICROSOFT EDGE'. The main heading is 'Obtén el navegador de Microsoft, descarga Edge hoy mismo'. Below this is a 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 is a footer with legal disclaimers about Google Play and Apple App Store.

2. Microsoft Edge web browser

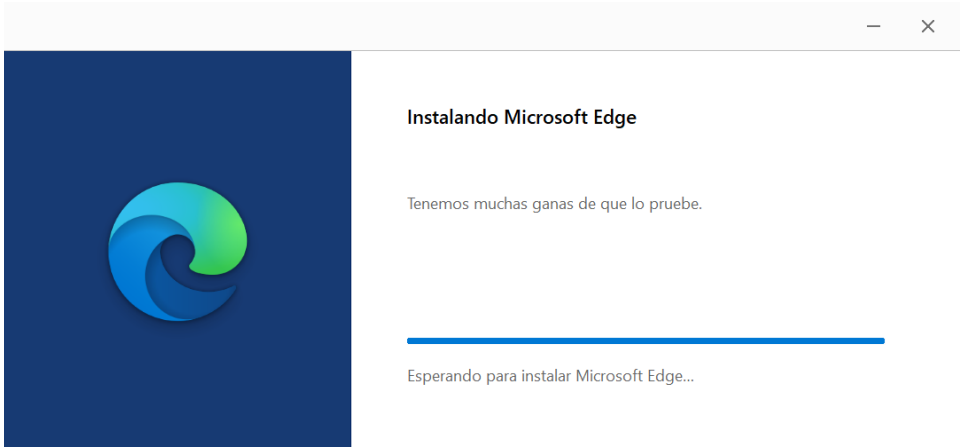
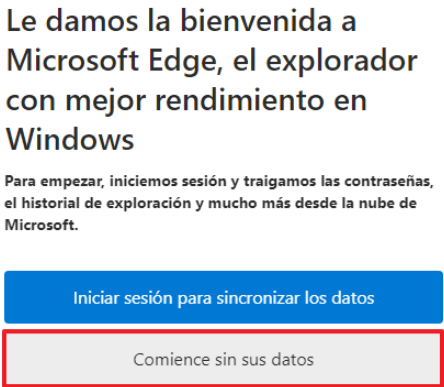
Passage	Description
3.	The downloaded file will appear in the location you have determined, depending on the configuration set in the browser you are using. The red box in the image corresponds to the normal download of the installer that requires an internet connection (Used during the guide). The yellow box in the image corresponds to the download for offline computers, where Microsoft Edge offers the Business solution for offline installations.
	

2.4 Installation and initial configuration

To install Microsoft Edge, perform the following steps:

Passage	Description
1.	Run the downloaded file by double-clicking on it, either in the version that requires an internet connection (Used during this guide) or the version without internet connection. 
2.	To begin with the installation of Microsoft Edge, elevation of privileges is required. To do this, click on the “Yes” option in the pop-up window (“User Account Control”) 

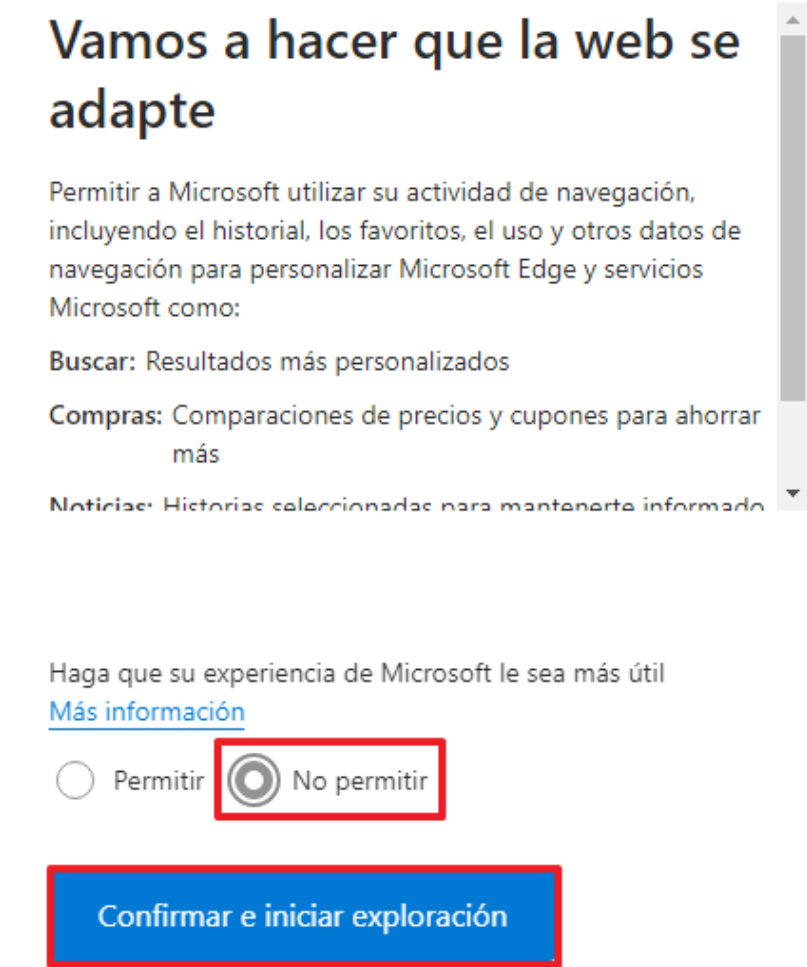
2. Microsoft Edge web browser

Passage	Description
3.	Once allowed to run, it will download and install automatically. 
4.	After completing the installation, on the first start-up, a welcome window will appear where security settings must be made.
5.	In the first Microsoft Edge configuration window check the option “Start without your data”. 

2. Microsoft Edge web browser

Passage	Description
6.	In the second Microsoft Edge configuration window, check the option “Continue without this data”. 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.	On the next screen, configure access to recent scan data. Tick the “Do not allow” option to restrict such access and click on “Confirm and continue”. 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. Microsoft Edge web browser

Passage	Description
8.	Finally, in the web adaptation settings, tick the option "Do not allow" to prevent Microsoft from using your browsing information. Click on "Confirm and start scan".  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.	After these settings, several browsing windows will open, one of which is oriented towards the aesthetic customisation of the browser. You can ignore them and continue with the next section.

2.5 Configuration guidelines

The Microsoft Edge browser has a graphical interface for editing its usage and security settings.

To access the configuration interface, start Microsoft Edge and click on the button  at the top right of the browser. Then select the **“Settings”** section, where the user-editable configuration options will appear.

An alternative method to access the configuration interface is to type **“edge://settings/profiles”** in the address bar.



2.5.1 Synchronisation and basic language settings

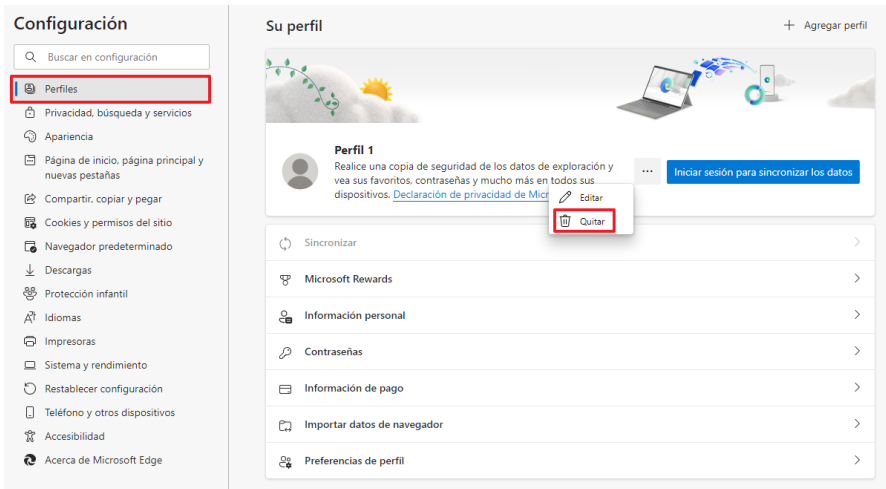
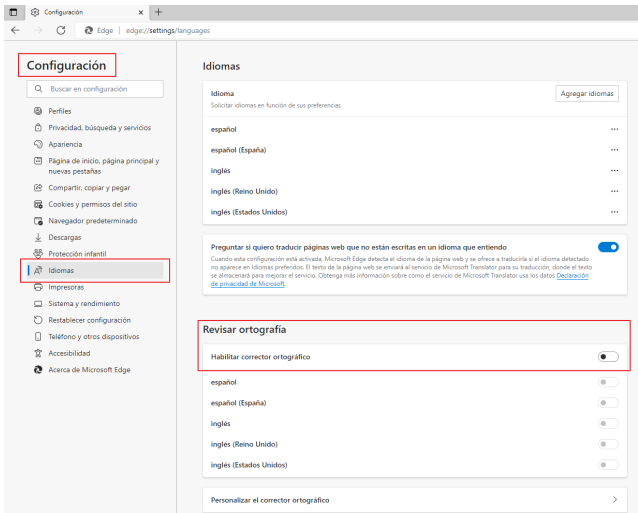
The Microsoft Edge browser enables automatic synchronisation with Microsoft services, allowing users to, among other things, automatically synchronise various items such as bookmarks, open tabs, passwords, extensions, etc.

This information is stored in the Microsoft account provided by the user for this purpose. It should be noted that in order to avoid privacy and security problems, it is recommended to disable this functionality in the browser.

Once the browser is installed, follow the steps below to make the basic language setting and disable the spell checker, so that no user data is collected by these methods:



2. Microsoft Edge web browser

Passage	Description
1.	In the “Profiles” section, and whenever possible, deletion of any synchronised accounts is recommended to prevent disclosure and/or collection of the information collected. This is not impeded by the existence of profiles to differentiate the use of the browser. 
2.	In the “Settings” menu, in the “Languages” section, access the “Check spelling” section. Disable the option “Enable spell check”. 

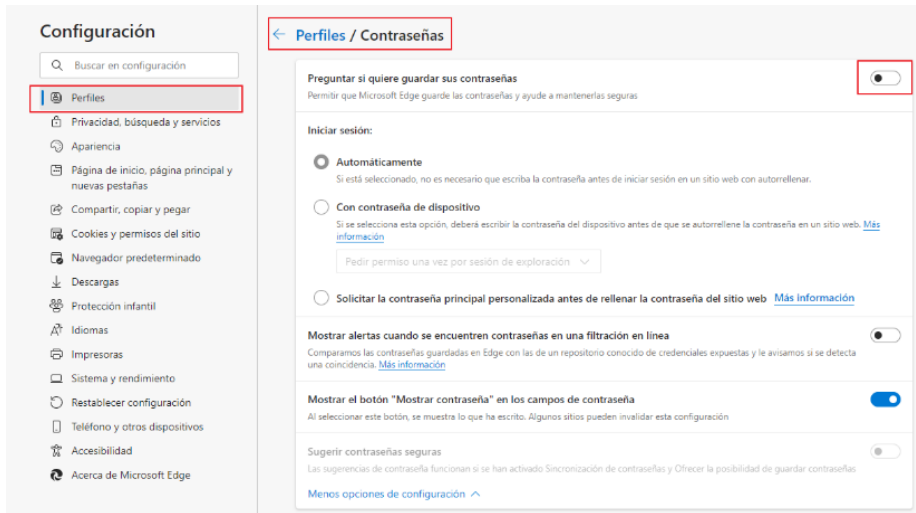
2. Microsoft Edge web browser

2.5.2 Profile section

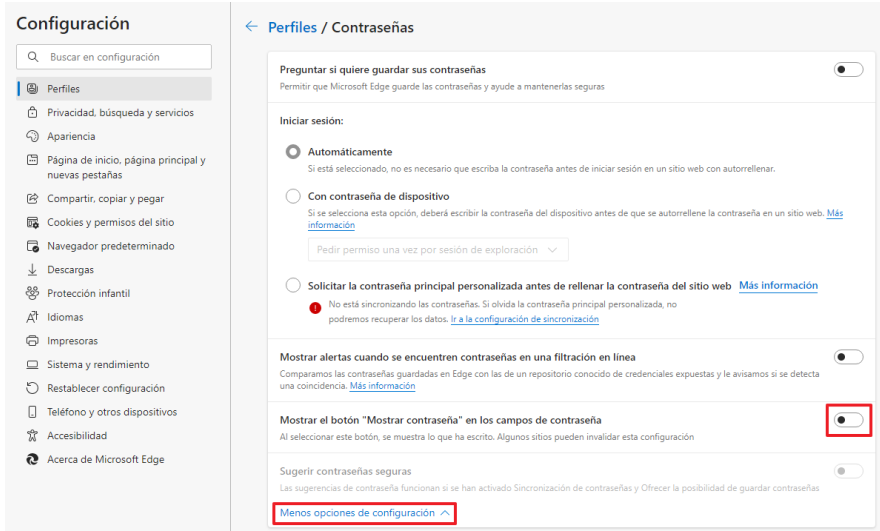
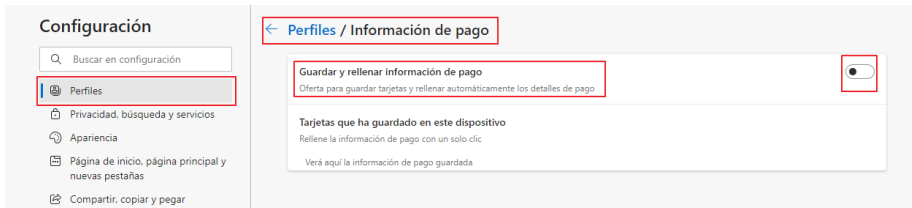
In this section, the settings to be taken into account will be indicated, so that the data stored in the browser are not exposed to possible unwanted attacks and to prevent them from being stored directly.

Each of the steps to be followed for the proper configuration of this section is described below:

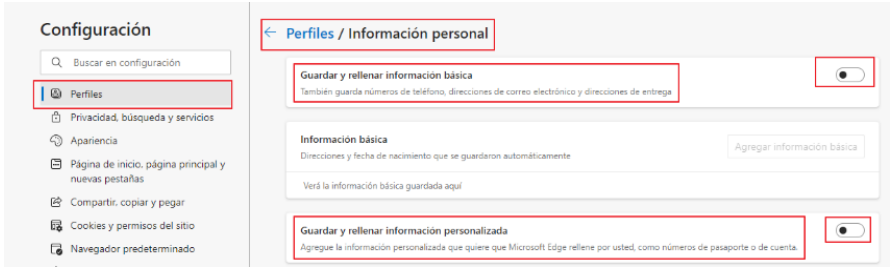


Passage	Description
1.	Because of the way credentials are stored, it is possible that a malicious attacker could gain access to user accounts and/or use "Stored Credentials" for unwanted logins.
2.	To avoid such misuse, disable the option "Ask if you want to save your passwords" in the "Profiles" section under "Passwords": 

2. Microsoft Edge web browser

Passage	Description
3.	Then click on the option “More configuration options” and disable the option “Show the “Show password” button in the password fields”. 
4.	The “Payment methods” information is an attractive element for attackers looking to make fraudulent use of it and, therefore, it is recommended not to have this information stored in the Microsoft Edge browser to avoid being the target of malicious attacks.
5.	Disable the option “Save and fill in payment information”, as shown in the image below, in the “Profiles” section under “Payment information”: 
6.	As in the previous case, the storage of information, although not critical, can provide an attacker with relevant information about the user’s movements, actions or other considerations.

2. Microsoft Edge web browser

Passage	Description
7.	To prevent the use of this information, disable the following options: + “Save and fill in basic information”. + “Save and fill in personalised information”. These can be found in the “Profiles” section, under “Personal information”: 
8.	In addition to the aforementioned configuration, the following options must be disabled in each of the aforementioned sections of the profiles section: + “Microsoft Rewards” section: • Disable “Earn Microsoft Rewards in Microsoft Edge”. + “Profile preference” section: • Disable “Allow single sign-on for professional or educational sites using this profile”.

2. Microsoft Edge web browser

2.5.3 Privacy, search and services section

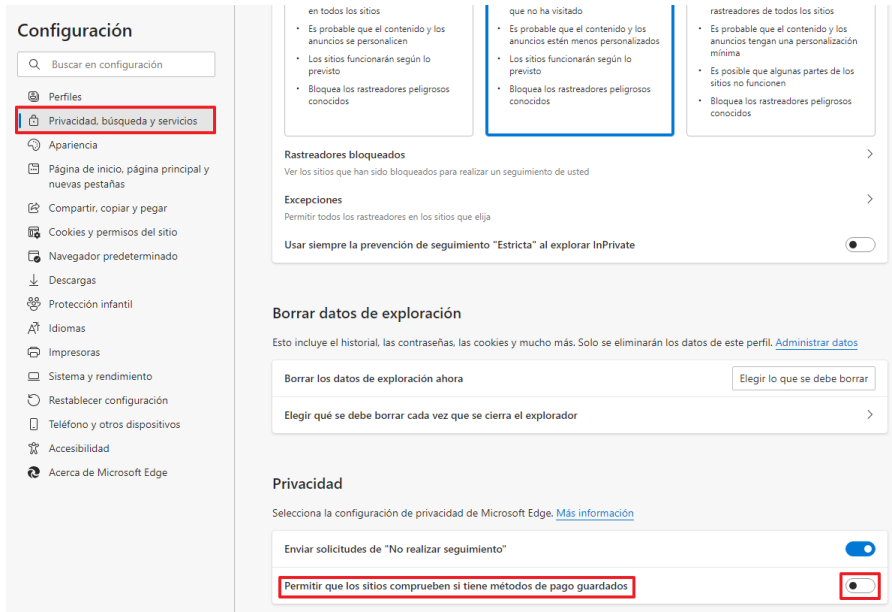
In this section, the privacy, search and service options will be configured to avoid obtaining unwanted and/or required information and to limit the functionalities of the services offered through the browser.

The settings to be configured are described below:

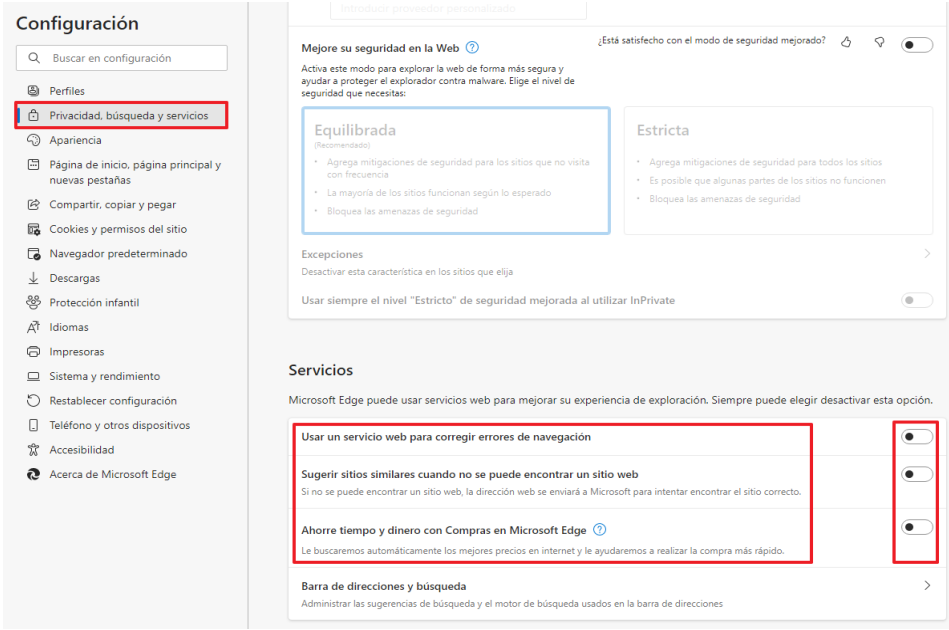


Passage	Description
1.	In the "Privacy, search and services" section itself, in the "Privacy" section, disable the "Send "do not track" requests" option, as shown in the image below: Configuración Buscar en configuración Perfiles Privacidad, búsqueda y servicios Apariencia Página de inicio, página principal 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 Los sitios funcionarán según lo previsto Bloquea los rastreadores peligrosos conocidos Los sitios funcionarán según lo previsto Bloquea los rastreadores peligrosos conocidos Es posible que algunas partes de los sitios no funcionen Bloquea los rastreadores peligrosos conocidos Rastreadores bloqueados Ver los sitios que han sido bloqueados para realizar un seguimiento de usted Excepciones Permitir todos los rastreadores en los sitios que elija Usar siempre la prevención de seguimiento "Estricta" al explorar InPrivate Borrar datos de exploración Esto incluye el historial, las contraseñas, las cookies y mucho más. Solo se eliminarán los datos de este perfil. Administrar datos Borrar los datos de exploración ahora Elegir lo que se debe borrar Elegir qué se debe borrar cada vez que se cierra el explorador Privacidad Selecciona la configuración de privacidad de Microsoft Edge. Más información Enviar solicitudes de "No realizar seguimiento" Permitir que los sitios comprueben si tiene métodos de pago guardados No realizar seguimiento Cualquier efecto de activar esto depende de si un sitio web responde a la solicitud y de cómo se interpreta la solicitud. Por ejemplo, algunos sitios podrían responder a esta solicitud mostrando los anuncios que no estén basados en otros sitios web que haya visitado. Muchos sitios seguirán recopilando y usando sus datos de exploración; por ejemplo, para mejorar la seguridad, para proporcionar contenido, servicios, anuncios y recomendaciones en sus sitios web y para generar estadísticas de informes. Enviar solicitud Cancelar Note: When this option is activated, a dialogue box will appear, click "Submit request" to continue.

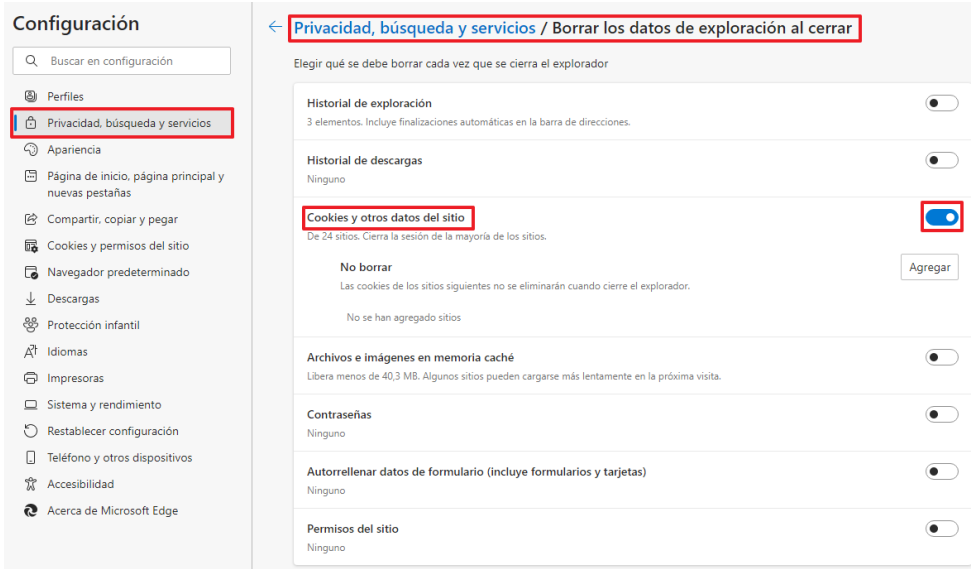
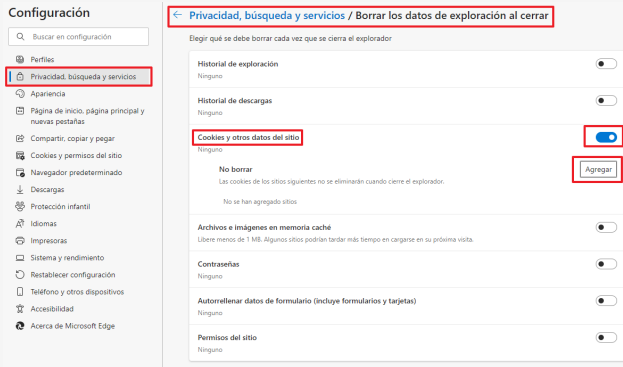
2. Microsoft Edge web browser

Passage	Description
2.	In the same section, disable the option “Allow sites to check if you have saved payment methods”.  The screenshot shows the 'Configuración' (Settings) window of Microsoft Edge. The left sidebar lists various settings categories, with 'Privacidad, búsqueda y servicios' (Privacy, search, and services) highlighted. The main content area shows the 'Rastreadores bloqueados' (Blocked trackers) section, which is currently expanded. Below this, the 'Borrar datos de exploración' (Clear browsing data) section is visible. The 'Privacidad' (Privacy) section is also visible, showing the 'Enviar solicitudes de "No realizar seguimiento"' (Send 'Do not track' requests) toggle, which is currently enabled. The 'Permitir que los sitios comprueben si tiene métodos de pago guardados' (Allow sites to check if you have saved payment methods) toggle is currently disabled, as indicated by the red box around the toggle switch.
3.	Next, in the “Optional diagnostic data” and “Customise your web experience” sections, make sure that both options are disabled as shown in the following image:  The screenshot shows the 'Configuración' (Settings) window of Microsoft Edge. The left sidebar lists various settings categories, with 'Privacidad, búsqueda y servicios' (Privacy, search, and services) highlighted. The main content area shows the 'Datos de diagnóstico opcionales' (Optional diagnostic data) section, which is currently expanded. Below this, the 'Personalizar su experiencia web' (Customize your web experience) section is visible. The '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) toggle is currently disabled, as indicated by the red box around the toggle switch. The '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) toggle is also currently disabled, as indicated by the red box around the toggle switch.

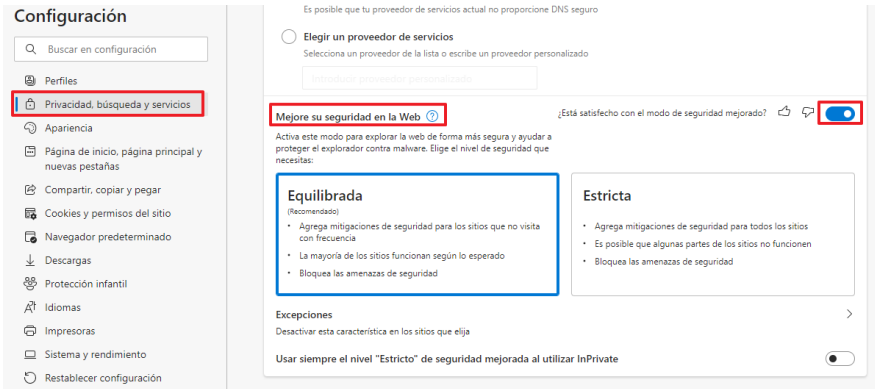
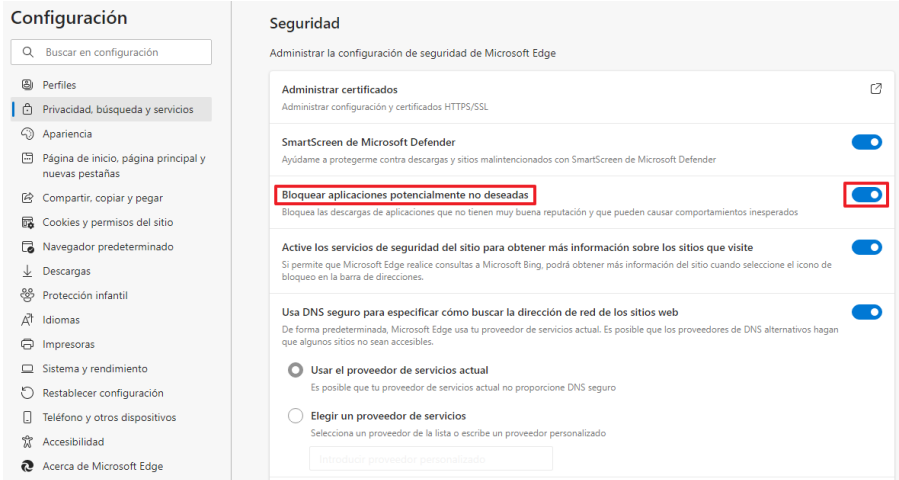
2. Microsoft Edge web browser

Passage	Description
4.	Continuing in the "Privacy, search and services" section, in the "Services" section, the following options related to web services functionalities offered by Microsoft Edge will be disabled, as shown in the following image: 
5.	Next, some settings must be defined that define the behaviour of the browser when the use of the browser is terminated so that the files generated by the browser during its execution are deleted. This encourages the loading of the latest versions of the pages visited, as well as the updated configuration for the website, on subsequent visits to the site, improving overall browsing security.

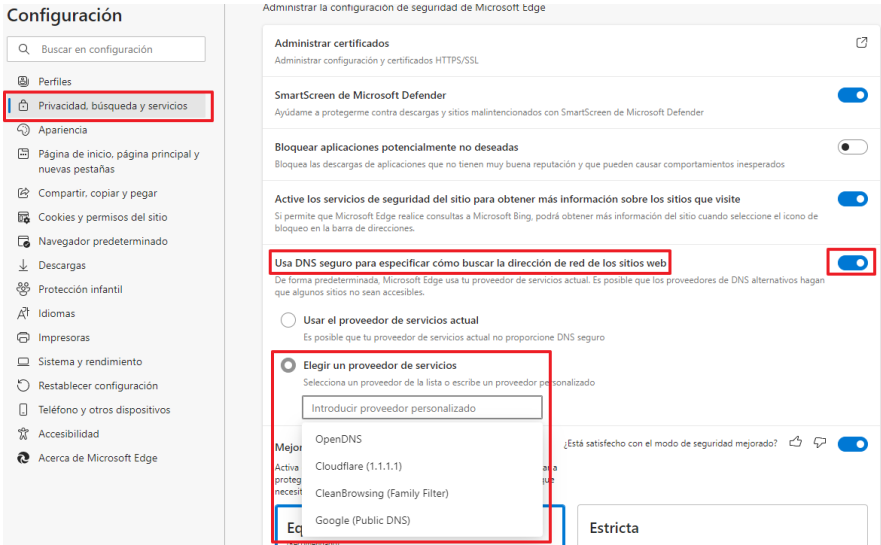
2. Microsoft Edge web browser

Passage	Description
6.	To do this, in the “Privacy, search and services” section, in the “Clear browsing data when closing” section, enable the “Cookies and other site data” option as shown in the following image:  The screenshot shows the 'Configuración' (Settings) window of Microsoft Edge. The left sidebar lists various settings categories, with 'Privacidad, búsqueda y servicios' (Privacy, search and services) highlighted. The main pane shows the 'Privacidad, búsqueda y servicios / Borrar los datos de exploración al cerrar' (Privacy, search and services / Clear browsing data when closing) section. Under the heading 'Elegir qué se debe borrar cada vez que se cierra el explorador' (Choose what to delete every time you close the browser), there are several toggle switches. The 'Cookies y otros datos del sitio' (Cookies and other site data) toggle is turned on, indicated by a blue switch and a red box. Other toggles include 'Historial de exploración' (Browsing history), 'Historial de descargas' (Download history), 'Archivos e imágenes en memoria caché' (Cached files and images), 'Contraseñas' (Passwords), 'Autorellenar datos de formulario' (Autofill form data), and 'Permisos del sitio' (Site permissions).
	Note: There are some pages that require third party cookies to function properly. If you detect that a page is not working as expected, you may need to enable third-party cookies for it to work properly or add it as an exception. To do this, you can generate an exception for third-party cookies on certain pages to improve your user experience by adding the site, as shown in the following image, by clicking on the “Add” button:  The screenshot shows the same 'Configuración' (Settings) window as above. In this view, the 'Agregar' (Add) button is highlighted with a red box, indicating where to click to add a site exception for cookies.

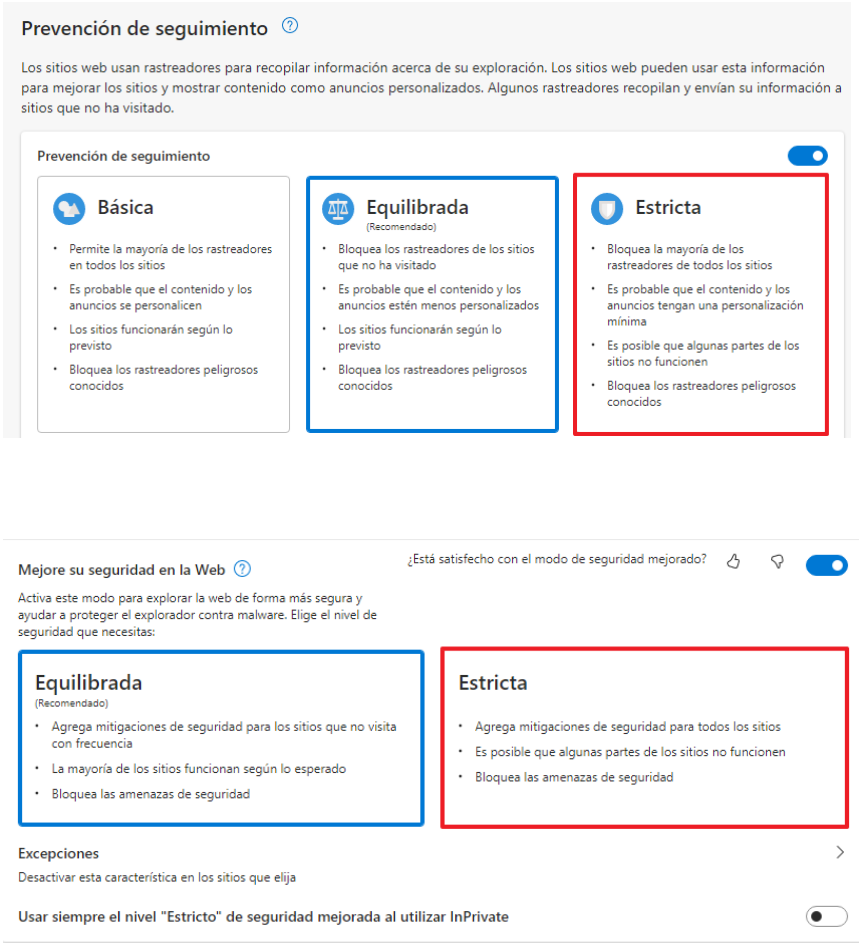
2. Microsoft Edge web browser

Passage	Description
7.	In the settings of the "Privacy, search and services" section, enable the option "Enhance your web security" in the "Security" section. To obtain this protection, click on the text "Enhance your web security" or enable the option from the side button, as shown in the following image:  This protection offered by the Microsoft Edge browser includes, among others, the following features: – Add security mitigations for sites you do not visit frequently. – Most sites perform as expected. – Block security threats.
8.	In the same section, enable the option "Block potentially unwanted applications": 

2. Microsoft Edge web browser

Passage	Description
9.	The “Use Secure DNS” functionality is enabled by default. However, by default it makes use of the DNS of the current service provider, which may result in unsecured connections being attempted against a website due to service interruptions. It is therefore possible to set one of the DNS provided by the browser or even a customised one if you are in a business environment: 
10.	Then make sure that the options “Microsoft Defender SmartScreen” and “Enable site security services to get more information about the websites you visit” are enabled. If not, enable both options.

2. Microsoft Edge web browser

Passage	Description
11	Finally, related to the settings aimed at preventing tracking and improving web security, it is possible to set up a more restrictive configuration by setting both settings to the "Strict" configuration. This setting is more secure but may cause certain websites to stop working as expected. Therefore, if this setting is enabled, it is possible to set exceptions for those websites that require it.  The screenshot displays two settings panels in Microsoft Edge. The top panel, 'Prevenção de seguimento', has a toggle switch turned on. It lists three options: 'Básica', 'Equilibrada (Recomendado)', and 'Estricta'. The 'Estricta' option is highlighted with a red border. The bottom panel, 'Mejore su seguridad en la Web', has a toggle switch turned on. It lists two options: 'Equilibrada (Recomendado)' and 'Estricta'. The 'Estricta' option is highlighted with a red border. Below these panels, there is an 'Excepciones' section with a link to 'Desactivar esta característica en los sitios que elija' and a toggle switch for 'Usar siempre el nivel "Estricto" de seguridad mejorada al utilizar InPrivate'.

2. Microsoft Edge web browser

2.5.4 Section home page, main page and new tabs

As will also be discussed in later sections, background data delivery is a very important part of security and privacy to prevent the execution of malicious code.



Passage	Description
1.	Within the “Home page, main page and new tabs” section, in the “New tab page” section, disable the “Pre-load new tab page for faster experience” option.

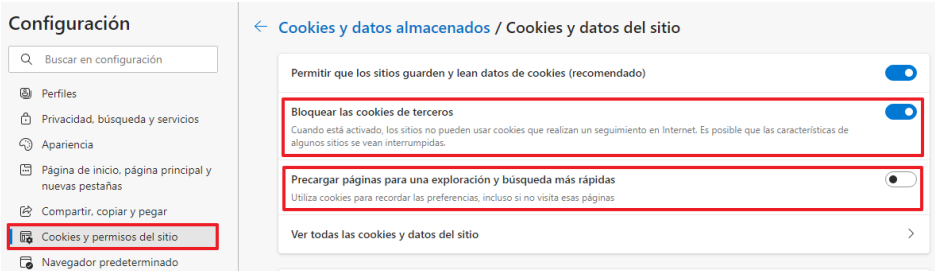
2. Microsoft Edge web browser

2.5.5 Cookies and site permissions section

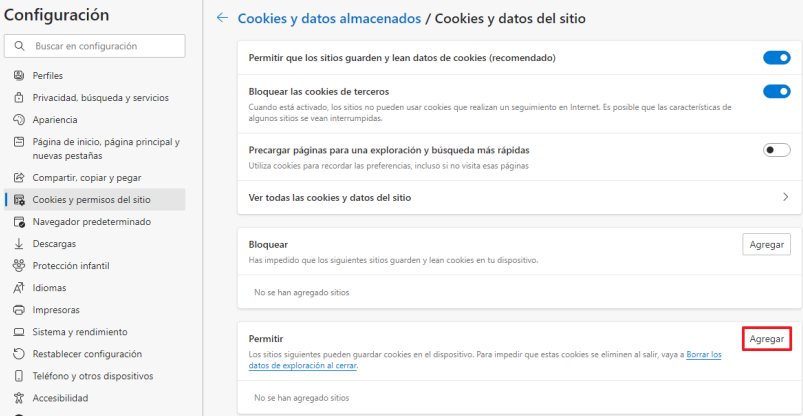
The configuration of cookies and background traffic is a very important part of security and privacy. Securely configuring these elements can prevent security breaches and potential theft of sensitive information, as an attacker could hide the execution of malicious code through background browser traffic.

To avoid these risks, we recommend the following settings in the Microsoft Edge browser:

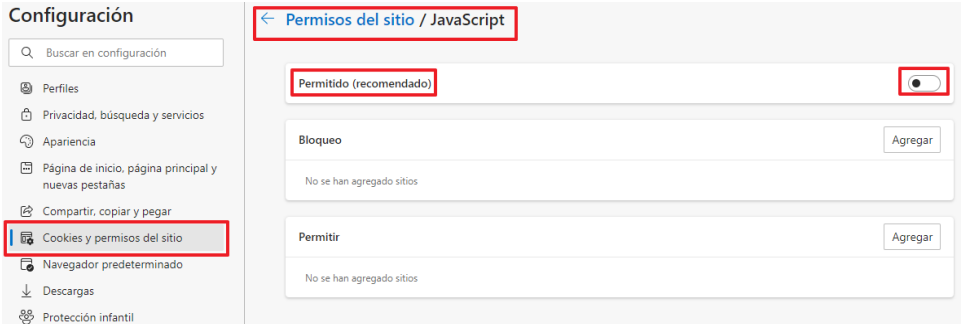
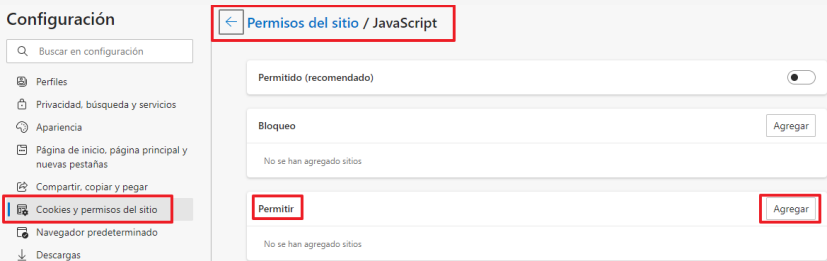
Cookie settings and background delivery of information are a very important part of security and privacy.

Passage	Description
1.	In the following, the aspects that prevent the storage and blocking of certain cookies will be modified to prevent the storage of information that is not necessary, as well as the blocking of information in the background.
2.	In the Edge settings, go to the “Cookies and site permissions” section, and then to the “Manage and delete cookies and site data” section. Once there, enable the “Block third-party cookies” option and disable the “Preload pages for faster browsing and searching” option, as shown in the image below: 

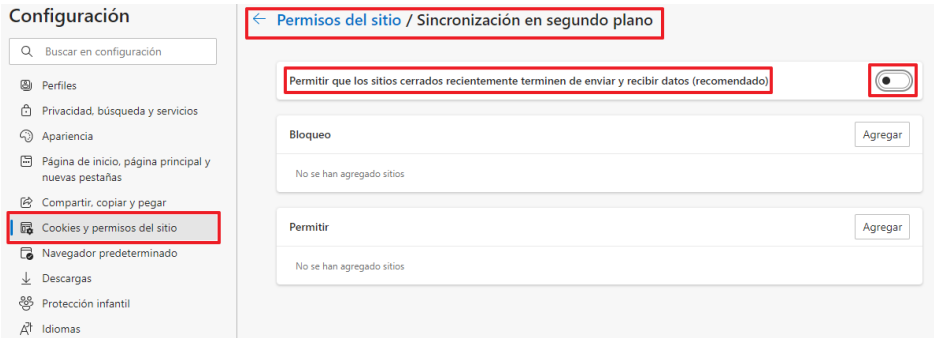
2. Microsoft Edge web browser

Passage	Description
	Note: There are some pages that require third party cookies to function properly. If you detect that a page is not working as expected, you may need to enable third party cookies for it to work properly. To do this, you can generate an exception for third-party cookies on certain pages to improve your user experience, as shown in the following image. 
3.	Continuing with the configurations, some aspects should be changed to avoid attacks on minimised windows, windows in the background, and code executions via JavaScript, which are commonly used for malicious attacks.

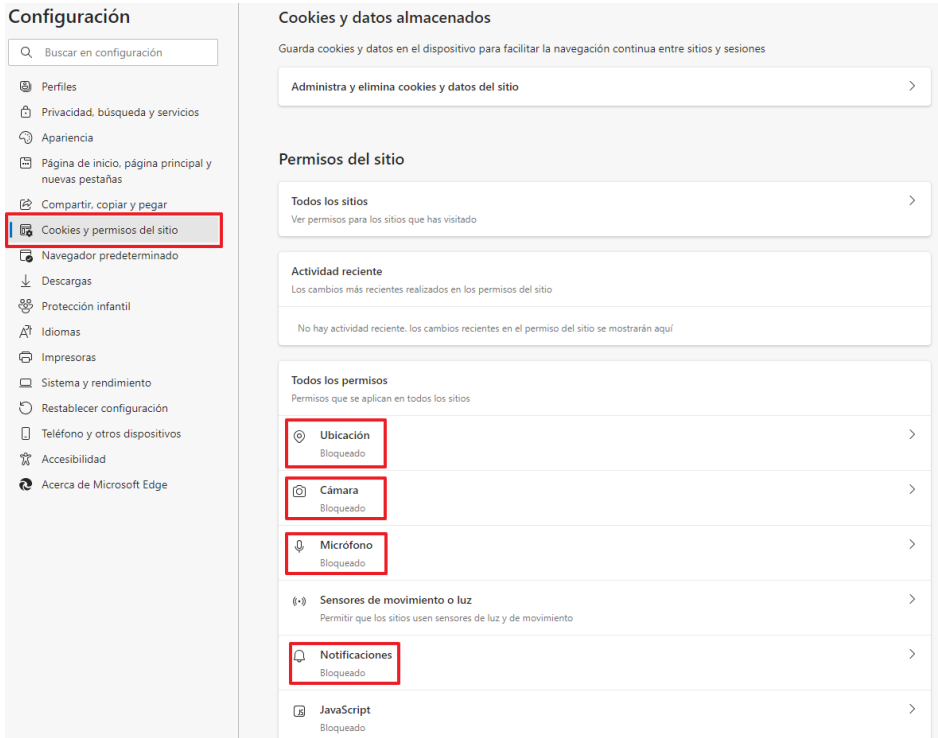
2. Microsoft Edge web browser

Passage	Description
4.	To limit and avoid the above, you must access the “Cookies and site permissions” section, in the “JavaScript” section. Once inside JavaScript, <u>it is recommended to disable</u> the “Allowed (recommended)” option as shown in the following image: 
	Note: In most cases, JavaScript should be kept enabled to provide full functionality on web pages that are visited. However, in some enterprise environments where enhanced levels of security are required, it is recommended to review these settings and block the use of JavaScript to prevent code execution attacks, adding exceptions only on those sites that are necessary for the organisation by adding them in the “Allow” section. 

2. Microsoft Edge web browser

Passage	Description
5.	Subsequently, in the same section, called “Cookies and site permissions”, the aspects relating to “Synchronisation in the background” shall be disabled, so as not to allow recently closed sites to carry out unwanted executions. Disable the option “Allow recently closed sites to finish sending and receiving data” as shown in the image below:  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' with a toggle switch for 'Permitir que los sitios cerrados recientemente terminen de enviar y recibir datos (recomendado)' turned off.
6.	To finish the settings in the “Cookies and site permissions” section, some aspects relating to the use of hardware communication elements of the equipment must be changed. This will allow the privacy settings to be set to suit the user's needs.
7.	The following items shall be set to “Locked” status: – “Location” – “Camera” – “Microphone” – “Notifications” – “Automatic downloads” – “USB devices” – “Serial ports” – “File editing” – “Clipboard” – “Payment controllers” – “Virtual reality” – “Augmented reality”

2. Microsoft Edge web browser

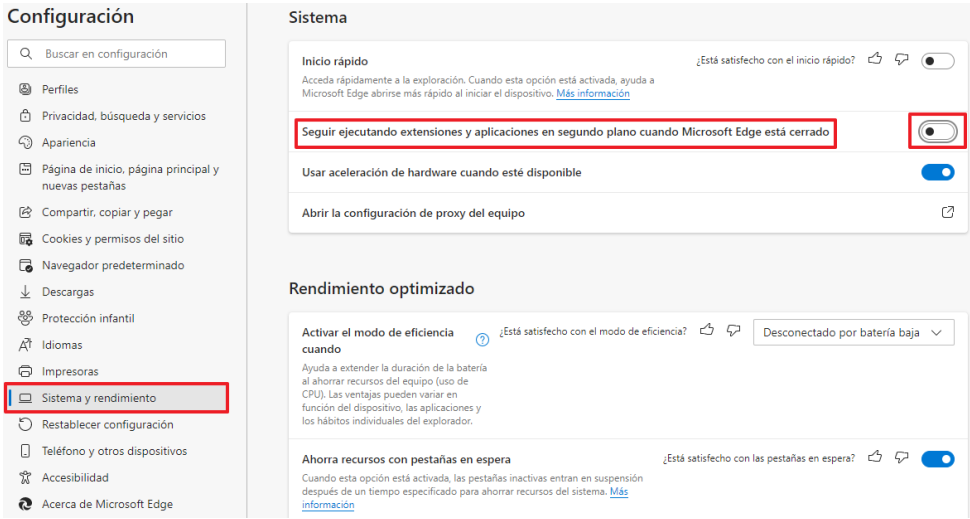
Passage	Description
	These settings may be modified, allowing their use or adding exceptions to websites that require the use of these elements:  Configuración Buscar en configuración - Perfiles - Privacidad, búsqueda y servicios - Apariencia - Página de inicio, página principal y nuevas pestañas - Compartir, 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 Micrófono Bloqueado Sensores de movimiento o luz Permitir que los sitios usen sensores de luz y de movimiento Notificaciones Bloqueado JavaScript Bloqueado

2. Microsoft Edge web browser

2.5.6 System and performance section

As discussed in previous sections, the execution of code in the background after closing the Microsoft Edge browser is susceptible to malicious attacks and should be disabled by following the steps below:



Passage	Description
1.	In the “System and Performance” section, under “System”, disable the option “Continue running extensions and applications in the background when Microsoft Edge is closed”, as shown in the image below: 

3. Checklist

Criticality	Description
High	Microsoft Edge must have the latest security-related software updates installed by manually installing the latest version available for download, the Microsoft Edge automatic update tool, or the Windows Update tool in the Windows operating system.
High	In case browser extensions are used, you should ensure that they are up to date and from reliable sources.
Medium	When a user switches from a secure (SSL-enabled) page to a non-secure page, Microsoft Edge is configured to notify the user.
Medium	Microsoft Edge is configured to block pop-up windows.
Medium	Microsoft accounts can be used and signed in to synchronise data in Microsoft Edge, with a user-provided account.
Medium	Microsoft Edge is configured not to auto-complete searches and URLs, without sending information to the default search engine.
Medium	Microsoft Edge is configured not to save site passwords.
Medium	Microsoft Edge is configured not to automatically sign in to websites that have your credentials stored.

3. Checklist

Criticality	Description
Medium	Microsoft Edge is configured not to save or autofill payment methods.
Medium	Microsoft Edge is configured to allow websites to not check for saved payment methods.
Medium	Microsoft Edge is set to block third-party cookies.
Medium	Microsoft Edge is configured not to preload information from pages.
Medium	Microsoft Edge is configured to allow closed pages to not send and receive data.
Medium	Microsoft Edge is configured to disallow the use of JavaScript, unless an exception is added.
Medium	Microsoft Edge is configured not to run background applications when you close the browser.

4. Decalogue of recommendations

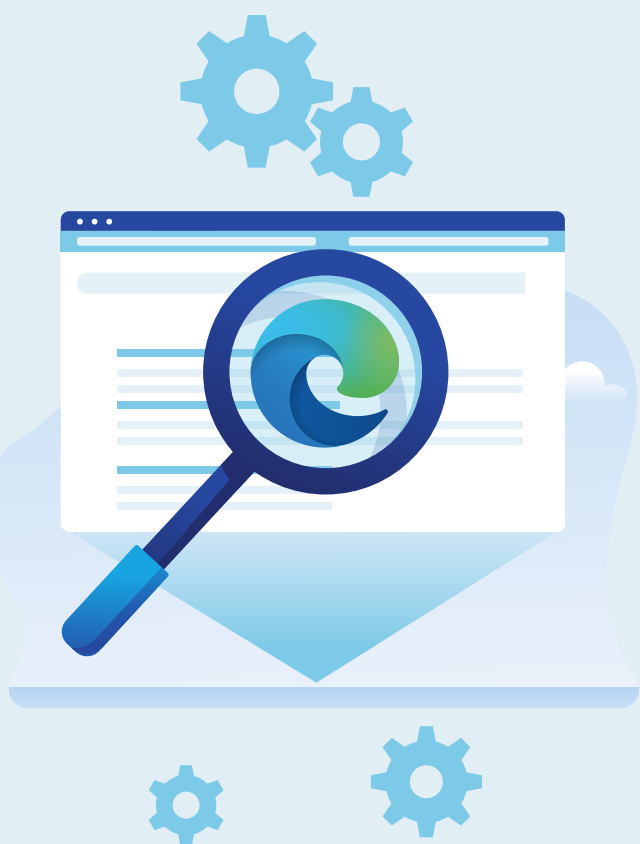
Here are ten security recommendations for using Microsoft Edge.



Decalogue of recommendations for Microsoft Edge

- 1 It is recommended to always use the latest stable version with the latest updates.
- 2 **A review of the security-related functions of the software** is recommended, as it will provide a better defence against possible attacks.
- 3 If **plug-ins** need to be **installed**, it is recommended to use **official** and/or reliable **sources**.

It is recommended that you **do not use the password vault available in Microsoft Edge**. Instead, it is recommended to **use other applications** that implement strong encryption to store passwords more securely.
- 4 It is recommended to **look at the site's identity button** (a padlock in the address bar to the left of the address bar) to quickly and easily find out whether **the connection to the page is encrypted** and, in some cases, who the owner is. This information helps in the detection of malicious pages.
- 5 The **use of secure protocols (https)** is **always** recommended, especially when personal data is used to secure end-to-end communications.
- 6 The **use of encryption software for sending personal information** is recommended as an additional security measure, including the use of secure protocols such as https.
- 7 The **use of two-factor authentication** is recommended for the use of online services. This adds an additional layer of security to accounts because additional verification will be required at login (SMS, phone call, authenticators, verification code, etc.).
- 8 It is recommended to **delete cookies and block background browsing** to prevent some websites from tracking search patterns and to safeguard user privacy.
- 9 It is recommended that you **clear your cache and delete temporary internet files** to solve common problems with websites.
- 10



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es