CCN-CERT

BP/32

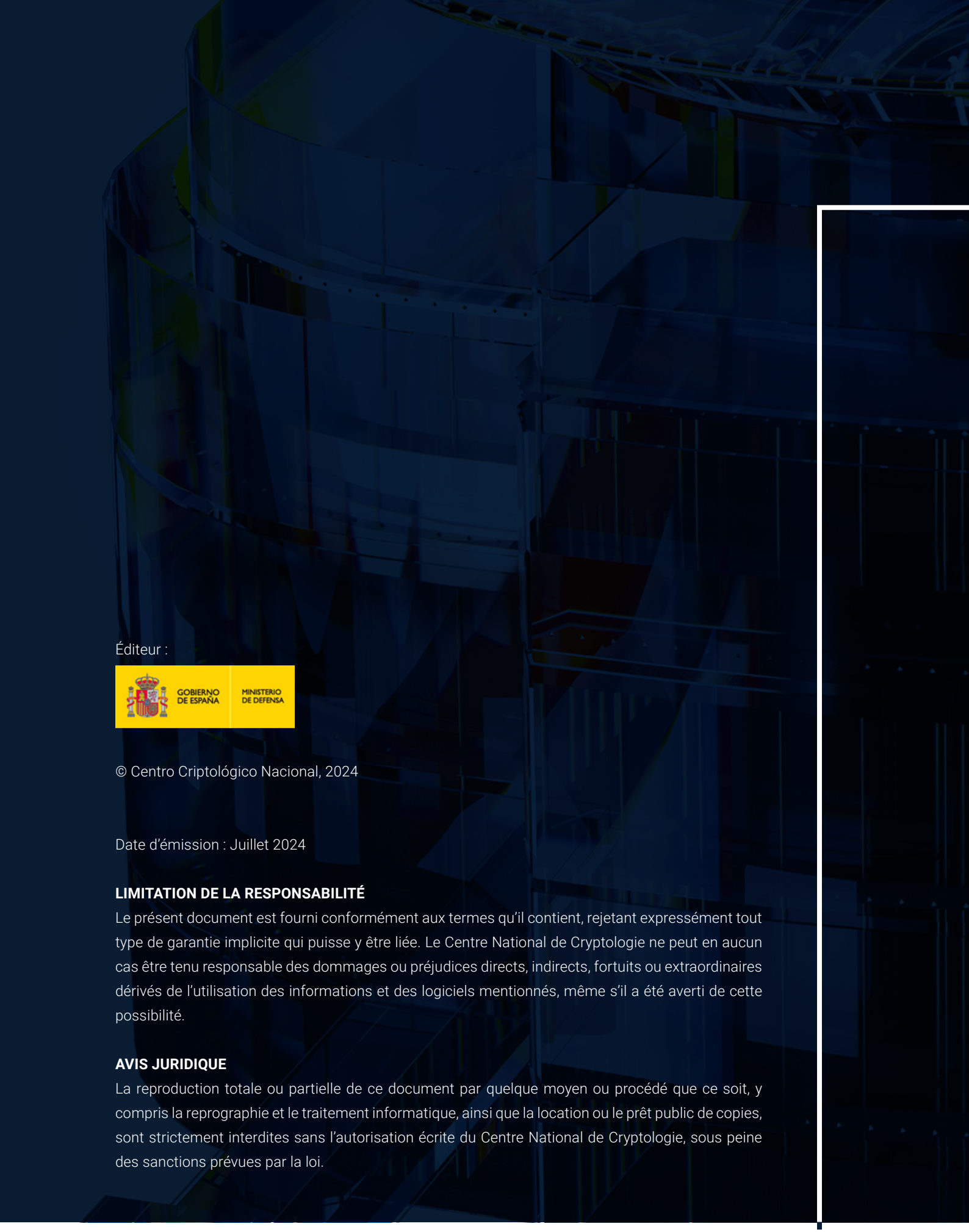
Recommandations de Sécurité pour le Système d'Exploitation MacOS

RAPPORT DE BONNES PRATIQUES

AVRIL 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional



Éditeur :

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Date d'émission : Juillet 2024

Index

1. Introduction

Ce guide a été conçu pour tirer le meilleur parti des ordinateurs macOS en fournissant les outils et les connaissances nécessaires pour protéger les données et assurer la data privacy. Dans ce but, nous allons explorer les paramètres de sécurité basiques que tous les utilisateurs de macOS devraient prendre en compte pour protéger leurs informations contre les menaces potentielles.

L'utilisation du système macOS présente de nombreux avantages : système d'exploitation intuitif, stabilité, optimisation matérielle et logicielle, etc. Toutefois, ces avantages ne doivent pas faire oublier l'importance de la confidentialité des données. Dans le monde numérique d'aujourd'hui, les informations personnelles, qu'il s'agisse de photos, de documents, de mots de passe ou de données financières, sont constamment menacées.

Une perte de données ou un accès non autorisé à ces informations peut entraîner des conséquences importantes. Ce guide fournit les lignes directrices pour protéger les données personnelles, naviguer en toute sécurité sur Internet et éviter les menaces courantes telles que les logiciels malveillants et l'hameçonnage.

2. Objet et portée

L'objectif de ce guide est de fournir aux utilisateurs de macOS un ensemble complet d'instructions et de recommandations pour établir et optimiser les paramètres de sécurité basiques sur leurs appareils, en effectuant les réglages les plus pertinents afin de garantir une plus grande sécurité aussi bien pour l'appareil que pour l'utilisateur.

Vous pourrez suivre les instructions de base à travers les différents menus Réglages disponibles dans le système d'exploitation, sans qu'il soit nécessaire d'exécuter des commandes, qu'elles soient simples ou complexes. De cette manière, les réglages seront accessibles à tout type d'utilisateur, quelles que soient ses connaissances technologiques.

Il est important de souligner que ces paramètres peuvent varier dans d'autres versions du système d'exploitation et que ce guide s'adresse aux utilisateurs iCloud qui possèdent un identifiant Apple. Par conséquent, les utilisateurs devront adapter chacune des étapes aux changements éventuels qui puissent exister, à la fois dans les versions antérieures et ultérieures du système d'exploitation, et en tenant compte de leur configuration iCloud spécifique.

3. Le système d'exploitation macOS

Les pages suivantes contiennent des informations qui vous guideront tout au long du processus de configuration des Réglages Système pour renforcer la sécurité de votre macOS. Chaque aspect sera expliqué de manière claire et concise, en fournissant les lignes directrices nécessaires pour protéger vos données et vos informations personnelles. Au fur et à mesure de cette progression, vous découvrirez que la sécurisation de votre système est plus simple qu'il n'y paraît.

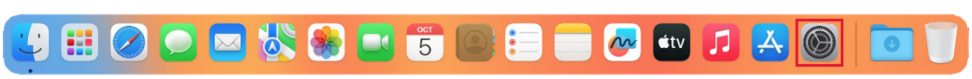
Le guide suit un parcours détaillé à travers les **"Réglages Système"** de macOS dans son édition **Ventura**. Vous pourrez suivre chaque étape en allant dans les Réglages du système, ce qui vous permettra d'aborder les paramètres de sécurité d'une manière simple.

4. Les réglages du système

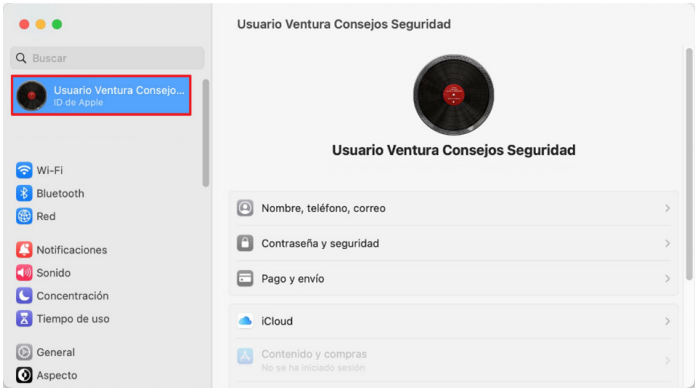
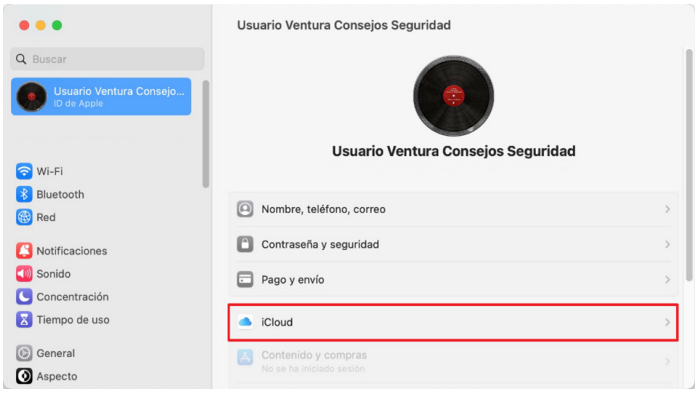
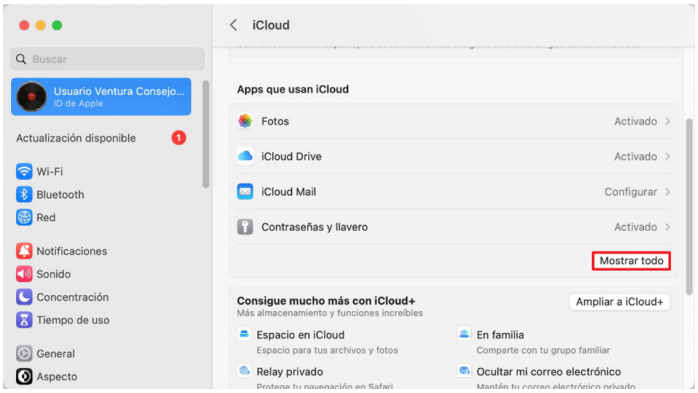
Les "Réglages du système" de macOS Ventura constituent le centre de contrôle qui permet aux utilisateurs de personnaliser et de configurer leur système d'exploitation macOS. À partir de cet élément, il est possible de définir les préférences liées à la sécurité, à la confidentialité, au réseau, à l'affichage, aux utilisateurs et plus encore. Ces réglages constituent la clé qui permet aux utilisateurs de personnaliser leur expérience utilisateur et d'assurer la sécurité de leurs appareils.

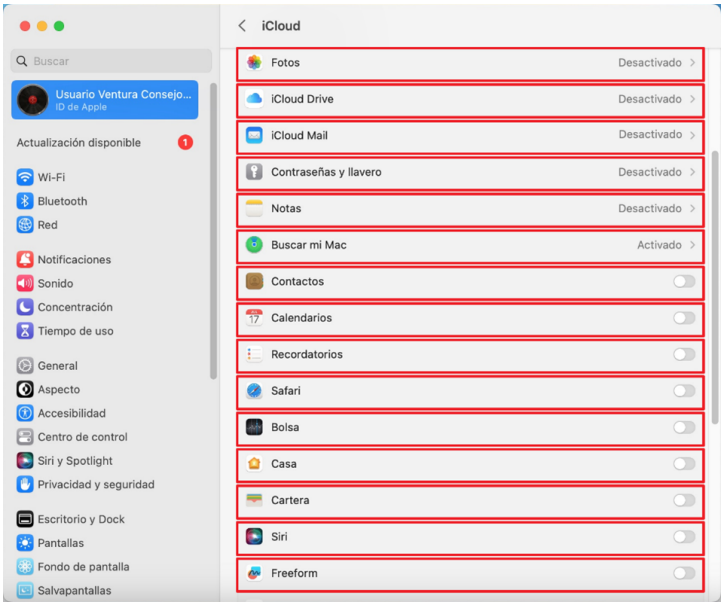
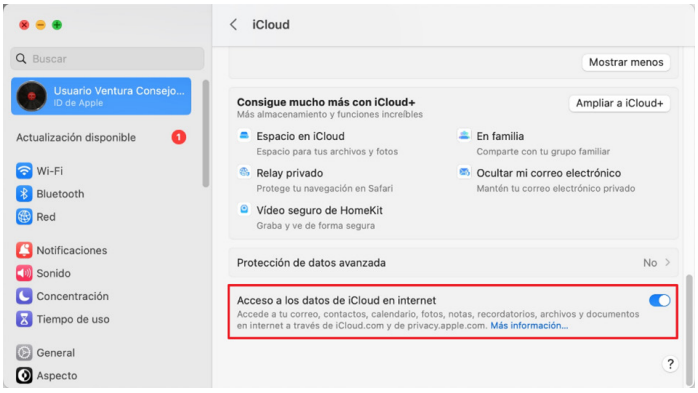
4.1. L'utilisateur iCloud

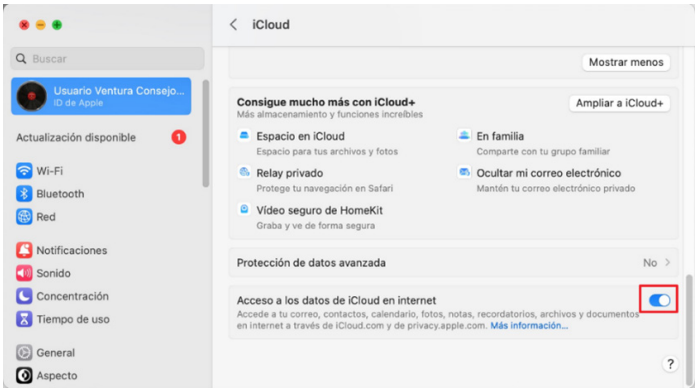
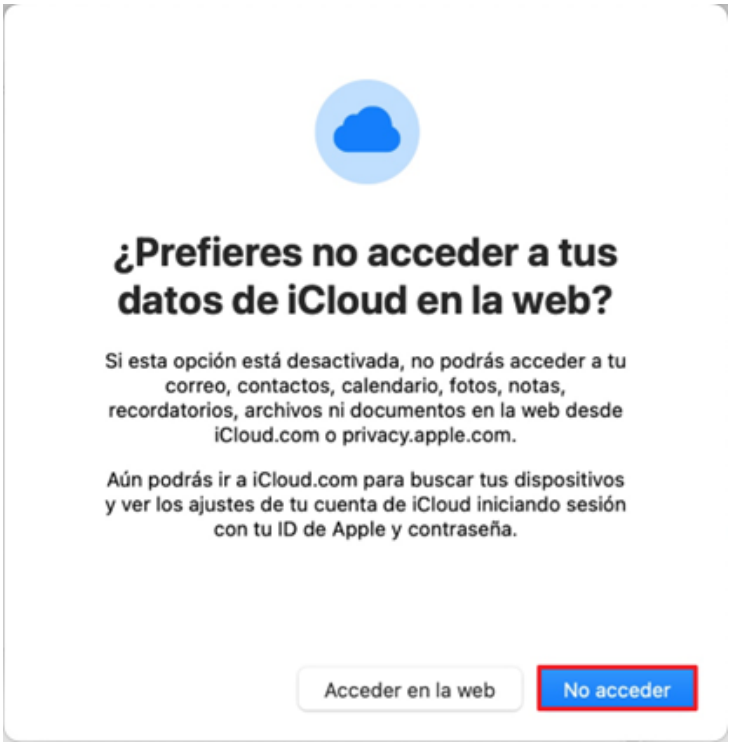
Les paramètres du compte iCloud permettent aux utilisateurs de personnaliser et de gérer la manière dont les données sont synchronisées et stockées dans le cloud d'Apple. Il s'agit notamment de la sauvegarde de données (photos, contacts, notes et autres) et du partage familial (localisation). Les préférences de stockage, les options de sécurité et l'accès aux services Apple tels que "Localiser mon Mac" peuvent également être configurés. Ces réglages permettent de mieux contrôler l'expérience et la vie privée de l'utilisateur dans l'écosystème Apple.

Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 

Remarque : Cet exemple d'utilisateur est représentatif et est utilisé à des fins d'illustration.

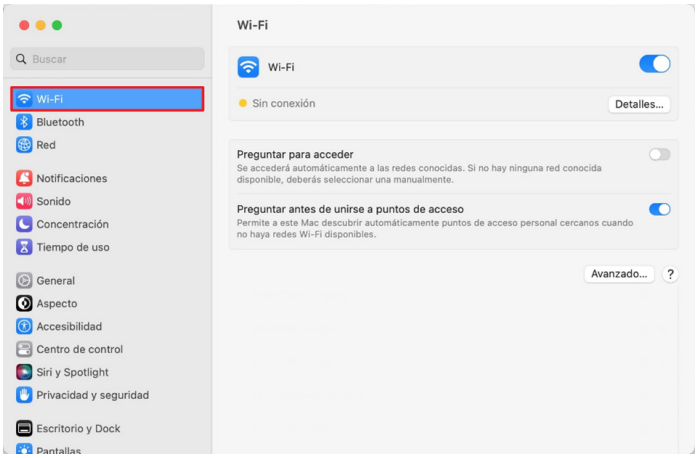
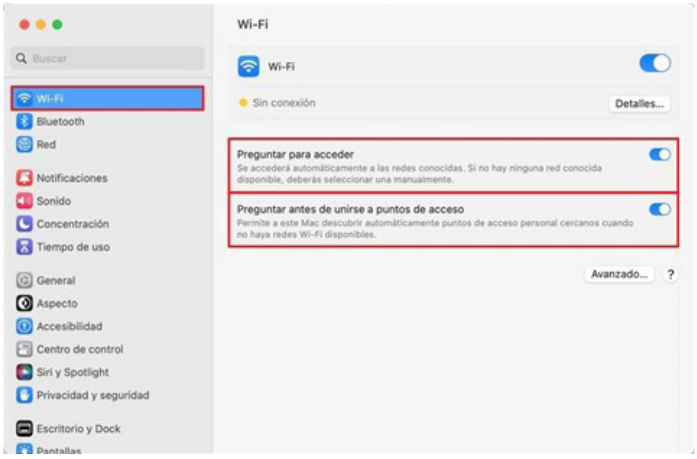
Étape	Description
3.	Cliquez sur [*votre nom*] en haut de la barre latérale (à gauche). 
4.	Cliquez sur **“iCloud”** à droite. 
5.	La fenêtre **“iCloud”** s’affiche. Faites défiler la page vers le bas et cliquez sur **“Tout afficher”.** 
6.	Modifiez les fonctionnalités suivantes comme indiqué ci-dessous : ◆ Photos : Désactivé. ◆ iCloud Drive : Désactivé. ◆ Mail iCloud : Désactivé. ◆ Mot de passe et trousseau : Désactivé. ◆ Notes : Désactivé. ◆ Localiser mon Mac : Activé.

Étape	Description
6.	◆ Contacts : Désactivé. ◆ Calendriers : Désactivé. ◆ Rappels : Désactivé. ◆ Safari : Désactivé. ◆ Bourse : Désactivé. ◆ Maison : Désactivé. ◆ Wallet : Désactivé. ◆ Siri : Désactivé. ◆ Freeform : Désactivé.  **Remarque : Si vous avez besoin d'utiliser l'une des fonctionnalités qui ont été désactivées auparavant, vous devrez examiner au cas par cas chaque fonctionnalité et décider ensuite si son activation est réellement nécessaire. Le document a été rédigé dans le but de limiter autant que possible l'utilisation des données sensibles par d'autres appareils synchronisés.**
7.	Faites défiler la page vers le bas pour trouver le curseur **"Accéder aux données iCloud sur le Web".** 

Étape	Description
8.	Cliquez sur le bouton **“Accéder aux données iCloud sur le Web”** pour désactiver l’option. 
9.	Une nouvelle fenêtre s’affiche. Cliquez sur **“Ne pas accéder”.** 

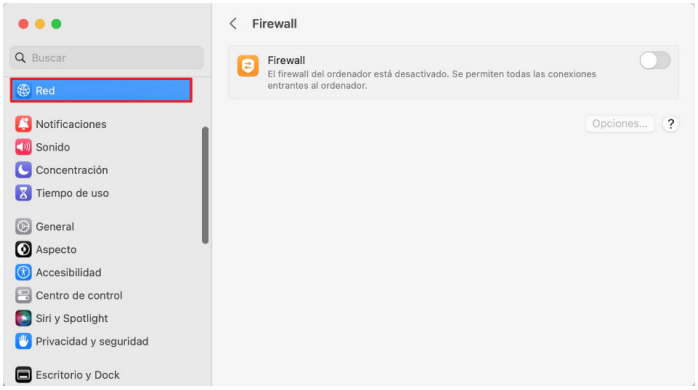
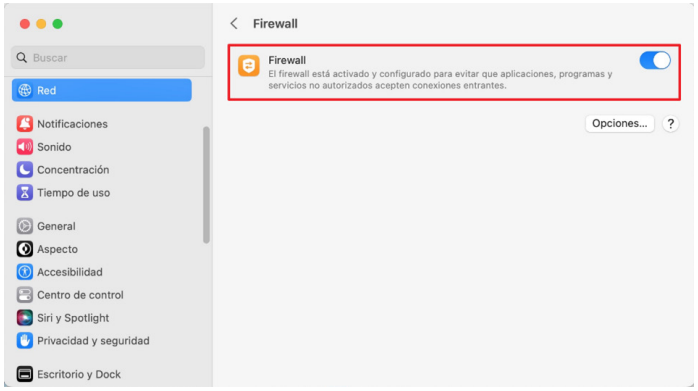
4.2. Wi-Fi

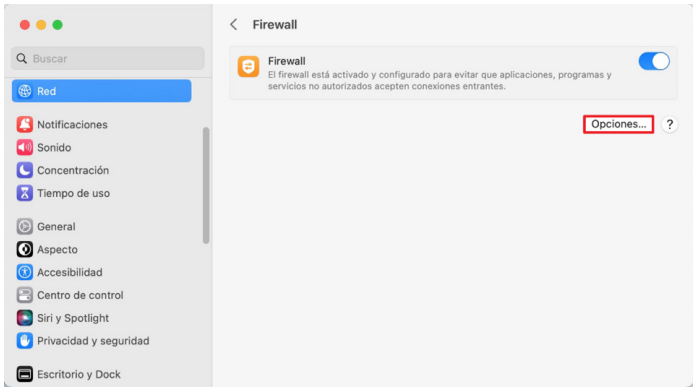
Les paramètres **Wi-Fi** de macOS Ventura permettent aux utilisateurs de se connecter en toute sécurité aux réseaux sans fil et de gérer leur accès.

Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Cliquez sur **"Wi-Fi"** dans la barre latérale (à gauche). Vous devrez peut-être faire défiler la page vers le bas. 
4.	Modifiez les fonctionnalités suivantes comme indiqué ci-dessous : ◆ Proposer des réseaux : Activé. ◆ Proposer des partages de connexion : Activé. 

4.3. Réseau

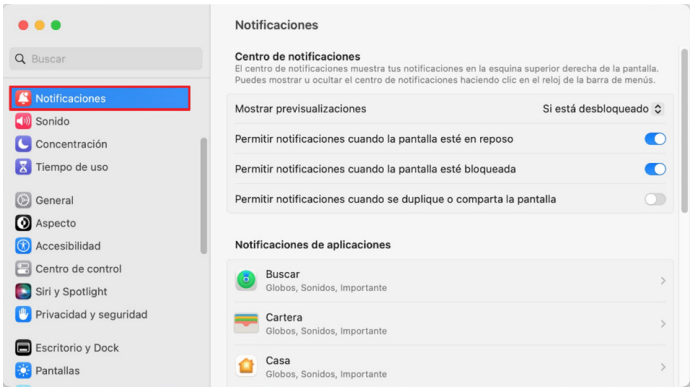
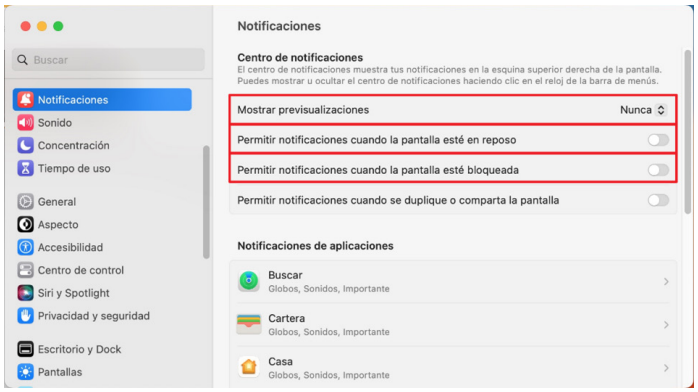
La section **“Réseau”** permet aux utilisateurs de gérer la connectivité et la sécurité des réseaux.

Étape	Description
1.	Connectez-vous avec votre nom d’utilisateur et votre mot de passe sur l’ordinateur macOS.
2.	Cliquez sur l’icône **“Réglages Système”** dans le Dock (en bas de l’écran, l’icône d’engrenage). 
3.	Cliquez sur **“Réseau”** dans la barre latérale (à gauche). Vous devrez peut-être faire défiler la page vers le bas. 
4.	Cliquez sur **“Coupe-feu”** et activez-le, comme le montre l’image suivante. 

Étape	Description
5.	Ensuite, cliquez sur **“Options de coupe-feu...”.** 
6.	Une nouvelle fenêtre s’affiche. Activez l’option **“Activer le mode furtif”.** 
7.	Une fois le mode furtif activé, cliquez sur **“OK”.** 

4.4. Notifications

Dans cette section, l'objectif consiste à réduire l'exposition des données sensibles lorsque l'ordinateur est verrouillé ou inactif. Dans de telles circonstances, il faudra donc désactiver certains paramètres de notification afin de garantir la confidentialité et la sécurité des données dans le système d'exploitation macOS.

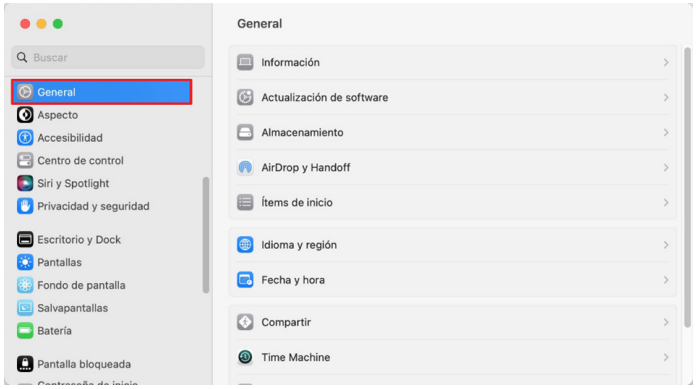
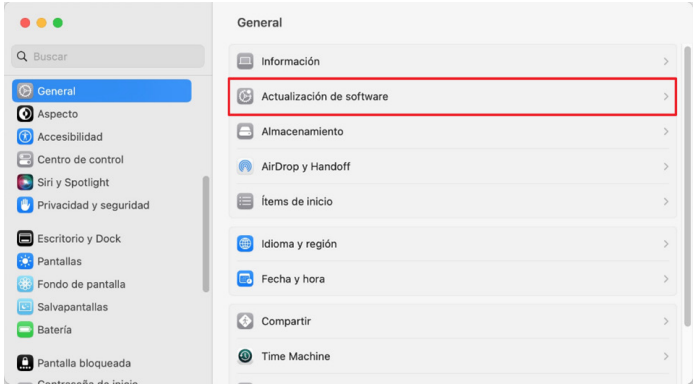
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Cliquez sur **"Notifications"** dans la barre latérale (à gauche). 
4.	Modifiez les réglages **"Notifications"** comme indiqué ci-dessous : ◆ Afficher les aperçus : Jamais. ◆ Autoriser les notifications lorsque le moniteur est en veille : Désactivé. ◆ Autoriser les notifications lorsque l'écran est verrouillé : Désactivé. 

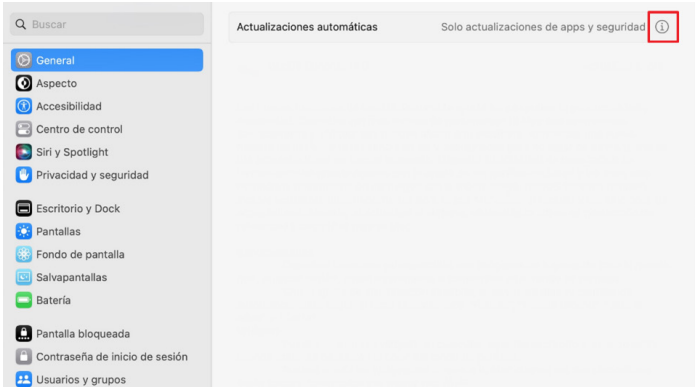
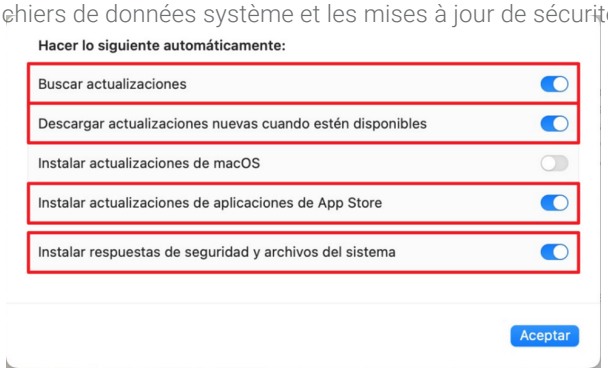
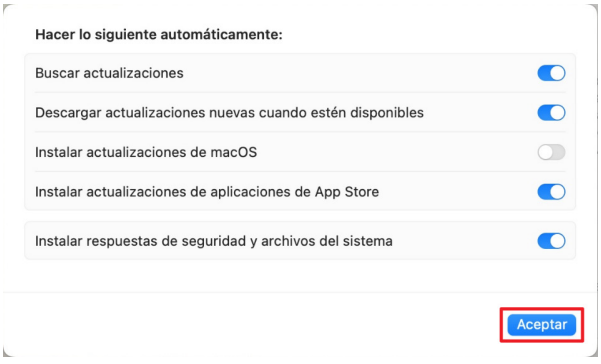
4.5. Général

Ce chapitre porte sur les modifications concernant les mises à jour du système d'exploitation macOS Ventura et d'autres aspects liés au partage des données.

4.5.1. Mise à jour de logiciels

Dans la section suivante, les utilisateurs sont invités à maintenir leurs systèmes et apps à jour afin d'améliorer la stabilité et la sécurité.

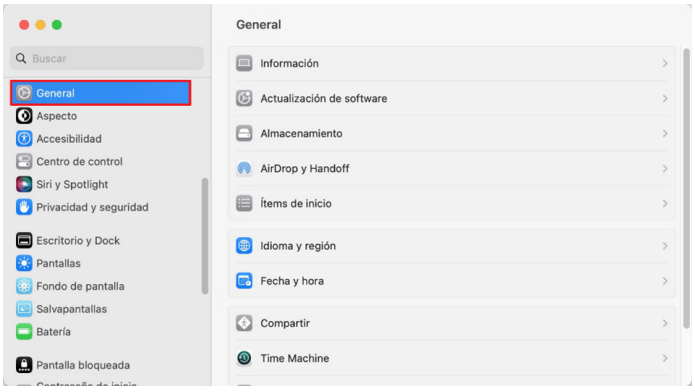
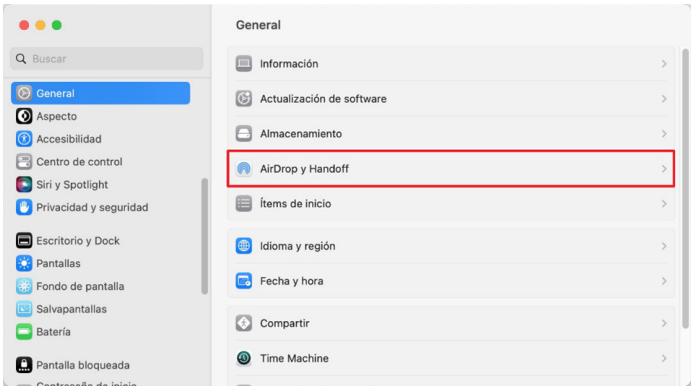
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Cliquez sur **"Général"** dans la barre latérale (à gauche). 
4.	Cliquez sur **"Mise à jour de logiciels".** 

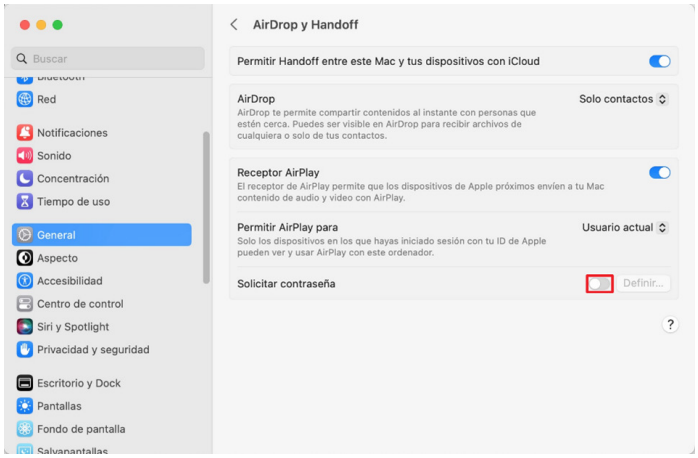
Étape	Description
5.	Dans la fenêtre **"Mise à jour de logiciels",** cliquez sur le bouton d'informations ⓘ situé à droite de l'option **"Mises à jour d'apps et de sécurité uniquement".** 
6.	Une nouvelle fenêtre s'affiche. Modifiez les réglages **"Automatiquement"** comme indiqué ci-dessous : ◆ Rechercher les mises à jour : Activé. ◆ Télécharger les nouvelles mises à jour lorsqu'elles sont disponibles : Activé. ◆ Installer les mises à jour d'apps depuis l'App Store : Activé ◆ Installer les fichiers de données système et les mises à jour de sécurité : Activé.  **Remarque : L'option "Installer les mises à jour de macOS" n'est pas activée car il est possible qu'une mise à jour récente du système d'exploitation entraîne des problèmes logiciels et matériels. Si vous souhaitez l'activer, il est recommandé d'effectuer une sauvegarde au préalable afin d'éviter toute perte de données.**
7.	Une fois les modifications effectuées, cliquez sur le bouton **"OK".** 

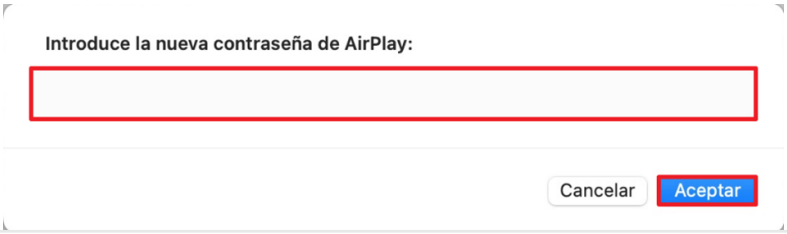
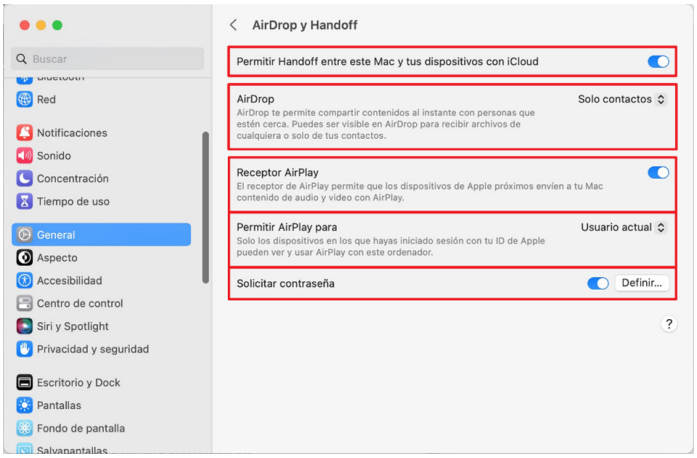
4.5.2. Airdrop y Handoff

Cette section porte sur les réglages Airdrop et Handoff. Vous pouvez les utiliser pour commencer une tâche sur un appareil Apple et la transférer sur un autre appareil, envoyer des fichiers vers des appareils Apple à proximité via AirDrop ou autoriser d'autres appareils à diffuser du contenu sur votre Mac. Dans les sections suivantes, nous allons vous montrer comment activer ou désactiver le transfert sur d'autres appareils Apple.

4.5.2.1. Autoriser le transfert sur d'autres appareil Apple

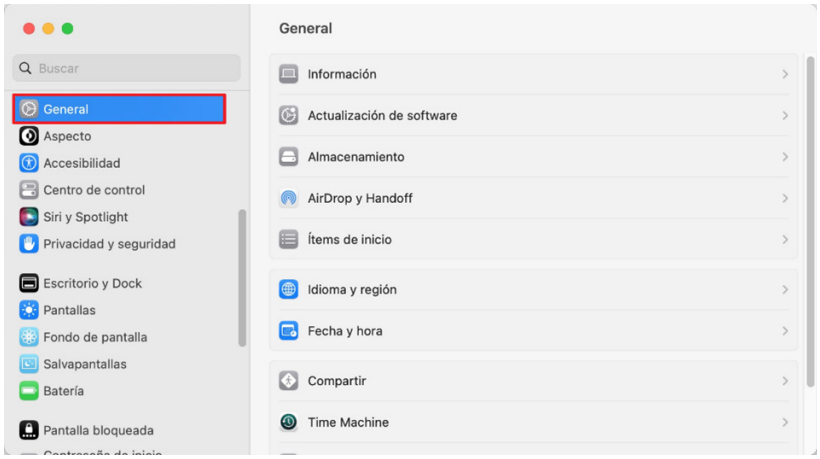
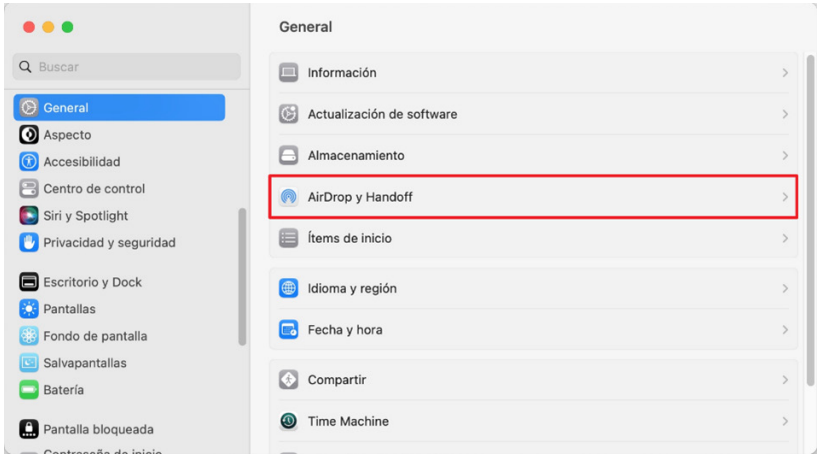
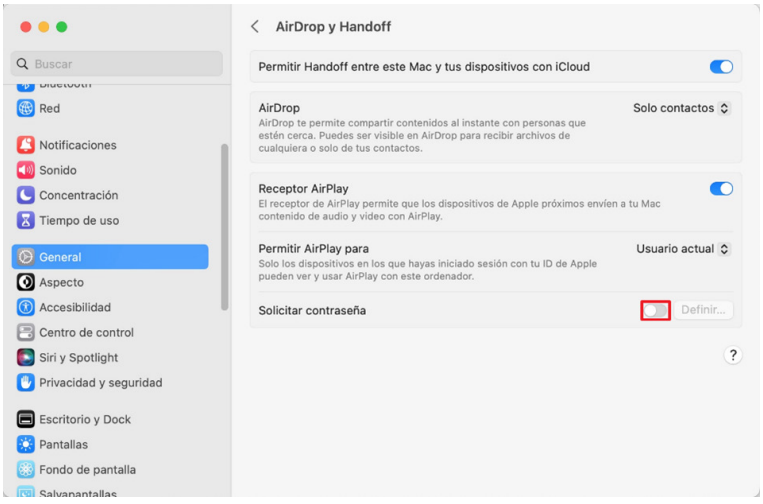
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Général"** dans la barre latérale (à gauche). 
4.	Ensuite, cliquez sur **"AirDrop et Handoff"** à droite. 

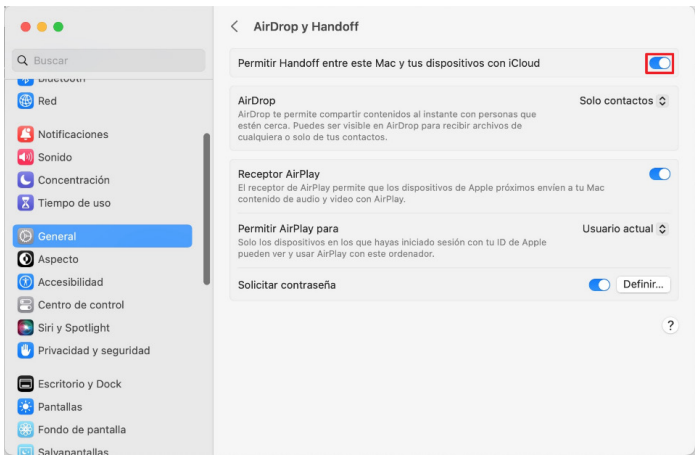
Étape	Description
5.	Dans la fenêtre **“AirDrop et Handoff”**, activez l’option **“Exiger le mot de passe”**. 
6.	Vous serez alors invité à élever vos privilèges. Saisissez le nom d’utilisateur et le mot de passe dans les zones de texte correspondantes et cliquez sur **“Modifier les paramètres”**. 

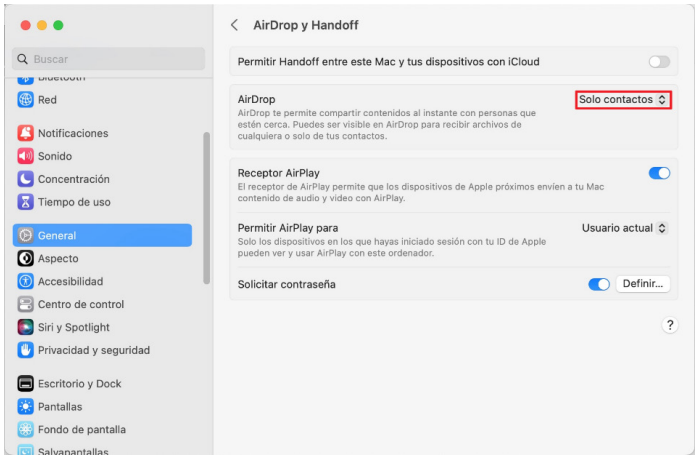
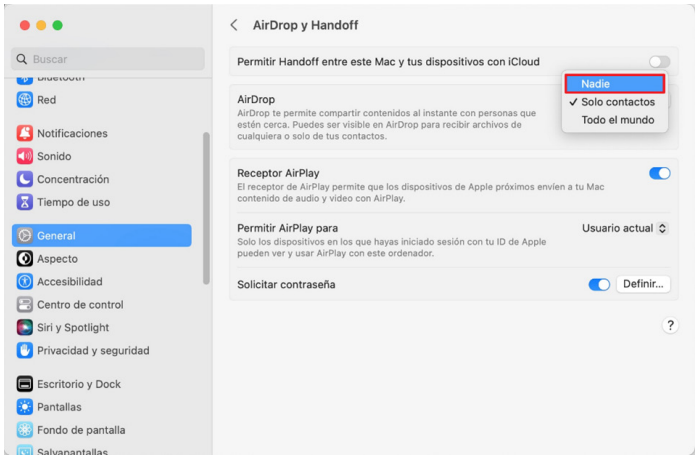
Étape	Description
7.	Saisissez le nouveau mot de passe AirPlay. Ce mot de passe sera requis à chaque fois que vous utiliserez la fonction AirPlay. Cliquez ensuite sur **"OK".** 
8.	Vérifiez et modifiez les paramètres suivants comme indiqué ci-dessous ◆ Autoriser Handoff entre ce Mac et vos appareils iCloud : Activé. ◆ AirDrop : Contacts uniquement. ◆ Récepteur AirPlay : Activé. ◆ Autoriser AirPlay pour : Utilisateur actif. ◆ Exiger le mot de passe : Activé. 

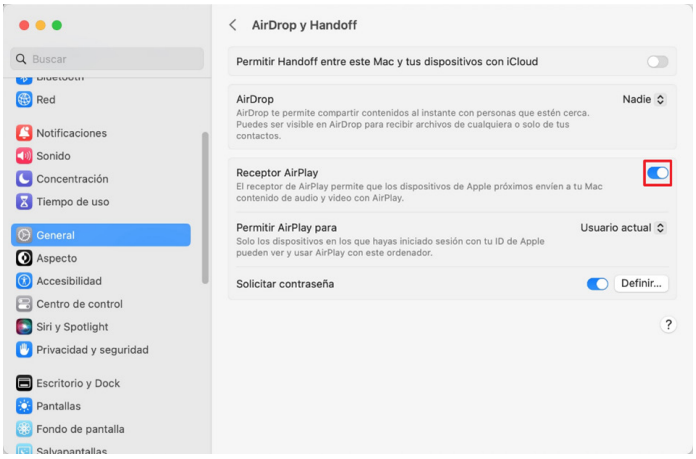
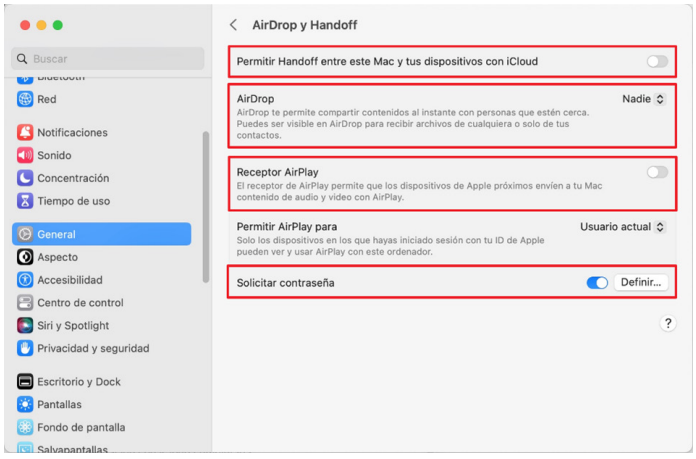
4.5.2.2. Désactiver le transfert sur d'autres appareils Apple

Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 

Étape	Description
3.	Faites défiler la page vers le bas et cliquez sur **"Général"** dans la barre latérale (à gauche). 
4.	Ensuite, cliquez sur **"AirDrop et Handoff".** 
5.	Dans la fenêtre **"AirDrop et Handoff"**, cliquez sur l'option et activez **"Exiger le mot de passe"**. 

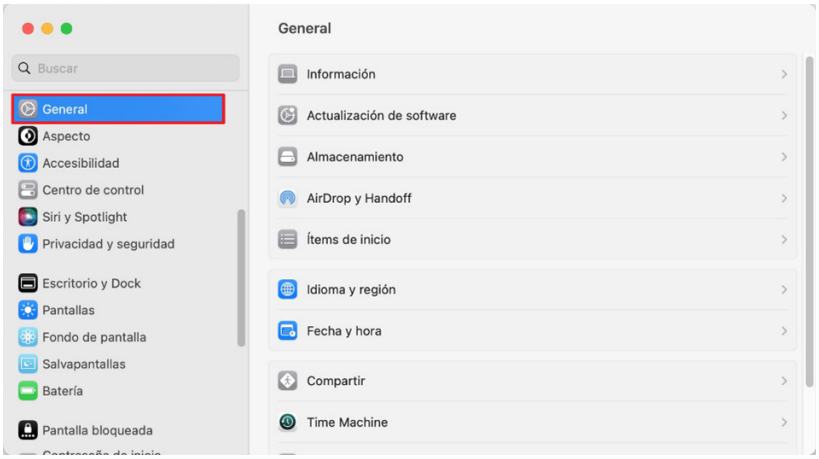
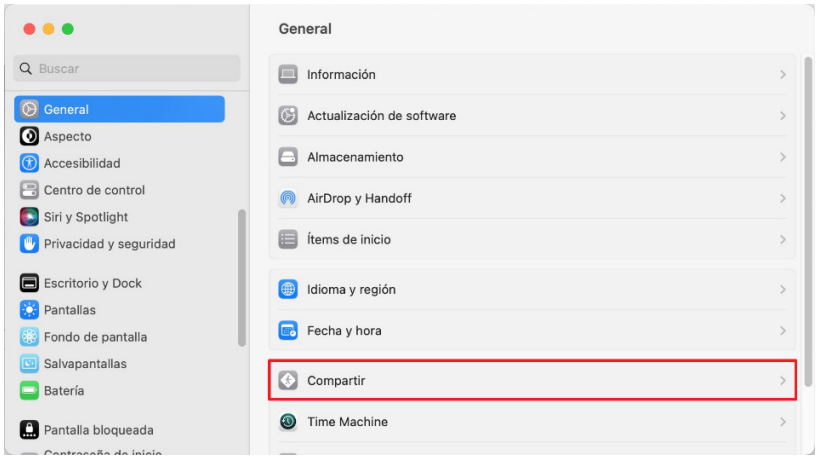
Étape	Description
6.	Vous serez alors invité à élever vos privilèges. Saisissez le nom d'utilisateur et le mot de passe dans les zones de texte correspondantes et cliquez sur **"Modifier les paramètres".** 
7.	Saisissez le nouveau mot de passe AirPlay. Ce mot de passe sera requis à chaque fois que vous utiliserez la fonction AirPlay. Cliquez ensuite sur **"OK".** 
8.	Dans la fenêtre **"AirDrop et Handoff"**, désactivez "**Autoriser Handoff entre ce Mac et vos appareils iCloud".** Pour ce faire, cliquez sur le bouton d'activation. 

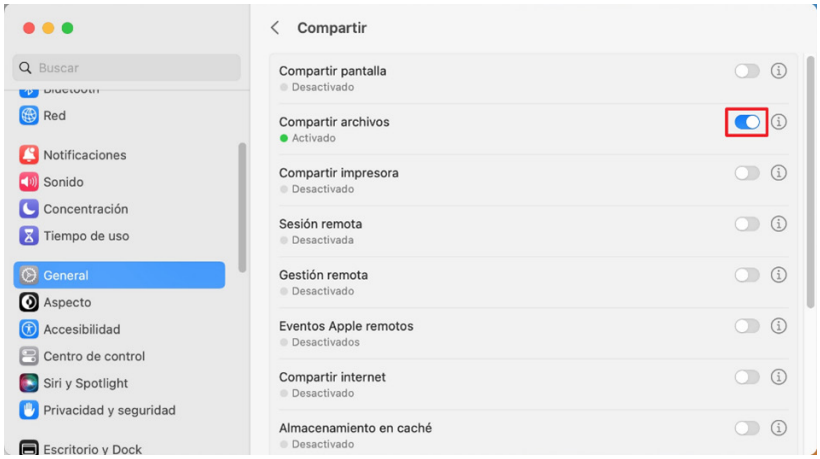
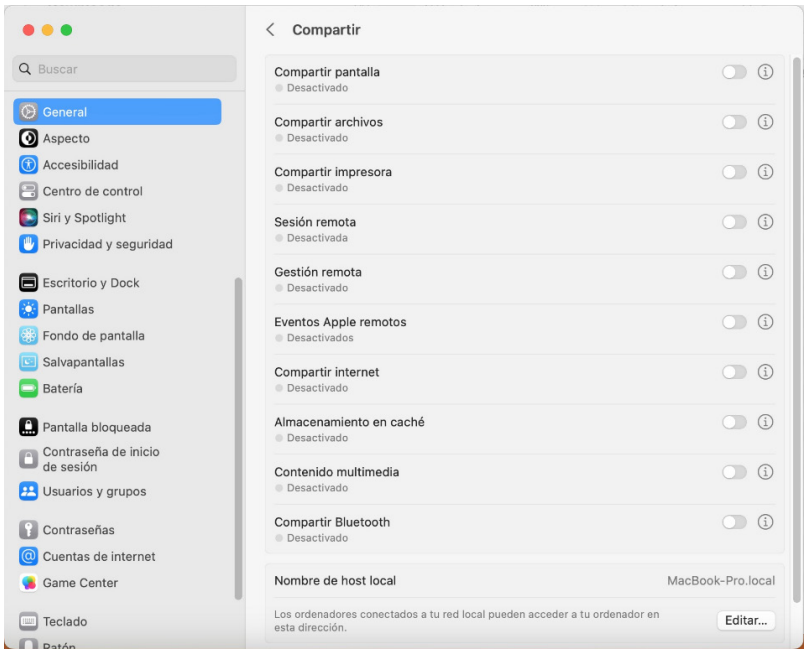
Étape	Description
9.	Ensuite, cliquez sur le bouton **“Ne pas autoriser Handoff”.** 
10.	Dans la fenêtre **“AirDrop et Handoff”,** restreignez **“AirDrop”.** Pour ce faire, cliquez sur le menu déroulant à droite. 
11.	Ensuite, sélectionnez l’option **“Réception désactivée”.** 

Étape	Description
12.	Dans la même fenêtre **“AirDrop et Handoff”**, désactivez **“Récepteur AirPlay”.** Pour ce faire, cliquez sur le bouton d’activation. 
13.	Vérifiez que les réglages ont été effectués comme indiqué ci-dessous : ◆ Autoriser Handoff entre ce Mac et vos appareils iCloud : Désactivé. ◆ AirDrop : Réception désactivée. ◆ Récepteur AirPlay : Désactivé. ◆ Exiger le mot de passe : Activé. 

4.5.3. Partage

Dans cette section, les réglages Partage vous permettent de définir des options pour partager votre ordinateur, vos fichiers, vos imprimantes, votre contenu multimédia, et d'autres éléments.

Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Général"** dans la barre latérale (à gauche). 
4.	Ensuite, cliquez sur **"Partage"** à droite. 

Étape	Description
5.	Dans la fenêtre **"Partage"**, désactivez le **"Partage de fichiers"**. Pour ce faire, cliquez sur le bouton d'activation. 
6.	Pour le reste des paramètres **"Partage"**, il faut savoir qu'ils sont tous désactivés par défaut sur macOS. Il convient donc de maintenir ces paramètres désactivés, à l'exception de ceux qui sont nécessaires à une utilisation spécifique.  **Remarque : Si l'une des fonctionnalités est activée, il est recommandé d'examiner au cas par cas chacune d'entre elles et décider ensuite si son activation est réellement nécessaire. Si vous considérez que la fonctionnalité doit rester activée, vous devrez respecter les critères suivants :** ◆ **Privilèges minimaux. Type d'utilisateur : standard, "partager uniquement" ou administrateur.** ◆ **Uniquement aux utilisateurs strictement nécessaires.** ◆ **Permissions minimales. Lecture ou écriture.** ◆ **Dispositifs minimaux à partager.**

4.6. Confidentialité et sécurité

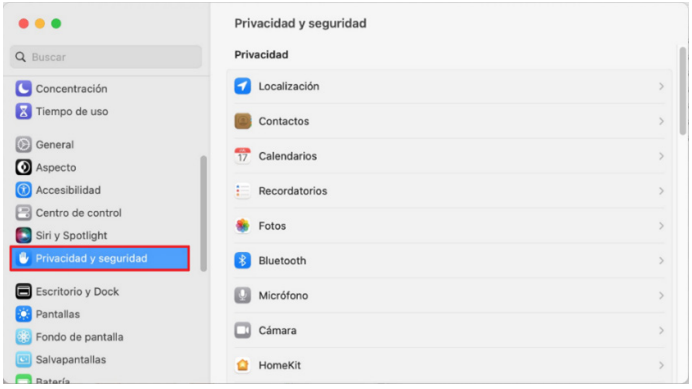
MacOS Ventura met l'accent sur les paramètres qui protègent la confidentialité et l'intégrité des données. Ces réglages vous permettent de protéger vos données chiffrées via l'activation de FileVault et de gérer les autorisations d'application ainsi que vos préférences avancées de sécurité. Ils sont essentiels car ils permettent aux utilisateurs d'avoir un contrôle total en choisissant ce qui est accessible par d'autres utilisateurs via Internet ou un réseau.

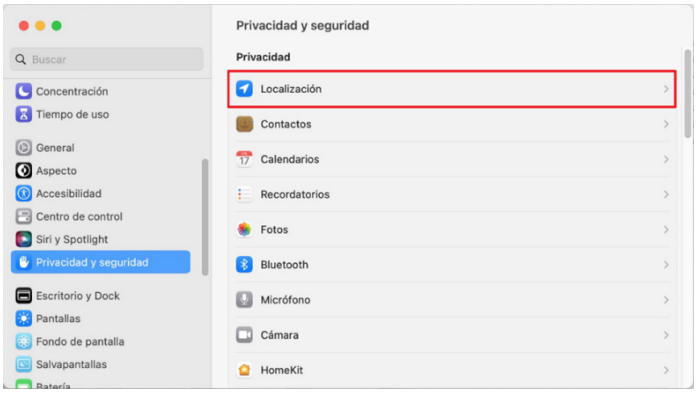
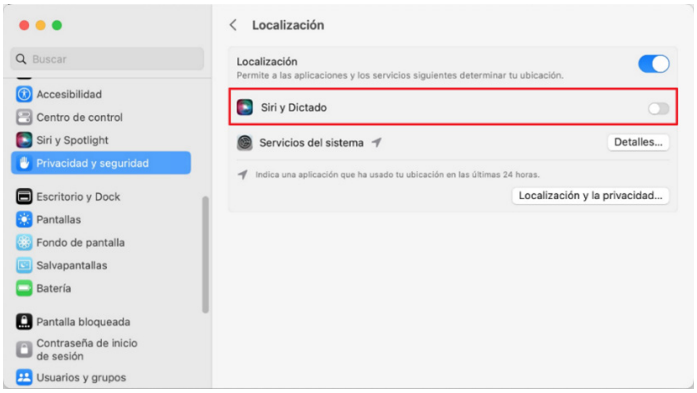
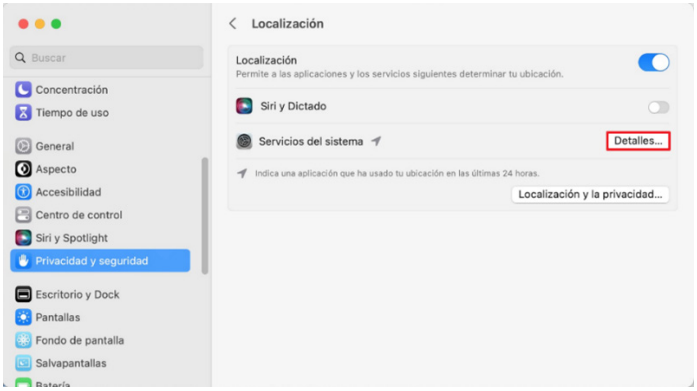
4.6.1. Confidentialité

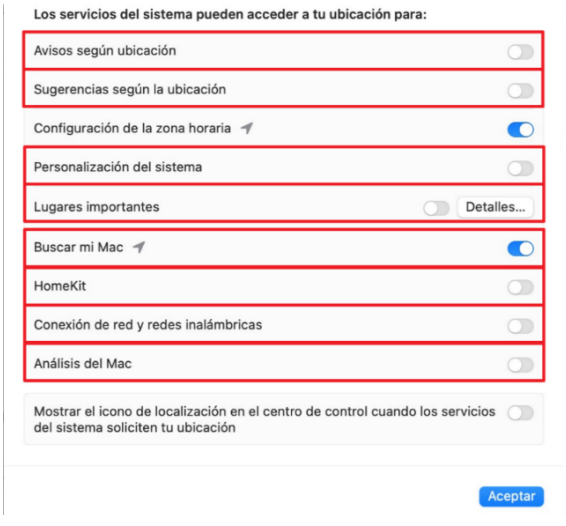
Cette section accorde la priorité à la confidentialité en fournissant des paramètres et des outils qui permettent aux utilisateurs de contrôler et de limiter l'accès à leurs informations. Ces réglages vous permettent de gérer les autorisations d'application et de décider quelles apps sont autorisées à collecter et à utiliser des informations concernant le lieu actuel de votre Mac, ou bien à accéder à vos photos ou au micro de votre Mac.

4.6.1.1. Service de localisation

Les paramètres de localisation permettent aux utilisateurs de contrôler l'accès des apps et des services système à leur position géographique. Cette fonctionnalité est essentielle pour protéger la confidentialité et garantir que seules les apps autorisées ont accès aux informations de localisation.

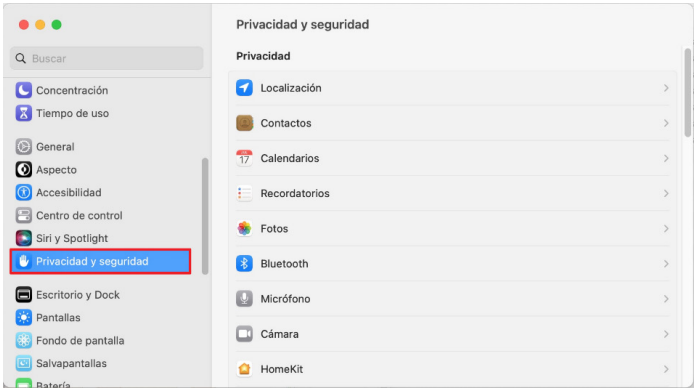
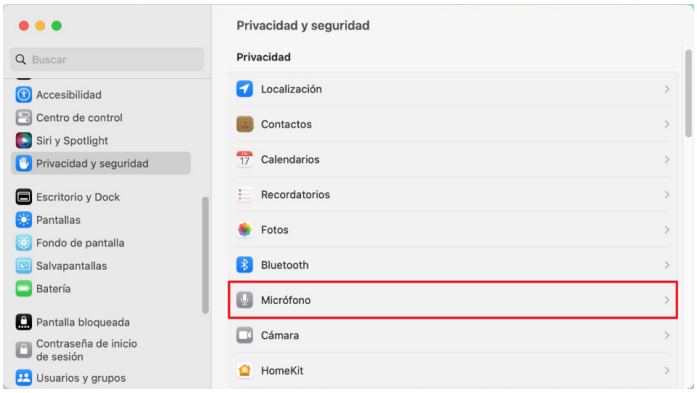
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Confidentialité et sécurité"** dans la barre latérale (à gauche). 

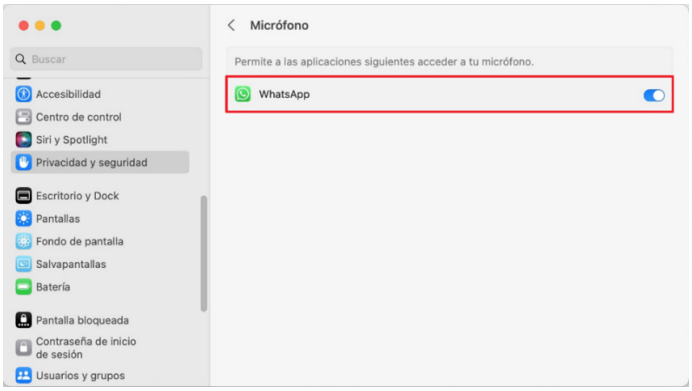
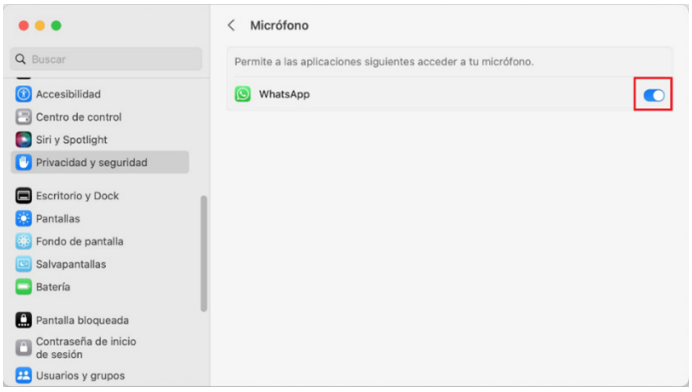
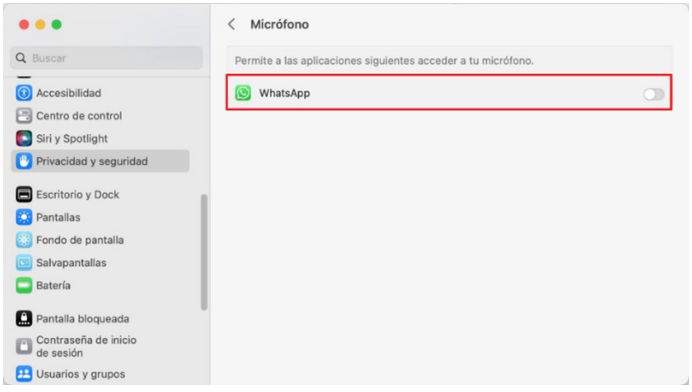
Étape	Description
4.	Ensuite, cliquez sur **“Service de localisation”**. 
5.	Dans la fenêtre **“Service de localisation”**, vérifiez que le bouton **“Siri et Dictée”** est désactivé.  **Remarque : la localisation pour “Siri et dictée” est désactivée par défaut.**
6.	Dans la fenêtre **“Service de localisation”**, cliquez sur le bouton **“Détails...”.** 

Étape	Description
7.	Vous serez alors invité à élever vos privilèges. Saisissez le **nom d'utilisateur** et le **mot de passe** dans les zones de texte appropriées et cliquez sur **"Déverrouiller".** 
8.	Dans la fenêtre **"Autoriser les services système à déterminer votre position"**, modifiez les paramètres suivants comme indiqué ci-dessous : ◆ Alertes selon le lieu : Désactivé. ◆ Suggestions selon le lieu : Désactivé. ◆ Personnalisation du fuseau horaire et du système : Désactivé. ◆ Lieux importants : Désactivé. ◆ Localiser mon Mac : Activé. ◆ HomeKit : Désactivé. ◆ Mise en réseau et sans fil : Désactivé. ◆ Analyse Mac : Désactivé.  **Remarque : Si vous souhaitez qu'une des fonctionnalités reste activée, il est recommandé d'examiner au cas par cas chaque fonctionnalité et de décider ensuite si son activation est réellement nécessaire.**
9.	Appuyez sur **"OK"** pour terminer.

4.6.1.2. Autres paramètres de confidentialité

Cette section consacrée à la confidentialité dans macOS va se concentrer sur la gestion des autorisations auxquelles les différentes apps ont accès. Il s'agit de contrôler quelles applications ont accès aux données sensibles, telles que l'appareil photo, le microphone et d'autres ressources du système, afin de protéger la vie privée et la sécurité des utilisateurs.

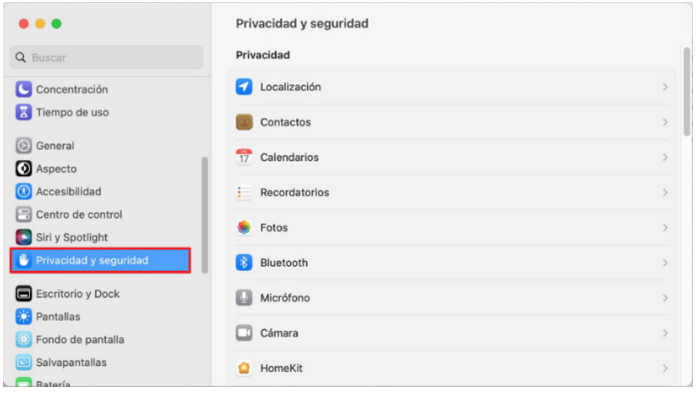
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Confidentialité et sécurité"** dans la barre latérale (à gauche). 
4.	Dans la fenêtre **"Confidentialité et sécurité"**, dans la section **"Confidentialité",** cliquez sur **"Micro".** 

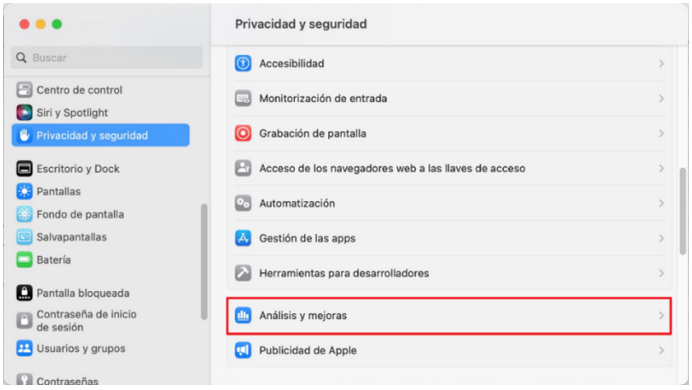
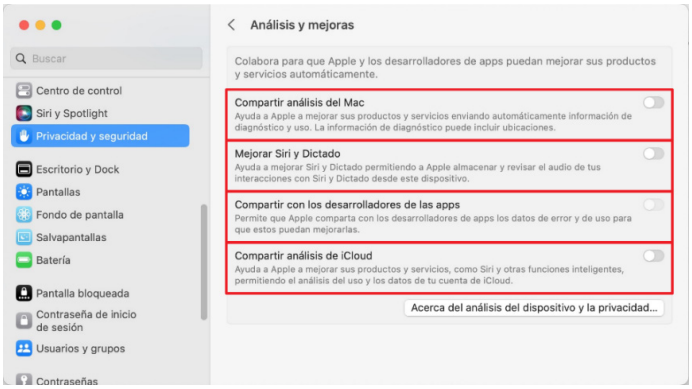
Étape	Description
5.	Dans la fenêtre **"Micro"**, vous pouvez vérifier quelles apps sont autorisées à accéder au micro et à l'utiliser.  **Remarque : Dans cet exemple, nous avons utilisé une app de messagerie instantanée pour montrer les paramètres qu'il faudrait appliquer.**
6.	Identifiez et désactivez toutes les apps qui ne requièrent pas l'accès au microphone en cliquant sur le bouton correspondant.  **Remarque : Nous avons utilisé l'application WhatsApp pour illustrer cet exemple.**
7.	À ce stade, l'accès au microphone est désactivé. 

Étape	Description
8.	Procédez de la même manière pour les autres ressources : ◆ Contacts ◆ Calendriers ◆ Rappels ◆ Photos ◆ Bluetooth ◆ Appareil Photo ◆ HomeKit ◆ Reconnaissance vocale ◆ Médias et Apple Music ◆ Fichiers et dossiers ◆ Accès complet au disque. Si l'une des fonctionnalités est activée, il est recommandé d'examiner au cas par cas chaque fonctionnalité et de décider ensuite si son activation est réellement nécessaire.

4.6.1.3. Analyse et améliorations

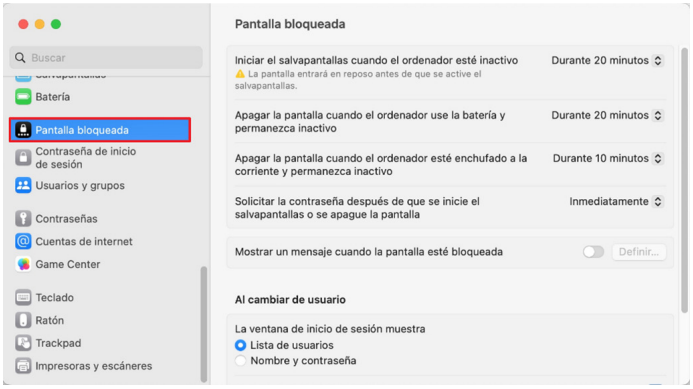
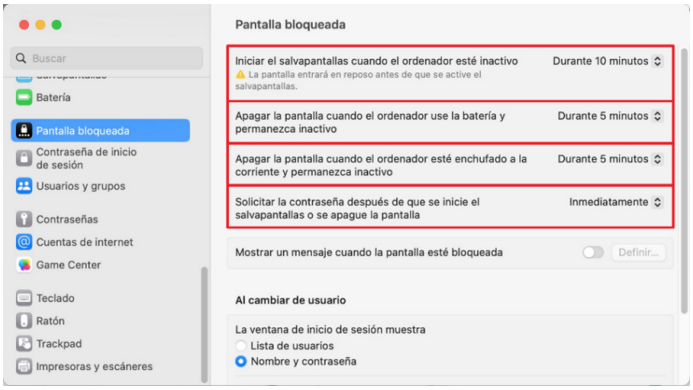
Dans cette section, nous allons définir les paramètres qui limitent les informations d'analyse que votre Mac partage avec Apple. En refusant de partager l'analyse, vous empêchez que macOS puisse recueillir automatiquement des informations d'analyse de votre Mac et les envoyer à Apple afin d'améliorer la qualité et les performances de ses produits.

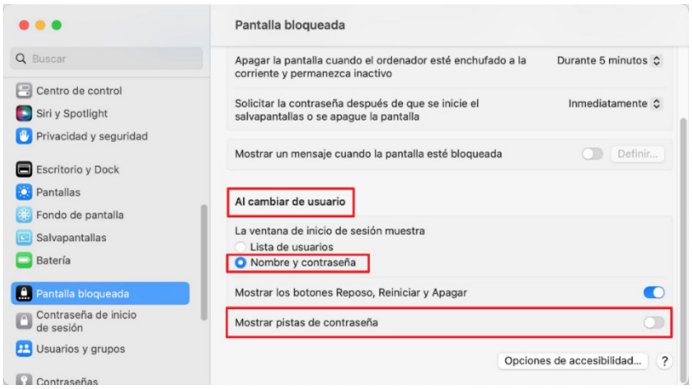
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Confidentialité et sécurité"** dans la barre latérale (à gauche). 

Étape	Description
4.	Faites défiler la page vers le bas et cliquez sur **“Analyse et améliorations”.** 
5.	Dans la fenêtre **“Analyse et améliorations”**, modifiez les paramètres suivants comme indiqué ci-dessous : ◆ Partager l’analyse Mac : Désactivé. ◆ Améliorer Siri et Dictée : Désactivé. ◆ Partager avec les développeurs d’apps : Désactivé. ◆ Partager l’analyse d’iCloud : Désactivé. 

4.7. Verrouillage de l’écran

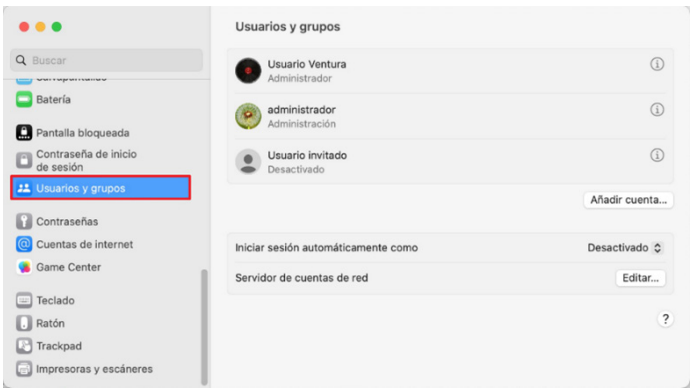
La fonction de verrouillage de l’écran de macOS Ventura permet aux utilisateurs de protéger leur Mac contre tout accès non autorisé. Ils peuvent régler l’économiseur d’écran pour qu’il démarre automatiquement et définir des mots de passe pour déverrouiller le système, garantissant ainsi la confidentialité et la sécurité de leur appareil en cas d’inactivité.

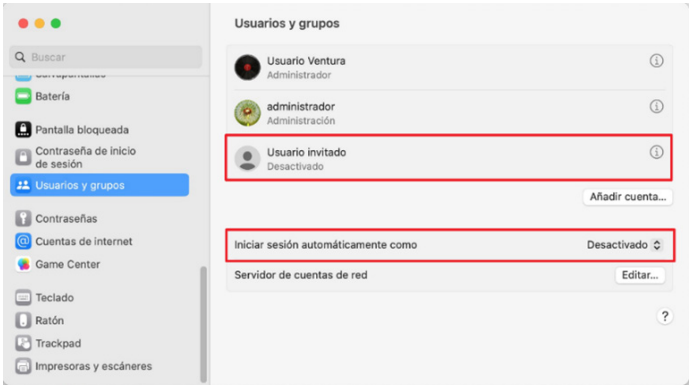
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler la page vers le bas et cliquez sur **"Écran vérrouillé"** dans le menu à gauche. 
4.	Dans la fenêtre **"Écran vérrouillé"**, modifiez les paramètres suivants comme indiqué ci-dessous : ◆ Lancer l'économiseur d'écran en cas d'inactivité : Pendant 10 minutes. ◆ Éteindre l'écran sur batterie en cas d'inactivité : Pendant 5 minutes. ◆ Éteindre l'écran sur adaptateur secteur en cas d'inactivité : Pendant 5 minutes. ◆ Exiger un mot de passe après le lancement de l'économiseur d'écran ou l'extinction de l'écran : Immédiatement.  **Remarque : Sur les ordinateurs de bureau fonctionnant sous macOS Ventura, le paramètre "Éteindre l'écran sur batterie en cas d'inactivité " ne s'applique pas, car ces périphériques n'utilisent pas de batterie.** **D'autre part, vous pouvez adapter ces paramètres à vos besoins, mais en fixant toujours un délai raisonnable.**

Étape	Description
5.	Dans la même fenêtre **"Écran vérrouillé"**, dans la section **"Au changement d'utilisateur"**, modifiez les paramètres suivants comme indiqué ci-dessous : ◆ La fenêtre d'ouverture de session affiche : Nom et mot de passe. ◆ Afficher les indices de mot de passe : Désactivé. 

4.8. Utilisateurs et groupes

La section "Utilisateurs et groupes" de macOS Ventura permet aux utilisateurs de gérer leurs comptes et de définir leurs préférences de connexion.

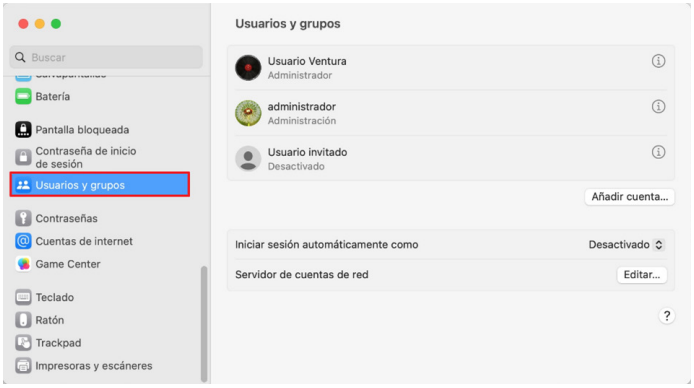
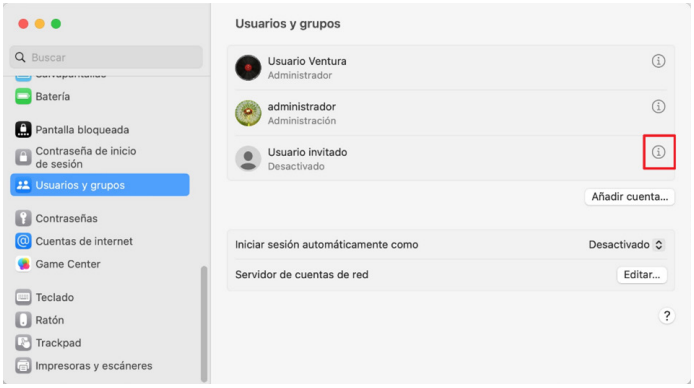
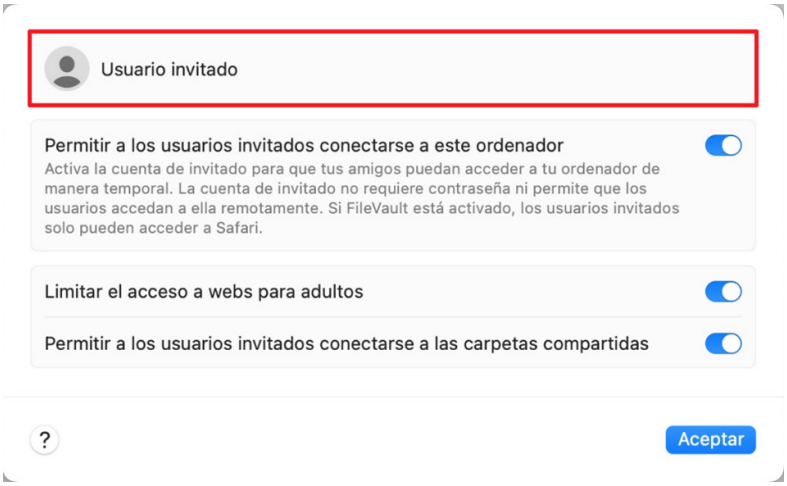
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 
3.	Faites défiler le menu de gauche et cliquez sur **"Utilisateurs et groupes".** 

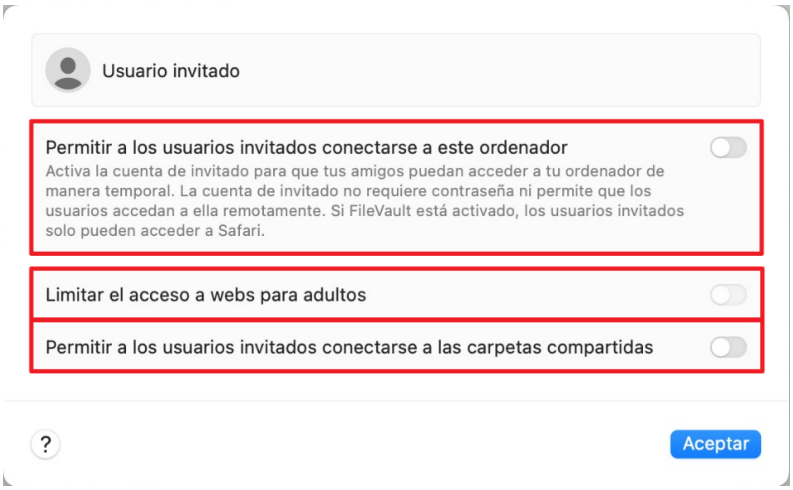
Étape	Description
4.	Dans la fenêtre **"Utilisateurs et groupes"**, vérifiez que les paramètres sont configurés comme indiqué ci-dessous : ◆ Utilisateur invité : Désactivé. ◆ Se connecter automatiquement en tant que : Désactivé.  **Remarque : Si l'une des configurations précédentes est différente de celle indiquée, suivez les étapes décrites dans les chapitres suivants :** **- 4.8.1 Désactiver "utilisateur invité"** **- 4.8.2 Désactiver "se connecter automatiquement"**

4.8.1. Désactiver "utilisateur invité"

L'"Utilisateur invité" est un compte spécial dans macOS Ventura qui permet aux utilisateurs d'accéder temporairement à un ordinateur Mac sans avoir besoin d'un compte d'utilisateur principal. Cependant, pour des raisons de sécurité, cette option sera désactivée dans ce processus de configuration.

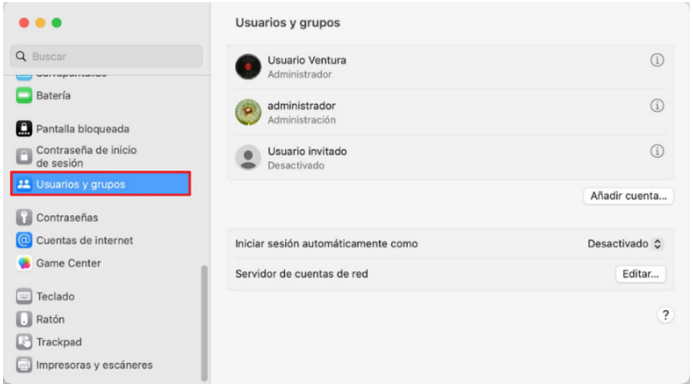
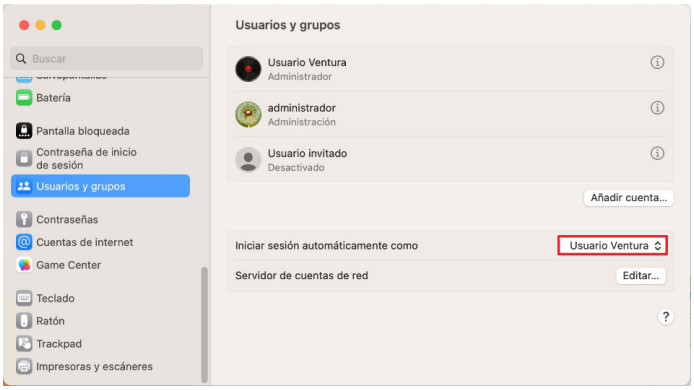
Étape	Description
1.	Connectez-vous avec votre nom d'utilisateur et votre mot de passe sur l'ordinateur macOS.
2.	Cliquez sur l'icône **"Réglages Système"** dans le Dock (en bas de l'écran, l'icône d'engrenage). 

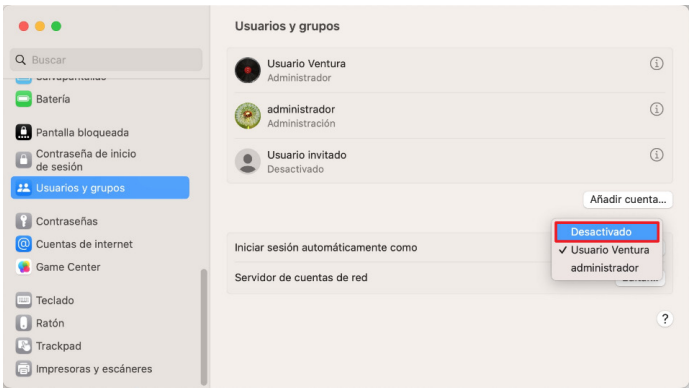
Étape	Description
3.	Faites défiler le menu de gauche et cliquez sur **“Utilisateurs et groupes”.** 
4.	Dans la fenêtre **“Utilisateurs et groupes”**, cliquez sur l’icône d’information ⓘ situé à droite du compte **“Utilisateur invité”**. 
5.	Dans la fenêtre ci-dessous, vous trouverez les différents paramètres pour le compte **“Utilisateur invité”.** 

Étape	Description
6.	Pour désactiver l'**"Utilisateur invité",** modifiez les paramètres suivants comme indiqué ci-dessous : ◆ Autoriser les invités à se connecter à cet ordinateur : Désactivé. ◆ Limiter les sites web pour adultes : Désactivé. ◆ Autoriser les invités à se connecter à des dossiers partagés : Désactivé.  **Remarque : L'option "Limiter les sites web pour adultes" doit être "Activée" lorsque l'on autorise un utilisateur invité mais que l'on souhaite bloquer son accès à certains sites web.**
7.	Une fois les modifications effectuées, cliquez sur le bouton **OK.** 

4.8.2. Désactiver “se connecter automatiquement”

Pour éviter que toute personne puisse accéder à votre Mac simplement en le redémarrant, il est recommandé de désactiver l’ouverture de session automatique.

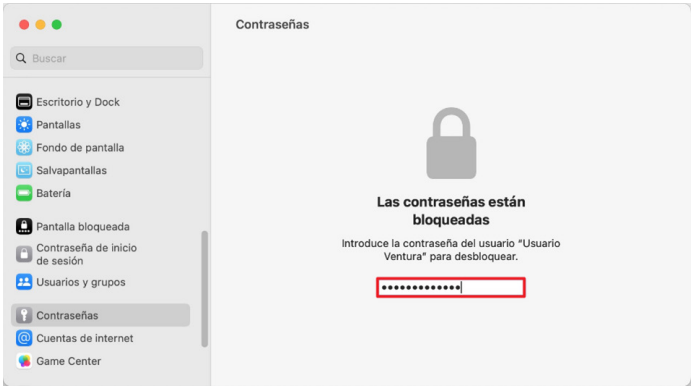
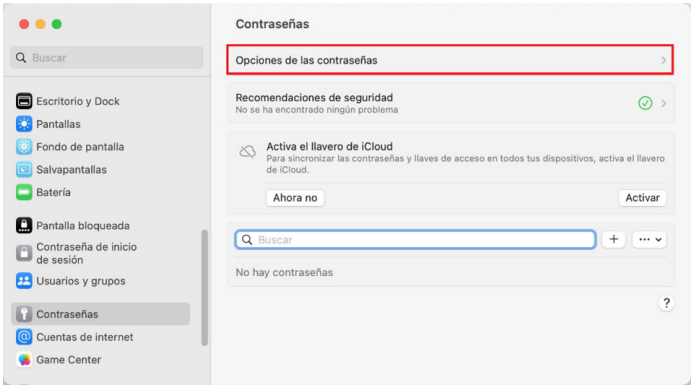
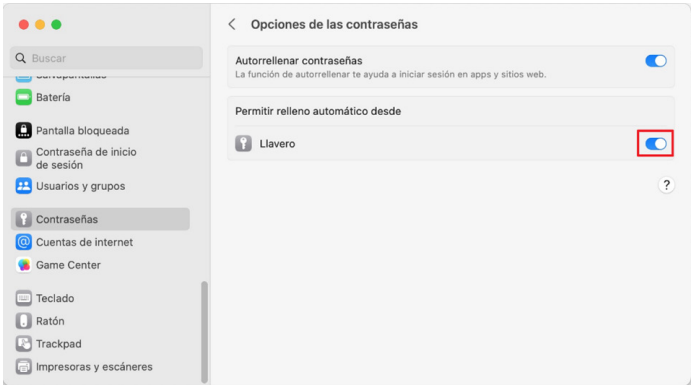
Étape	Description
1.	Connectez-vous avec votre nom d’utilisateur et votre mot de passe sur l’ordinateur macOS.
2.	Cliquez sur l’icône **“Réglages Système”** dans le Dock (en bas de l’écran, l’icône d’engrenage). 
3.	Faites défiler le menu de gauche et sélectionnez **“Utilisateurs et groupes”.** 
4.	Dans la fenêtre **“Utilisateurs et groupes”**, cliquez sur l’utilisateur configuré à droite de l’option **“Se connecter automatiquement en tant que”.** 

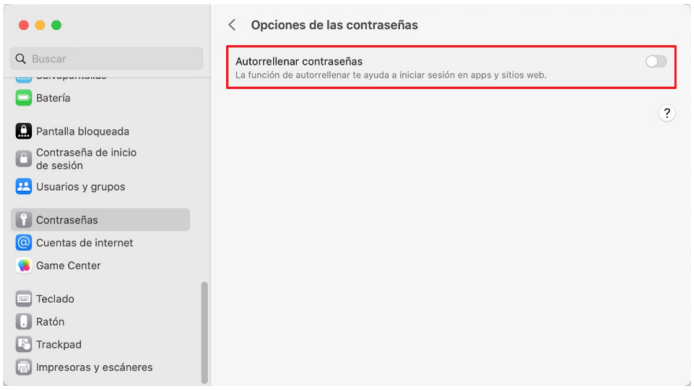
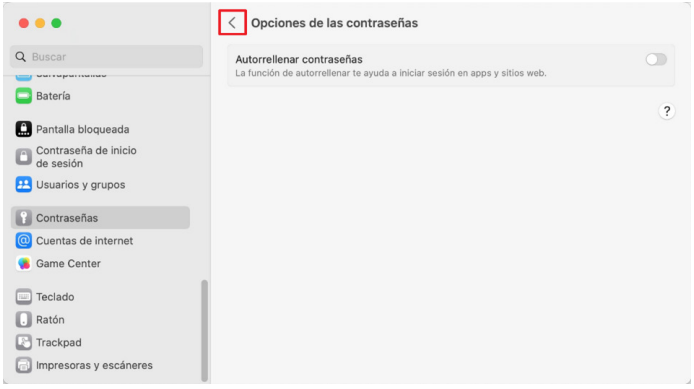
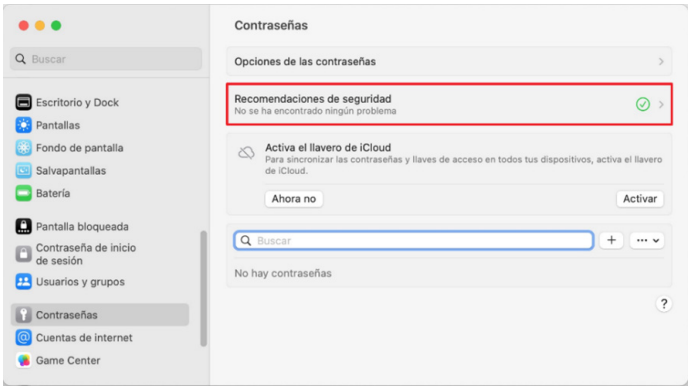
Étape	Description
5.	Dans la fenêtre de sélection affichée, sélectionnez **“Désactivé”.** 

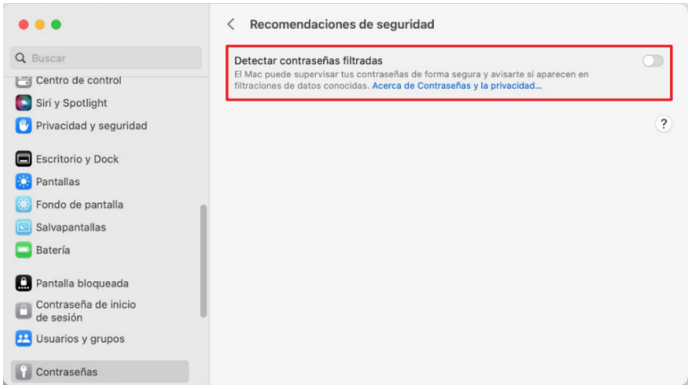
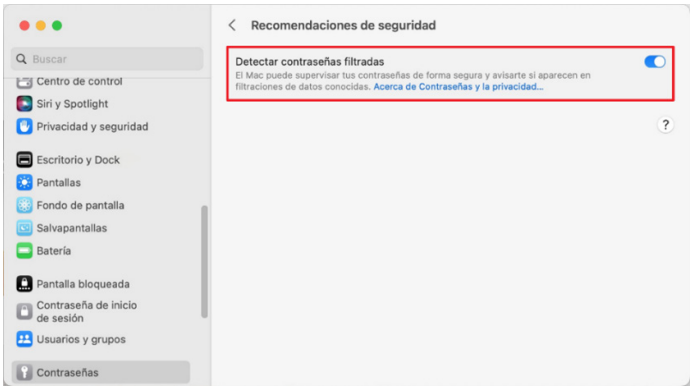
4.9. Mots de passe

Dans cette section, nous allons activer les recommandations de sécurité pour les mots de passe.

Étape	Description
1.	Connectez-vous avec votre nom d’utilisateur et votre mot de passe sur l’ordinateur macOS.
2.	Cliquez sur l’icône **“Réglages Système”** dans le Dock (en bas de l’écran, l’icône d’engrenage). 
3.	Faites défiler le menu de gauche et cliquez sur **“Mots de passe”.** 

Étape	Description
4.	Dans la fenêtre **“Mots de passe”**, entrez votre mot de passe d’utilisateur pour accéder à la configuration. 
5.	Dans la fenêtre **“Mots de passe”**, cliquez sur **“Options des mots de passe”.** 
6.	Dans la fenêtre **“Options des mots de passe”**, cliquez sur le bouton pour désactiver le **“Trousseau”.** 

Étape	Description
7.	Ensuite, dans la même fenêtre, décochez l'option **"Préremplir mots de passe"** comme indiqué dans l'image ci-dessous : 
8.	Cliquez sur "<" pour revenir à la fenêtre **"Mots de passe".** 
9.	Parmi les options qui s'affichent, cliquez sur **"Recommandations de sécurité"**. 

Étape	Description
10.	Identifier le paramètre **"Détecter les mots de passe compromis".** MacOS Ventura permet au système d'analyser et d'alerter l'utilisateur si l'un des mots de passe figure sur des listes exposées ou ayant fait l'objet d'une fuite. 
11.	Activez le paramètre **"Détecter les mots de passe compromis"**, comme le montre l'image suivante. 

5. Checklist

Criticité	Description
Élevée	Les mises à jour et les mises à niveau pour macOS et ses applications intégrées fonctionnent correctement. **Note : Vous pouvez consulter les versions macOS en cliquant sur le lien suivant : https://support.apple.com/es-es/HT201260**
Élevée	Les autorisations d'accès sont définies pour les différents utilisateurs et chacun d'eux possède un compte utilisateur distinct.
Élevée	Le coupe-feu intégré à macOS est activé pour empêcher les connexions indésirables en provenance d'Internet ou d'autres réseaux.
Élevée	Les points d'accès Wi-Fi sont sécurisés, protégés par un mot de passe et chiffrés.
Élevée	L'ouverture de session automatique est désactivée.
Élevée	La synchronisation de l'appareil avec les différentes applications iCloud est désactivée.
Élevée	Examiner et désactiver les applications inutiles.
Élevée	Désactiver "Préremplir les mots de passe" et le "Trousseau iCloud".
Moyenne	Les notifications du système sont désactivées lors du verrouillage de l'écran.
Moyenne	Le mode furtif est activé pour empêcher votre Mac de répondre à d'éventuelles tentatives d'accès depuis le réseau. De cette manière, votre Mac apparaîtra invisible aux utilisateurs potentiellement malveillants.
Moyenne	Le paramètre "Localiser mon Mac" est activé, ce qui permet l'effacement ou le verrouillage à distance de l'ordinateur.
Moyenne	Assurez-vous que l'ordinateur n'a pas de partages réseau inutiles (dossiers, fichiers, etc.).

5. Checklist

Criticité	Description
Moyenne	L'appareil dispose d'un temps de verrouillage automatique de l'écran en cas d'inactivité.
Moyenne	L'appareil fait une demande de connexion à un réseau Wi-Fi sécurisé connu et ne se connecte pas automatiquement.
Moyenne	L'appareil fait une demande de connexion à des points d'accès proches lorsqu'il n'y a pas de point d'accès connu et ne se connecte pas automatiquement.
Moyenne	L'identifiant de l'utilisateur est nécessaire pour se connecter à nouveau après le verrouillage de l'appareil.
Basse	Éviter l'envoi d'informations d'analyse à Apple sur l'appareil et sur l'utilisateur.
Basse	Les fonctionnalités de Continuité, qui permettent de poursuivre vos tâches d'un appareil Apple à l'autre, sont restreintes.

6. Décalogue de recommandations

Voici dix recommandations en matière de sécurité pour les systèmes d’exploitation MacOS

Dix recommandations pour MacOS pour les systèmes d'exploitation MacOS

1. Maintenez le système **d'exploitation** et les **applications à jour** pour bénéficier des **correctifs de sécurité et des nouvelles fonctionnalités.**

2. Si vous avez besoin **d'installer des modules additionnels,** il est recommandé d'utiliser **l'App Store**, des **sources officielles et/ou des sources de confiance.**

3. **Il n'est pas conseillé de gérer les mots de passe** à l'aide des trousseaux. Il existe des gestionnaires plus performants qui utilisent un cryptage fort et qui sont capables de stocker les mots de passe de manière **plus sécurisée.**

4. Utilisez **l'authentification à deux facteurs** pour améliorer votre sécurité en ligne. Cela ajoute une **couche de sécurité supplémentaire à vos comptes car une vérification additionnelle sera requise lors de chaque ouverture de session** (SMS, appel téléphonique, authentificateurs, code de vérification, etc.).

5. Effectuez **régulièrement des copies de sauvegarde de vos données** sur un disque dur externe ou dans le Cloud.

6. Soyez particulièrement **prudent** avant de cliquer sur des liens inconnus ou sur des pièces jointes à vos courriels afin d'éviter **l'hameçonnage**.

7. Activez **FileVault ou une autre solution** de **chiffrement de disque** dur pour **protéger les données en cas de perte ou de vol de votre appareil.**

8. **Ne vous connectez qu'à des réseaux Wi-Fi sécurisés** et évitez les réseaux ouverts ou non vérifiés.

9. **Configurez le verrouillage de l'écran** et les **notifications** pour limiter l'accès au contenu.

10. Activez le **coupe-feu de macOS** pour **protéger la connexion Internet** et installez un **logiciel antivirus pour vous protéger contre les malwares**, entre autres.

Centro Criptológico Nacional 20 ANIVERSARIO

CCN-CERT centro criptológico nacional

Annexe A. Recommandations supplémentaires

A.1. Mots de passe

Un mot de passe fort est essentiel pour protéger les comptes et les données en ligne. Veillez à créer des mots de passe uniques et complexes qui combinent lettres, chiffres et caractères spéciaux. Il est crucial d'éviter les informations personnelles évidentes, telles que le nom ou la date de naissance, et de penser à utiliser des phrases ou des acronymes faciles à mémoriser. De même, il est essentiel de garder les mots de passe à jour et de ne jamais les partager avec d'autres utilisateurs ou de les réutiliser sur plusieurs comptes ou pour accéder à plusieurs services.

Les mots de passe sécurisés constituent un élément fondamental de la protection des informations et des données privées dans un monde de plus en plus numérique. Ils constituent la première ligne de défense contre les cybermenaces potentielles et les accès non autorisés.

A.2. Antivirus

Malgré la réputation de macOS en matière de sécurité, l'utilisation d'un antivirus sur les appareils Mac est essentielle en raison de l'évolution constante des cybermenaces. L'antivirus offre un certain nombre d'avantages clés, dont les suivants :

- Protection actualisée pour détecter les menaces et supprimer les programmes malveillants.
- Détection proactive des comportements suspects, essentielle pour prévenir les attaques de type "zero-day".
- Modules de sécurité pour la navigation sur le web afin d'éviter les sites malveillants et l'hameçonnage.

- Protéger les données personnelles contre le vol et les failles de sécurité qui présentent des risques pour la vie privée de l'utilisateur.
- Maintenir les performances du système sans le ralentir de manière significative.
- Empêcher la propagation de logiciels malveillants à d'autres appareils du réseau.

En résumé, un antivirus sur macOS fournit une couche de sécurité supplémentaire et permet de protéger la confidentialité, les données et les performances du système. Toutefois, il devrait s'accompagner de pratiques de sécurité solides et d'une formation de sensibilisation en ligne, car aucun antivirus n'est infaillible.

A.3. Les copies de sauvegarde avec time machine

Time Machine, un outil de sauvegarde intégré à macOS, est essentiel pour l'intégrité et la récupération des données. Il s'agit d'un outil simple d'emploi qui offre de nombreuses fonctionnalités : copies de sauvegarde automatiques, historique des versions, reprise après sinistre, protection de l'ensemble du système et options de stockage flexibles. Bien qu'il existe d'autres solutions sur le marché, le choix dépendra de la spécificité des besoins et des préférences de chaque utilisateur et/ou organisation.

A.4. Le chiffrement de disque avec filevaultt

Le chiffrement de disque, tel que FileVault sur macOS, est essentiel pour protéger les données contre tout accès non autorisé à vos informations en cas de perte ou de vol de votre appareil Mac. Activer FileVault permet de renforcer la sécurité de vos données en empêchant une personne de les déchiffrer ou d'y accéder sans saisir votre mot de passe d'ouverture de session. L'outil vous permet de créer une clé de secours pour déverrouiller le disque et accéder à vos données chiffrées si vous oubliez votre mot de passe. Faites très attention et conservez cette clé en lieu sûr.

Il convient de garder à l'esprit qu'il existe d'autres solutions de chiffrement sur le marché. Le choix de l'outil dépendra de la spécificité des besoins individuels de chaque utilisateur et/ou organisation.

Centro Criptológico Nacional

ANIVERSARIO

CCN-CERT

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es