

CCN-CERT BP/32



Recomendaciones de Seguridad en Sistemas Operativos macOS

INFORME DE BUENAS PRÁCTICAS

MAYO 2024

ccn-cert
centro criptológico nacional

20 ANIVERSARIO
Centro
Criptológico
Nacional

Edita:



© Centro Criptológico Nacional, 2024

Fecha de edición: abril de 2024

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

Índice

1. Introducción	4
2. Objetivo y alcance	5
3. Sistema operativo macOS	6
4. Ajustes del sistema	7
4.1 Usuario iCloud	7
4.2. Wi-fi	11
4.3. Red	12
4.4. Notificaciones	13
4.5. General	15
4.5.1. Actualización de software	15
4.5.2. AirDrop y Handoff	17
4.5.2.1. Para más de un dispositivo de Apple	17
4.5.2.2. Para un solo dispositivo de Apple	19
4.5.3. Compartir	24
4.6. Privacidad y seguridad	26
4.6.1. Privacidad	26
4.6.1.1. Localización	26
4.6.1.2. Otras configuraciones de privacidad	29
4.6.1.3. Análisis y mejoras	31
4.7. Pantalla bloqueada	32
4.8. Usuarios y grupos	34
4.8.1. Deshabilitar usuario invitado	35
4.8.2. Desactivar iniciar sesión automáticamente	35
4.9. Contraseñas	39
5. Lista de comprobación	43
6. Decálogo	45
Anexo A. Recomendaciones adicionales	47
Anexo A.1. Contraseñas	47
Anexo A.2. Antivirus	47
Anexo A.3. Time machine y Copia de seguridad	48
Anexo A.4. Cifrado de disco y Filevault	48

1. Introducción

Esta guía está diseñada para aprovechar al máximo los equipos con macOS, brindando las herramientas y el conocimiento necesarios para proteger los datos y la privacidad. Se explorarán una serie de configuraciones básicas de seguridad que todos los usuarios de macOS deben considerar para mantener su información a salvo de amenazas potenciales.

Las ventajas de utilizar macOS son numerosas: sistema operativo intuitivo, estabilidad, optimización de hardware y software, etc. Sin embargo, estas ventajas no deben eclipsar la importancia de salvaguardar los datos y la privacidad. En el mundo digital actual, la información personal, desde fotos y documentos hasta contraseñas y datos financieros, está en constante riesgo.

La pérdida o el acceso no autorizado a esta información pueden tener consecuencias significativas. En esta guía, se ofrecen pautas para proteger los datos personales, navegar de forma segura por Internet y evitar amenazas comunes, como malware y phishing.

2. Objetivo y alcance

El propósito de esta guía es proporcionar a los usuarios de macOS un conjunto completo de instrucciones y recomendaciones para establecer y optimizar las configuraciones de seguridad básicas en sus dispositivos, realizando los ajustes más relevantes con el fin de garantizar una mayor seguridad tanto para el dispositivo como para el usuario.

Esto será realizado a través de los diferentes menús de configuración de los que dispone el sistema operativo, no siendo necesario la ejecución de comandos, ya sean simples o complejos. De este modo, las configuraciones serán accesibles a cualquier tipo de usuario independientemente de su conocimiento tecnológico.

Es importante destacar que estas configuraciones pueden variar en otras versiones del sistema operativo y, además, que esta guía se ha realizado considerando a un usuario con una cuenta de iCloud (ID de Apple). Por lo tanto, los usuarios deberán adaptar los pasos del presente documento a los posibles cambios que puedan existir, tanto en versiones anteriores como posteriores del sistema operativo, y teniendo en cuenta su configuración específica de iCloud.

3. Sistema operativo macOS

Durante las siguientes secciones se desarrollarán una serie de configuraciones del sistema que permitirán fortalecer la seguridad de macOS. Se explicará cada aspecto de manera clara y concisa, proporcionando las directrices necesarias para proteger los datos e información personal. A medida que se avanza, se descubre que garantizar la seguridad del sistema es más sencillo de lo que parece.

La guía seguirá un recorrido detallado a través de los **“Ajustes del Sistema”** de macOS en su edición **Ventura**. Cada paso se realizará ingresando a las configuraciones del sistema, lo que permitirá abordar las configuraciones de seguridad de manera sencilla.

4. Ajustes del sistema

Los “Ajustes del Sistema” en macOS Ventura son el centro de control para que los usuarios personalicen y configuren su sistema operativo macOS. Desde este elemento, es posible ajustar preferencias de seguridad, privacidad, redes, pantallas, usuarios y más. Son la clave para que los usuarios adapten su experiencia de usuario y garanticen la seguridad de sus dispositivos.

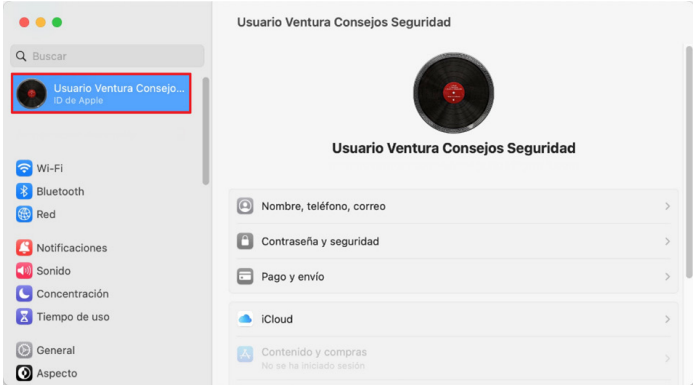
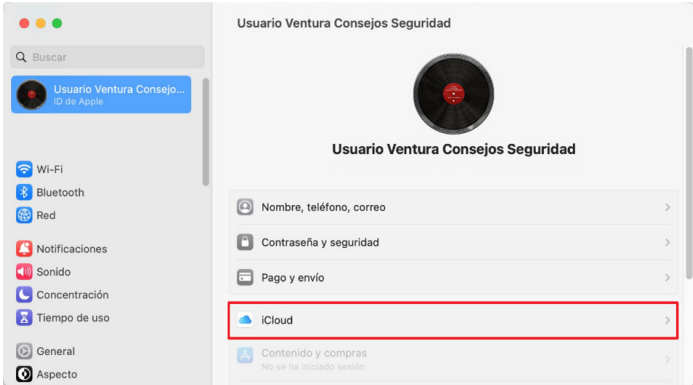
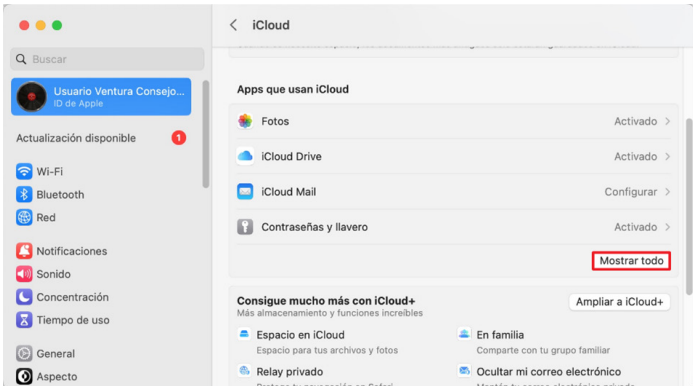
4.1. Usuario iCloud

Las configuraciones en la cuenta de iCloud permiten a los usuarios personalizar y gestionar la forma en que se sincronizan y almacenan datos en la nube de Apple. Esto incluye opciones para respaldar fotos, contactos, notas y otros datos, así como habilitar la ubicación y el uso compartido con familiares. También se pueden configurar preferencias de almacenamiento, opciones de seguridad y acceso a servicios de Apple como “Buscar mi Mac”. Estas configuraciones ofrecen mayor control sobre la experiencia y la privacidad del usuario en el ecosistema de Apple.

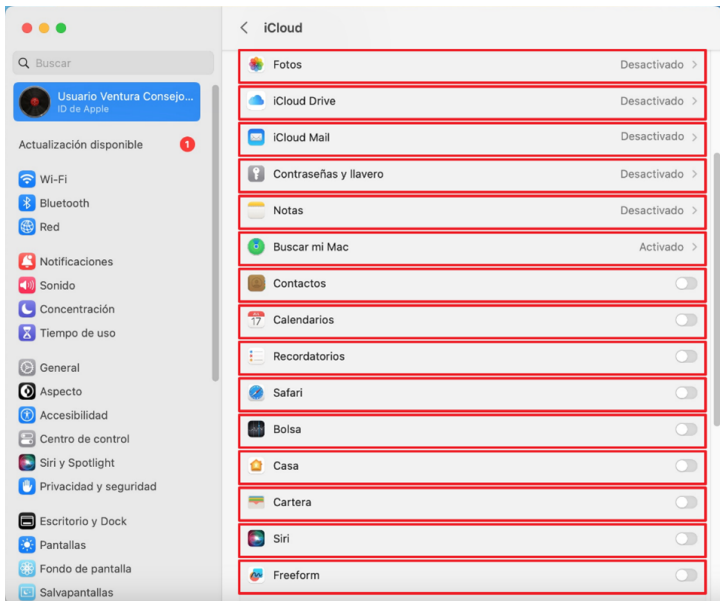
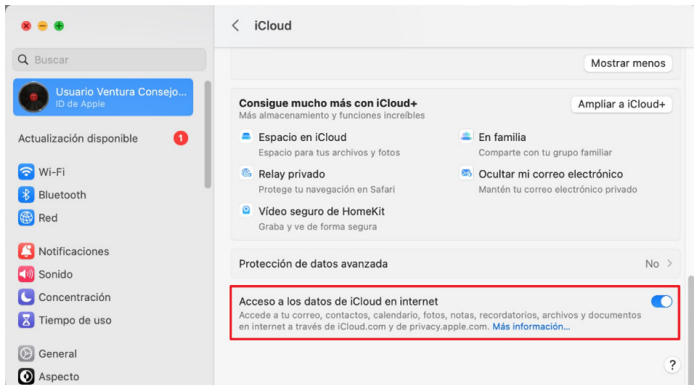
Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 

Nota: El usuario mostrado en esta guía es representativo y se utiliza con fines ilustrativos

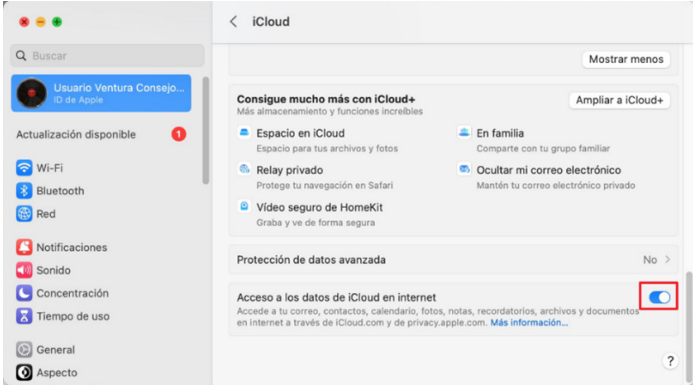
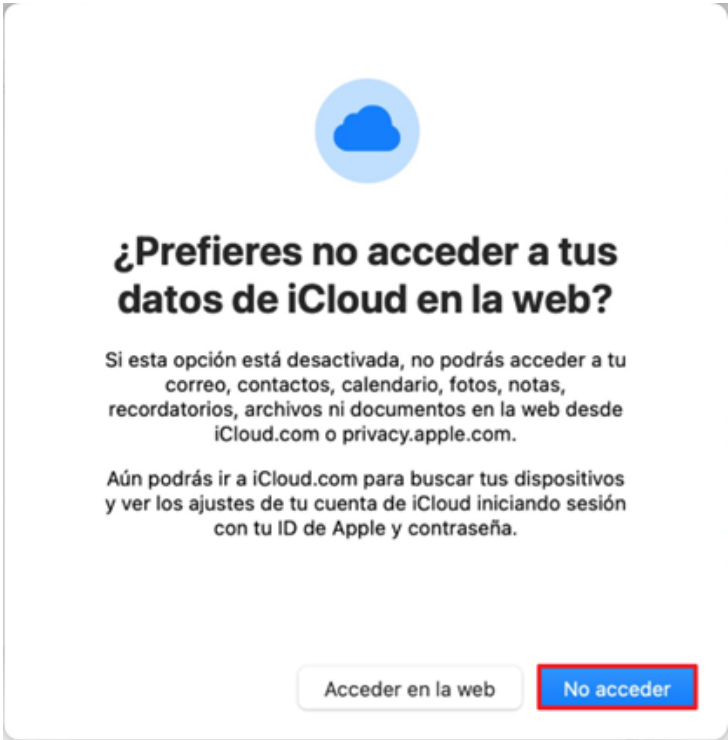
4. Ajustes del sistema

Paso	Descripción
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione su cuenta. 
4.	A continuación, haga clic sobre "iCloud". 
5.	En la ventana "iCloud" navegue hasta encontrar el botón "Mostrar todo" y haga clic sobre este. 
6.	Modifique las siguientes configuraciones tal y como se indica a continuación: ◆ Fotos: Desactivado. ◆ iCloud Drive: Desactivado. ◆ iCloud Mail: Desactivado. ◆ Contraseña y llavero: Desactivado. ◆ Notas: Desactivado. ◆ Buscar mi Mac: Activado.

4. Ajustes del sistema

Paso	Descripción
6.	◆ Contactos: Desactivado. ◆ Calendarios: Desactivado. ◆ Recordatorios: Desactivado. ◆ Safari: Desactivado. ◆ Bolsa: Desactivado. ◆ Casa: Desactivado. ◆ Cartera: Desactivado. ◆ Siri: Desactivado. ◆ Freeform: Desactivado.  Nota: Si requiere el uso de alguna de las configuraciones desactivadas con anterioridad, deberá valorar cada configuración en particular y si es necesario mantenerla(s) activada(s). El documento se ha elaborado tratando de limitar al máximo la posibilidad de uso de información por parte de otros dispositivos sincronizados.
7.	En la misma ventana, navegue y localice “Acceso a los datos de iCloud en internet”. 

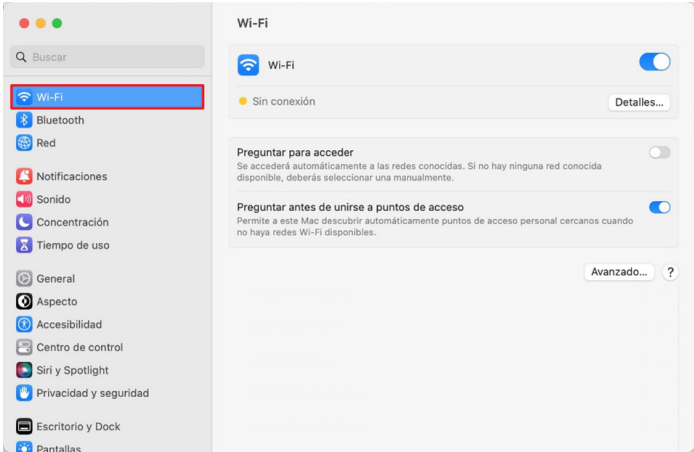
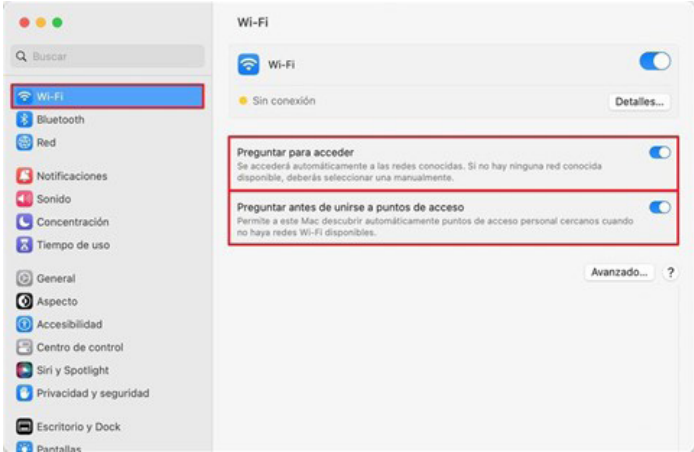
4. Ajustes del sistema

Paso	Descripción
8.	Haga clic sobre el botón "Acceso a los datos de iCloud en internet" para desactivar la opción. 
9.	En la siguiente ventana, pulse sobre el botón "No acceder". 

4. Ajustes del sistema

4.2. Wi-Fi

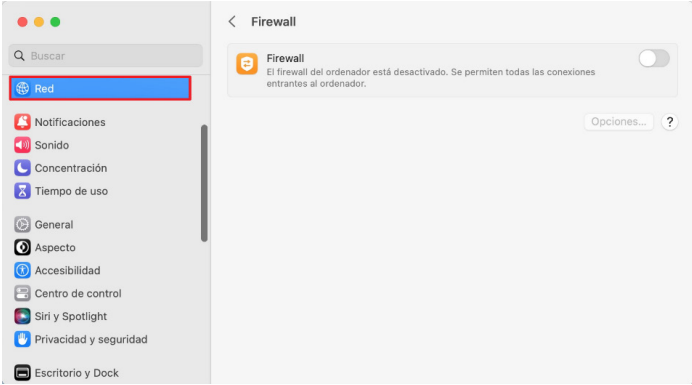
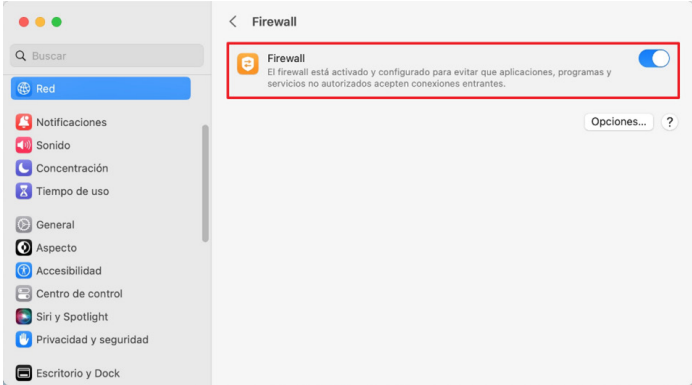
La configuración de **Wi-Fi** en macOS Ventura permite a los usuarios conectarse de manera segura a redes inalámbricas y gestionar su acceso.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Wi-Fi” . 
4.	En la ventana “Wi-Fi” , modifique las siguientes configuraciones tal y como se muestra a continuación: ◆ Preguntar para acceder: Activado. ◆ Preguntar antes de unirse a puntos de acceso: Activado. 

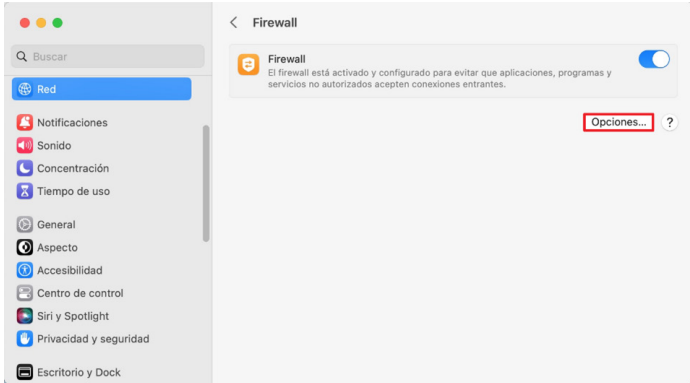
4. Ajustes del sistema

4.3. Red

La sección de **Red** permite a los usuarios gestionar la conectividad y la seguridad de las redes.

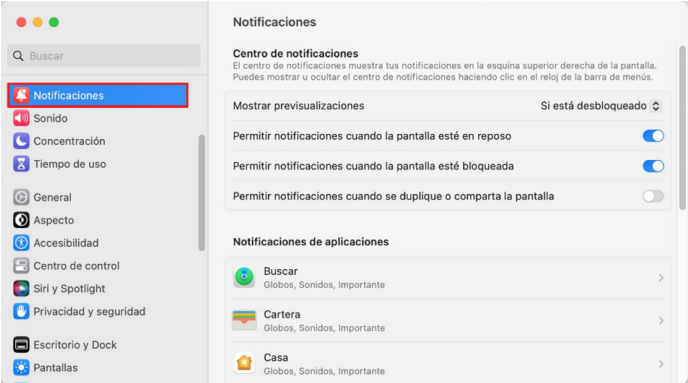
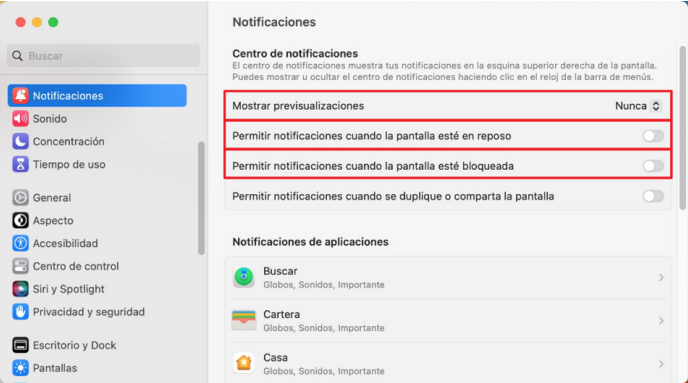
Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "Red" . 
4.	Posteriormente haga clic sobre "Firewall" y actívelo, tal y como se muestra en la siguiente imagen. 

4. Ajustes del sistema

Paso	Descripción
5.	A continuación, pulse sobre el botón "Opciones...". 
6.	En la ventana emergente, active la opción "Activar modo encubierto". 
7.	Finalizada la activación, haga clic sobre el botón "Aceptar". 

4.4. Notificaciones

En esta sección, el objetivo es reducir la exposición de información cuando el equipo se encuentra bloqueado o en reposo. Por lo tanto, se procederá a desactivar varias configuraciones de notificaciones en dichas circunstancias, garantizando así la privacidad y la seguridad de los datos en el sistema operativo macOS.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Notificaciones” . 
4.	En la ventana “Notificaciones” modifique las siguientes configuraciones tal y como se muestra a continuación: ◆ Mostrar previsualizaciones: Nunca. ◆ Permitir notificaciones cuando la pantalla esté en reposo: Desactivado. ◆ Permitir notificaciones cuando la pantalla esté bloqueada: Desactivado. 

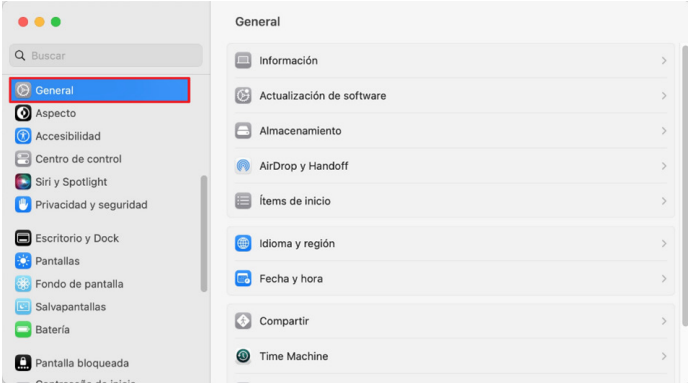
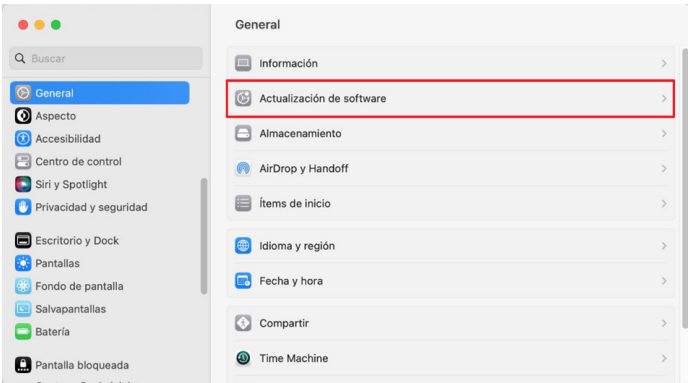
4. Ajustes del sistema

4.5. General

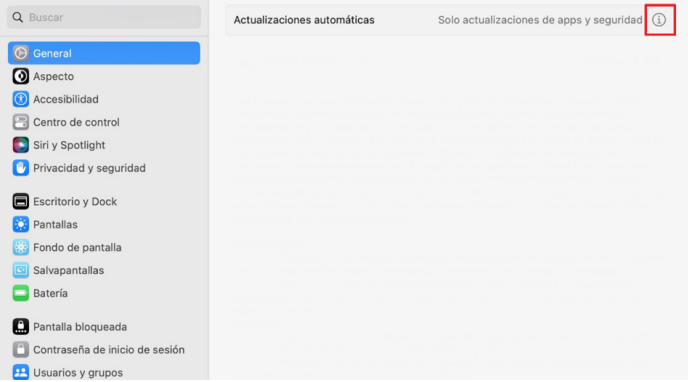
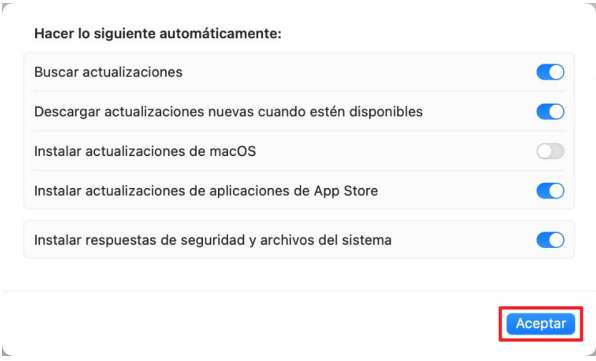
En esta sección se realizarán modificaciones con respecto a las actualizaciones del sistema operativo de macOS Ventura y otros aspectos relacionados con la compartición de datos.

4.5.1. Actualización de software

En el siguiente apartado, se permite a los usuarios mantener sus sistemas y aplicaciones actualizados para mejorar la estabilidad y la seguridad.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "General" . 
4.	Posteriormente, haga clic sobre "Actualización de Software" . 

4. Ajustes del sistema

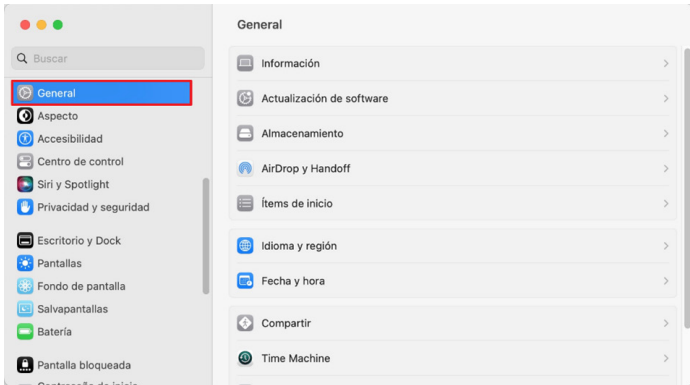
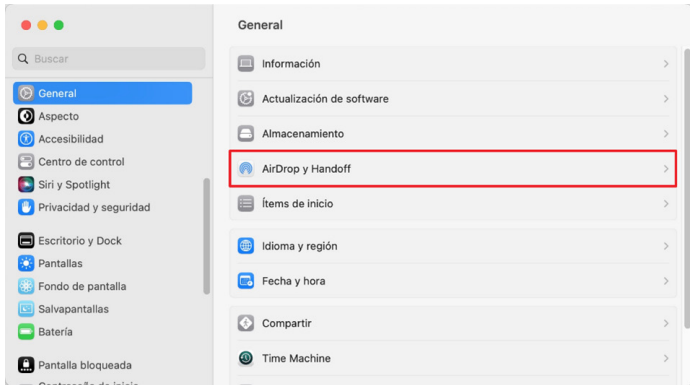
Paso	Descripción
5.	En la ventana “Actualización de software”, haga clic sobre el icono de información ⓘ, situado en el lado derecho de la opción “Solo actualizaciones de apps y seguridad”. 
6.	En la nueva ventana que aparecerá “Hacer lo siguiente automáticamente:” modifique las siguientes configuraciones tal y como se muestra a continuación: ◆ Buscar actualizaciones: Activado. ◆ Descargar actualizaciones nuevas cuando estén disponibles: Activado. ◆ Instalar actualizaciones de aplicaciones de App Store: Activado ◆ Instalar respuestas de seguridad y archivos del sistema: Activado.  Nota: Relacionado con la opción “Instalar actualizaciones macOS”, esta no se activa debido a que es posible que una actualización de sistema operativo recién publicada pueda generar problemas a nivel software y hardware. Si se desea habilitar, se recomienda que previamente se realice una copia de seguridad para evitar pérdidas de información.
7.	Realizada las modificaciones, pulse sobre el botón “Aceptar”. 

4. Ajustes del sistema

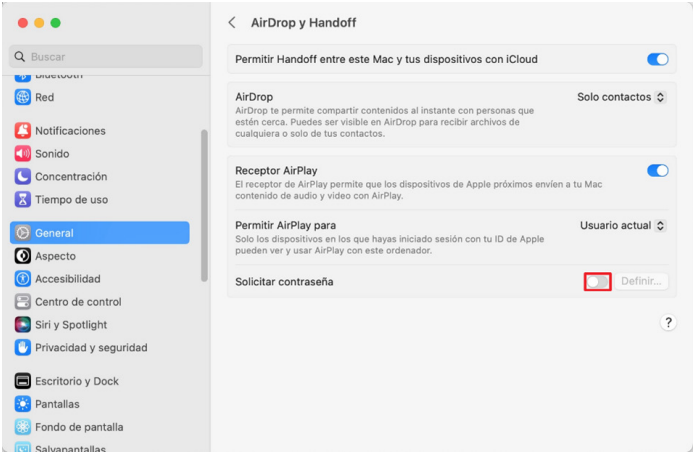
4.5.2. Airdrop y Handoff

Esta sección se centra en empezar algo en un dispositivo Apple y retomarlo en otro, enviar archivos a dispositivos Apple cercanos con AirDrop o permitir que otros dispositivos reproduzcan contenido a través del Mac. Se realizarán las configuraciones para los casos de más de un dispositivo de Apple y para solo un dispositivo de Apple en las secciones siguientes.

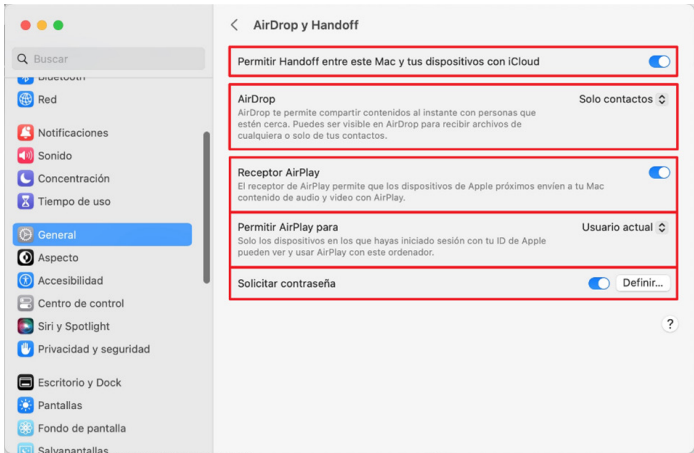
4.5.2.1. Para más de un dispositivo de Apple

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “General” . 
4.	Posteriormente, haga clic sobre “AirDrop y Handoff” . 

4. Ajustes del sistema

Paso	Descripción
5.	En la ventana “AirDrop y Handoff”, haga clic sobre el botón de activación para la opción “Solicitar contraseña”. 
6.	A continuación, se solicitará elevación de privilegios. Introduzca el nombre de usuario y la contraseña en los cuadros de texto correspondiente y haga clic en “Modificar ajustes”. 

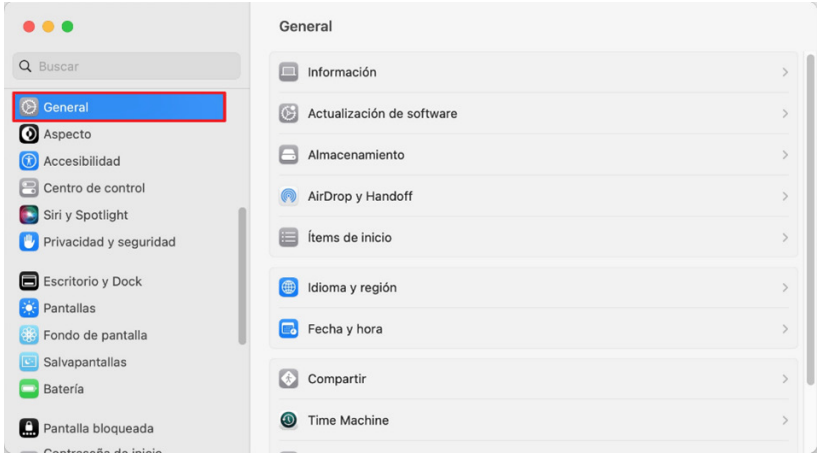
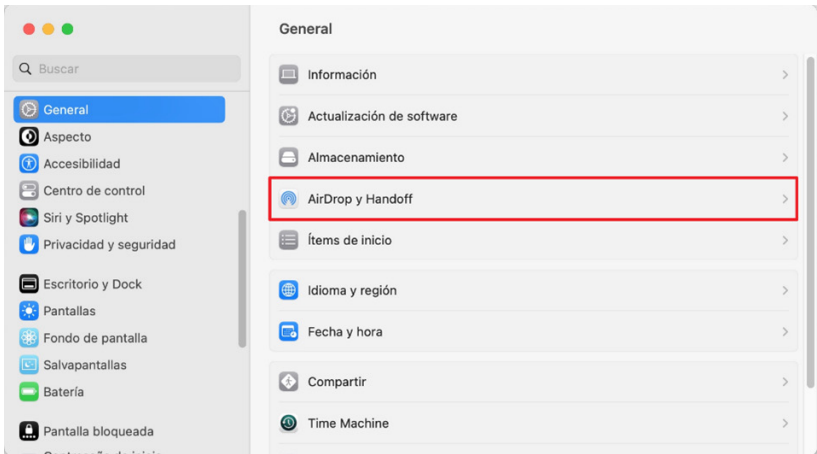
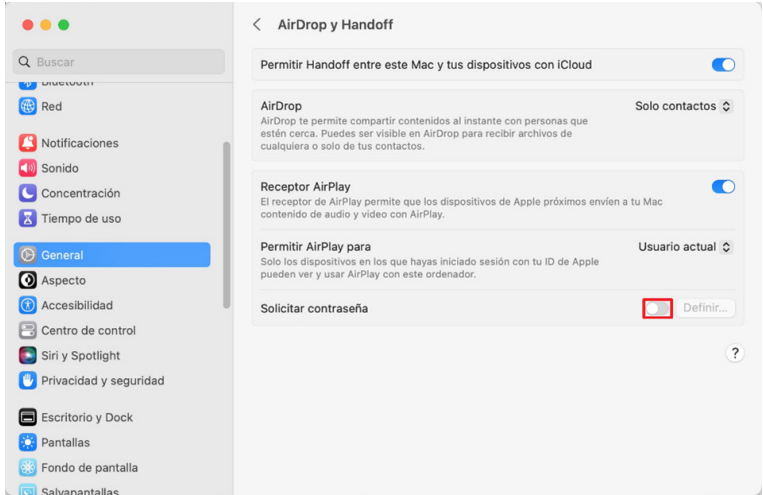
4. Ajustes del sistema

Paso	Descripción
7.	Introduzca la nueva contraseña de AirPlay. Dicha contraseña será necesaria cada vez se haga uso dicha función. Posteriormente pulse "Aceptar". 
8.	Verifique y modifique las siguientes configuraciones tal y como se muestra a continuación: ◆ Permitir Handoff entre este Mac y tus dispositivos con iCloud: Activado. ◆ AirDrop: Solo contactos. ◆ Receptor AirPlay: Activado. ◆ Permitir AirPlay para: Usuario actual. ◆ Solicitar contraseña: Activado. 

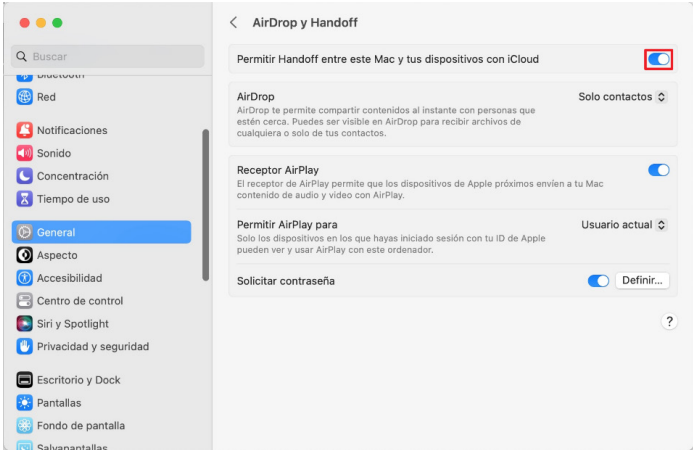
4.5.2.2. Para un solo dispositivo de Apple

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 

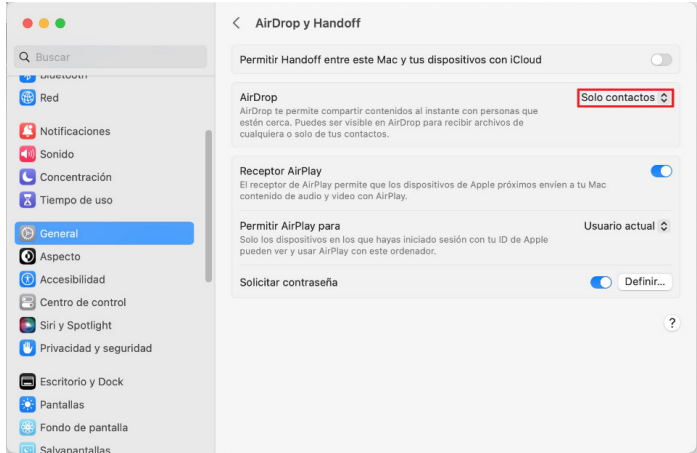
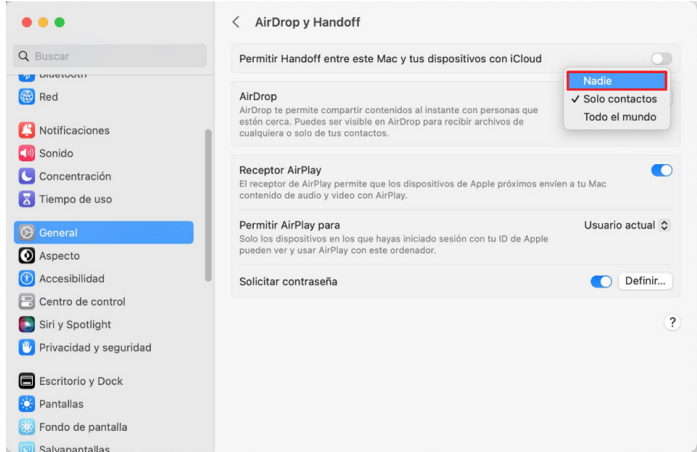
4. Ajustes del sistema

Paso	Descripción
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “General”. 
4.	Posteriormente, haga clic sobre “AirDrop y Handoff”. 
5.	En la ventana “AirDrop y Handoff”, haga clic sobre el botón de activación para la opción “Solicitar contraseña”. 

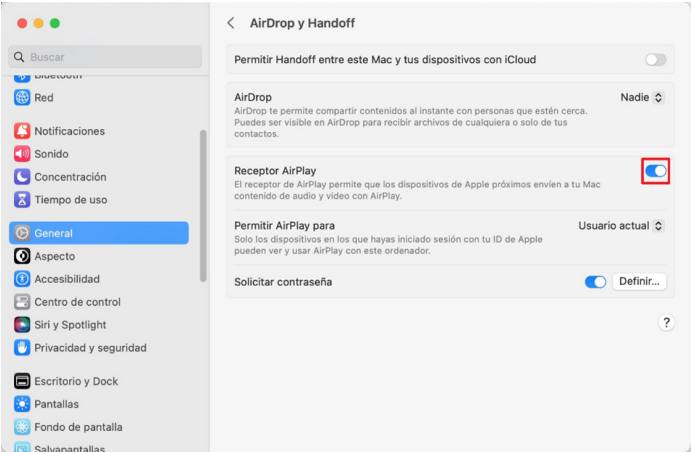
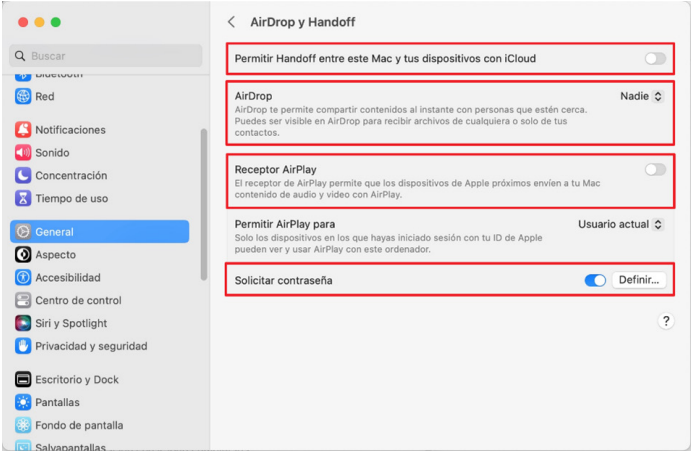
4. Ajustes del sistema

Paso	Descripción
6.	A continuación, se solicitará elevación de privilegios. Introduzca el nombre de usuario y la contraseña en los cuadros de texto correspondiente y haga clic en “Modificar ajustes”.  The image shows a system dialog titled "AirDrop y Handoff". It contains the text "AirDrop y Handoff está intentando modificar tus ajustes del sistema." followed by "Introduce la contraseña para permitir esta operación." Below this are two input fields: "Nombre de usuario" and "Contraseña", both highlighted with red rectangles. At the bottom are two buttons: "Cancelar" and "Modificar ajustes", with the latter also highlighted with a red rectangle.
7.	Introduzca la nueva contraseña de AirPlay. Dicha contraseña será necesaria cada vez se haga uso dicha función. Posteriormente pulse “Aceptar”.  The image shows a dialog titled "Introduce la nueva contraseña de AirPlay:". It features a single large text input field highlighted with a red rectangle. At the bottom right, there are two buttons: "Cancelar" and "Aceptar", with the latter highlighted with a red rectangle.
8.	En la ventana “AirDrop y Handoff”, desactive “Permitir Handoff entre este Mac y tus dispositivos con iCloud”. Para ello haga clic sobre el botón de activación.  The image shows the "AirDrop y Handoff" settings window. The "Permitir Handoff entre este Mac y tus dispositivos con iCloud" toggle switch is highlighted with a red rectangle and is currently turned on. Other settings visible include "AirDrop" (set to "Solo contactos"), "Receptor AirPlay" (turned on), "Permitir AirPlay para" (set to "Usuario actual"), and "Solicitar contraseña" (turned on).

4. Ajustes del sistema

Paso	Descripción
9.	A continuación, pulse sobre el botón “No permitir Handoff”. 
10.	De nuevo, en la ventana “AirDrop y Handoff”, restrinja “AirDrop”. Para ello haga clic sobre el desplegable. 
11.	A continuación, seleccione la opción “Nadie”. 

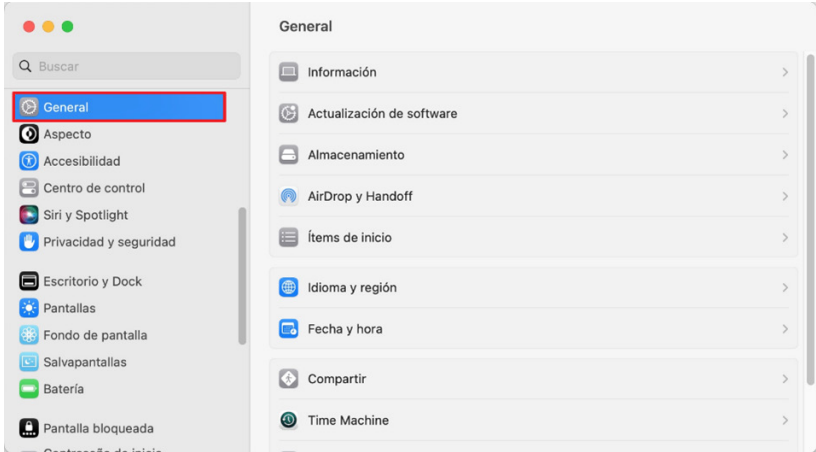
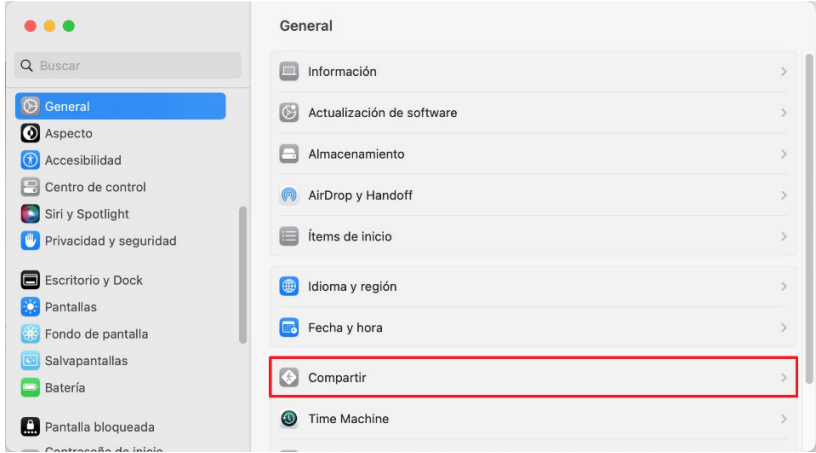
4. Ajustes del sistema

Paso	Descripción
12.	En la misma ventana “AirDrop y Handoff”, desactive “Receptor AirPlay”. Para ello haga clic sobre el botón de activación. 
13.	Verifique que las configuraciones realizadas se han establecido tal y como se indica a continuación: ◆ Permitir Handoff entre este Mac y tus dispositivos con iCloud: Desactivado. ◆ AirDrop: Nadie. ◆ Receptor AirPlay: Desactivado. ◆ Solicitar contraseña: Activado. 

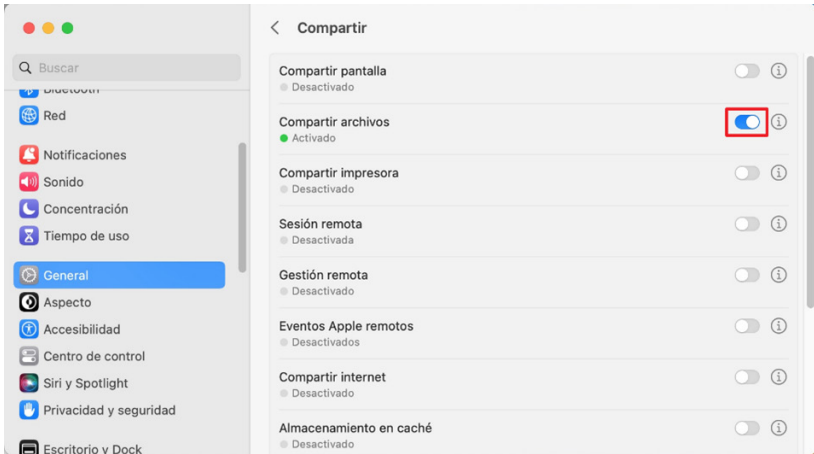
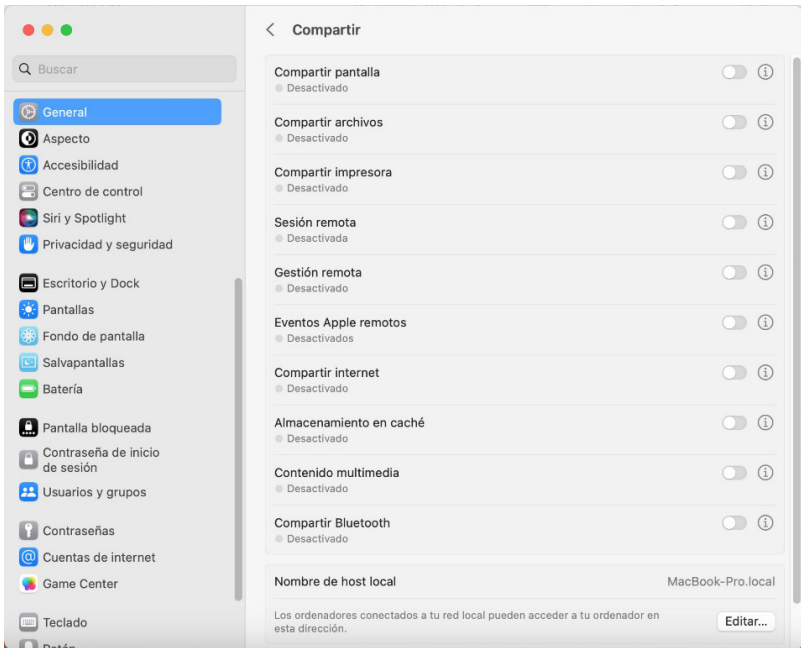
4. Ajustes del sistema

4.5.3. Compartir

En esta sección de configuración, se pueden realizar diferentes acciones para que recursos, dispositivos o conexiones puedan ser compartidos.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “General” . 
4.	Posteriormente haga clic sobre “Compartir” .. 

4. Ajustes del sistema

Paso	Descripción
5.	En la ventana "Compartir", desactive "Compartir archivos". Para ello haga clic sobre el botón de activación. 
7.	Para el resto de configuraciones de la ventana "Compartir", los sistemas macOS establecen estas configuraciones en desactivado por defecto. Por tanto, mantenga las configuraciones en estado desactivado a excepción de aquellas que se requieran para un uso concreto.  Nota: Si alguna de las configuraciones está activada, se recomienda valorar cada configuración en particular y valorar si es necesario mantenerla(s) activada(s). En caso de mantener alguna de las funciones activas se deben seguir los siguientes criterios: ◆ Mínimos privilegios. Tipo de Usuario: estándar, solo compartir o administrador. ◆ Solo a los usuarios estrictamente necesarios. ◆ Mínimos permisos. Lectura o Escritura. ◆ Mínimos dispositivos a compartir.

4. Ajustes del sistema

4.6. Privacidad y seguridad

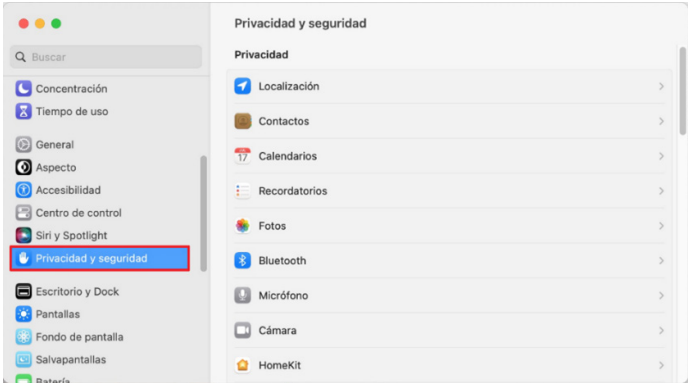
MacOS Ventura se centra en configuraciones que protegen la privacidad y la integridad de los datos. Esto incluye la activación de funciones como FileVault para el cifrado de datos, la gestión de permisos de aplicaciones y la configuración de preferencias de seguridad avanzadas. Estas configuraciones son esenciales para garantizar que los usuarios tengan un control completo sobre quién y qué puede acceder a su información en el sistema.

4.6.1. Privacidad

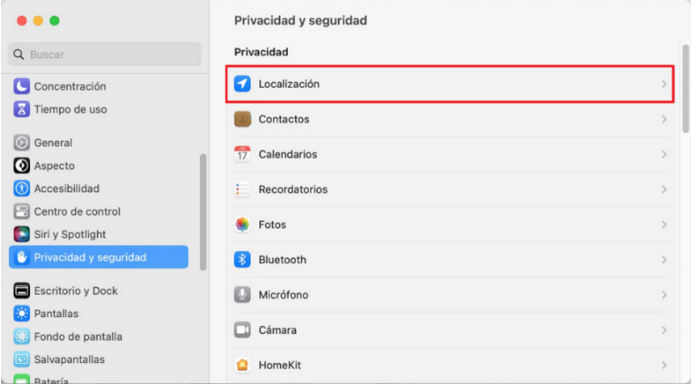
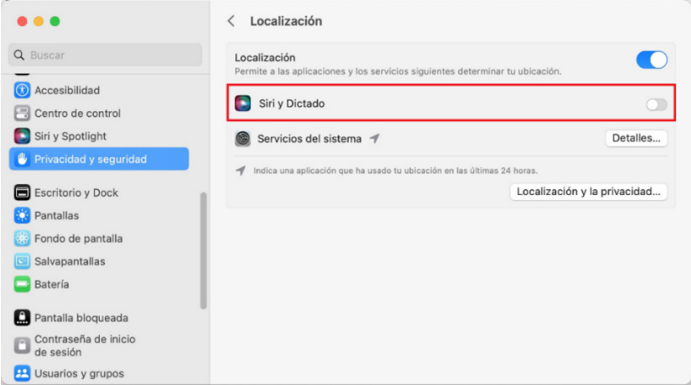
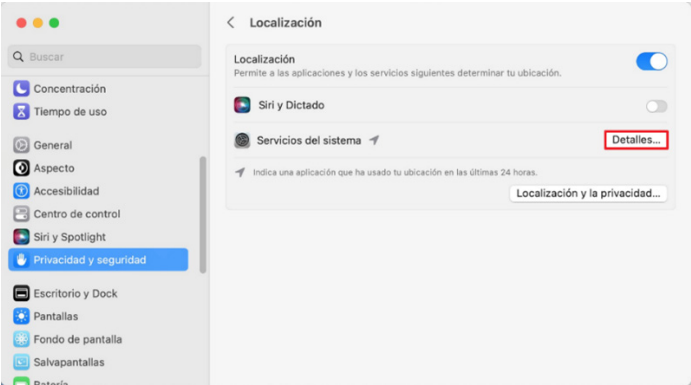
En esta sección se prioriza la privacidad al proporcionar configuraciones y herramientas que permiten a los usuarios controlar y limitar el acceso a su información. Esto incluye la gestión de permisos de aplicaciones, que permite a los usuarios decidir qué aplicaciones tienen acceso a datos sensibles como la ubicación, la cámara o el micrófono.

4.6.1.1. Localización

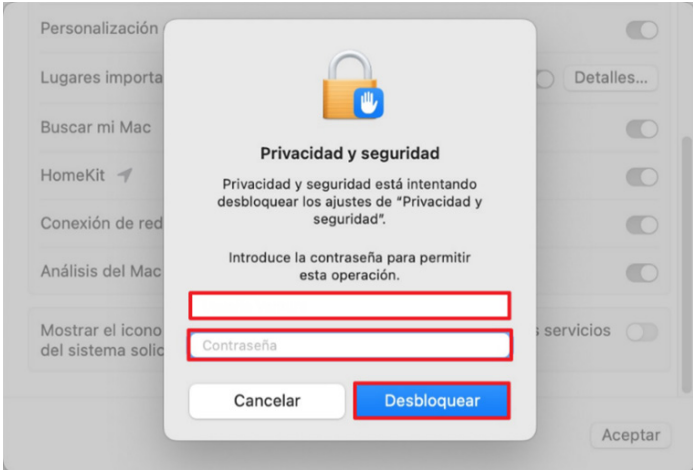
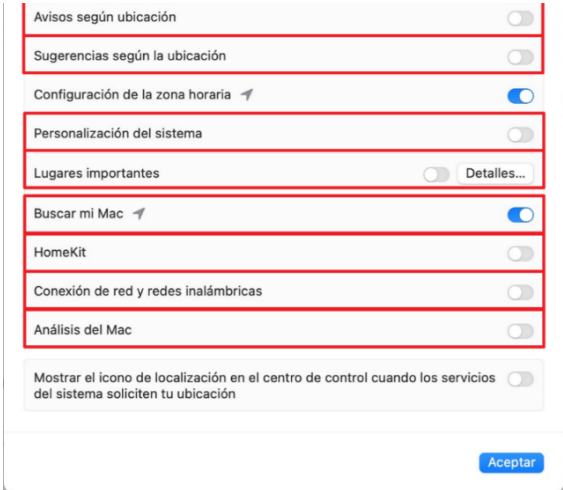
Las configuraciones de localización permiten a los usuarios controlar el acceso de las aplicaciones y servicios a su ubicación geográfica. Esta función es esencial para proteger la privacidad y garantizar que solo las aplicaciones autorizadas tengan acceso a la información de ubicación.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "Privacidad y seguridad" . 

4. Ajustes del sistema

Paso	Descripción
4.	Posteriormente, haga clic sobre “Localización”. 
5.	En la ventana “Localización”, verifique que la localización para “Siri y Dictado” se encuentra desactivado.  Nota: La localización para “Siri y Dictado” se encuentra desactivada por defecto.
6.	A continuación, en la ventana “Localización” haga clic sobre el botón “Detalles...”. 

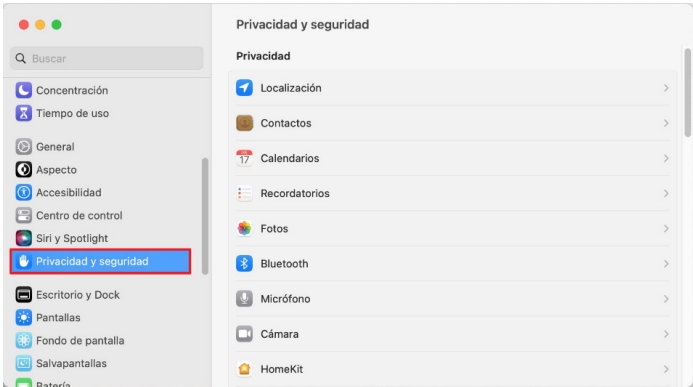
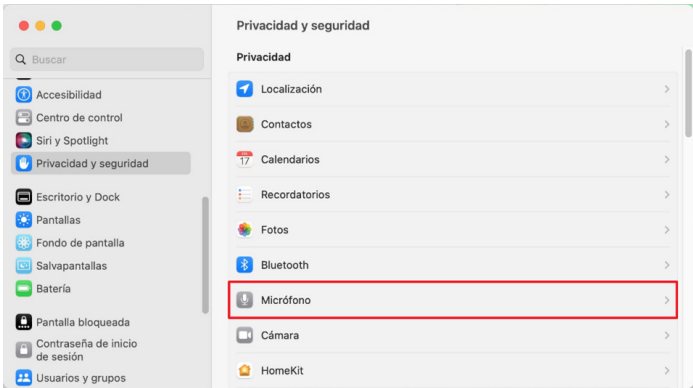
4. Ajustes del sistema

Paso	Descripción
7.	A continuación, se solicitará elevación de privilegios. Introduzca el nombre de usuario y la contraseña en los cuadros de texto correspondiente y haga clic en “Desbloquear”. 
8.	En la ventana “Los servicios del sistema pueden acceder a tu ubicación para:”, modifique las siguientes configuraciones tal y como se muestra a continuación: Avisos según ubicación: Desactivado. ◆ Sugerencia según la ubicación: Desactivado. ◆ Personalización del sistema: Desactivado. ◆ Lugares importantes: Desactivado. ◆ Buscar mi Mac: Activado. ◆ HomeKit: Desactivado. ◆ Conexión de red y redes inalámbricas: Desactivado. ◆ Análisis del Mac: Desactivado.  Nota: Si alguna de las configuraciones se desea mantener habilitada, se recomienda valorar cada configuración en particular y valorar si es necesario mantenerla(s) activada(s).
9.	Pulse “Aceptar” para finalizar.

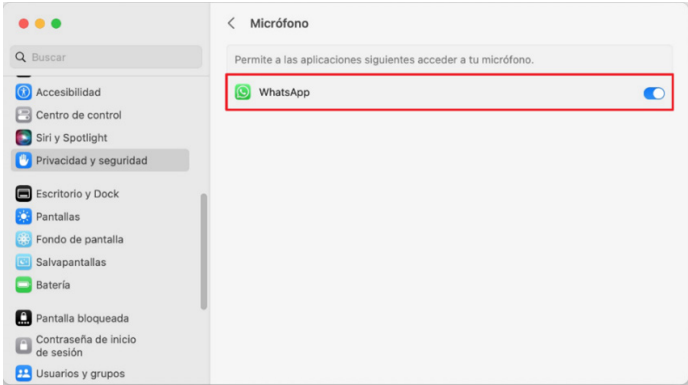
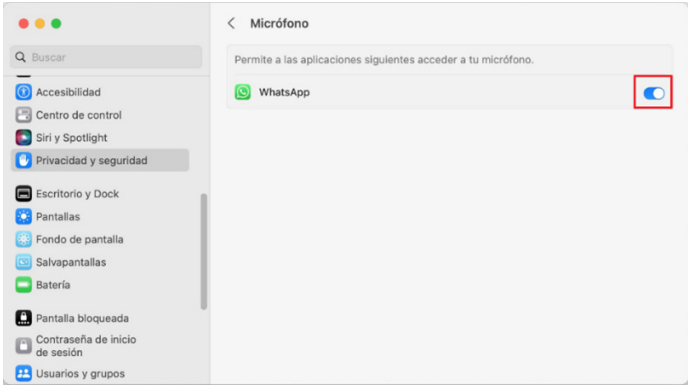
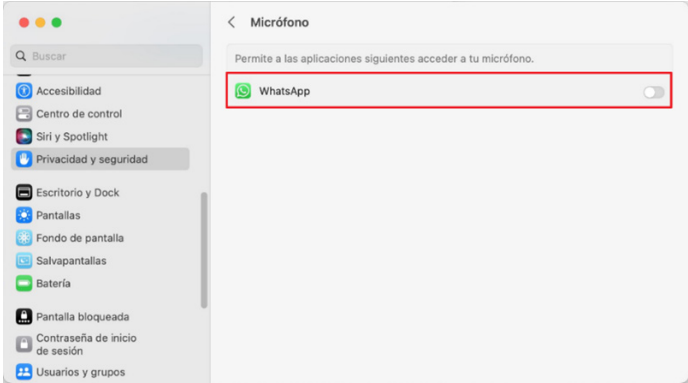
4. Ajustes del sistema

4.6.1.2. Otras configuraciones de privacidad

El apartado de privacidad en macOS, se enfocará en revisar y gestionar los permisos a los que acceden las diferentes aplicaciones. Esto implica controlar qué aplicaciones tienen acceso a datos sensibles, como la cámara, el micrófono y otros recursos del sistema, con el objetivo de proteger la privacidad y la seguridad de los usuarios.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "Privacidad y seguridad" . 
4.	En la ventana "Privacidad y Seguridad" en la sección de "Privacidad" , seleccione "Micrófono" . 

4. Ajustes del sistema

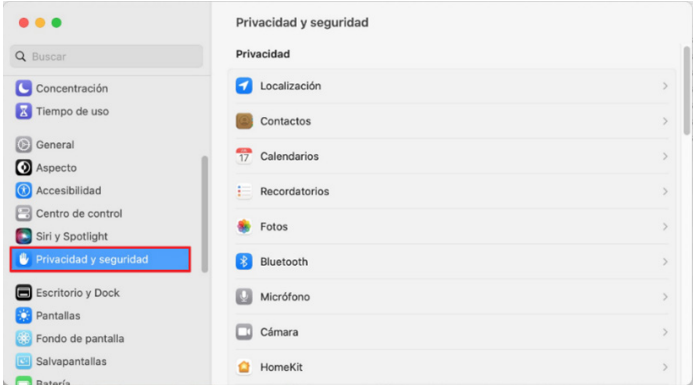
Paso	Descripción
5.	En la ventana "Micrófono", podrá comprobar las aplicaciones que tienen permiso para acceder y utilizar el micrófono.  Nota: En este ejemplo se ha hecho uso de una aplicación de mensajería instantánea para mostrar la configuración a aplicar.
6.	Identifique y desactive todas aquellas aplicaciones que no requieran de acceso al micrófono haciendo clic sobre el botón correspondiente.  Nota: Para este ejemplo se ha hecho uso de la aplicación WhatsApp.
7.	En este punto la configuración de las aplicaciones para que puedan acceder al micrófono estará desactivada. 

4. Ajustes del sistema

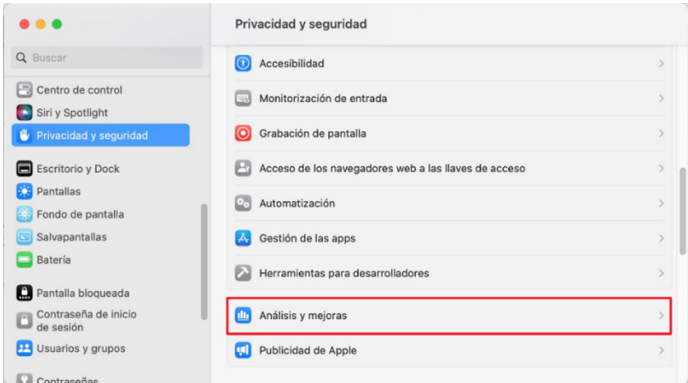
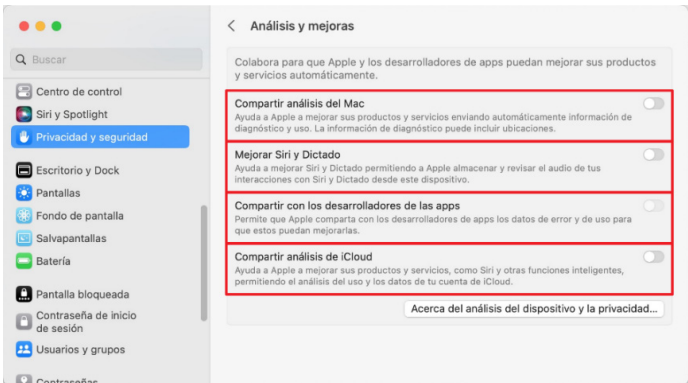
Paso	Descripción
8.	Ejecute los mismos pasos para el resto de los recursos de privacidad existentes: ◆ Contactos. ◆ Calendarios. ◆ Recordatorios. ◆ Fotos. ◆ Bluetooth. ◆ Cámara. ◆ HomeKit. ◆ Reconocimiento de voz. ◆ Multimedia y Apple Music. ◆ Archivos y carpetas. ◆ Acceso total al disco. Si alguna de las configuraciones está habilitada, se recomienda valorar cada configuración en particular y valorar si es necesario mantenerla(s) activada(s) por cada aplicación.

4.6.1.3. Análisis y mejoras

En este apartado se definen las configuraciones que limitan la información que el sistema operativo macOS comparte con Apple a través de diferentes informes de productos y servicios.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "Privacidad y seguridad". 

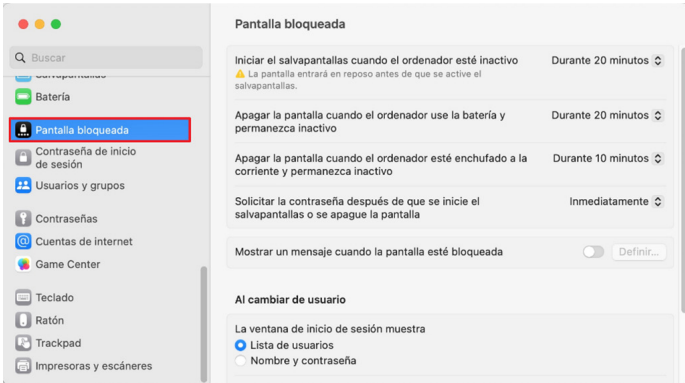
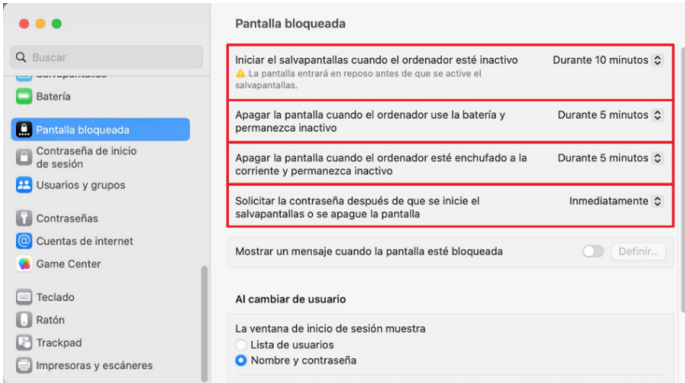
4. Ajustes del sistema

Paso	Descripción
4.	En “Privacidad y seguridad”, navegue y seleccione “Análisis y mejoras”. 
5.	En la ventana “Análisis y mejoras” modifique las siguientes configuraciones tal y como se muestra a continuación: ◆ Compartir análisis del Mac: Desactivado. ◆ Mejorar Siri y Dictado: Desactivado. ◆ Compartir con los desarrolladores de las apps: Desactivado. ◆ Compartir análisis de iCloud: Desactivado. 

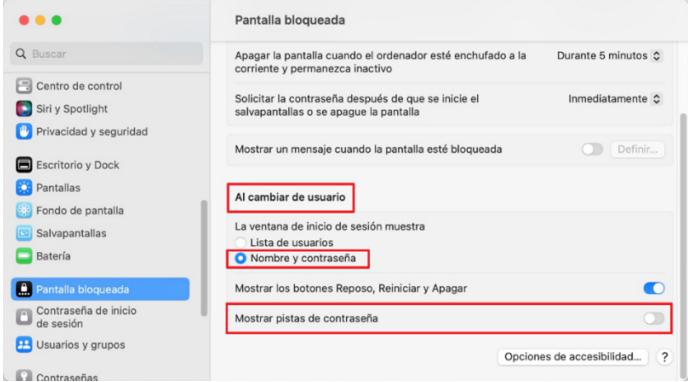
4.7. Pantalla bloqueada

La función de pantalla de bloqueo en macOS Ventura permite a los usuarios proteger su Mac de accesos no autorizados. Pueden configurar el inicio automático del salvapantallas y establecer contraseñas para desbloquear el sistema, garantizando así la privacidad y la seguridad de su dispositivo cuando este no se encuentra en uso.

4. Ajustes del sistema

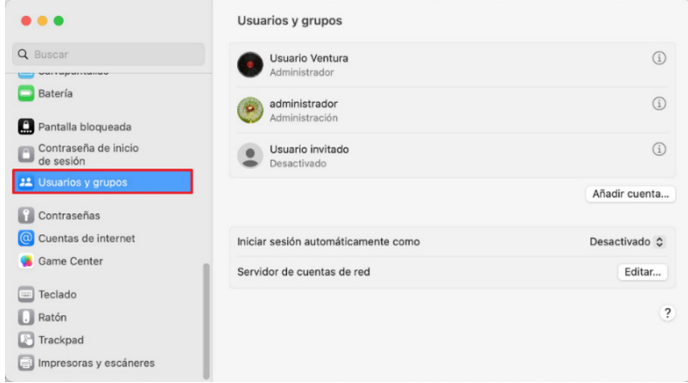
Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Pantalla bloqueada” . 
4.	En la ventana “Pantalla bloqueada”, realice los siguientes cambios tal y como se muestra a continuación: ◆ Iniciar el salvapantallas cuando el ordenador esté inactivo: Durante 10 minutos. ◆ Apagar la pantalla cuando el ordenador use la batería y permanezca inactivo: Durante 5 minutos. ◆ Apagar la pantalla cuando el ordenador esté enchufado a la corriente y permanezca inactivo: Durante 5 minutos. ◆ Solicitar la contraseña después de que se inicie el salvapantallas o se apague la pantalla: Inmediatamente.  Nota: En los equipos de escritorio con macOS Ventura, la configuración “Apagar la pantalla cuando el ordenador use la batería y permanezca inactivo” no se aplicará, ya que estos dispositivos no utilizan batería. Por otro lado, ajuste estos parámetros a sus necesidades, pero estableciendo siempre un tiempo prudencial.

4. Ajustes del sistema

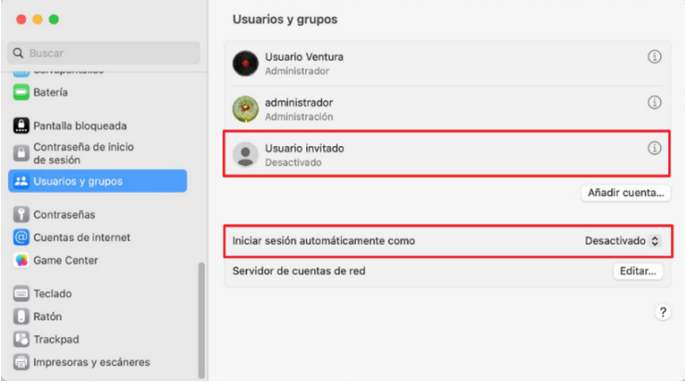
Paso	Descripción
5.	En la misma ventana de “Pantalla de bloqueo”, realice los siguientes cambios en la sección “Al cambiar de usuario”: ◆ La ventana de inicio de sesión muestra: Nombre y contraseña. ◆ Mostrar pista de contraseña: Desactivado. 

4.8. Usuarios y grupos

La sección de “Usuarios y Grupos” en macOS Ventura permite a los usuarios gestionar cuentas y configurar preferencias de inicio de sesión.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Usuarios y grupos”. 

4. Ajustes del sistema

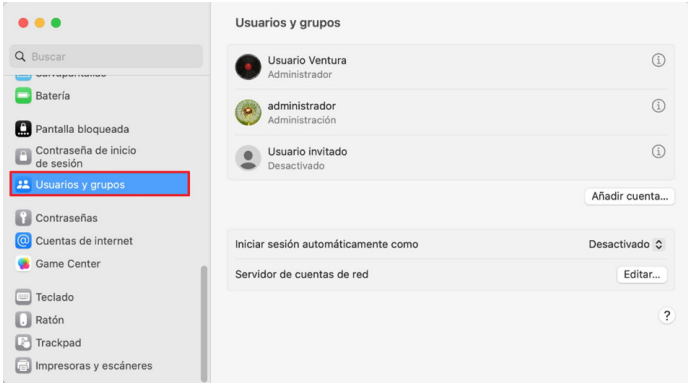
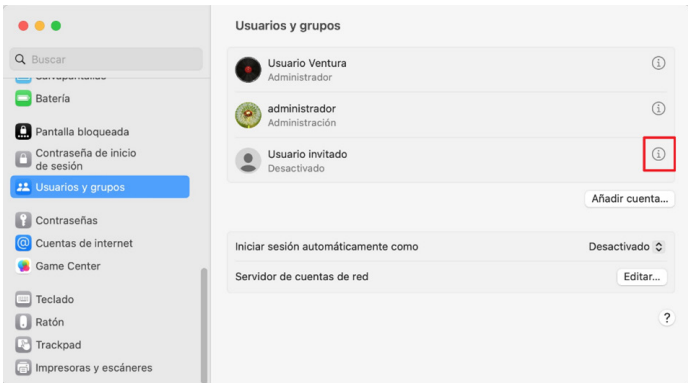
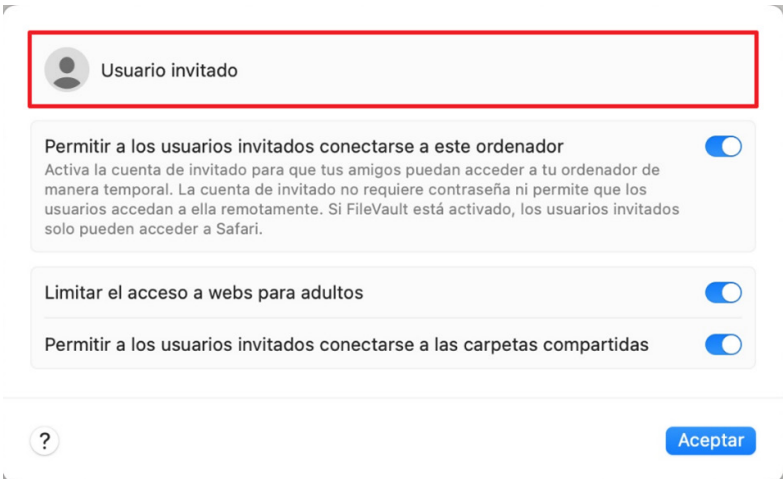
Paso	Descripción
4.	En la ventana “Usuarios y grupos”, compruebe que las siguientes opciones están configuradas tal y como se muestra a continuación: ◆ Usuario invitado: Desactivado. ◆ Iniciar sesión automática como: Desactivado.  Nota: Si algunas de las configuraciones anteriores se encuentran diferente a como se ha indicado, siga los pasos de las siguientes secciones según se requiera: - 4.8.1 Deshabilitar usuario invitado - 4.8.2 Desactivar iniciar sesión automáticamente

4.8.1. Deshabilitar usuario invitado

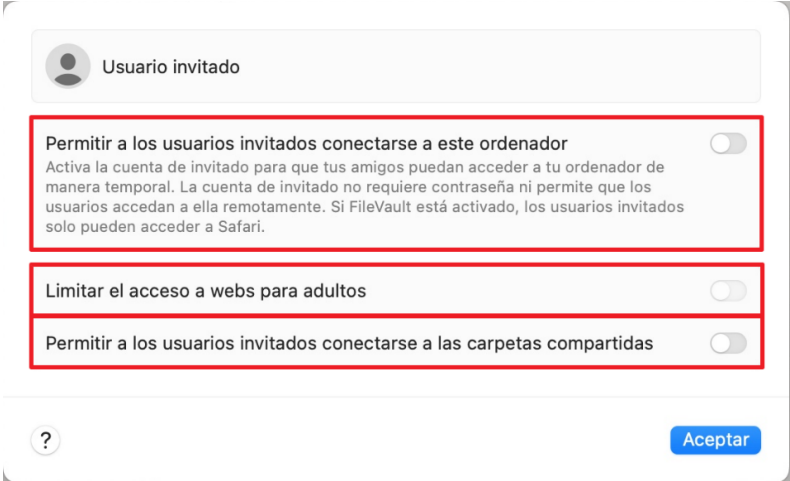
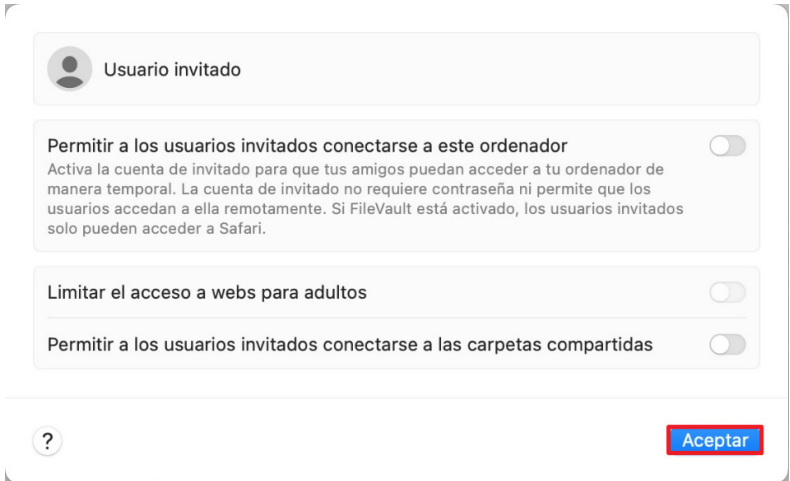
El “Usuario Invitado” es una cuenta especial en macOS Ventura que permite a los usuarios acceder temporalmente a un Mac sin necesidad de una cuenta de usuario principal. Sin embargo, por motivos de seguridad, se procederá a deshabilitar esta opción en este proceso de configuración.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 

4. Ajustes del sistema

Paso	Descripción
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Usuarios y grupos”.  A screenshot of the macOS System Settings application. The left sidebar contains various settings categories, and 'Usuarios y grupos' (Users and Groups) is highlighted with a red rectangle. The main pane on the right shows the 'Usuarios y grupos' settings, including a list of users: 'Usuario Ventura' (Administrator), 'administrador' (Administration), and 'Usuario invitado' (Deactivated). Below the list are options for automatic login and network account server.
4.	En la ventana “Usuarios y grupos”, haga clic sobre el icono de información ubicado al lado derecho de la cuenta “Usuario invitado”.  A screenshot of the macOS System Settings application, specifically the 'Usuarios y grupos' pane. The 'Usuario invitado' (Deactivated) user entry is selected, and the information icon (a circle with an 'i') to its right is highlighted with a red rectangle.
5.	En la ventana que se muestra a continuación, se encuentran las diferentes configuraciones para la cuenta de invitado.  A screenshot of the 'Usuario invitado' (Guest User) configuration window. The window title bar shows 'Usuario invitado' with a red rectangle around it. Below the title bar are three toggle switches, all of which are turned on: 'Permitir a los usuarios invitados conectarse a este ordenador' (Allow guest users to connect to this computer), 'Limitar el acceso a webs para adultos' (Limit access to adult websites), and 'Permitir a los usuarios invitados conectarse a las carpetas compartidas' (Allow guest users to connect to shared folders). At the bottom right is an 'Aceptar' (Accept) button.

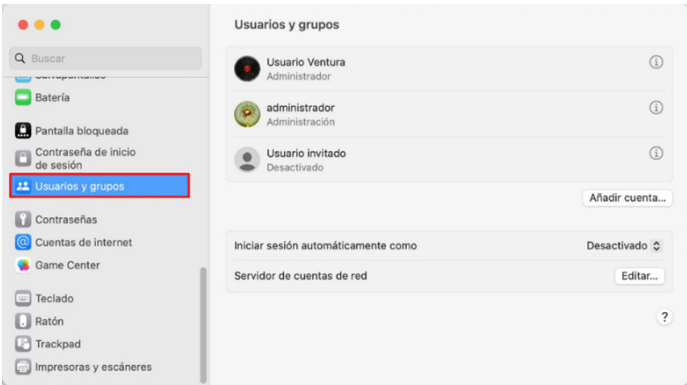
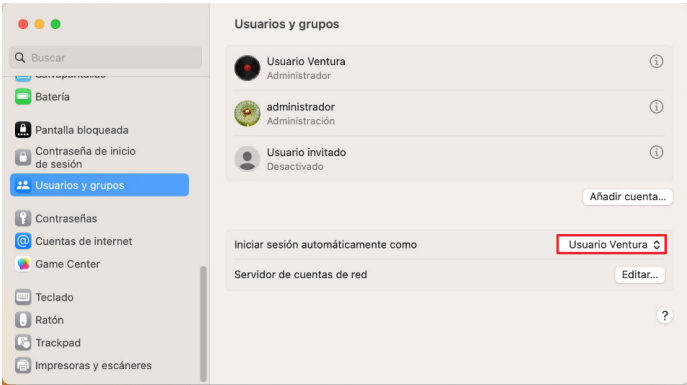
4. Ajustes del sistema

Paso	Descripción
6.	Para deshabilitar el "Usuario invitado", realice las siguientes modificaciones tal y como se muestra a continuación: ◆ Permitir a los usuarios invitados conectarse a este ordenador: Desactivado. ◆ Limitar el acceso a webs para adultos: Desactivado. ◆ Permitir a los usuarios invitados conectarse a las carpetas compartidas: Desactivado.  Nota: La opción "Limitar el acceso a webs para adultos" deberá definirse como activada cuando se permita el uso de un usuario invitado, pero se desee impedir el acceso a sitios web no deseados.
7.	Una vez que ha realizado los cambios, haga clic sobre el botón Aceptar. 

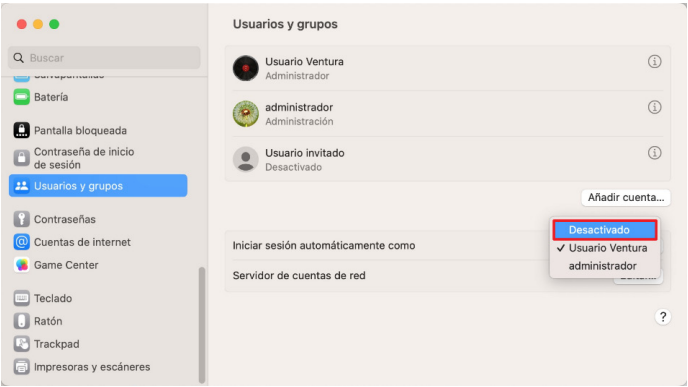
4. Ajustes del sistema

4.8.2. Desactivar iniciar sesión automáticamente

Con el fin de evitar que cualquier persona ingrese al dispositivo Mac se recomienda desactivar las configuraciones que permiten el inicio de sesión automáticamente.

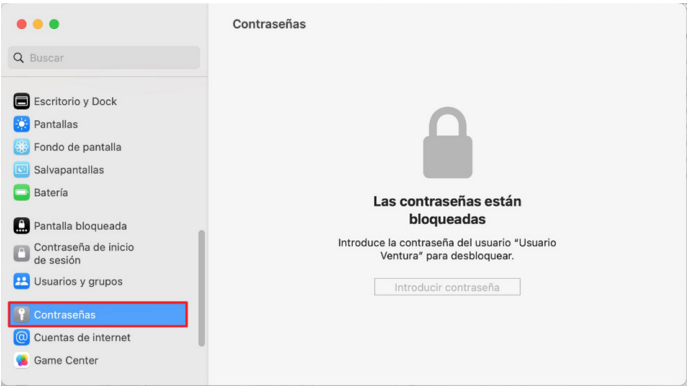
Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los “Ajustes del sistema” que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione “Usuarios y grupos” . 
4.	En la ventana “Usuarios y grupos” , en la parte derecha de la opción “Iniciar sesión automáticamente como” , haga clic sobre el usuario que se encuentra configurado. 

4. Ajustes del sistema

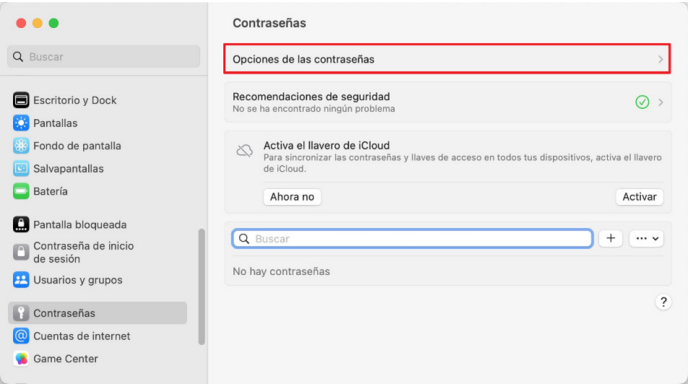
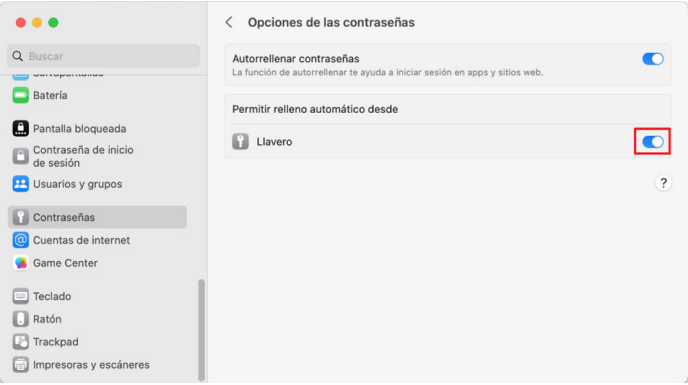
Paso	Descripción
5.	En la ventana de selección desplegada, seleccione "Desactivado". 

4.9. Contraseñas

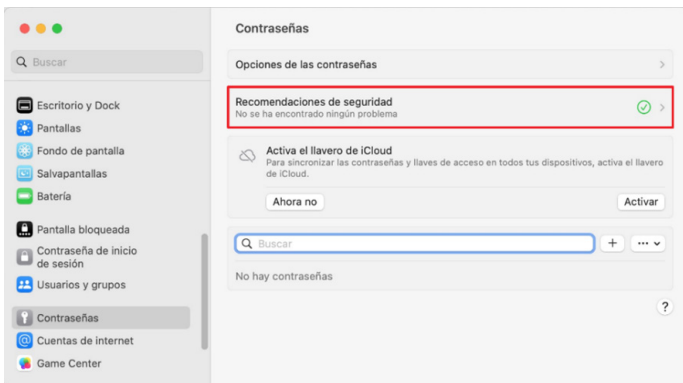
En este apartado se activarán las recomendaciones de seguridad para las contraseñas del sistema.

Paso	Descripción
1.	Inicie sesión con su usuario y contraseña en el equipo macOS.
2.	Una vez en el escritorio del sistema operativo, inicie los "Ajustes del sistema" que se encuentra en el Dock (En la parte inferior de la pantalla, el icono del engranaje). 
3.	En la ventana de ajustes del sistema, navegue en el menú izquierdo y seleccione "Contraseñas". 

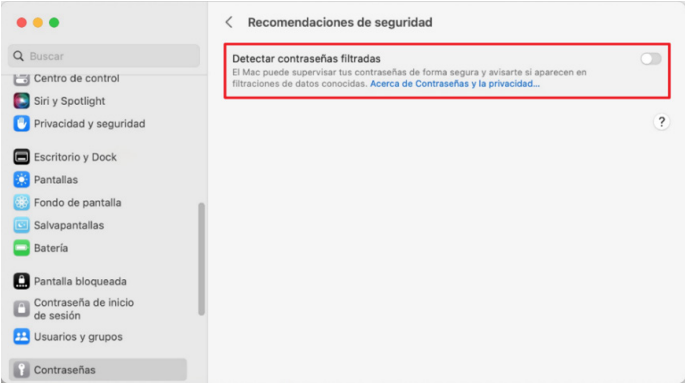
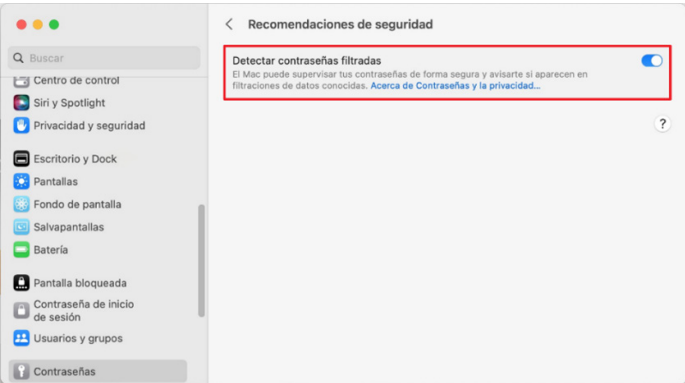
4. Ajustes del sistema

Paso	Descripción
4.	En la ventana “Contraseñas”, introduzca la contraseña de su usuario para poder acceder a la configuración. 
5.	En la ventana “Contraseñas” haga clic sobre “Opciones de las contraseñas”. 
6.	En la ventana “Opciones de Contraseñas” haga clic sobre el botón para desactivar el “Llavero”. 

4. Ajustes del sistema

Paso	Descripción
7.	Posteriormente en la misma ventana, desactive la opción "Autorrellenar Contraseñas" tal y como se muestra en la imagen. 
8.	Haga clic sobre "<" para volver a la ventana "Contraseñas". 
9.	En las opciones que aparecen, haga clic sobre "Recomendaciones de seguridad". 

4. Ajustes del sistema

Paso	Descripción
10.	Identifique la configuración “Detectar contraseñas filtradas”. MacOS Ventura permite al sistema analizar y alertar al usuario si alguna de las contraseñas se encuentra en listas expuestas o que han sido filtradas.  The screenshot shows the macOS Ventura System Settings app. On the left is a sidebar with various settings categories. The 'Contraseñas' (Passwords) category is selected at the bottom. The main pane on the right is titled 'Recomendaciones de seguridad' (Security Recommendations). Within this pane, the 'Detectar contraseñas filtradas' (Detect filtered passwords) option is highlighted with a red rectangle. The toggle switch for this option is currently turned off.
11.	Active la configuración “Detectar contraseña filtradas”, tal y como se muestra en la siguiente imagen.  This screenshot is identical to the one in step 10, but the toggle switch for 'Detectar contraseñas filtradas' is now turned on, as indicated by the blue position of the switch and the red rectangle highlighting it.

5. Lista de comprobación

Criticidad	Descripción
Alta	El equipo macOS, debe disponer de un sistema operativo en soporte y las aplicaciones de actualizados, incluyendo en todo momento las actualizaciones de seguridad. Nota: Puede consultar las versiones de macOS a través del siguiente enlace: https://support.apple.com/es-es/HT201260
Alta	Se dispone de un control de acceso para los usuarios que inician sesión en el sistema macOS a través de usuarios diferenciados y con los privilegios estrictamente necesarios.
Alta	El firewall del equipo macOS está activado para proteger las conexiones entrantes.
Alta	Las conexiones a Internet a través de Wi-Fi se realizan a través de puntos de acceso seguros que estén protegidos con una contraseña segura y cifrados.
Alta	El inicio de sesión automático en macOS esta deshabilitado.
Alta	Desactivar la sincronización del equipo con las diferentes aplicaciones de iCloud.
Alta	Comprobación y desactivación de las aplicaciones a las funciones o recursos del equipo.
Alta	Desactivar el uso de Autorellenado de contraseñas y llavero de iCloud.
Media	Las notificaciones del sistema están desactivadas para el bloqueo de pantalla.
Media	El modo encubierto está activado con el fin de ocultar la respuesta a escaneos de puertos y evitando que las solicitudes no deseadas sean visibles.
Media	El equipo está activado para "Buscar mi Mac". Permitiendo un borrado o bloqueo del mismo en remoto.
Media	Asegúrese de que el equipo no dispone de elementos compartidos en la red que no sean necesarios (carpetas, archivos, etc.).

5. Lista de comprobación

Criticidad	Descripción
Media	El equipo dispone de un tiempo para el bloqueo de pantalla automático por inactividad del mismo.
Media	El equipo solicita la conexión a una red Wi-Fi segura conocida y no se conecta de forma automática.
Media	El equipo solicita la conexión a puntos de acceso cercanos cuando no exista uno conocido y no se conecta de forma automática.
Media	Es necesario la introducción de usuario y para volver a iniciar sesión después de que el equipo se haya bloqueado.
Baja	Evitar el envío de informes y análisis sobre el equipo y usuario.
Baja	Se ha limitado la reproducción o continuación de las actividades del usuario en otro dispositivo.

6. Decálogo de recomendaciones

A continuación, se indican diez recomendaciones de seguridad en Sistemas Operativos macOS



Decálogo de recomendaciones para Sistemas Operativos macOS

- 1 Mantener el sistema **operativo** y las **aplicaciones actualizadas** para recibir **parches de seguridad** y **nuevas características**.
- 2 Si se necesita **instalar complementos**, se recomienda la utilización de la **App Store**, **fuentes oficiales y/o confiables**.
- 3 Se aconseja **no usar el almacén de contraseñas disponible en macOS**. En su lugar se recomienda el uso de **otras aplicaciones** que **implementen un sistema de cifrado robusto** para guardar las contraseñas de forma **más segura**.
- 4 Uso del **dobles factor de autenticación** para el uso de servicios online. Esto añade una **capa adicional de seguridad a las cuentas** debido a que será necesario una **verificación adicional en el inicio de sesión** (SMS, llamada telefónica, autenticadores, código de verificación, etc.).
- 5 Realizar **copias de seguridad periódicas de los datos de relevancia** en unidades externas o servicios en la nube.
- 6 Tener especial **precaución** al hacer clic en **enlaces y archivos adjuntos** en correos electrónicos para evitar el **phishing**.
- 7 Habilitar **FileVault u otra solución** para **cifrar el disco duro y proteger los datos en caso de pérdida o robo del dispositivo**.
- 8 **Conectarse solo a redes Wi-Fi seguras** y evitar redes abiertas o no verificadas.
- 9 **Configurar el bloqueo de pantalla y notificaciones** para limitar el acceso al contenido sobre el equipo.
- 10 Habilitar **el firewall de macOS** para **proteger la conexión a Internet** e implementar un **software antivirus ante ataques de malware**, entre otros.

Anexo A.

Recomendaciones adicionales

A.1. Contraseñas

Una contraseña segura es esencial para proteger las cuentas y datos en línea. Asegúrese de crear contraseñas únicas y complejas que combinen letras, números y caracteres especiales. Evitar información personal obvia, como nombres o fechas de nacimiento, y considerar el uso de frases o acrónimos memorables es crucial. De igual modo mantener las contraseñas actualizadas y no compartirlas en múltiples cuentas o servicios es esencial para garantizar la máxima seguridad en línea.

Las contraseñas seguras son una pieza fundamental en la protección de los datos en un mundo cada vez más digital. Son la primera línea de defensa contra posibles amenazas cibernéticas y el acceso no autorizado a cuentas y la información personal.

A.2. Antivirus

A pesar de la reputación de seguridad de macOS, utilizar un antivirus en dispositivos Mac es esencial debido a las amenazas cibernéticas en constante evolución. Los antivirus ofrecen una serie de beneficios clave como los siguientes:



Protección contra malware actualizado para detectar y eliminar amenazas.



Detección proactiva de comportamientos sospechosos, crucial para prevenir ataques de día cero.

Anexo A. Recomendaciones adicionales



Módulos de seguridad de navegación web para evitar sitios maliciosos y el phishing.



Salvaguardar datos personales contra robos y brechas de privacidad.



Mantenimiento del rendimiento del sistema sin ralentizarlo significativamente.



Prevención de la propagación de malware a otros dispositivos en la red.

En resumen, un antivirus en macOS brinda una capa adicional de seguridad para proteger la privacidad, datos y rendimiento del sistema, pero debe complementarse con prácticas sólidas de seguridad y la concienciación en línea, ya que ningún antivirus es infalible.

A.3. Time machine y copia de seguridad

Time Machine, una herramienta de copia de seguridad de macOS, es esencial para la integridad y recuperación de datos. Esta ofrece simplicidad y comodidad con copias automáticas, historial de versiones, recuperación ante desastres, protección de todo el sistema y opciones de almacenamiento flexibles. Aunque existen alternativas en el mercado, la elección depende de las necesidades y preferencias de cada usuario y/u organización.

A.4. Cifrado de disco y Filevault

El cifrado de disco, como FileVault en macOS, es esencial para proteger los datos de accesos no autorizados en caso de pérdida o robo del dispositivo Mac, así como utilizar una contraseña de usuario o una clave de recuperación para acceder a los datos cifrados. Es de suma importancia guardar la clave de recuperación en un lugar seguro.

Activar FileVault es una medida sencilla y efectiva para mejorar la seguridad y privacidad de tus datos. Es importante tener en cuenta que existen otras alternativas en el mercado para cifrar los datos, y la elección de la herramienta adecuada dependerá de las necesidades individuales de cada usuario y/o de la organización.



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es