CCN-CERT

BP/32

MacOS Operating System Security Recommendations

BEST PRACTICE REPORT

MAY 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional

Edited by:

Date of issue: abril de 2024

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

Index

1. Introduction

This guide is designed to get the most out of macOS computers by providing the tools and knowledge needed to protect data and privacy. It will explore a number of basic security settings that all macOS users should consider to keep their information safe from potential threats.

The advantages of using macOS are numerous: intuitive operating system, stability, hardware and software optimisation, and so on. However, these advantages should not overshadow the importance of safeguarding data and privacy. In today's digital world, personal information, from photos and documents to passwords and financial data, is constantly at risk.

Loss or unauthorised access to this information can have significant consequences. This guide provides guidelines on how to protect personal data, surf the Internet safely and avoid common threats such as malware and phishing.

2. Objective and scope

The purpose of this guide is to provide macOS users with a comprehensive set of instructions and recommendations for establishing and optimising basic security settings on their devices, making the most relevant adjustments in order to ensure greater security for both the device and the user.

This will be done through the different configuration menus available in the operating system, without the need to execute commands, whether simple or complex. In this way, the configurations will be accessible to any type of user, regardless of their technological knowledge.

It is important to note that these settings may vary in other versions of the operating system, and also that this guide has been made considering a user with an iCloud account (Apple ID). Therefore, users will need to adapt the steps in this document to the possible changes that may exist, both in earlier and later versions of the operating system, and taking into account their specific iCloud settings.

3. MacOS operating system

In the following sections, a number of system settings will be developed to strengthen the security of macOS. Each aspect will be explained in a clear and concise manner, providing the necessary guidelines to protect your data and personal information. As you progress, you will discover that securing your system is simpler than it sounds.

The guide will follow a detailed walkthrough through the **"System Settings"** of macOS in its **Ventura** edition. Each step will be done by going into the system settings, which will allow security settings to be addressed in a straightforward manner.

4. System settings

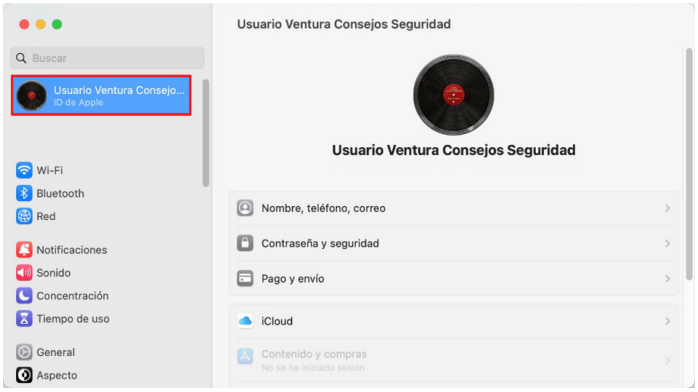
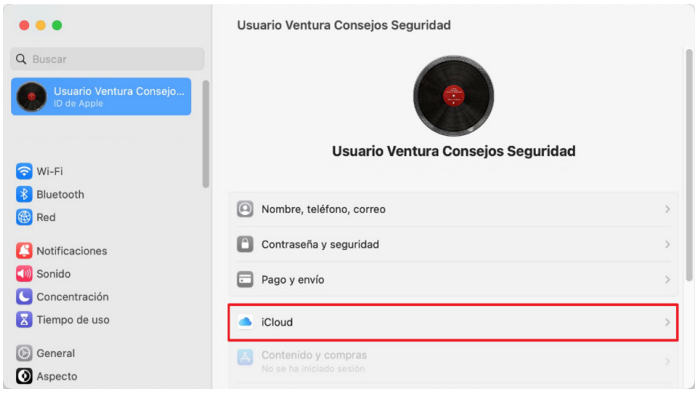
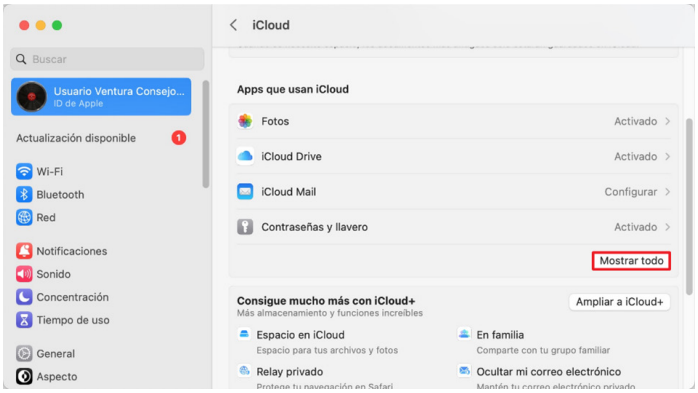
The "System Settings" in macOS Ventura is the control centre for users to customise and configure their macOS operating system. From this element, it is possible to adjust preferences for security, privacy, networking, displays, users and more. They are the key for users to tailor their user experience and ensure the security of their devices.

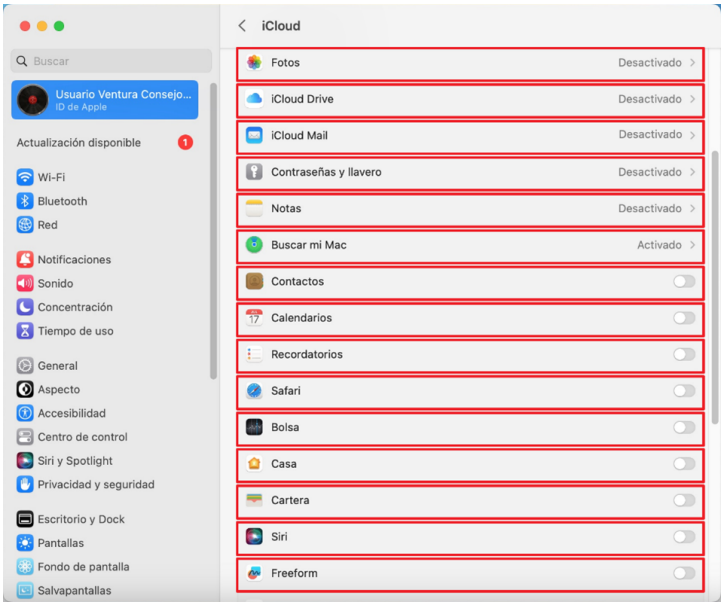
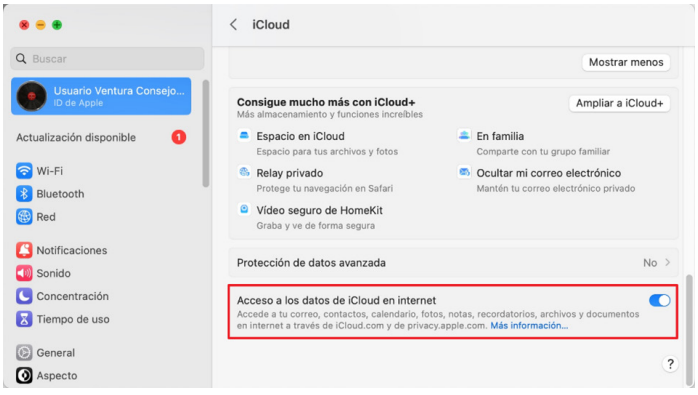
4.1. iCloud user

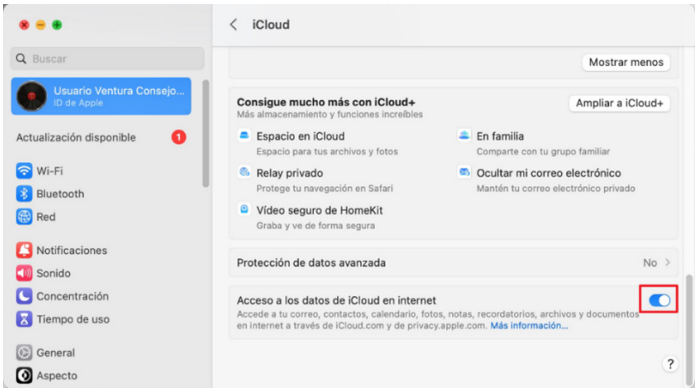
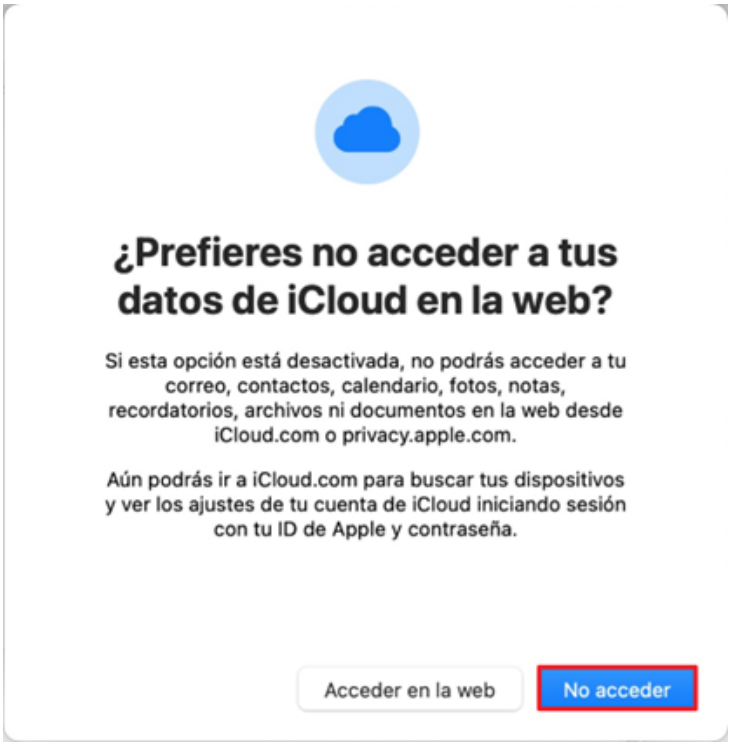
Settings in the iCloud account allow users to customise and manage how data is synced and stored in Apple's cloud. This includes options for backing up photos, contacts, notes and other data, as well as enabling location and family sharing. Storage preferences, security options and access to Apple services such as Find My Mac can also be configured. These settings offer greater control over the user's experience and privacy in the Apple ecosystem.

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 

Note: The user shown in this guide is representative and is used for illustrative purposes.

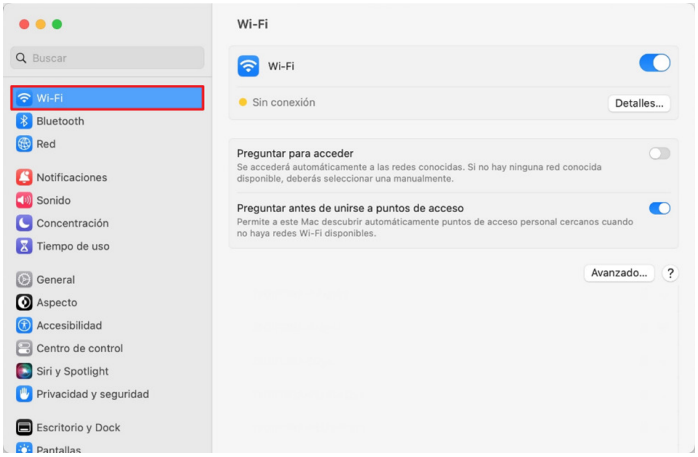
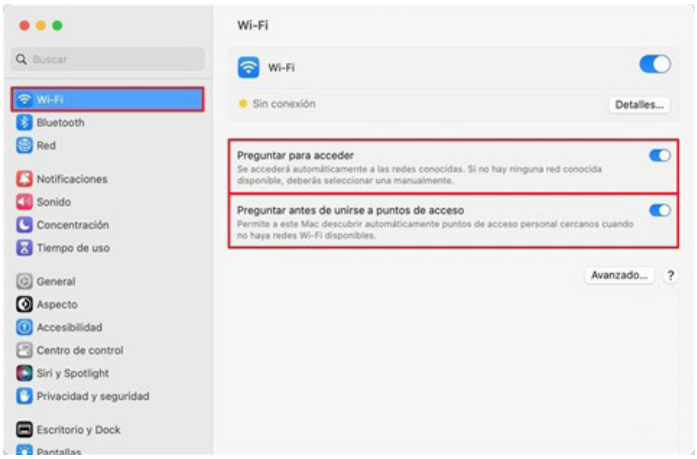
Passage	Description
3.	In the system settings window, navigate to the left menu and select your account. 
4.	Then click on **"iCloud".** 
5.	In the **"iCloud"** window, navigate to the **"Show all"** button and click on it. 
6.	Modify the following settings as indicated below: ◆ Photos: Deactivated. ◆ iCloud Drive: Disabled. ◆ iCloud Mail: Disabled. ◆ Password and key fob: Disabled. ◆ Notes: Disabled. ◆ Find My Mac: On.

Passage	Description
6.	◆ Contacts: Disabled. ◆ Calendars: Disabled. ◆ Reminders: Disabled. ◆ Safari: Disabled. ◆ Stock exchange: Deactivated. ◆ House: Deactivated. ◆ Portfolio: Deactivated. ◆ Siri: Disabled. ◆ Freefrom: Disabled.  **Note: If you require the use of any of the previously disabled settings, you will need to assess each particular setting(s) and whether it is necessary to keep it/them enabled. The document has been prepared in an attempt to limit as much as possible the possibility of use of information by other synchronised devices.**
7.	In the same window, navigate and locate **"Access iCloud data on the internet".** 

Passage	Description
8.	Click on the **"Access iCloud data on the internet"** button to disable the option. 
9.	In the next window, click on the **"No access"** button. 

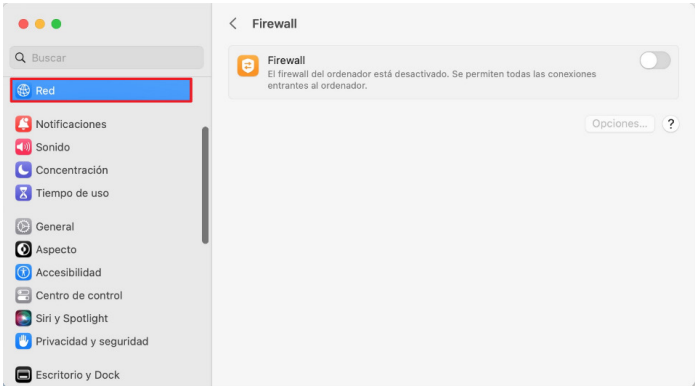
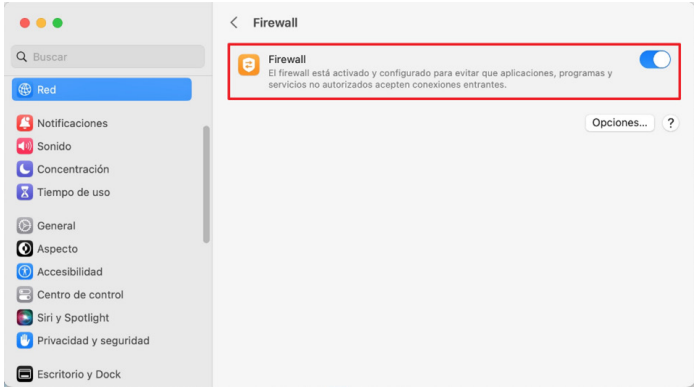
4.2. Wi-Fi

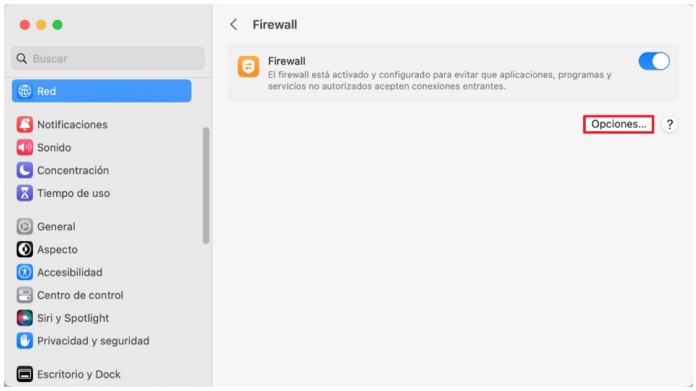
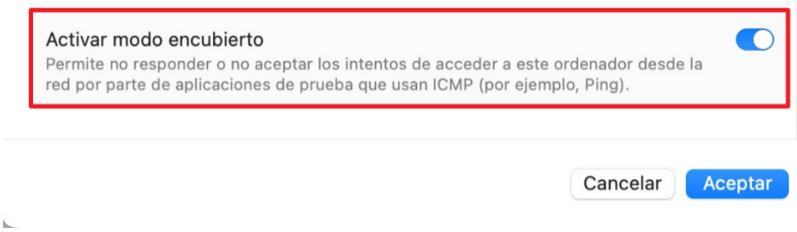
Wi-Fi settings in macOS Ventura allow users to securely connect to wireless networks and manage their access.

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Wi-Fi".** 
4.	In the **"Wi-Fi"** window, modify the following settings as shown below: ◆ Ask for access: On. ◆ Ask before joining hotspots: Enabled. 

4.3. Network

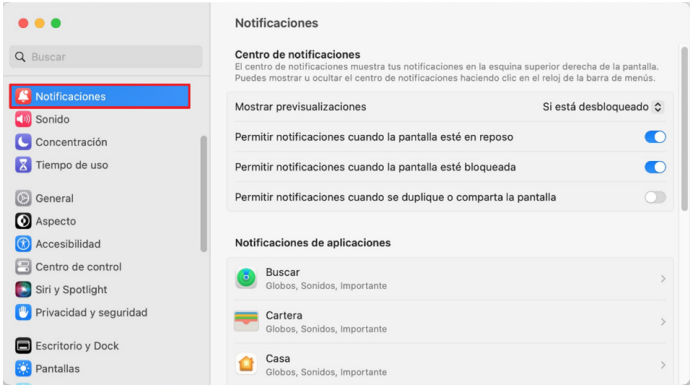
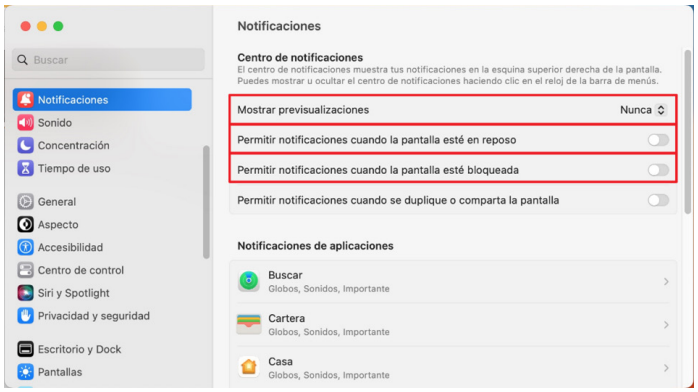
The Network section allows users to manage network connectivity and security.

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Network"**. 
4.	Then click on **"Firewall"** and activate it, as shown in the following image. 

Passage	Description
5.	Then click on the **"Options..."** button. 
6.	In the pop-up window, activate the option **"Enable covert mode".** 
7.	Once activation is complete, click on the **"OK"** button. 

4.4. Notifications

In this section, the aim is to reduce the exposure of information when the computer is locked or idle. Therefore, several notification settings will be disabled in such circumstances, ensuring privacy and data security in the macOS operating system.

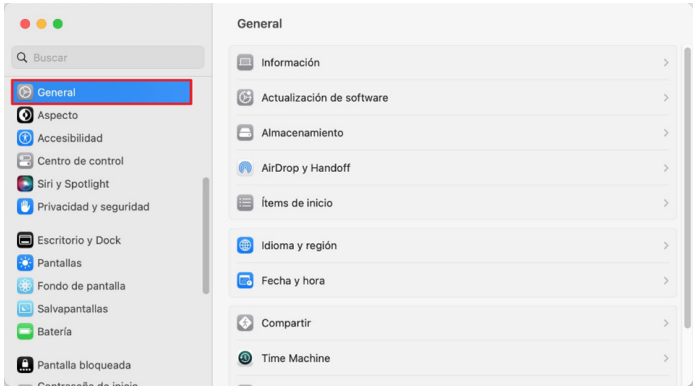
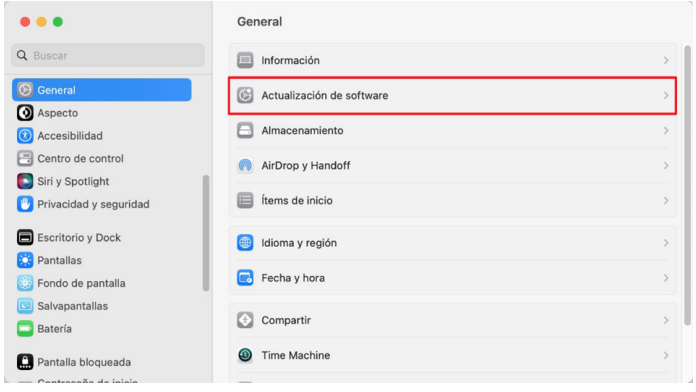
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Notifications".** 
4.	In the **"Notifications"** window, modify the following settings as shown below: ◆ Show previews: Never. ◆ Allow notifications when the screen is idle: Off. ◆ Allow notifications when the screen is locked: Disabled. 

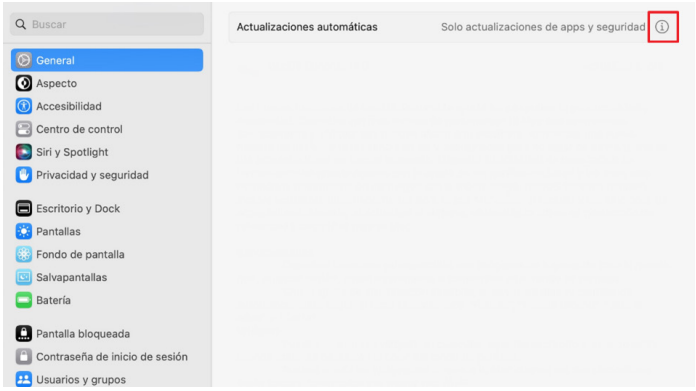
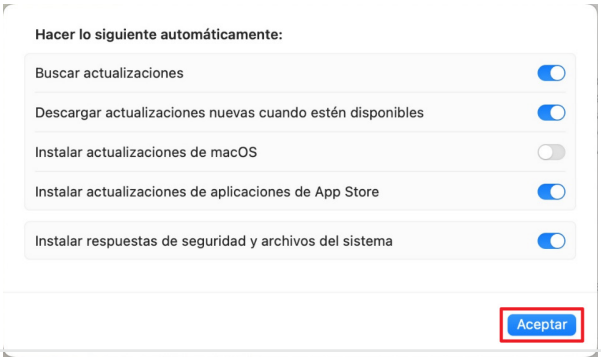
4.5. General

In this section, modifications will be made with respect to macOS Ventura operating system updates and other aspects related to data sharing.

4.5.1. Software update

In the next section, users are enabled to keep their systems and applications up to date to improve stability and security.

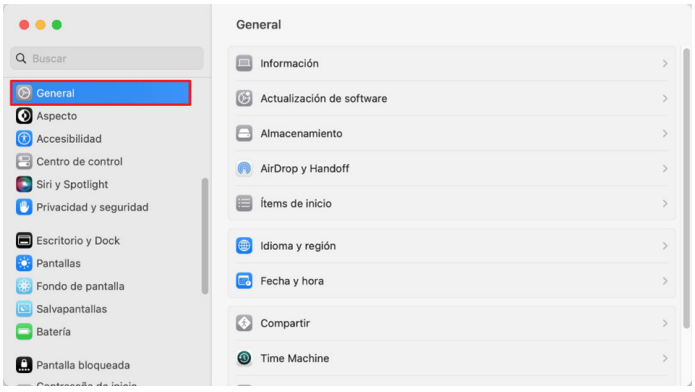
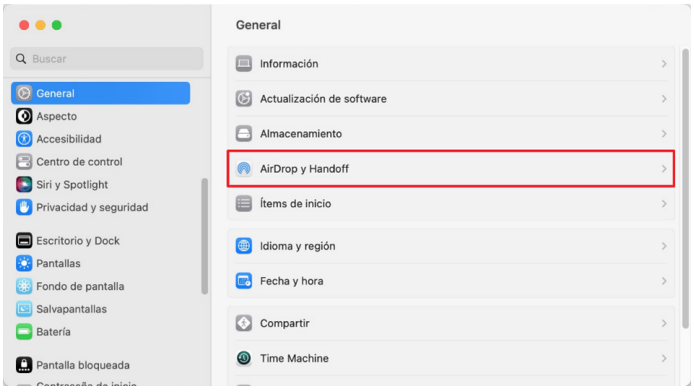
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"General"**. 
4.	Then click on **"Software Update".** 

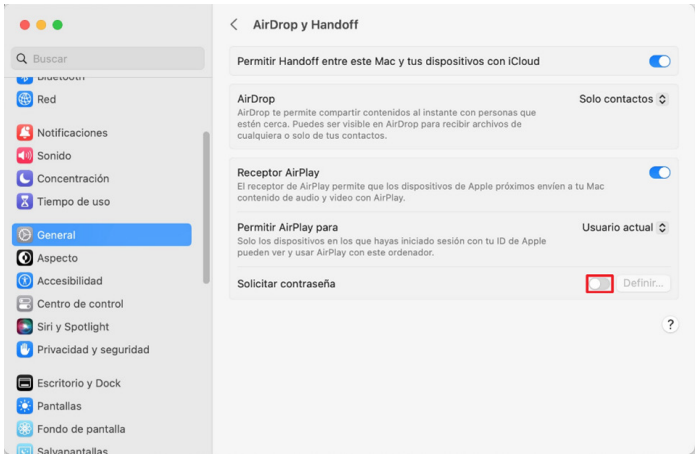
Passage	Description
5.	In the **"Software Update"** window, click on the information icon ⓘ, located on the right side of the **"App and security updates only"** option. 
6.	In the new window that appears **"Do the following automatically:"** modify the following settings as shown below: ◆ Check for updates: Enabled. ◆ Download new updates when available: Enabled. ◆ Install app updates from the App Store: On ◆ Install security responses and system files: Enabled.  **Note: Related to the option "Install macOS updates", this option is not enabled because it is possible that a recently released operating system update may cause software and hardware problems. If you wish to enable this option, it is recommended that a backup be made beforehand to avoid data loss.**
7.	Once you have made your changes, click on the **"OK"** button. 

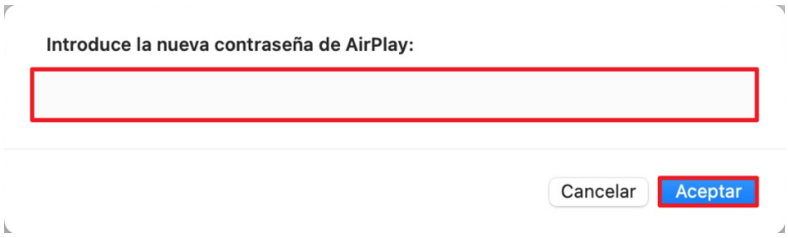
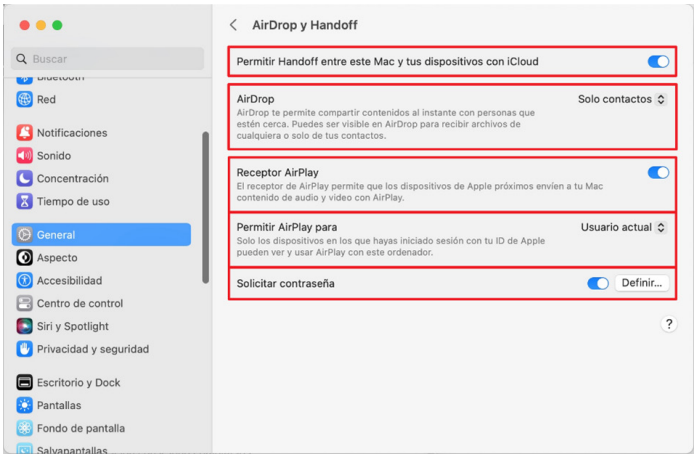
4.5.2. AirDrop and Handoff

This section focuses on starting something on one Apple device and picking it up on another, sending files to nearby Apple devices with AirDrop, or allowing other devices to play content through the Mac. Settings for more than one Apple device and for only one Apple device will be covered in the following sections.

4.5.2.1. For more than one Apple device

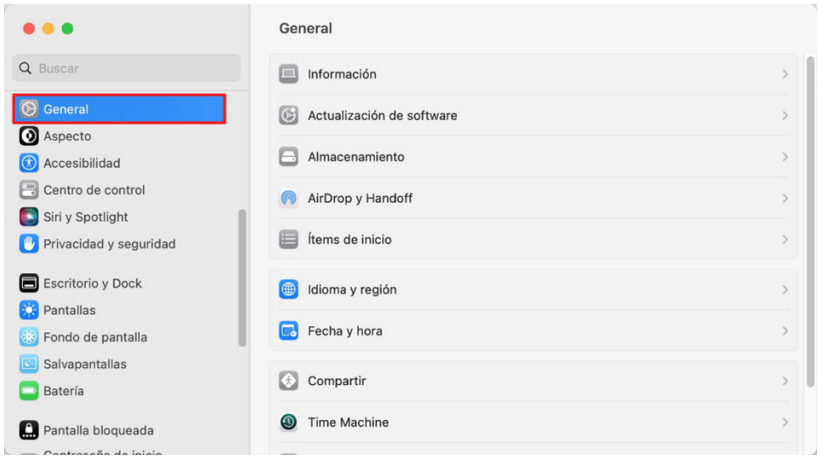
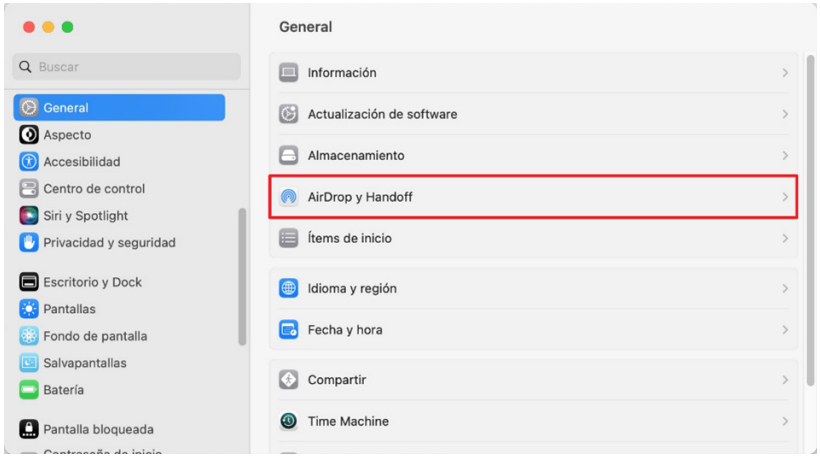
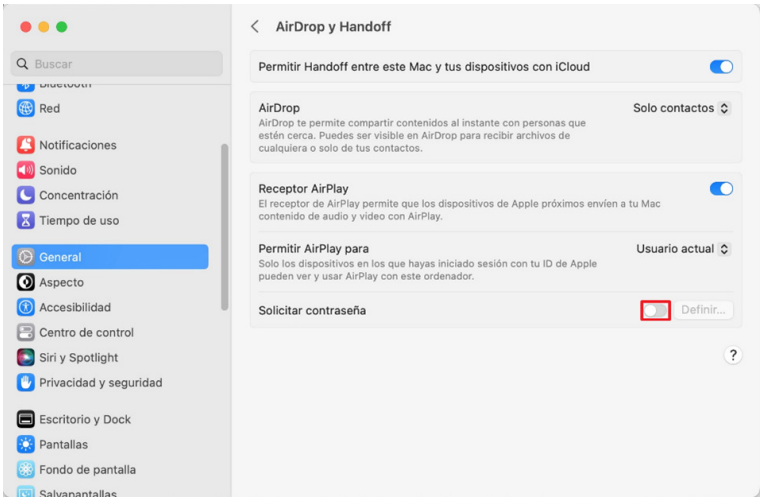
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"General".** 
4.	Then click on **"AirDrop and Handoff".** 

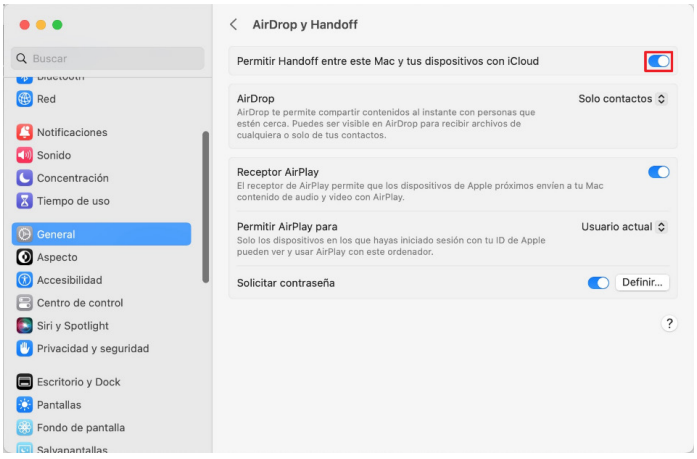
Passage	Description
5.	In the **"AirDrop and Handoff"** window, click on the activation button for the **"Request Password"** option.. 
6.	You will then be prompted for elevation of privileges. Enter the user name and password in the corresponding text boxes and click on **"Modify settings".** 

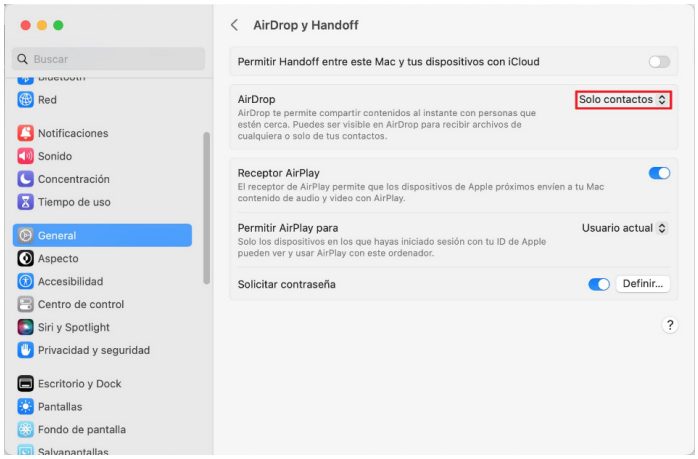
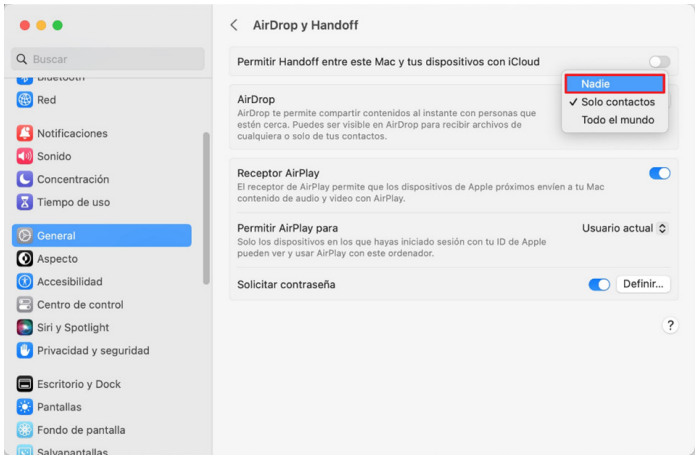
Passage	Description
7.	Enter the new AirPlay password. This password will be required each time the AirPlay function is used. Then click **"OK".** 
8.	Check and modify the following settings as shown below: ◆ Allow Handoff between this Mac and your iCloud-enabled devices: On. ◆ AirDrop: Contacts only. ◆ AirPlay receiver: On. ◆ Allow AirPlay for: Current user. ◆ Request password: Enabled. 

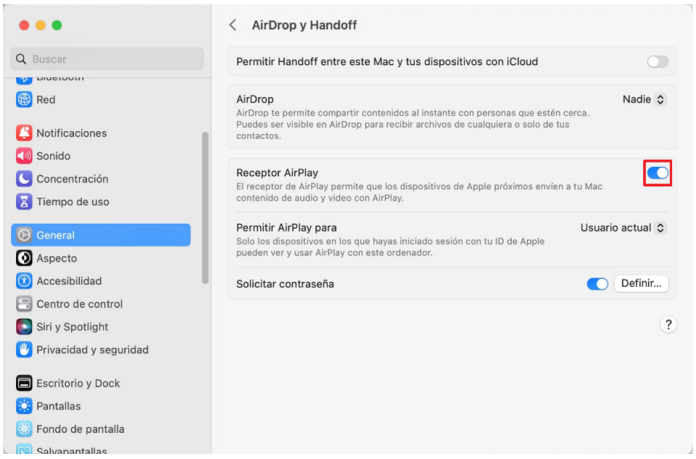
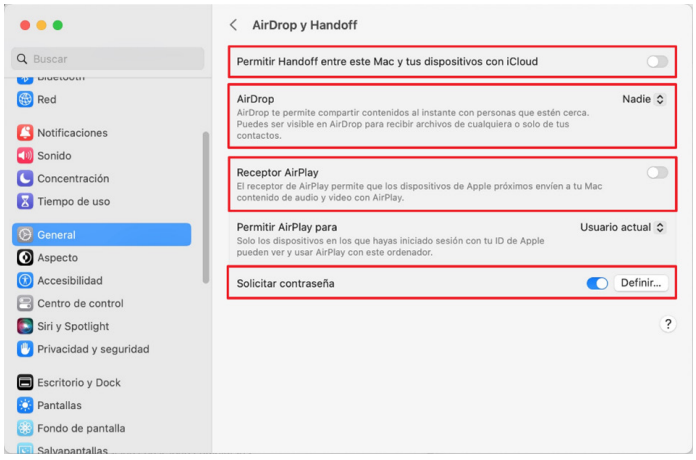
4.5.2.2. For a single Apple Device

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 

Passage	Description
3.	In the system settings window, navigate to the left menu and select **"General".** 
4.	Then click on **"AirDrop and Handoff".** 
5.	In the **"AirDrop and Handoff"** window, click on the activation button for the **"Request Password"** option. 

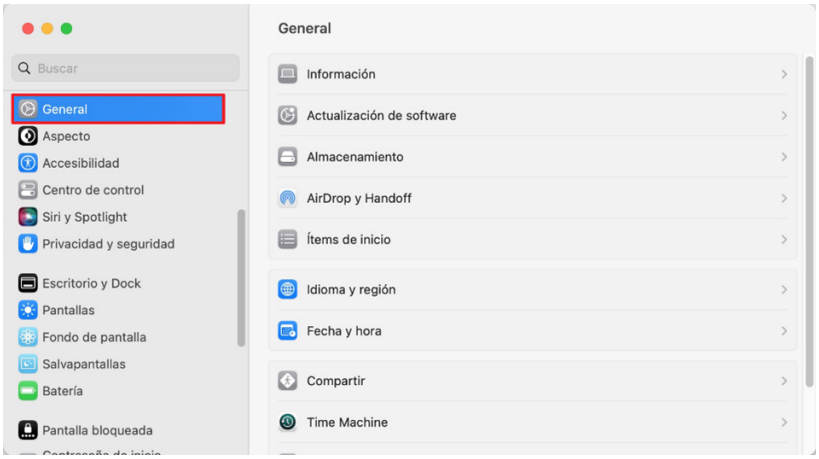
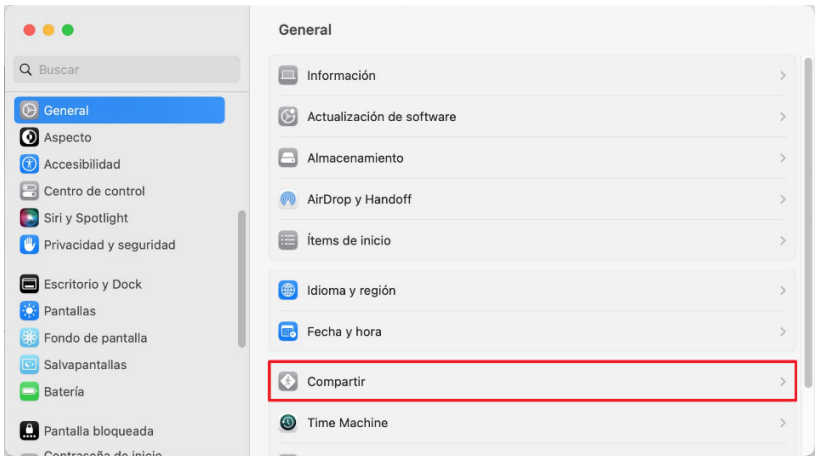
Passage	Description
6.	In the **"AirDrop and Handoff"** window, click on the activation button for the **"Request Password"** option. 
7.	You will then be prompted for elevation of privileges. Enter the user name and password in the corresponding text boxes and click on **"Modify settings"**. 
8.	In the **"AirDrop and Handoff"** window, deactivate **"Allow Handoff between this Mac and your iCloud-enabled devices"**. To do this, click on the activation button. 

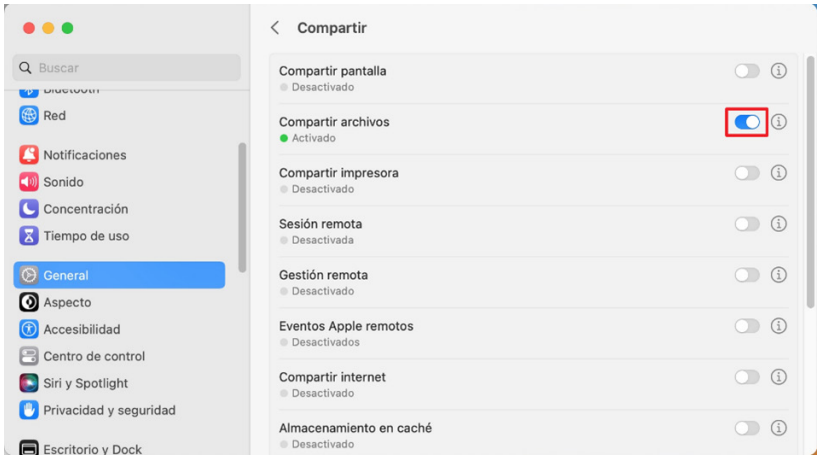
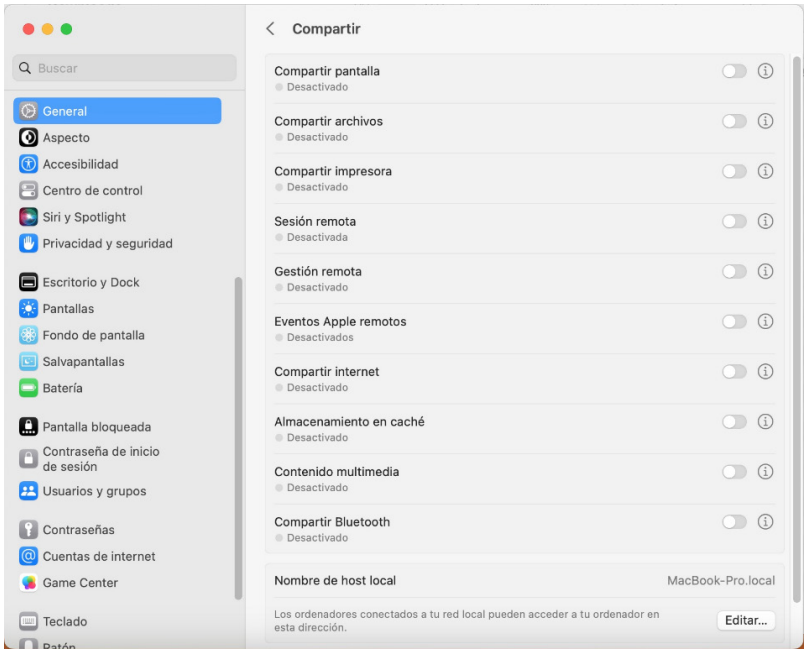
Passage	Description
9.	Then click on the **"Do not allow Handoff"** button. 
10.	Again, in the **"AirDrop and Handoff"** window, restrict **"AirDrop"**. To do this, click on the drop-down menu. 
11.	Then select the **"Nobody"** option. 

Passage	Description
12.	In the same **"AirDrop and Handoff"** window, deactivate "**AirPlay Receiver".** To do this, click on the activation button. 
13.	Verify that the settings have been made as indicated below: ◆ Allow Handoff between this Mac and your iCloud-enabled devices: Disabled. ◆ AirDrop: No one. ◆ AirPlay receiver: Disabled. ◆ Request password: Enabled. 

4.5.3. Sharing

In this configuration section, different actions can be performed so that resources, devices or connections can be shared.

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"General".** 
4.	Then click on **"Sharing".** 

Passage	Description
5.	In the **"Sharing"** window, deactivate **"File Sharing"**. To do this, click on the activation button. 
7.	For all other settings in the **"Sharing"** window, macOS systems set these settings to disabled by default. Therefore, keep the settings in a disabled state except for those that are required for a specific use.  **Note: If any of the settings are activated, it is recommended to evaluate each setting individually and assess whether it is necessary to keep it(s) activated. In case of keeping any of the functions active, the following criteria should be followed:** ◆ **Minimal privileges. User type: standard, share only or administrator.** ◆ **Only to strictly necessary users.** ◆ **Minimum permissions. Read or Write.** ◆ **Minimum devices to be shared.**

4.6. Privacy and security

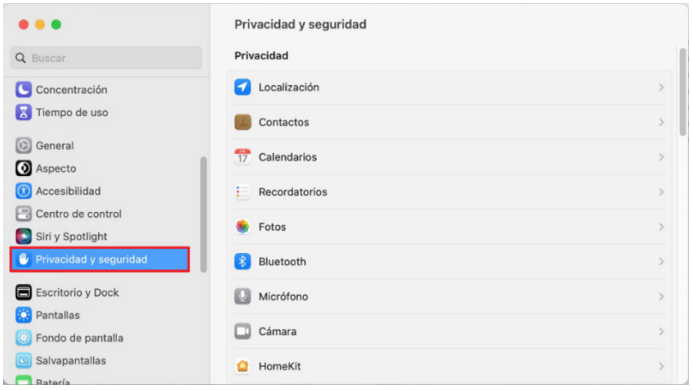
MacOS Ventura focuses on settings that protect privacy and data integrity. This includes enabling features such as FileVault for data encryption, managing application permissions, and configuring advanced security preferences. These settings are essential to ensure that users have complete control over who and what can access their information on the system.

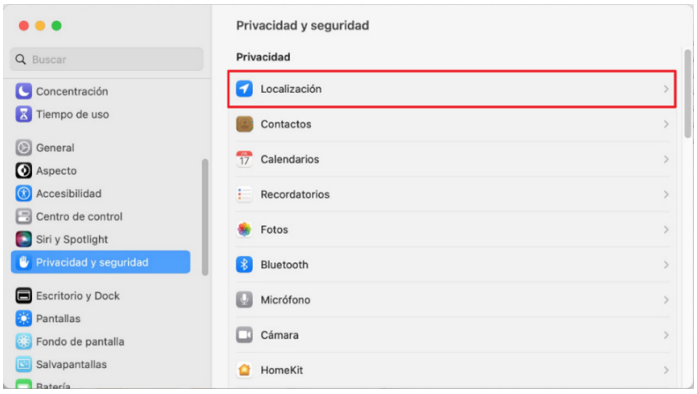
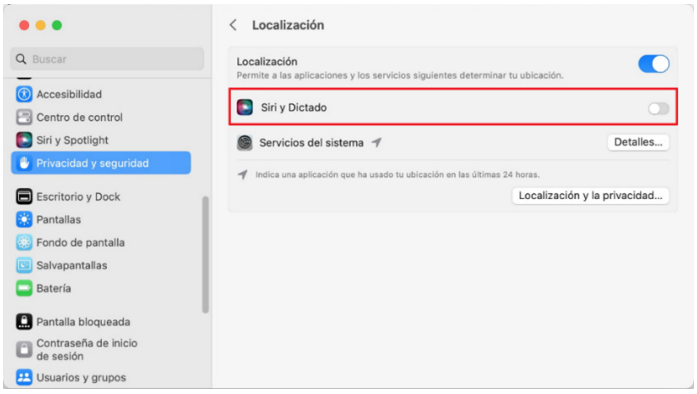
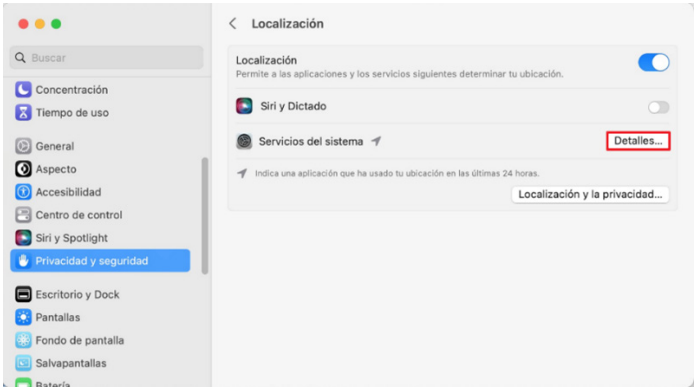
4.6.1. Privacy

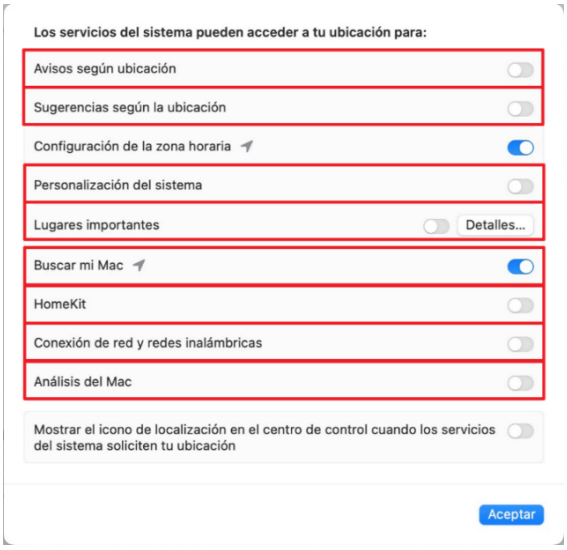
This section prioritises privacy by providing settings and tools that allow users to control and limit access to their information. This includes application permissions management, which allows users to decide which applications have access to sensitive data such as location, camera or microphone.

4.6.1.1. Location

Location settings allow users to control the access of applications and services to their geographic location. This feature is essential to protect privacy and ensure that only authorised applications have access to location information.

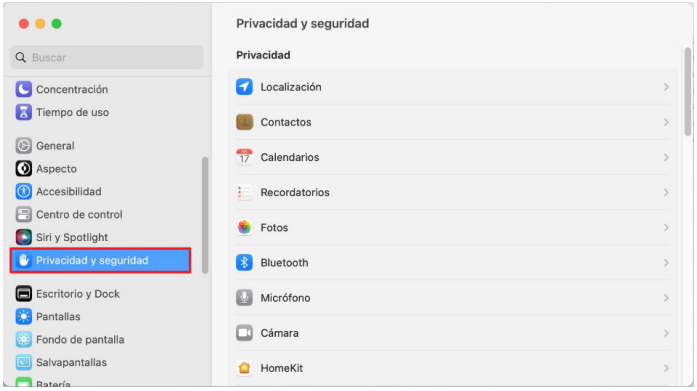
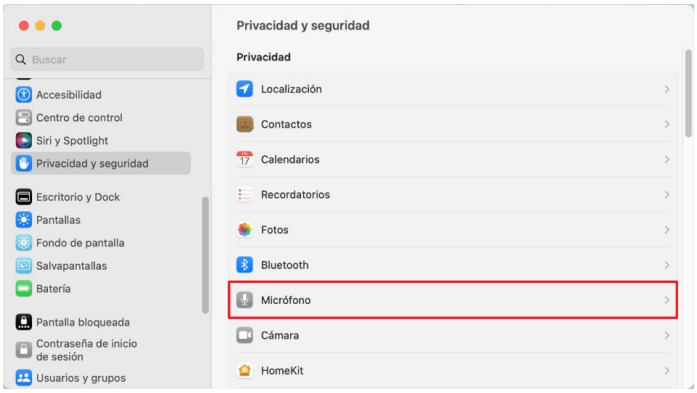
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Privacy and Security".** 

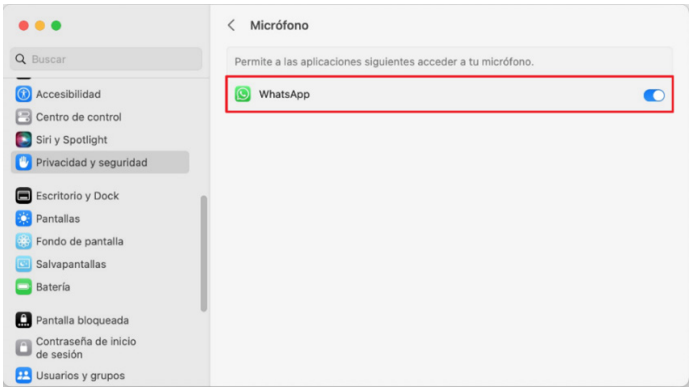
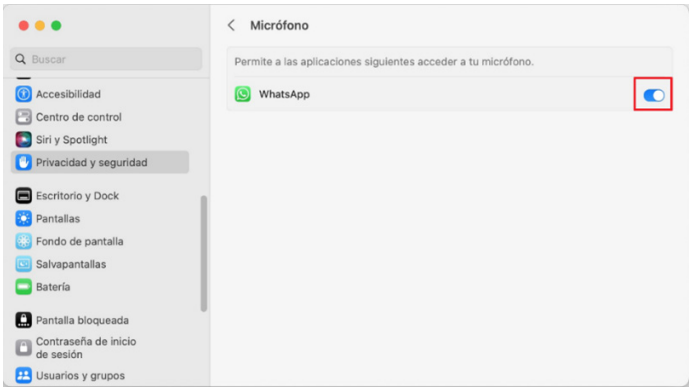
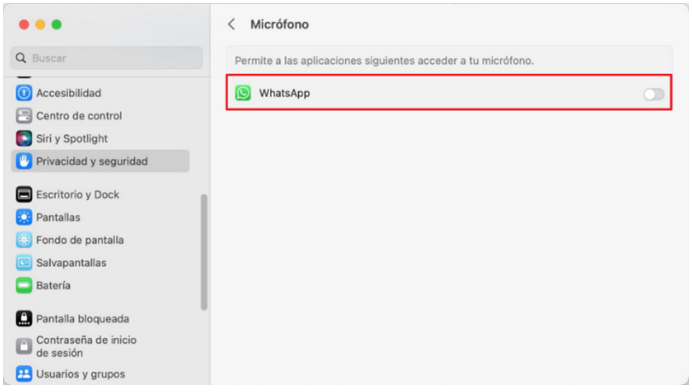
Passage	Description
4.	Then click on **"Localisation".** 
5.	In the **"Location"** window, verify that the location for **"Siri and Dictation"** is disabled.  **Note: Localisation for "Siri and Dictation" is disabled by default.**
6.	In the **"Location"** window, click on the **"Details..."** button. 

Passage	Description
7.	You will then be prompted for elevation of privileges. Enter the **user name** and **password in the** appropriate text boxes and click **"Unlock".** 
8.	In the **"System services can access your location for:"** window, modify the following settings as shown below: ◆ Location based warnings: Disabled. ◆ Suggested by location: Off. ◆ System customisation: Off. ◆ Important places: Off. ◆ Find My Mac: On. ◆ HomeKit: Disabled. ◆ Network connection and wireless networks: Disabled. ◆ Mac Analysis: Off.  **Note: If any of the settings are to be kept enabled, it is recommended to evaluate each setting individually and assess whether it is necessary to keep it(s) enabled.**
9.	Press **"OK"** to finish.

4.6.1.2. Other privacy settings

The privacy section in macOS will focus on reviewing and managing the permissions that different applications have access to. This involves controlling which apps have access to sensitive data, such as the camera, microphone and other system resources, in order to protect users' privacy and security.

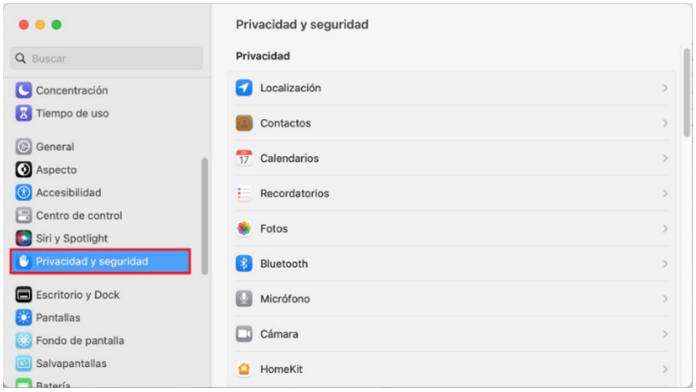
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select "**Privacy and Security".** 
4.	In the "**Privacy and Security"** window in the **"Privacy"** section, select **"Microphone".** 

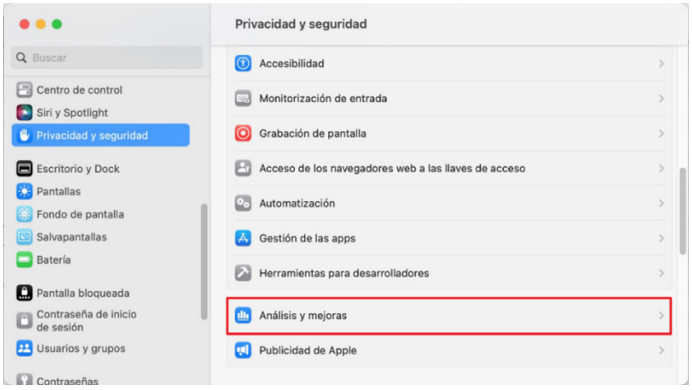
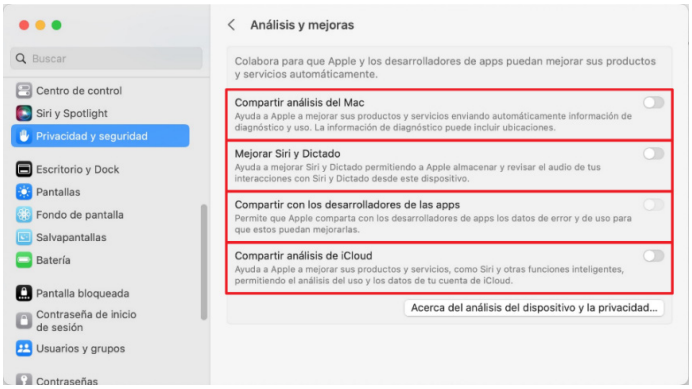
Passage	Description
5.	In the **"Microphone"** window, you can check which applications have permission to access and use the microphone.  **Note: In this example, use has been made of an instant messaging application to show the settings to be applied.**
6.	Identify and disable all applications that do not require access to the microphone by clicking on the corresponding button.  **Note: For this example, the WhatsApp application has been used.**
7.	At this point the setting for applications to access the microphone will be disabled. 

Passage	Description
8.	Perform the same steps for the rest of the existing privacy resources: ◆ Contacts. ◆ Calendars. ◆ Reminders. ◆ Photos. ◆ Bluetooth. ◆ Camera. ◆ HomeKit. ◆ Voice recognition. ◆ Multimedia and Apple Music. ◆ Files and folders. ◆ Full access to the disc. If any of the settings are enabled, it is recommended to evaluate each setting on a case-by-case basis and assess whether it is necessary to keep them enabled per application.

4.6.1.3. Analysis and improvements

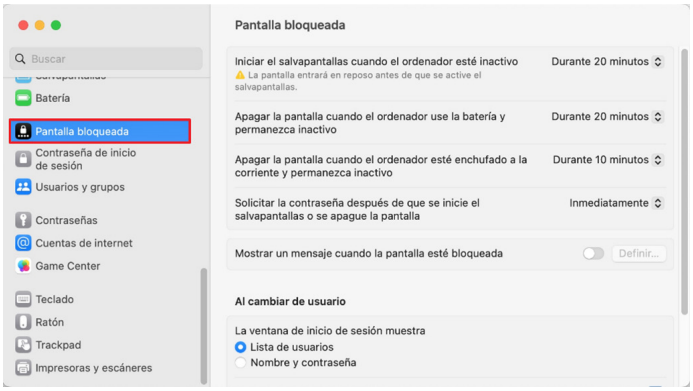
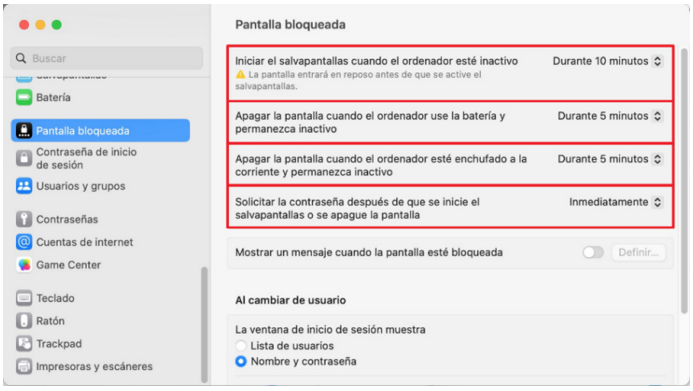
This section defines the settings that limit the information that the macOS operating system shares with Apple through various product and service reports.

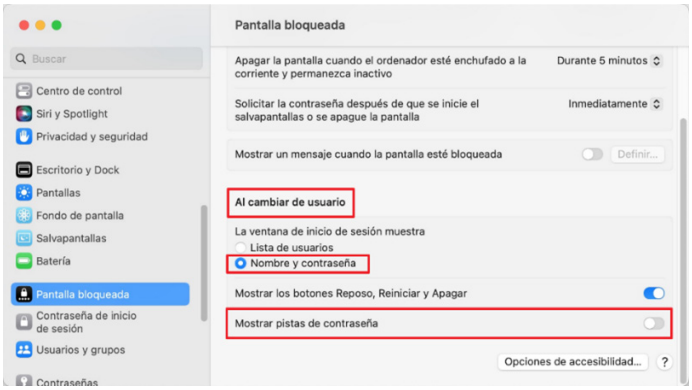
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Privacy and Security".** 

Passage	Description
4.	Under **"Privacy and Security"**, navigate to and select **"Analytics and Enhancements".** 
5.	In the **"Analysis and improvements"** window, modify the following settings as shown below: ◆ Share Mac reviews: Disabled. ◆ Improve Siri and Dictation: Disabled. ◆ Sharing with app developers: Disabled. ◆ iCloud analytics sharing: Disabled. 

4.7. Locked screen

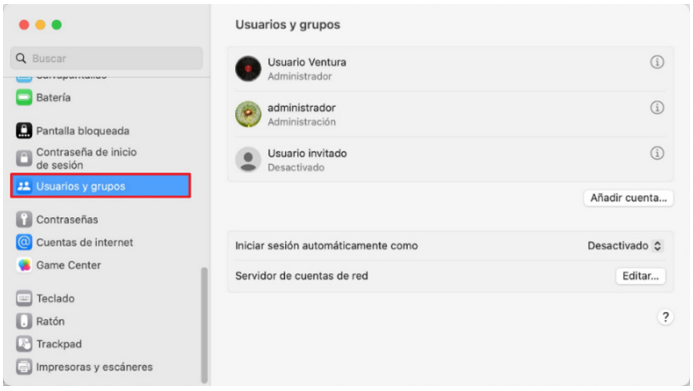
The lock screen feature in macOS Ventura allows users to protect their Mac from unauthorised access. They can set the screen saver to start automatically and set passwords to unlock the system, ensuring the privacy and security of their device when it is not in use.

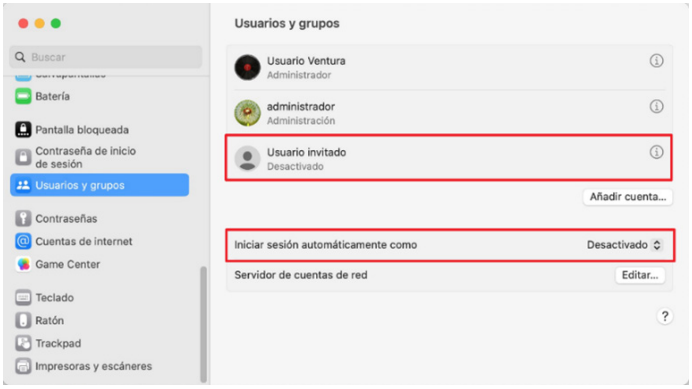
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Lock Screen".** 
4.	In the **"Locked Screen"** window, make the following changes as shown below: ◆ Start the screensaver when the computer is idle: For 10 minutes. ◆ Turn off the display when the computer is using the battery and remains idle: For 5 minutes. ◆ Turn off the screen when the computer is plugged into the mains and remains idle: For 5 minutes. ◆ Prompt for password after screensaver starts or screen is turned off: Immediately.  **Note: On desktops running macOS Ventura, the setting "Turn off the display when the computer uses battery power and remains idle" will not apply, as these devices do not use battery power.** **On the other hand, adjust these parameters to your needs, but always within a reasonable time frame.**

Passage	Description
5.	In the same **"Lock Screen"** window, make the following changes in the **"When changing user"** section: ◆ The login window displays: Name and password. ◆ Show password hint: Disabled. 

4.8. Users and groups

The **"Users and Groups"** section in macOS Ventura allows users to manage accounts and set login preferences.

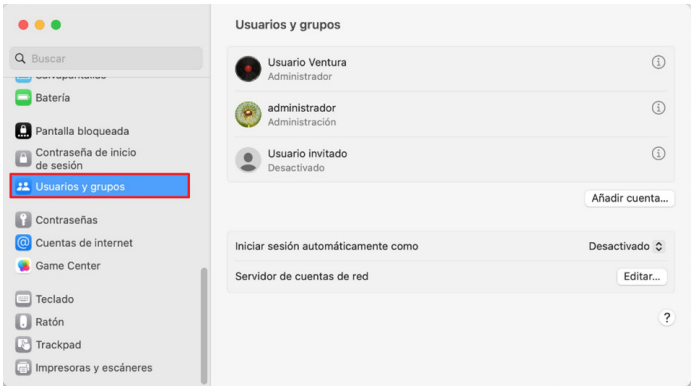
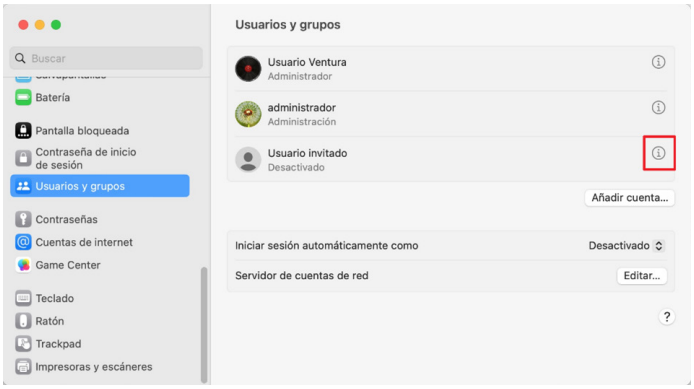
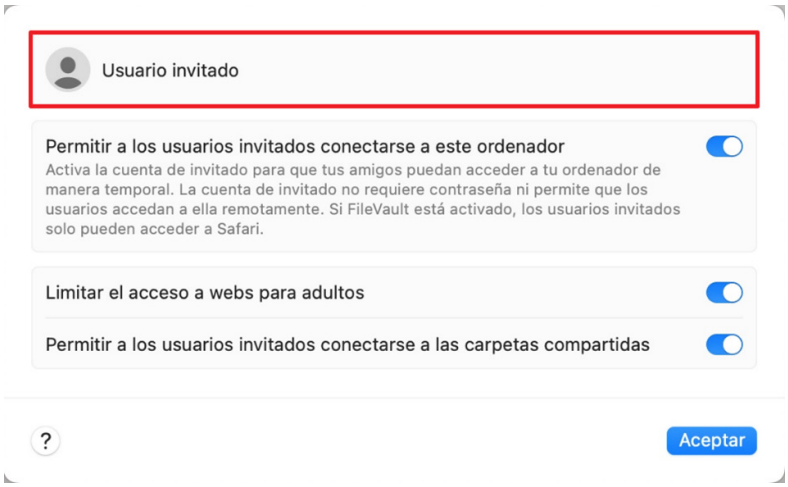
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select **"Users and groups".** 

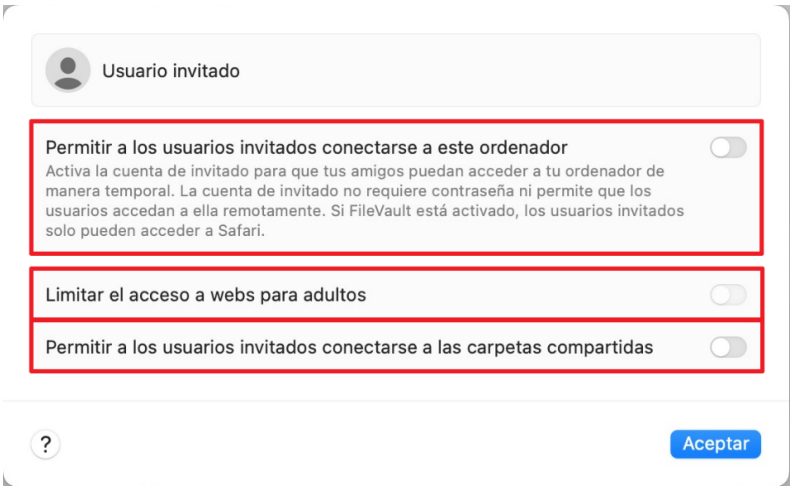
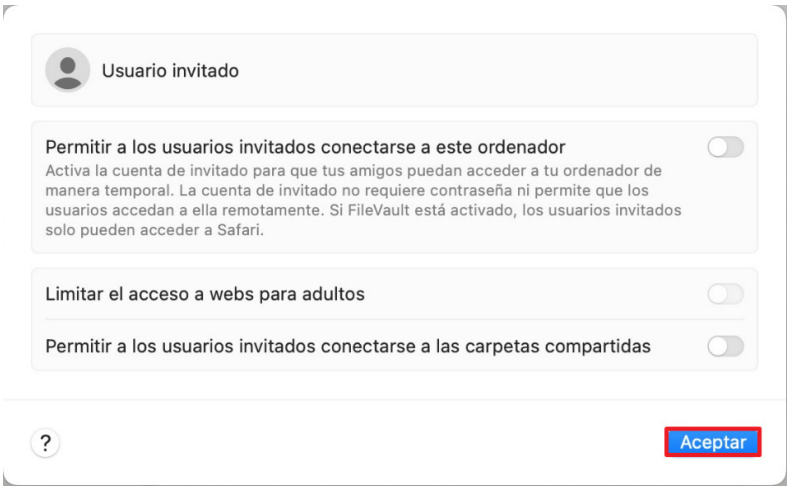
Passage	Description
4.	In the **"Users and Groups"** window, check that the following options are configured as shown below: ◆ Guest user: Deactivated. ◆ Automatic login as: Disabled.  **Note: If any of the above configurations are found to be different than indicated, follow the steps in the following sections as required:** **- 4.8.1 Disable guest user** **- 4.8.2 Disable automatic login**

4.8.1. Disable guest user

The "Guest User" is a special account in macOS Ventura that allows users to temporarily access a Mac without the need for a primary user account. However, for security reasons, this option will be disabled in this configuration process.

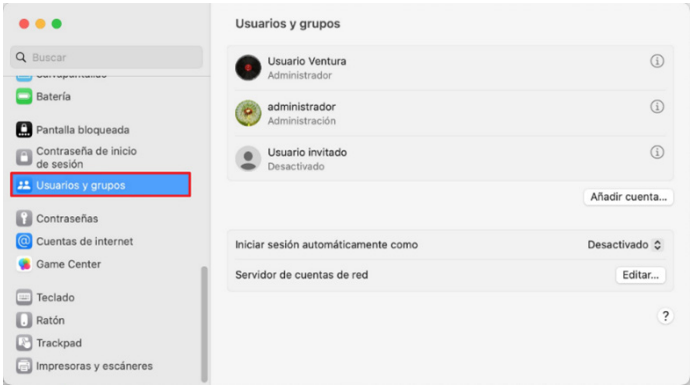
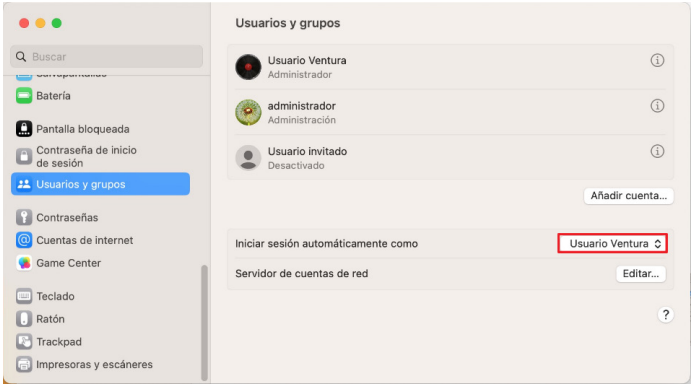
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 

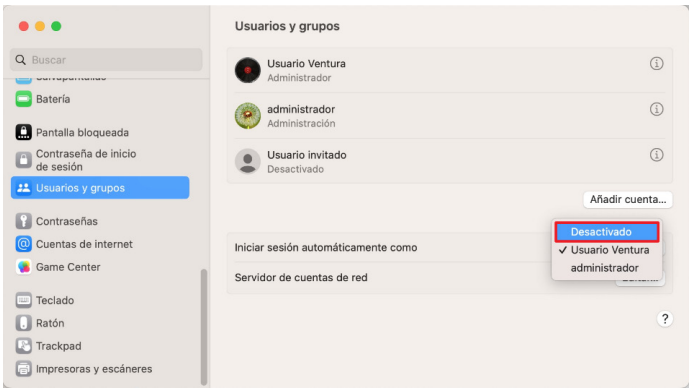
Passage	Description
3.	In the system settings window, navigate to the left menu and select **"Users and groups".** 
4.	In the **"Users and Groups"** window, click on the information icon on the right-hand side of the **"Guest User"** account. 
5.	In the window shown below, you will find the different settings for the guest account. 

Passage	Description
6.	To disable the **"Guest User"**, make the following modifications as shown below: ◆ Allow guest users to connect to this computer: Disabled. ◆ Limit access to adult websites: Disabled. ◆ Allow guest users to connect to shared folders: Disabled.  **Note: The option "Limit access to adult websites" should be set to on when you allow the use of a guest user, but wish to prevent access to undesirable websites.**
7.	Once you have made your changes, click on the **OK** button. 

4.8.2. Disable automatic login

In order to prevent anyone from logging in to your Mac device, it is recommended that you disable the settings that allow automatic login.

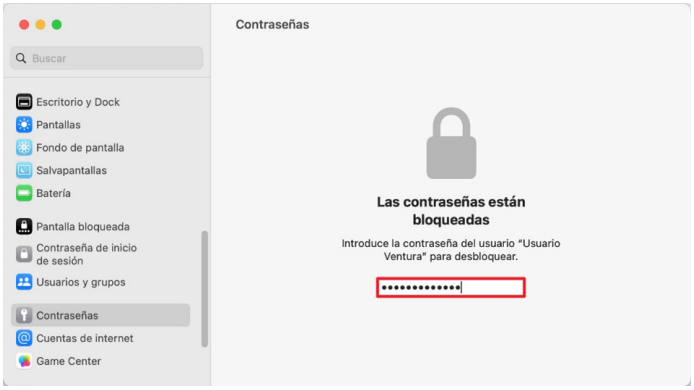
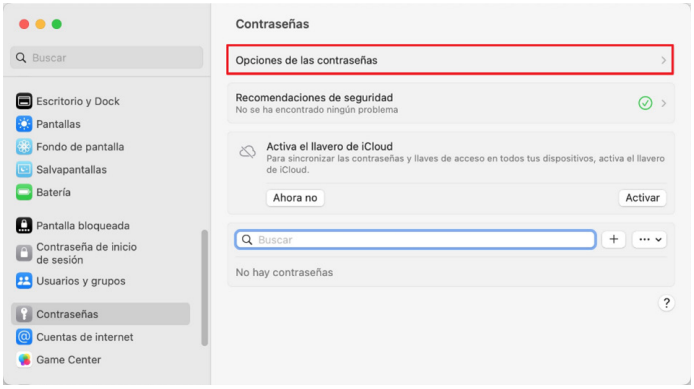
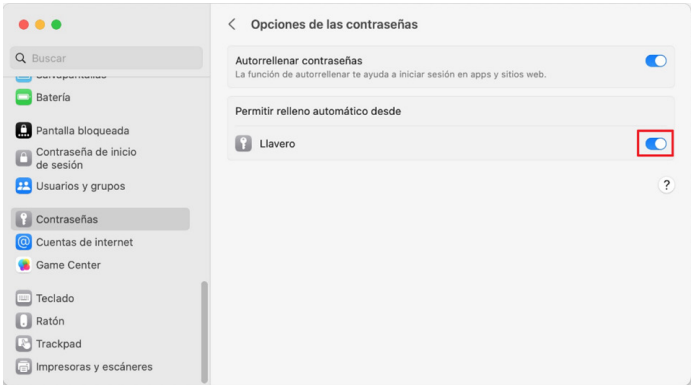
Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the **"System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the System Settings window, navigate to the left menu and select **Users and Groups.** 
4.	In the **"Users and groups"** window, click on the configured user on the right-hand side of the **"Automatically log in as"** option. 

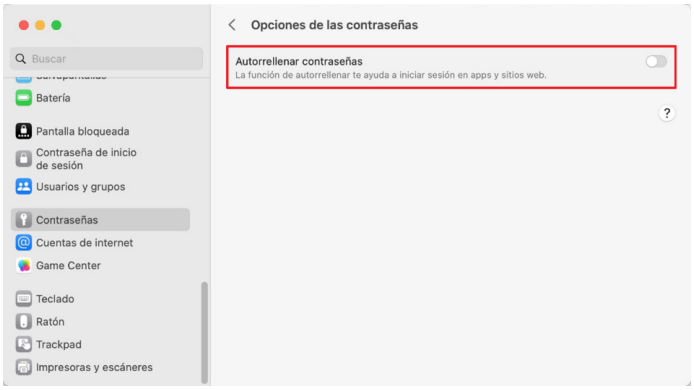
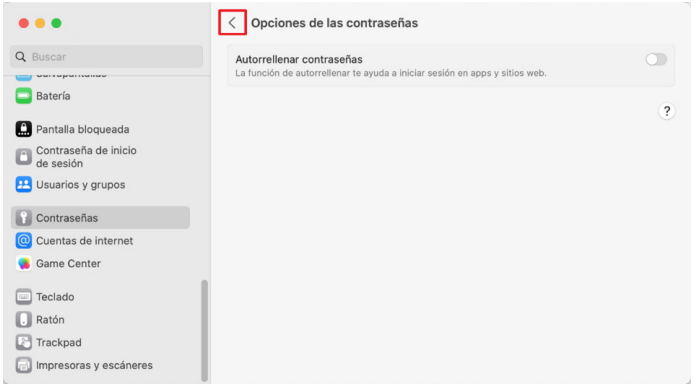
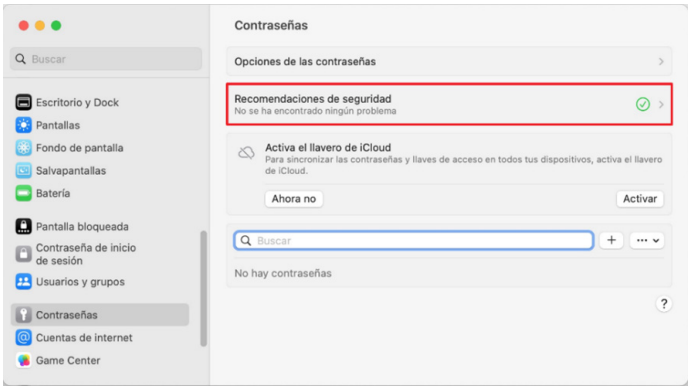
Passage	Description
5.	In the displayed selection window, select **"Disabled".** 

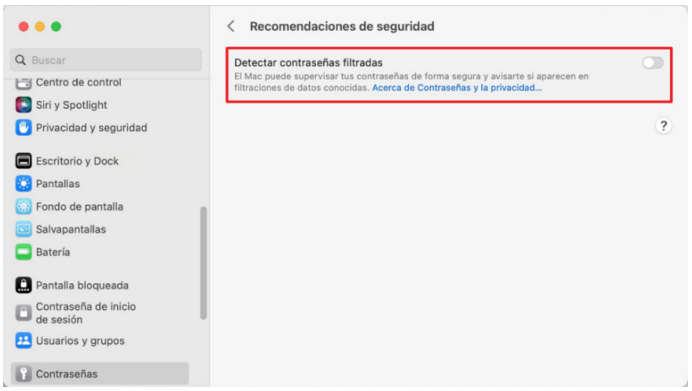
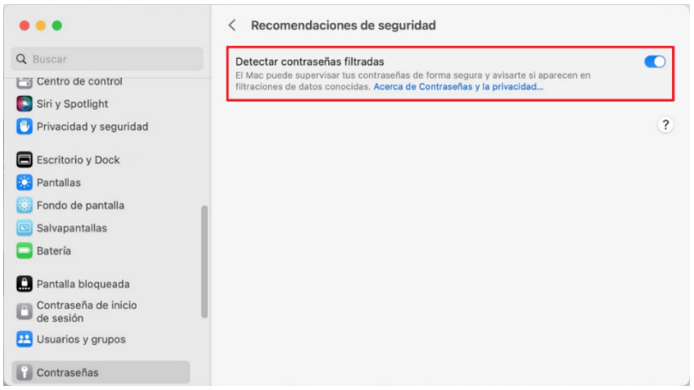
4.9. Passwords

In this section, the security recommendations for system passwords shall be activated.

Passage	Description
1.	Log in with your username and password on the macOS computer.
2.	Once on the operating system desktop, launch the "**System Settings"** located in the Dock (at the bottom of the screen, the gear icon). 
3.	In the system settings window, navigate to the left menu and select "**Passwords".** 

Passage	Description
4.	In the **"Passwords"** window, enter your user password to access the configuration. 
5.	In the **"Passwords"** window, click on **"Password Options".** 
6.	In the **"Password Options"** window, click on the button to deactivate the **"Keychain".** 

Passage	Description
7.	Then in the same window, uncheck the **"AutoFill Passwords"** option as shown in the image. 
8.	Click on **"<"** to return to the **"Passwords"** window. 
9.	In the options that appear, click on **"Security recommendations".** 

Passage	Description
10.	Identify the **"Detect leaked passwords"** setting. MacOS Ventura allows the system to analyse and alert the user if any of the passwords are on exposed or leaked lists. 
11.	Activate the setting **"Detect filtered passwords"**, as shown in the following image. 

5. Checklist

Criticality	Description
High	The macOS computer must have a supported operating system and applications up to date, including security updates at all times. **Note: You can check the macOS versions through the following link: https://support.apple.com/es-es/HT201260**
High	Access control is available for users logging into the macOS system through separate users with strictly necessary privileges.
High	The macOS firewall is enabled to protect incoming connections.
High	Connections to the Internet via Wi-Fi are made through secure access points that are password protected and encrypted.
High	Automatic login on macOS is disabled.
High	Disable the synchronisation of the device with the different iCloud applications.
High	Checking and disabling of applications to equipment functions or resources.
High	Disable the use of iCloud Password Autofill and iCloud Keychain.
Medium	System notifications are disabled for screen lock.
Medium	Covert mode is enabled in order to hide the response to port scans and prevent unwanted requests from being visible.
Medium	The device is enabled to "Find My Mac". Allowing remote wiping or locking of the computer.
Medium	Make sure that the computer does not have any unnecessary network shares (folders, files, etc.).

Criticality	Description
Medium	The device has a time for automatic screen locking in case of inactivity.
Medium	The device requests connection to a known secure Wi-Fi network and does not connect automatically.
Medium	The equipment requests connection to nearby access points when there is no known access point and does not connect automatically.
Medium	User input is required and to log in again after the computer has been locked.
Low	Avoid sending reports and analysis on the equipment and user.
Low	Playback or continuation of the user's activities on another device has been limited.

6. Decalogue of recommendations

The following are ten security recommendations for macOS Operating Systems

Decalogue of recommendations for macOS Operating Systems

1. Keep the **operating system** and **applications** up to date to receive **security patches** and **new features**.
2. If you need to **install add-ons**, it is recommended that you use the **App Store**, **official and/or trusted sources.**
3. It is advisable **not to use the password vault available in macOS.** Instead, it is recommended to use **other applications** that **implement strong encryption to store passwords more securely.**
4. Use of **two-factor authentication** 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.).
5. Regularly **back up relevant data to external drives** or **cloud services**.
6. Be especially cautious when **clicking on links** and **attachments in e-mails to avoid phishing**.
7. **Enable FileVault** or **another solution** to **encrypt the hard disk** to **protect data in case the device is lost or stolen.**
8. **Connect only to secure Wi-Fi networks** and avoid open or unverified networks.
9. **Configure the screen lock** and **notifications** to limit access to content on the device.
10. **Enable the macOS firewall** to **protect the Internet connection** and implement antivirus **software to protect against malware attacks,** among others.

Centro Criptológico Nacional 20 ANIVERSARIO

CCN-CERT centro criptológico nacional

Annex A. Further recommendations

A.1. Passwords

A strong password is essential to protect online accounts and data. Be sure to create unique and complex passwords that combine letters, numbers and special characters. Avoiding obvious personal information, such as names or dates of birth, and considering the use of memorable phrases or acronyms is crucial. Similarly, keeping passwords up to date and not sharing them across multiple accounts or services is essential to ensure maximum online security.

Strong passwords are a vital part of data protection in an increasingly digital world. They are the first line of defence against potential cyber threats and unauthorised access to accounts and personal information.

A.2. Antivirus

Despite macOS's reputation for security, using an antivirus on Mac devices is essential due to ever-evolving cyber threats. Antivirus offers a number of key benefits including the following:

- Up-to-date malware protection to detect and remove threats.
- Proactive detection of suspicious behaviour, crucial to prevent zero-day attacks.

- Web browsing security modules to prevent malicious sites and phishing.
- Safeguarding personal data against theft and privacy breaches.
- Maintaining system performance without significantly slowing down the system.
- Preventing the spread of malware to other devices on the network.

In short, an antivirus on macOS provides an additional layer of security to protect privacy, data and system performance, but it must be complemented by sound security practices and online awareness, as no antivirus is foolproof.

A.3. Time machine and backup

Time Machine, a macOS backup tool, is essential for data integrity and recovery. It offers simplicity and convenience with automatic copies, version history, disaster recovery, system-wide protection and flexible storage options. While there are alternatives on the market, the choice depends on the needs and preferences of each user and/or organisation.

A.4. Disk encryption and FileVault

Disk encryption, such as FileVault on macOS, is essential to protect data from unauthorised access if your Mac device is lost or stolen, as well as using a user password or recovery key to access encrypted data. It is of utmost importance to keep the recovery key in a safe place.

Enabling FileVault is a simple and effective measure to improve the security and privacy of your data. It is important to keep in mind that there are other alternatives on the market to encrypt data, and the choice of the right tool will depend on the individual needs of each user and/or organisation.

Centro Criptológico Nacional

ANIVERSARIO

CCN-CERT

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es