centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 459

# Guía práctica de seguridad de servicios de Apple



Marzo 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.03.18 09:44:55 +01'00'

© Centro Criptológico Nacional, 2020
NIPO: 083-20-058-6

Fecha de edición: marzo de 2020
Mónica Salas y Raúl Siles (DinoSec) han colaborado en la elaboración del presente informe.

**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. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL ..... 7
2. INTRODUCCIÓN ..... 8
3. OBJETO ..... 8
4. ENTORNO DE APLICACIÓN DE ESTA GUÍA ..... 9
5. CUENTAS ASOCIADAS A LOS SERVICIOS DE APPLE ..... 9
5.1 ID de Apple ..... 11
5.1.1 Qué es el ID de Apple ..... 11
5.1.2 Alta del ID de Apple ..... 12
5.1.3 Creación de un nuevo ID de Apple ..... 13
5.1.4 Segundo factor de autentificación (2FA) ..... 15
5.1.5 Alias del ID de Apple ..... 17
5.1.6 Dispositivos de confianza ..... 18
5.1.7 iForgot: restablecimiento de una contraseña olvidada ..... 20
5.1.8 Ajustes de la cuenta asociada al ID de Apple ..... 23
5.1.9 Iniciar sesión con Apple - "Sign in with Apple" ..... 26
5.2 Cuenta de iCloud ..... 27
5.2.1 Bloqueo de activación ..... 28
5.2.2 Gestión de la cuenta de iCloud ..... 29
5.2.3 Alias de correo ..... 32
5.2.4 Uso del almacenamiento en iCloud por apps de terceros ..... 33
5.3 Cuenta de iTunes/App Store ..... 33
5.3.1 Compras del grupo "Familia" ..... 34
5.4 Otras cuentas vinculadas a los servicios de Apple ..... 35
5.4.1 Cuenta de FaceTime ..... 36
5.4.2 Cuenta de iMessage ..... 37
6. GESTIÓN REMOTA DE DISPOSITIVOS: SERVICIO "BUSCAR" ..... 38
6.1 Borrado remoto de dispositivos ..... 41
6.2 Modo perdido ..... 42
6.2.1 Modo perdido/bloquear en macOS ..... 43
6.2.2 Modo perdido en iOS ..... 44
6.3 Ajustes vinculados a "Buscar" en iOS ..... 45
6.4 Ajustes vinculados a "Buscar" en macOS ..... 46
6.5 Interfaz web de "Buscar" ..... 47
6.6 App "Buscar" ..... 48
6.7 Servicio "Encontrar sin conexión" ..... 49
6.8 Servicio "Compartir mi ubicación" ..... 51
6.9 Grupo "Familia" ..... 52
6.9.1 Roles de "En familia" ..... 54
6.9.2 Funciones compartidas entre el grupo "Familia" ..... 55
7. SERVICIOS PROPIETARIOS DE APPLE ..... 60
7.1 Continuidad ..... 60
7.1.1 APNs (Apple Push Notification service) ..... 61
7.1.2 Handoff ..... 62

7.1.3 Portapapeles universal ..... 65
7.1.4 Recepción de llamadas telefónicas ..... 65
7.1.5 Reenvío de mensajes ..... 66
7.1.6 Instant Hotspot ..... 67
7.1.7 Desbloqueo automático, inicio de sesión y acceso a funciones administrativas con un Apple Watch ..... 68
7.1.8 Continuidad de cámara ..... 69
7.1.9 Dibujo y marcación ..... 70
**7.2 Comunicaciones propietarias de Apple ..... 70**
7.2.1 AirDrop ..... 70
7.2.2 iMessage ..... 76
7.2.3 FaceTime ..... 80
7.2.4 Bonjour (macOS) ..... 81
**7.3 Compartición de contraseñas de redes Wi-Fi ..... 82**
**8. GESTIÓN DE CREDENCIALES EN ICLOUD ..... 83**
**8.1 Mecanismo de depósito del llavero de iCloud ..... 85**
8.1.1 Recuperación de la copia del llavero en depósito ..... 86
**8.2 Gestión de las contraseñas almacenadas en el llavero ..... 87**
8.2.1 iOS ..... 87
8.2.2 macOS ..... 87
8.2.3 Uso del llavero por parte de Safari ..... 87
8.2.4 Autorrelleno de contraseñas y de códigos de seguridad ..... 88
**9. APPLE PAY ..... 89**
**10. ASISTENTE PERSONAL "SIRI" ..... 90**
**10.1 Funcionamiento de Siri ..... 93**
**10.2 Atajos de Siri ..... 94**
**11. APPS CON FUNCIONALIDAD LIGADA A LA CUENTA DE ICLOUD ..... 95**
**11.1 Recordatorios ..... 95**
**11.2 iCloud Drive ..... 97**
**11.3 Mail ..... 98**
11.3.1 Correo cifrado (macOS) ..... 100
11.3.2 Correo no deseado ..... 101
11.3.3 Mail drop ..... 102
**11.4 Notas ..... 103**
**11.5 Calendarios ..... 106**
11.5.1 Compartición de calendarios ..... 106
**11.6 Atajos ..... 108**
**11.7 Fotografías y vídeos ..... 109**
11.7.1 Compartición de fotografías y vídeos ..... 110
11.7.2 Etiquetado de personas en "Fotos" ..... 112
**12. COPIAS DE SEGURIDAD Y RESTAURACIÓN EN ICLOUD ..... 112**
**12.1 Copia de seguridad ..... 112**
12.1.1 Copia de seguridad de archivos ..... 113
12.1.2 Copia de seguridad de calendarios ..... 113

12.1.3 Copia de seguridad de recordatorios ..... 114
12.1.4 Copia de seguridad de "Fotos" ..... 114
12.1.5 Copia de seguridad de los marcadores de Safari ..... 114
**12.2 Restauración de datos desde iCloud ..... 115**
12.2.1 Restauración completa desde copia de seguridad en iCloud ..... 115
12.2.2 Restauración de elementos individuales de iCloud ..... 115
**13. RESUMEN DE LAS RECOMENDACIONES DE SEGURIDAD DE LOS SERVICIOS DE APPLE ..... 118**
**14. REFERENCIAS ..... 119**

## PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2020



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

# 1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

## 2. INTRODUCCIÓN

El uso cotidiano de plataformas informáticas, tanto en el plano profesional como personal, incluyendo dispositivos móviles (tabletas, *smartphones*, accesorios, *wearables*, etc.) y ordenadores (personales o PCs, y Mac), ha traído consigo la aparición de multitud de servicios ligados a ellos, crecientes en número y capacidades, de los que no siempre es posible prescindir.

Estos servicios, asociados a una cuenta de usuario hospedada en el proveedor, están orientados a mejorar la usabilidad de los propios dispositivos y a proporcionar una mejor experiencia de usuario. Lejos de estar exentos de amenazas, su disponibilidad en la nube de cada proveedor permite que sea posible vulnerarlos sin disponer de acceso físico al dispositivo víctima por parte de un potencial atacante. Dado que es habitual que los distintos datos recopilados por estos servicios incluyan información sensible, con impacto sobre la privacidad y la seguridad del usuario, es necesario poner en marcha todos los mecanismos disponibles para garantizar la protección de esta información, que se transfiere desde los dispositivos físicos hacia Internet, quedando almacenada en sistemas gestionados por el proveedor.

Se considera "servicio" a toda funcionalidad asociada a la infraestructura de un proveedor con capacidades de integración entre diferentes componentes. La presente guía se centra en los servicios puestos a disposición por parte de Apple para los usuarios de dispositivos móviles o tradicionales vinculados a una cuenta de usuario de Apple denominada "ID de Apple" (Apple ID). Estos servicios requieren de acceso a redes de comunicaciones, e implican transferencia de datos entre el dispositivo propio y la nube de Apple, pudiendo involucrar en algunos casos, otros dispositivos propiedad de terceros.

La concienciación, el sentido común y las buenas prácticas en la configuración y el uso de los dispositivos móviles y sus servicios asociados constituyen una de las mejores defensas para prevenir y detectar este tipo de incidentes y amenazas de seguridad [Ref.- 402]. El usuario debe evaluar conveniente y concienzudamente qué servicios le son necesarios y de cuáles puede prescindir, securizando al máximo los primeros y desactivando los segundos.

Es importante reseñar que tanto la funcionalidad asociada a estos servicios como sus mecanismos de acceso y utilización no están bajo el control total del usuario, ya que son actualizados a criterio del proveedor. Debido a ello, son muy cambiantes, por lo que todos los aspectos tratados en la presente guía pueden sufrir variaciones en el futuro.

## 3. OBJETO

El propósito del presente documento es definir una lista de recomendaciones de seguridad y privacidad asociadas al uso de una cuenta de usuario de Apple como parte de la configuración de dispositivos basados en plataformas Apple (concretamente macOS, iOS, iPadOS y watchOS) cuyo objetivo es proteger tanto el propio dispositivo móvil y sus comunicaciones como los datos de usuario que se gestionan y almacenan en servidores externos de Apple y, muy en particular, la información de carácter más sensible y confidencial.

La presente guía complementa a las guías de la serie CCN-STIC-450, en particular, las vinculadas a plataformas del ecosistema Apple, y proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad y buenas prácticas necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles de Apple en virtud de los servicios existentes en la nube en la actualidad, y se ha redactado considerando como requisito el equilibrio entre

seguridad y funcionalidad, a fin de poder hacer uso de la mayoría de capacidades disponibles en los mismos de forma segura.

Adicionalmente, se recomienda la lectura de las guías CCN-CERT asociadas a plataformas móviles en general y a sistemas operativos Apple en particular, así como a servicios de otros fabricantes o proveedores:

- CCN-STIC-450 - Seguridad de dispositivos móviles [Ref.- 400]
- CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management) [Ref.- 401]
- CCN-CERT BP-03/16 - Buenas Prácticas: Dispositivos móviles [Ref.- 402]
- CCN-STIC- 455C - Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 11.x) [Ref.- 408]
- CCN-STIC- 455D - Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 12.x) [Ref.- 409]
- CCN-STIC-458 - Guía práctica de seguridad de macOS 10.14 Mojave [Ref.- 412]
- CCN-STIC-455E - Configuración segura de iOS 13 [Ref.- 413]
- CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android [Ref.- 405]
- CCN-CERT IA-03/20 - Informe de amenazas: Dispositivos y comunicaciones móviles [Ref.- 414]

## 4. ENTORNO DE APLICACIÓN DE ESTA GUÍA

Los contenidos de la presente guía son aplicables a los sistemas operativos de Apple vinculados a una cuenta de usuario de Apple como, por ejemplo, iOS (y de manera equivalente iPadOS) y macOS.

Los servicios de Apple analizados han sido probados y verificados sobre dos terminales iPhone SE[1] ejecutando iOS 13.2.2/13.3, un ordenador MacBook Pro Retina 13 pulgadas (de principios de 2015[2]) con macOS 10.15.2 (Catalina), configurados en idioma español, y un MacBook Air 13 pulgadas (de 2017) con macOS 10.14.6 (Mojave) configurado en inglés; pueden por tanto existir variaciones de configuración o uso en otros dispositivos o versiones de sistema operativo. Aunque la mayor parte de los apartados cubren tanto las plataformas móviles como las tradicionales, algunos ejemplos de configuración se proporcionan solo para iOS, por considerarse que los dispositivos móviles que suelen acompañar al usuario de asiduamente en todo tipo de situación (profesional y personal), están más expuestos a compromisos de seguridad y privacidad.

La elaboración de la presente guía corresponde con los servicios de Apple disponibles para los usuarios entre los meses de octubre a diciembre de 2019 y de enero a marzo de 2020.

## 5. CUENTAS ASOCIADAS A LOS SERVICIOS DE APPLE

Apple ofrece un amplio abanico de servicios, tanto en el ámbito profesional como en el personal y el familiar. La lista completa de servicios (así como su estado actual de funcionamiento) puede consultarse en la [Ref.- 4], por ejemplo, la App Store, FaceTime, Buscar mi iPhone o iCloud.

Es importante reseñar que existe cierta confusión a nivel conceptual sobre la relación entre el ID de Apple y la cuenta de iCloud, y que esta relación cambia de unas versiones de iOS y

[1] https://es.wikipedia.org/wiki/IPhone_SE
[2] https://www.applesfera.com/portatil/analisis-macbook-pro-13-2015

macOS a otras. La cuenta de iCloud es la que proporciona la mayor parte de servicios ofrecidos por defecto al usuario de Apple, y, en particular, los vinculados a la gestión de dispositivos y de compartición; por su parte, el ID de Apple puede emplearse en otros servicios, como la App Store, Apple TV+, o Apple Developers. Esto implica que es posible disponer en un mismo dispositivo de distintos ID de Apple, cada uno asociado a un servicio. Sin embargo, los interfaces de usuario son confusos ya que, mientras que en macOS 10.14 (Mojave) toda la configuración vinculada al ID de Apple se alberga bajo la sección "Preferencias del sistema - iCloud" (ver <Figura 2>), en macOS 10.15 (Catalina) existe una sección independiente bajo "Preferencias del sistema" denominada "ID de Apple" en la que se configura específicamente la cuenta de iCloud (ver <Figura 1 >). La opción "Cerrar sesión" de Mojave se ubica en "Preferencias del sistema - iCloud", mientras que en Catalina y en iOS se encuentra en "Preferencias del sistema - ID de Apple", y su invocación cerrará la sesión no solo en la cuenta de iCloud sino en cualquier otra cuenta que se haya dado de alta en el dispositivo, aunque esté vinculada a otro ID de Apple.

Por su parte, en iOS la sección "ID de Apple" dentro de "Ajustes" alberga la mayor parte de servicios de iCloud: aunque existe un submenú específico en esta sección denominado "iCloud", otros servicios vinculados inexorablemente a iCloud (como "Buscar" y "Dispositivos de confianza") caen fuera de dicho submenú y se ubican directamente en el menú "ID de Apple".

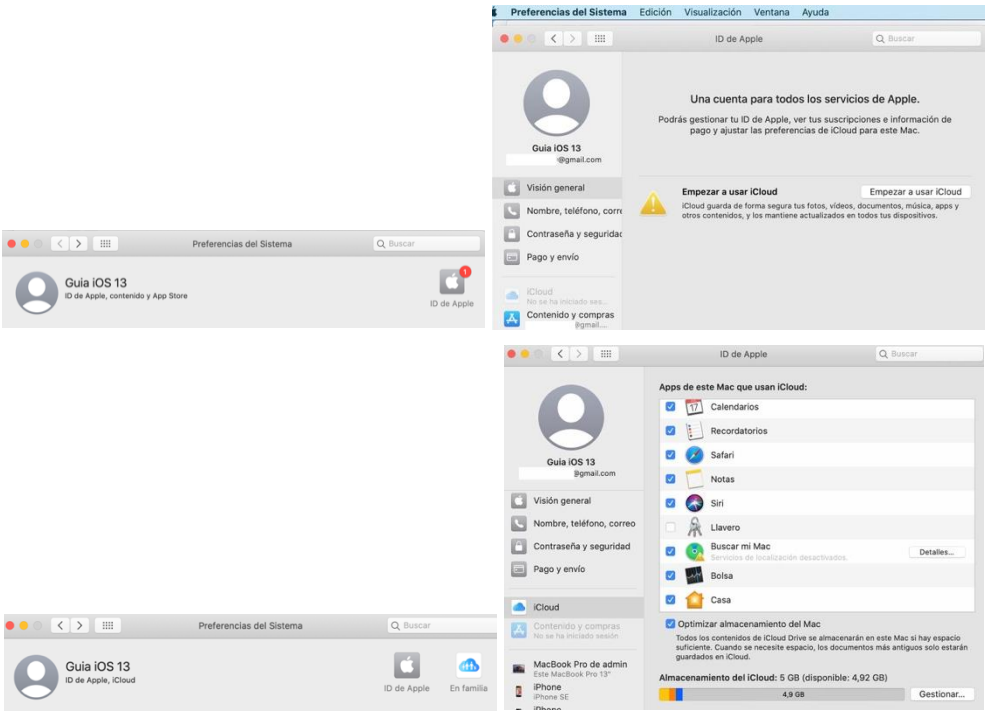



*Figura 1 - ID de Apple (sin asociar y asociado a una cuenta de iCloud) en macOS 10.15 (Catalina)*

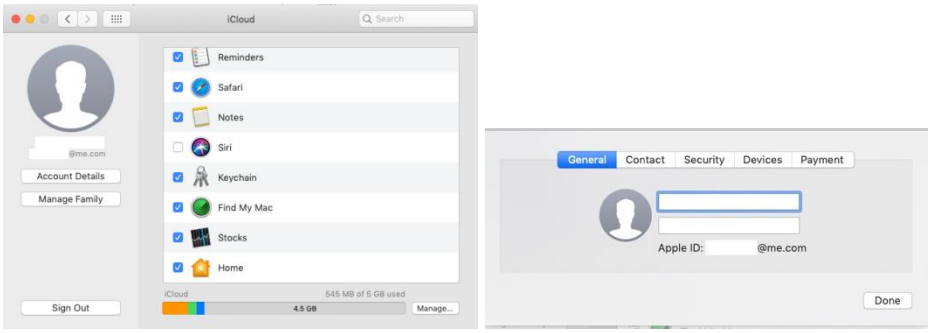



*Figura 2 - ID de Apple asociado a una cuenta de iCloud en macOS 10.14 (Mojave)*

**IMPORTANTE:** Para simplificar, a lo largo de la presente guía, y salvo que se especifique lo contrario, los términos ID de Apple y los relacionados con "sesión" harán referencia al ámbito de los servicios de iCloud.

Asimismo, el término "cuenta de iCloud" hará referencia al ID de Apple que se utiliza en el dispositivo para todos los servicios vinculados a iCloud.

## 5.1 ID DE APPLE

Recomendaciones de seguridad:

Dada la extrema sensibilidad de los servicios vinculados al ID de Apple, se recomienda proteger esta cuenta mediante:

- La no reutilización de las credenciales asociadas al ID de Apple para ningún otro servicio.
- Elección de una contraseña lo más robusta posible, preferiblemente de tipo "*passphrase*", que no debe anotarse en ningún medio, ni electrónico ni físico.
- Proteger el acceso a la cuenta de usuario mediante un segundo factor de autentificación (o 2FA, Two-Factor Authentication).
- En la medida de lo posible, emplear un ID de Apple exclusivo para los servicios de iCloud, independizándolo del resto de servicios, como el ID de Apple de la App Store.

### 5.1.1 QUÉ ES EL ID DE APPLE

El ID de Apple (o Apple ID) es una cuenta de usuario necesaria para acceder a servicios y productos de Apple. Consta de una dirección de correo electrónico (que actúa como identificador de la cuenta) y una contraseña.

En términos generales, se definirá un ID de Apple "principal"[3], que permitirá al dispositivo acceder a todos los servicios vinculados a iCloud, y potencialmente también a otros servicios como los de la App Store (e iTunes hasta macOS Mojave), salvo que el usuario decida utilizar otros IDs de Apple "secundarios" específicos para estos últimos.

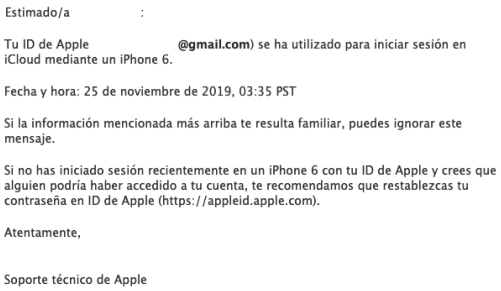
El ID de Apple "principal" (en adelante, "ID de Apple"), concretamente constituye el vínculo entre todos los dispositivos Apple del usuario. No es requisito indispensable para el acceso y

[3] Apple no cataloga los distintos IDs de Apple que puedan estar dados de alta en un dispositivo usando los términos "principal" ni "secundario". Se ha decidido utilizar esta terminología únicamente para clarificar que es posible tener varios IDs de Apple en el dispositivo, pero solo uno de ellos estará vinculado a los principales servicios disponibles, relacionados con iCloud.

uso de los dispositivos, pero sin él ciertos servicios no estarán disponibles (por ejemplo, la instalación y actualización de apps del mercado oficial o App Store).

Los eventos relevantes relativos al ID de Apple del usuario se notifican a través del correo electrónico de la cuenta asociada a dicho ID de Apple, entre ellos, los relativos a la seguridad de la cuenta, como inicios de sesión desde dispositivos que nunca han sido utilizados previamente para acceder a ella, o cambios en los datos personales. Desde el punto de vista de seguridad, ***se recomienda prestar especial atención a los mensajes de correo relativos a la actividad de la cuenta vinculada al ID de Apple, a fin de detectar con la máxima rapidez posible situaciones irregulares, pero siendo a su vez conscientes de la existencia de campañas de phishing que hacen uso de mensajes similares a estos para obtener detalles o comprometer la cuenta***.

En la [Ref.- 14] se describe los datos vinculados al ID de Apple que se almacenan en los servidores de Apple.



Estimado/a :

Tu ID de Apple @gmail.com) se ha utilizado para iniciar sesión en iCloud mediante un iPhone 6.

Fecha y hora: 25 de noviembre de 2019, 03:35 PST

Si la información mencionada más arriba te resulta familiar, puedes ignorar este mensaje.

Si no has iniciado sesión recientemente en un iPhone 6 con tu ID de Apple y crees que alguien podría haber accedido a tu cuenta, te recomendamos que restablezcas tu contraseña en ID de Apple (https://appleid.apple.com).

Atentamente,

Soporte técnico de Apple

*Figura 3 - Notificación de evento de seguridad vinculado al ID de Apple*

### 5.1.2 ALTA DEL ID DE APPLE

Cuando se intente dar de alta en un nuevo dispositivo un ID de Apple que ya está siendo utilizado en otros dispositivos, será preciso autorizar el ingreso del nuevo dispositivo en cualquiera de los que ya sean considerados "de confianza" (ver apartado "5.1.6. Dispositivos de confianza").

Complementariamente, debido a la función "Bloqueo de activación" (ver apartado "5.2.1. Bloqueo de activación"), podrá solicitarse el código de desbloqueo de otro dispositivo.

#### 5.1.2.1 Alta del ID de Apple en iOS

Si el ID de Apple no se dio de alta durante el proceso de configuración inicial del ordenador, es posible añadirlo desde "Ajustes - Iniciar sesión en el iPhone" (<Figura 6>).

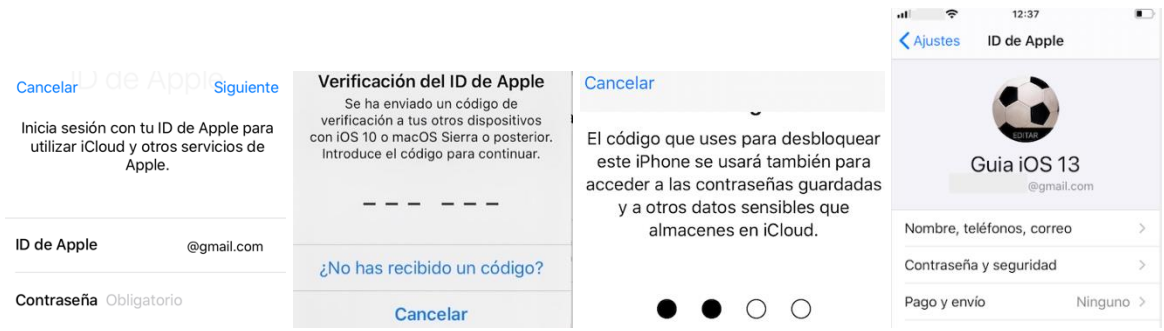



*Figura 4 - Configuración del ID de Apple en iOS 13*

#### 5.1.2.2 Alta del ID de Apple en macOS

Si el ID de Apple no se dio de alta durante el proceso de configuración inicial del ordenador, es posible añadirlo desde "Preferencias del sistema - Inicia sesión con el ID de Apple", y seguir los pasos del asistente. Si la cuenta ya dispone de dispositivos de confianza (ver apartado "5.1.6. Dispositivos de confianza"), será necesario aprobar el ingreso del Mac en cualquiera de ellos, y luego introducir en éste el código de autorización. Si la cuenta no está configurada con segundo factor de autentificación, se deberá proporcionar el código recibido a través de un mensaje SMS.

Tras la comprobación de los datos anteriores, la cuenta quedará dada de alta en el Mac y se interrogará al usuario sobre su autorización para habilitar el servicio "Buscar mi Mac" (ver apartado "6. Gestión remota de dispositivos: Servicio "Buscar"").

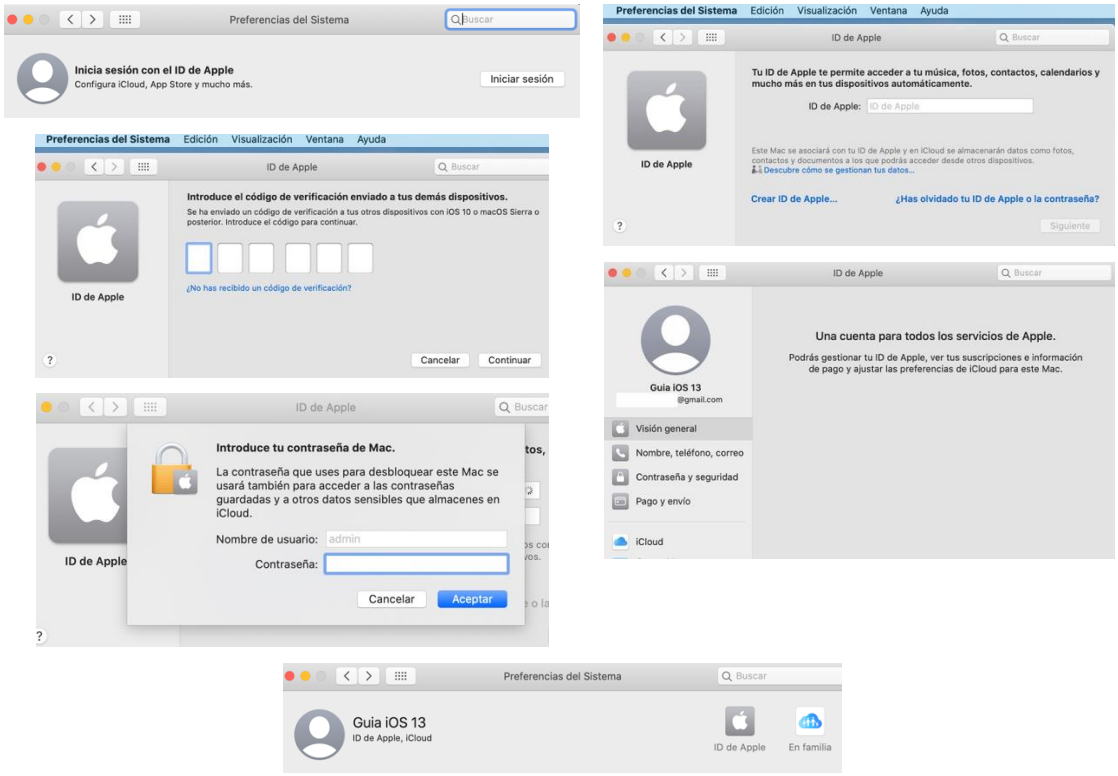



*Figura 5 - Configuración del ID de Apple en macOS*

### 5.1.3 CREACIÓN DE UN NUEVO ID DE APPLE

La creación de un nuevo ID de Apple se puede realizar:

- iOS:
  - Durante el proceso de activación de un nuevo dispositivo: ver apartado "Proceso de activación del dispositivo móvil" de la guía "Configuración segura de iOS 13" [Ref.- 413].
  - Desde el interfaz móvil accesible desde "Ajustes - Inicia sesión en el iPhone":

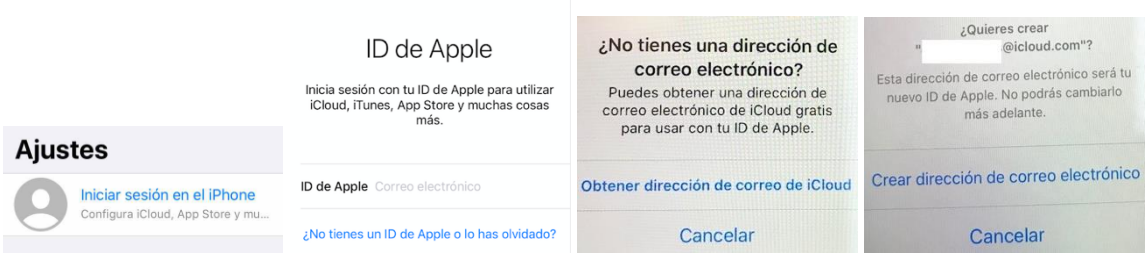



*Figura 6 - Creación de un ID de Apple desde un iPhone*

- macOS:
  - Durante la instalación inicial del Mac o su reinstalación tras haber sido restaurado a fábrica.
  - Cuando un nuevo usuario dado de alta en el sistema ingresa por primera vez: ver apartado "Apple ID" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.-412].

**NOTA:** durante el proceso de alta de un ID de Apple, se ofrece al usuario tanto utilizar una dirección de correo ya existente como la posibilidad de crear una cuenta de correo electrónico en el dominio "icloud.com" (ver <Figura 4>).

- A través del interfaz web de https://appleid.apple.com/account#!&page=create. El usuario debe proporcionar una dirección de e-mail ya existente, seleccionar una contraseña, y rellenar las preguntas de seguridad, junto a su fecha de nacimiento.

**IMPORTANTE:** la contraseña proporcionada durante la creación de un ID de Apple nunca debe coincidir con la contraseña de la cuenta de correo electrónica que se vincule a él. Se recomienda seleccionar una contraseña robusta, suficientemente larga, y, preferiblemente, de tipo "*passphrase*" (frase de paso), en vez de una "*password*" (palabra de paso).

Una vez rellenos los campos requeridos, se enviará un mensaje con el código de validación a la dirección de correo electrónico especificada, el cual deberá introducirse para que la creación de la cuenta de usuario de Apple sea efectiva. Tras la creación de la cuenta, se mostrará su interfaz de gestión.

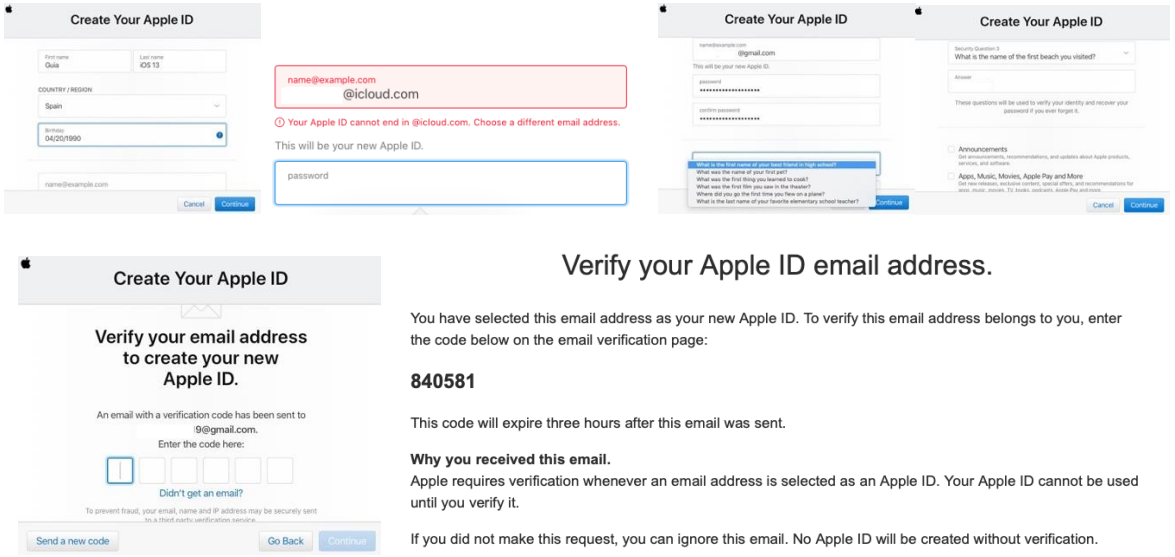



*Figura 7 - Creación de un ID de Apple desde el interfaz web*

El restablecimiento a fábrica de un dispositivo requiere introducir la contraseña vinculada al ID de Apple.

### 5.1.4 SEGUNDO FACTOR DE AUTENTIFICACIÓN (2FA)

**NOTA:** en la [Ref.- 5] se proporciona el enlace a la página de soporte de Apple que detalla la configuración del segundo factor de autentificación (2FA) en una cuenta de usuario de Apple.

Se distinguen dos escenarios para el establecimiento de un 2FA vinculado a un nuevo ID de Apple:

1) Si el dispositivo dispone de una tarjeta SIM, el número de teléfono vinculado a ella se ofrecerá como mecanismo de 2FA (mediante SMS o llamada de teléfono). Se permite sustituir este número de teléfono por otro, pero no prescindir por completo de él.

2) Si el dispositivo no dispone de tarjeta SIM, por defecto no se habilitará el 2FA, siendo necesario activarlo posteriormente accediendo a los ajustes de un dispositivo vinculado a dicho ID de Apple (sección "Ajustes - Contraseña y seguridad" en dispositivos iOS y "Preferencias del sistema - iCloud - Detalles de la cuenta - [Seguridad] Segundo factor de autentificación" en equipos macOS):

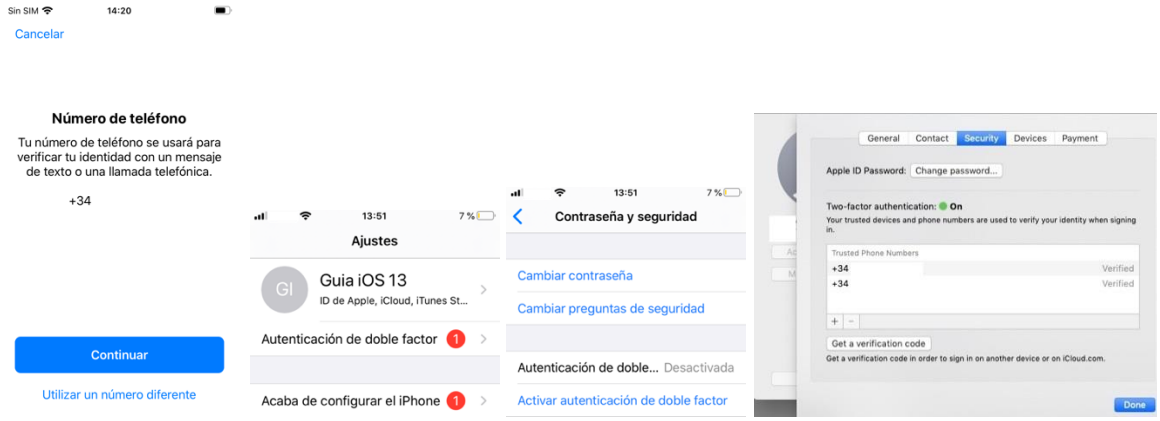



*Figura 8 - Establecimiento de un número de teléfono como 2FA*

**NOTA:** si durante el proceso de adición del 2FA en un dispositivo se identifica que algún otro de los dispositivos vinculados a la cuenta del usuario dispone de tarjeta SIM, se ofrecerá directamente al usuario utilizar ese número como 2FA (imagen izquierda de la <Figura 8>).

Adicionalmente, al añadir el 2FA se solicitará también respuesta a dos de las tres preguntas de seguridad que el usuario haya definido. Una vez más, se destaca la importancia de proteger el contenido de dichas respuestas (y no necesariamente responder fielmente a las preguntas planteadas).

Una vez configurado, el 2FA se requerirá para todas aquellas operaciones que impliquen interacción con acceso al ID de Apple (por ejemplo, vincular un nuevo dispositivo). El 2FA solo podrá desactivarse en las dos semanas siguientes a su activación [Ref.- 5], a través del enlace "volver a los ajustes de seguridad anteriores" proporcionado en el correo electrónico durante su alta (no es posible deshabilitarlo desde el dispositivo móvil). El usuario será redirigido al interfaz iforgot.apple.com, desde el cual le será obligatorio cambiar la contraseña de la cuenta para proceder a la desactivación del 2FA.

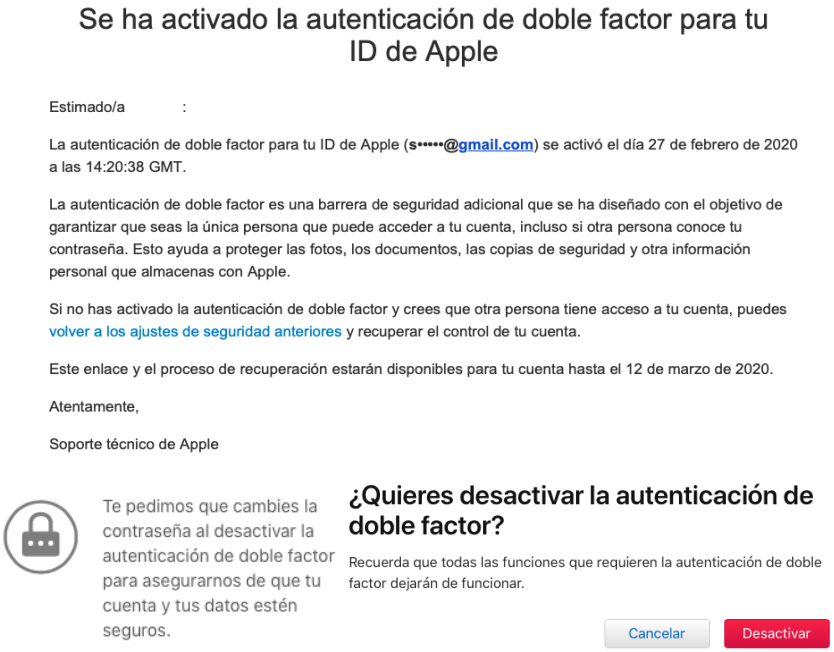
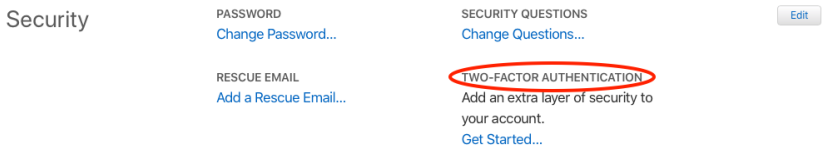



*Figura 9 - Desactivación del 2FA*

Con el 2FA activado, el usuario ya no tendrá que responder a las preguntas de seguridad al iniciar sesión en un nuevo dispositivo. Apple afirma que, transcurridas las dos semanas mencionadas anteriormente, eliminará las preguntas de seguridad de sus sistemas.

**IMPORTANTE:** al dar de alta un número de teléfono como 2FA, el interfaz ofrece la opción de *mensaje de texto* (SMS) o *llamada telefónica* como medios para obtener el código de validación. Se recomienda utilizar "llamada telefónica", dado que el mensaje de texto podría ser visualizado por un tercero con acceso visual al dispositivo sin que el propietario sea consciente de ello.



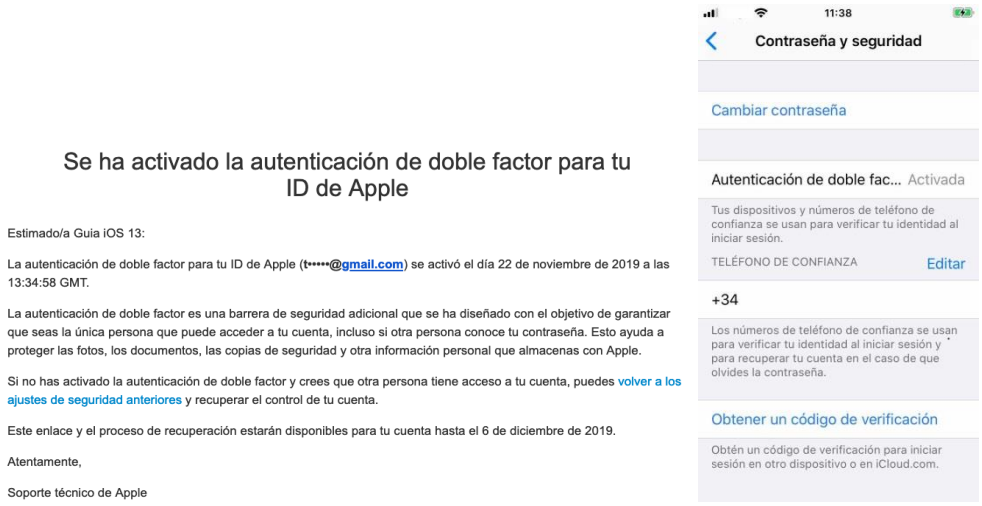



*Figura 10 - Configuración de un 2FA para el ID de Apple*

### 5.1.5 ALIAS DEL ID DE APPLE

Cuando se activa el correo electrónico de iCloud para una cuenta del dominio @icloud.com, la dirección de correo se añade como un "alias" de inicio de sesión al ID de Apple. En servicios como iMessage y FaceTime, el alias puede utilizarse para buscar usuarios y establecer conexiones con ellos.

Los alias vinculados a un ID de Apple se pueden consultar en el interfaz https://appleid.apple.com/account/manage posicionando el cursor sobre los iconos "". Desde ese interfaz es posible añadir nuevos alias, los cuales deben haber sido añadidos previamente como alias de iCloud Mail (ver apartado "5.2.3. Alias de correo").

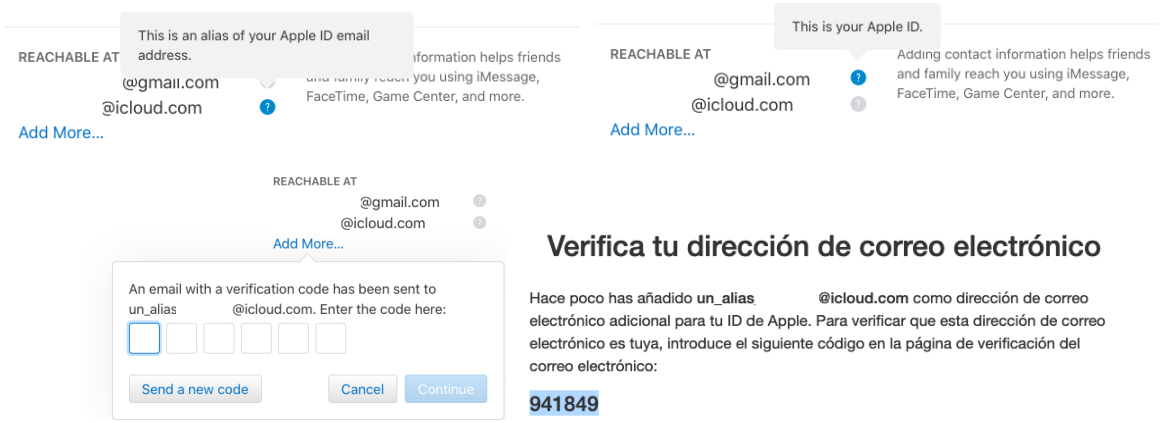



*Figura 11 - Alias del ID de Apple*

Cuando se añade un nuevo alias al ID de Apple, en los dispositivos de confianza de la cuenta se recibirá una notificación para consultar al usuario si desea utilizar dicho alias para sus comunicaciones de iMessage y FaceTime.




*Figura 12 - Notificación para aceptar un alias del ID de Apple en iMessage y FaceTime*

### 5.1.6 DISPOSITIVOS DE CONFIANZA

**Recomendaciones de seguridad:**

- Asegurarse de eliminar de la cuenta vinculada al ID de Apple cualquier dispositivo que deje de pertenecer al usuario.
- Prestar especial atención a solicitudes de acceso a la cuenta de usuario por parte de nuevos dispositivos.

Aquellos dispositivos en los que se ha iniciado sesión tras la validación de un 2FA pasan a ser considerados dispositivos "de confianza", y ya no será necesario introducir en ellos el 2FA a partir de ese momento, a menos que se borren sus contenidos, se cierre sesión en iCloud, o se cambie la contraseña. Complementariamente, cuando se intente iniciar sesión para el ID de Apple desde un dispositivo nuevo, se recibirá en todos los dispositivos de confianza vinculados al ID de Apple un mensaje solicitando confirmación; si se acepta, aparecerá el código de verificación que deberá ser introducido en el nuevo dispositivo.

Para obtener la lista de dispositivos de confianza, se debe acceder al menú "Preferencias del sistema - iCloud - Detalles de la cuenta - Dispositivos" (macOS) o a "Ajustes - ID de Apple" (iOS).

El nombre con el que el dispositivo se muestra en el listado de dispositivos de confianza es el que figura en "Ajustes - General - Información" (iOS) o el denominado "Nombre del ordenador" (*ComputerName*) (macOS, ver apartado "Nombre del equipo" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412]).

La opción "Obtener un código de verificación" en un dispositivo de confianza permite que se genere un código de 2FA que puede introducirse en otro dispositivo o navegador web en el que se esté intentando iniciar sesión con la cuenta de usuario de Apple.



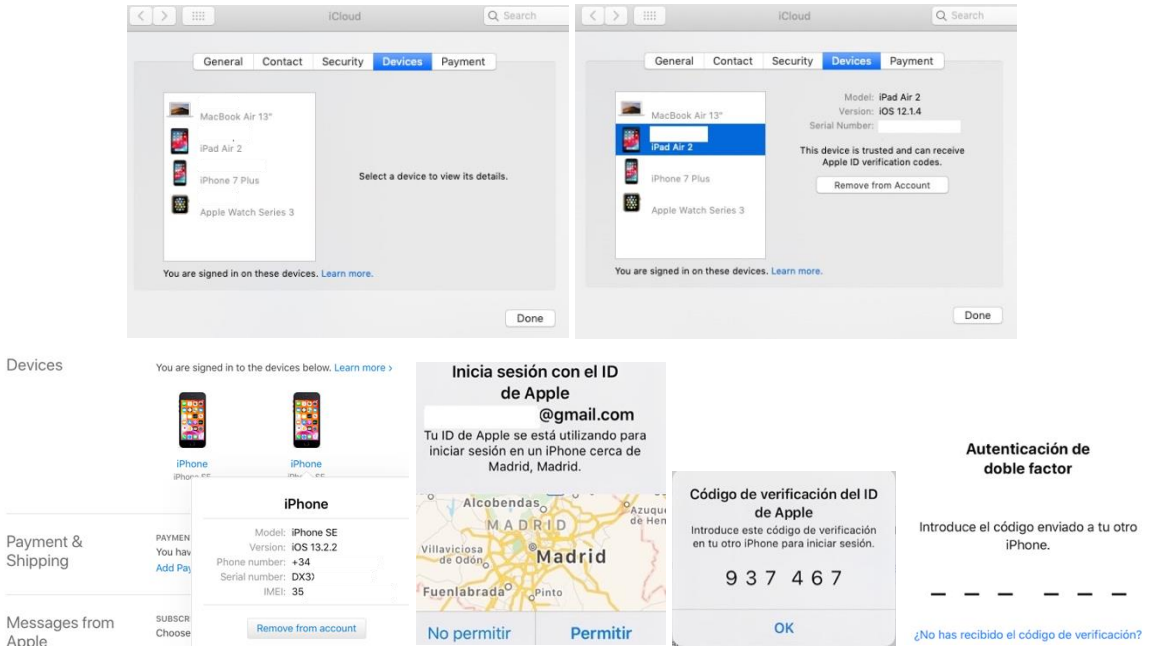



*Figura 13 - ID de Apple protegido con 2FA*

A fecha de elaboración de la presente guía, no existe ningún mecanismo conocido para que el usuario catalogue sus dispositivos y elija selectivamente el subconjunto que quiere considerar "de confianza" para recibir códigos de validación y aprobar solicitudes de ingreso en el servicio de Apple ID. Ni siquiera al deshabilitar el servicio "Buscar mi iPhone" / "Buscar mi Mac" el dispositivo dejará de ser de confianza.

Un dispositivo solo dejará de ser de confianza si se elimina de la cuenta de usuario de Apple, bien accediendo a ella desde un navegador web de confianza, bien desde el correspondiente menú de "Información del dispositivo" de otro dispositivo iOS (<Figura 15>) o "Mis dispositivos" de macOS; el dispositivo puede volver a aparecer en la lista si tenía sesión abierta en la cuenta y accede a Internet después de haber sido eliminado [Ref.- 9]. Por tanto, el único modo de garantizar que un dispositivo deja de ser de confianza es cerrar sesión en él y eliminarlo de la cuenta de usuario de Apple.

**NOTA:** en ocasiones, si los contenidos de un dispositivo han sido borrados de forma local sin haber cerrado previamente sesión en la cuenta de iCloud, el bloqueo de activación seguirá vigente en el dispositivo, y éste seguirá perteneciendo a los dispositivos de confianza de la cuenta de usuario de Apple. Para desvincularlo de ella una vez el equipo ya no es visible para iCloud (no se puede establecer comunicación con él a través de Internet), se puede pulsar en el símbolo "(x)" a la derecha del nombre del equipo.

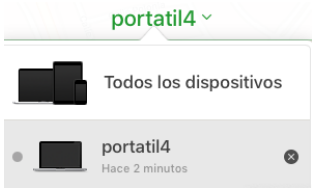



*Figura 14 - Eliminación de un dispositivo de la cuenta de iCloud*

El acceso a la cuenta de usuario o ID de Apple desde un navegador web de un ordenador interrogará al usuario para determinar si ese navegador también se quiere incluir en la lista de confianza, de forma que futuros accesos a la cuenta a través suyo no requieran la introducción

del 2FA (imagen izquierda de la <Figura 15>). ***Desde el punto de vista de seguridad, se recomienda no confiar en el navegador web, sino validar siempre el acceso al ID de Apple a través del 2FA.***

Desde el punto de vista de seguridad, se recomienda prestar atención a los mensajes de inicio de sesión para detectar cualquier acceso no permitido a la cuenta de usuario vinculada al ID de Apple. Asimismo, si un dispositivo considerado de confianza deja de serlo (en especial, si ha sido sustraído), o si se requiere acceder temporalmente a la cuenta de usuario desde un dispositivo ajeno, se recomienda proceder a "Eliminar de la cuenta" dicho dispositivo tan pronto sea posible.

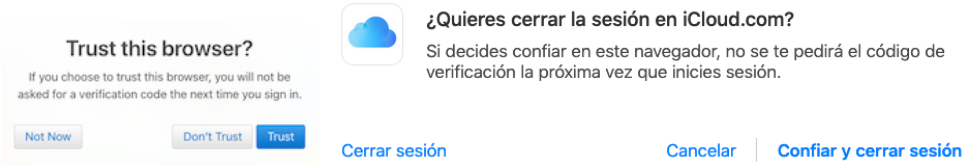



*Figura 15 - Gestión de navegadores web y dispositivos de confianza*

### 5.1.7 IFORGOT: RESTABLECIMIENTO DE UNA CONTRASEÑA OLVIDADA

iForgot es un servicio que permite restablecer la contraseña vinculada al ID de Apple [Ref.- 7]. Ofrece tanto un interfaz web (<Figura 16>) como un interfaz móvil (<Figura 17>).

#### 5.1.7.1 Restablecimiento de la contraseña del ID de Apple sin 2FA

Si la cuenta de usuario de Apple no está protegida con un 2FA (opción desaconsejada), uno de los mecanismos de verificación que se ofrecen para restablecer la contraseña se basa en la fecha de nacimiento y las respuestas a las preguntas de seguridad. Dado que responder a estas preguntas con información veraz puede implicar que las respuestas sean conocidas por terceros (hay mucha información personal públicamente disponible si se hace uso de redes sociales, o por mero conocimiento del individuo), ***se recomienda proporcionar siempre respuestas falsas***, que no tengan ninguna relación con la pregunta planteada, haciendo imposible su adivinación. Adicionalmente, dado que el texto de las respuestas se muestra en claro en la pantalla, ***nunca debe introducirse esta información*** en presencia de terceros.

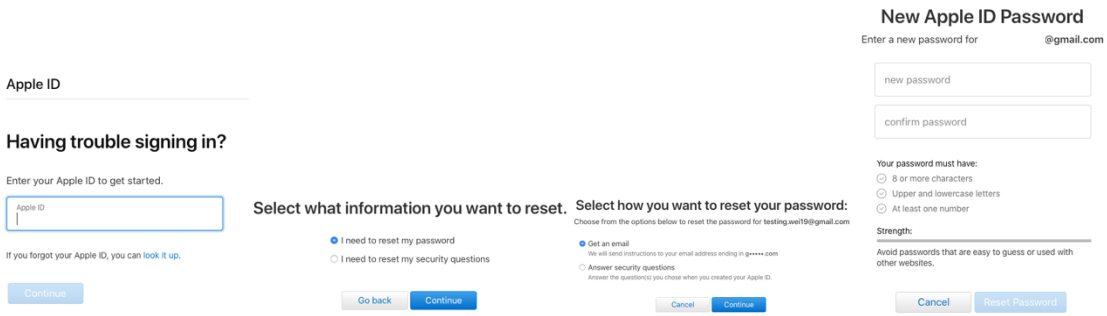



*Figura 16 - Servicio iForgot para restablecer la contraseña del ID de Apple desde el interfaz web*

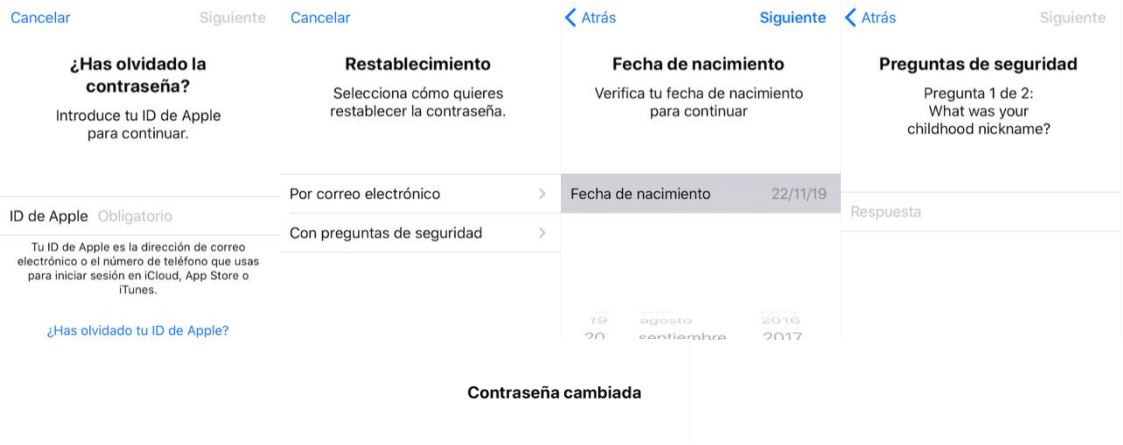



*Figura 17 - Servicio iForgot para restablecer la contraseña del ID de Apple sin 2FA desde un iPhone con iOS 13*

**IMPORTANTE:** en las pruebas realizadas durante la elaboración de la presente guía, se ha comprobado el siguiente escenario:

- Se dispone de un iPhone con iOS 13 en el que está dado de alta un ID de Apple con una sesión activa.
- Se accede de forma exitosa al interfaz web de iForgot para resetear la contraseña del ID de Apple basándose únicamente en las preguntas de seguridad.
- El iPhone comienza a presentar pantallas y notificaciones solicitando la introducción de la nueva contraseña (imagen izquierda de la <Figura 18>).
- Se constata que, aunque la nueva contraseña del ID de Apple no se actualice en el iPhone, el servicio "Buscar mi iPhone" es capaz de localizar el dispositivo móvil si éste tiene la ubicación activa; si tiene conexión de datos pero no ubicación, el servicio "Buscar mi iPhone" puede determinar si está online (imagen central de la <Figura 18>) o no (imagen derecha de la <Figura 18>).

El anterior escenario implicaría que las sesiones que estén abiertas en los dispositivos de confianza se mantienen en este estado, incluso aunque se cambie la contraseña del ID de Apple y no se actualice en dichos dispositivos. Esto constituye una ventaja de seguridad ante la sustracción de un dispositivo, ya que el propietario legítimo del dispositivo podría ***cambiar la contraseña para proteger la cuenta*** (acción necesaria desde el punto de vista de seguridad) pero todavía podría hacer uso del servicio "Buscar mi iPhone" para poder localizar el dispositivo móvil mientras el iPhone mantenga la conectividad.

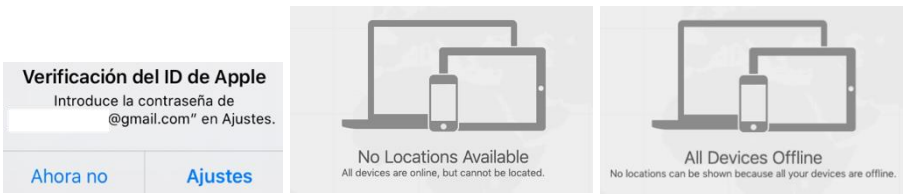



*Figura 18 - Servicio "Buscar mi iPhone" tras cambiar la contraseña del ID de Apple y no actualizarla en el dispositivo*

### 5.1.7.2 Restablecimiento de la contraseña del ID de Apple con 2FA

Si la cuenta está protegida con 2FA, el menú "*Cambiar contraseña*" disponible en iOS bajo "*Ajustes - [Entrada ID de Apple, iCloud, iTunes Store…] Contraseña y seguridad*" o en macOS bajo "*Preferencias del sistema - iCloud - Detalles de la cuenta - [Seguridad]*" (<Figura 8>)

permitirá modificar la contraseña vinculada al ID de Apple previa introducción del método de acceso al dispositivo.

Se recomienda cerrar sesión en los demás dispositivos tras cambiar la contraseña del ID de Apple.

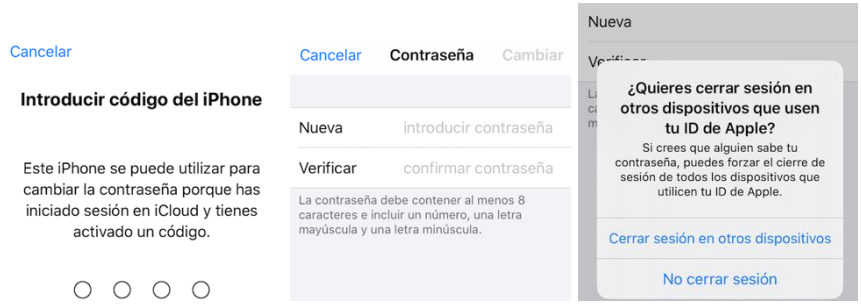



*Figura 19 - Modificación de la contraseña del ID de Apple con 2FA desde iOS 13*

**IMPORTANTE**: durante las pruebas realizadas en la elaboración de la presente guía, se ha constatado que, si el 2FA fue activado en un plazo inferior a dos semanas, es posible restablecer la contraseña vinculada al ID de Apple desde un dispositivo que **no es de confianza**, incluso llegar a desactivar el 2FA, sin más que conocer la fecha de nacimiento definida por el propietario y responder a dos preguntas de seguridad. El menú de restablecimiento de la contraseña permite incluso ignorar el número de teléfono en el que se confió. Este hecho se ilustra en la <Figura 20>. Ninguno de los dispositivos de confianza recibirá alerta o notificación alguna sobre este hecho.

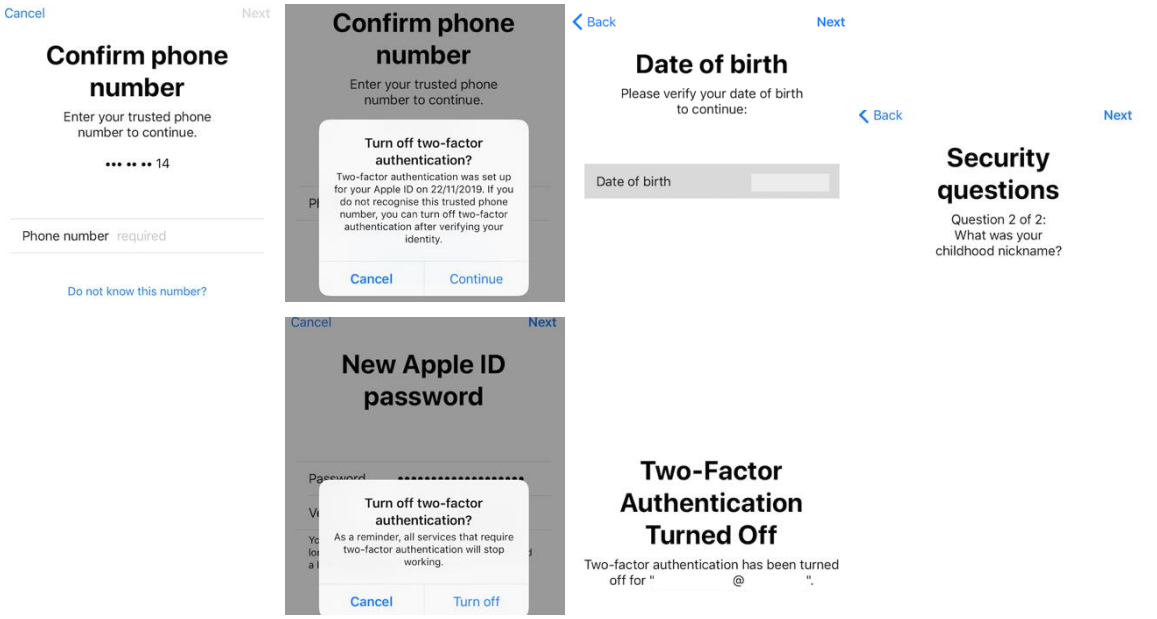



*Figura 20 - Intento de restablecimiento de la contraseña desde un iPhone ajeno a la cuenta*

Si la antigüedad de la activación del 2FA es mayor a dos semanas, el intento de restablecimiento de la contraseña vinculada al ID de Apple requerirá confirmación del número de teléfono de confianza y de una de las dos opciones siguientes:

- Acceso autorizado al dispositivo en el que se dio de alta la cuenta de usuario de Apple (segunda imagen de la <Figura 21>).

- Acceso a los mensajes SMS asociados al número de confianza para poder obtener e introducir un código de verificación (tercera y cuarta imagen de la <Figura 21>).

Seguidamente, habrá que introducir el método de desbloqueo del dispositivo de confianza de la cuenta de usuario de Apple.

Si no se puede realizar ninguna de las validaciones anteriores y se selecciona "No puedo usar este número", o se desconoce la contraseña del dispositivo de confianza, se iniciará un procedimiento especial que requerirá interacción con el soporte de Apple (última imagen de la <Figura 21>).

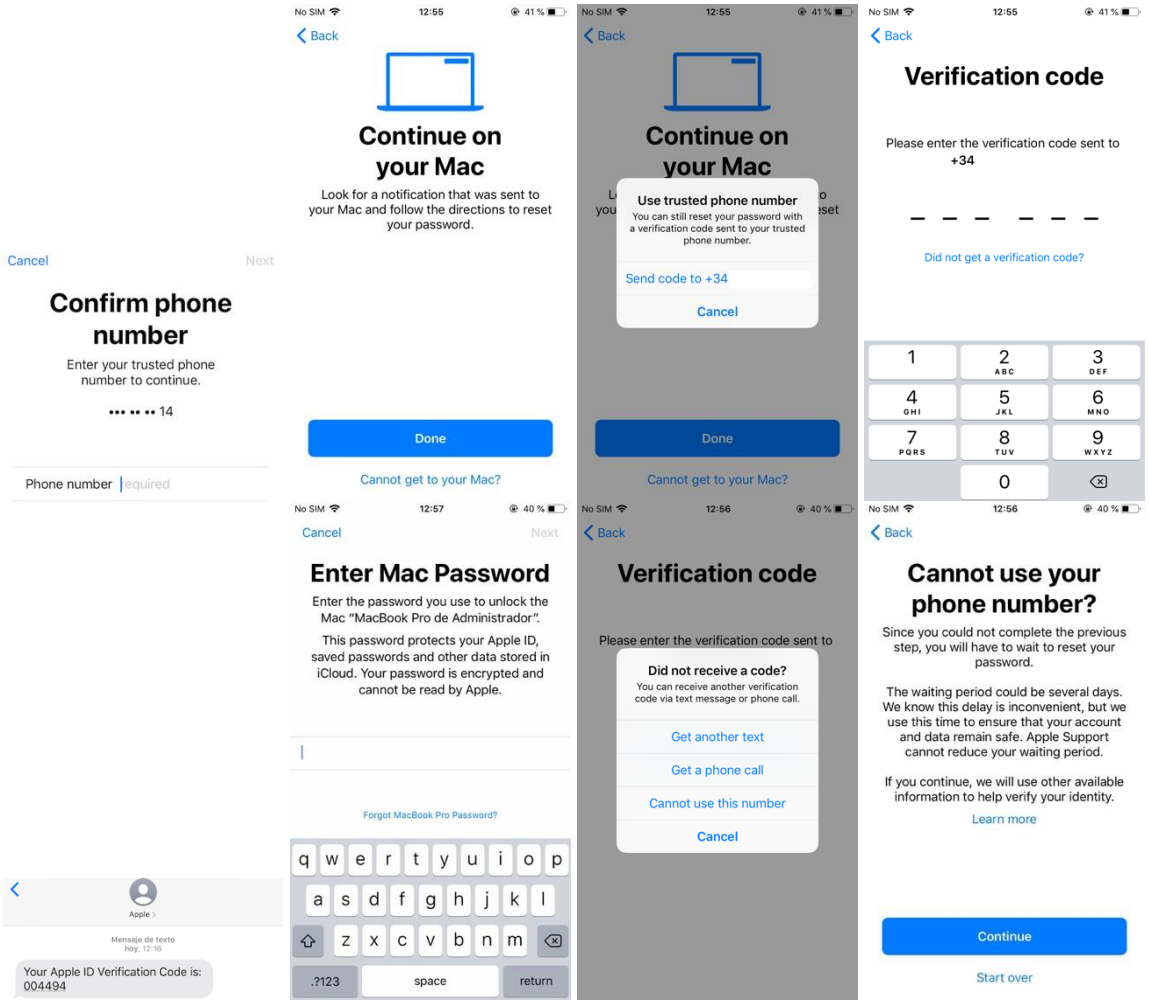



*Figura 21 - Intento de restablecimiento de contraseña con 2FA de antigüedad mayor a 2 semanas*

### 5.1.8 AJUSTES DE LA CUENTA ASOCIADA AL ID DE APPLE

Es posible gestionar la cuenta correspondiente al ID de Apple, tanto a través del interfaz web (enlace "Manage", ver <Figura 22>) como desde un dispositivo físico.

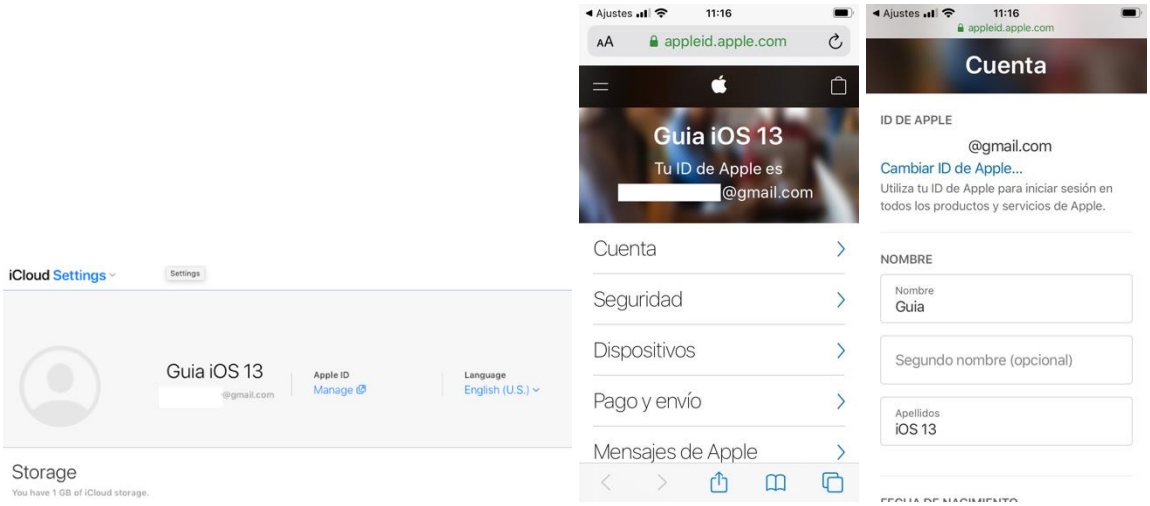



*Figura 22 - Gestión de un ID de Apple*

Para dispositivos iPhone, los ajustes se despliegan al seleccionar el primer campo con el nombre y el e-mail de la cuenta de usuario de Apple.

En versiones de iOS hasta iOS 12 inclusive, si se empleaba una cuenta para los servicios de iCloud distinta a la de los servicios de iTunes/App Store, se mostraban las dos direcciones bajo el nombre del propietario de la cuenta. En iOS 13 solo se muestra la dirección asignada a la cuenta de iCloud, siendo necesario consultar los valores de las entradas "Suscripciones" y/o "iTunes y App Store" para ver las cuentas en uso (imagen central de la <Figura 23>). Si ambas cuentas coinciden, aparecerá la imagen izquierda de la <Figura 23>. En este último caso, desde el menú "Ajustes - iTunes Store y App Store - [Pinchar sobre la entrada <ID de Apple>] - Ver ID de Apple", es posible acceder también a los ajustes del ID de Apple (primera imagen de la <Figura 24>).




*Figura 23 - Configuración de cuenta de usuario de Apple, ID de Apple, asociada al dispositivo*

Las recomendaciones de seguridad (más relevantes) asociadas a los distintos campos de estas subsecciones se proporcionan a continuación. La consulta y/o modificación de algunos de ellos (por ejemplo, el "Nombre") puede requerir la autentificación del usuario a través de la contraseña asociada a la cuenta, el código de acceso del dispositivo, y/o la introducción del 2FA (si está activo).

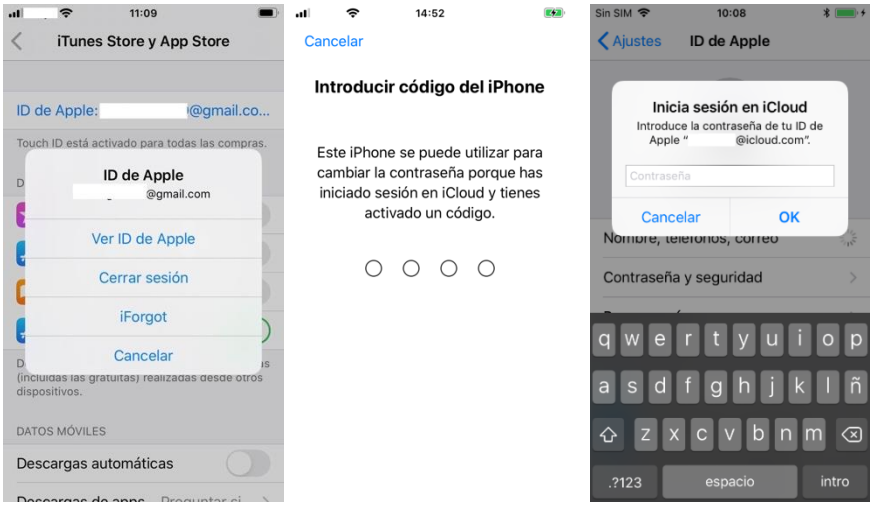



*Figura 24 - Solicitud de autentificación en la cuenta del usuario de Apple*

**Nombre, teléfonos, correo**

Desde el punto de vista de privacidad, ***se desaconseja utilizar una foto de perfil*** que vincule al propietario con su identidad real. ***Se aconseja desactivar*** los campos "Anuncios" y "Apps, música, películas, Apple Pay…" de la sección "Nombre, teléfonos, correo".

**Contraseña y seguridad**

La contraseña de la cuenta de usuario de Apple es el elemento fundamental para su protección y la de todos los servicios vinculados a ella, por lo que ***se recomienda seleccionar una contraseña robusta, suficientemente larga, y, preferiblemente, de tipo "passphrase"*** *(frase de paso), en vez de una "password" (palabra de paso).*

- "Cambiar contraseña": se recomienda cambiar periódicamente la contraseña, en especial, si existe sospecha de compromiso (por mínimo que sea) por parte de un tercero.
- "Autenticación de doble factor" (2FA): descrito en el apartado "5.1.4. Segundo factor de autentificación (2FA)").
- "Teléfono de confianza" (ver imagen derecha de la <Figura 23>): A través de "Editar", se permite eliminar el número actual y/o añadir otros números adicionales.
- "Obtener un código de verificación": una vez que el dispositivo forma parte de los dispositivos de confianza asociados a la cuenta de iCloud, se pueden generar en él códigos de autorización de acceso a la cuenta para dispositivos no vinculados a ella.

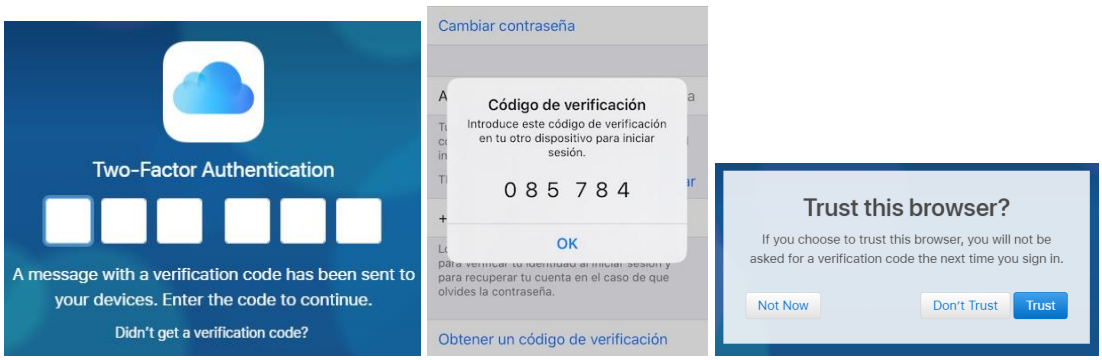



*Figura 25 - Segundo factor de autentificación de la cuenta de iCloud.*

**Pago y envío**

Ver apartado "9. Apple Pay".

### 5.1.9 INICIAR SESIÓN CON APPLE - "SIGN IN WITH APPLE"

La funcionalidad denominada "Iniciar sesión con Apple" (*Sign in with Apple*)[4] permite al usuario utilizar su ID de Apple para acceder a los servicios de apps y sitios web que soporten este tipo de identificador para sus mecanismos de autentificación, en vez de tener que crear un nuevo perfil de usuario en el servicio objetivo. Este servicio puede utilizarse tanto en plataformas Apple (iOS y macOS) como Android y Windows. Una app soporta esta funcionalidad si el desarrollador ha obtenido el "App Id" para ella asociando las capacidades de iniciar sesión con Apple, y configura las claves, identificadores y perfiles necesarios en su cuenta de desarrollador[5].

Según indica Apple en su página web de soporte [Ref.- 15], el principal beneficio de esta funcionalidad es proteger la privacidad del usuario, ya que evita que los servicios de apps y sitios web puedan rastrearle. Apple solo compartirá con la app o el sitio web el nombre y la dirección de correo del usuario (frente a Google, que puede compartir la fotografía de perfil y otra información de la cuenta de usuario). Adicionalmente, para aquellas apps y sitios web que requieran que el usuario proporcione una dirección de e-mail, Apple ofrece la opción "Ocultar mi correo electrónico", que genera direcciones de correo únicas y aleatorias cuyo formato es "*<cadena-alfanumérica-única>@privaterelay.appleid.com*" [Ref.- 16], y que Apple vincula de forma interna con la cuenta de iCloud del usuario, de forma que cualquier comunicación que se reciba a esta cuenta le será reenviada a su dirección de correo personal de forma transparente.

**NOTA:** durante las pruebas realizadas durante la elaboración de la presente guía, se constata que la opción para ocultar el correo electrónico no está disponible para todas las apps (ver tercera imagen de la <Figura 26>).

La funcionalidad "Iniciar sesión con Apple" requiere que el ID de Apple disponga de autentificación de doble factor (2FA) y que se haya iniciado sesión en la cuenta de iCloud en el dispositivo; el usuario deberá validar el inicio de sesión a través de un método de desbloqueo biométrico (Touch ID/Face ID) o en su defecto del método de desbloqueo tradicional del dispositivo móvil. Las apps o sitios que soporten la funcionalidad mostrarán un botón "Continuar con Apple" en el inicio de sesión.

[4] El mecanismo "Sign in with Apple" está basado en OAuth 2.0 y OpenID Connect (https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth)
[5] https://developer.apple.com/sign-in-with-apple/get-started/




*Figura 26 - "Iniciar sesión con Apple" (Sign in wih Apple)*

A fecha de elaboración de la presente guía, son pocas las apps que incluyen esta funcionalidad. Sin embargo, Apple ha establecido el 20 de abril del 2020 como fecha límite para que apps y sitios web que ofrecen inicios de sesión a través de otras plataformas de terceros (*Single Sign On*, SSO, como Google, Facebook, Twitter, Amazon, etc.), incluyan "Iniciar sesión con Apple"[6].

Para consultar las apps que están utilizando el servicio, se puede acceder al menú "Seguridad - Apps y sitios web que usan el id de Apple - Gestionar" del interfaz web https://appleid.apple.com/account/manage.

En el documento de la [Ref.- 17] (no oficial) se proporcionan detalles técnicos sobre esta funcionalidad.

## 5.2 CUENTA DE ICLOUD

iCloud es un servicio multiplataforma de Apple en la nube [Ref.- 6] destinado inicialmente a proporcionar un lugar para el almacenamiento de diversa información por parte de otros servicios de Apple (como "Fotos", "Contactos" y "Copia de seguridad en iCloud"), de forma que pueda ser compartida por todos los dispositivos vinculados al mismo ID de Apple. La cuenta de iCloud está directamente ligada al ID de Apple, ya que se toma como cuenta de iCloud la que se defina como ID de Apple en los dispositivos.

Cuando un usuario inicia sesión en iCloud, se crea y almacena en sus dispositivos una identidad RSA de 2.048 bits, que se utilizará en servicios como AirDrop [Ref.- 21].

La principal utilidad de la cuenta de iCloud desde el punto de vista de seguridad es la vinculación que el servicio "Buscar" ("Buscar mi Mac" en macOS) tiene de ella (ver apartado "6. Gestión remota de dispositivos: Servicio "Buscar"").

Respecto al resto de servicios de Apple, se recomienda valorar cuidadosamente la sensibilidad de la información asociada a ellos, y deshabilitar la sincronización para aquellos cuyos datos no se desea almacenar en la nube de Apple. Desde el punto de vista de seguridad, los servicios más importantes se describen a continuación. Para que dichos servicios estén disponibles, la sesión en iCloud debe mantenerse abierta en el dispositivo. Por otro lado, Apple proporciona también capacidades de almacenamiento y sincronización de datos en la nube a través de

[6] New Guidelines for Sign in with Apple: https://developer.apple.com/news/?id=09122019b

iCloud para los desarrolladores de apps de terceros, que pueden ser gestinonadas individualmente para cada app desde las secciones de ajustes de iCloud de iOS y macOS.

Apple proporciona cierto espacio de almacenamiento gratuito en iCloud cuando se da de alta un nuevo ID de Apple[7], y ofrece ampliaciones previa suscripción al plan correspondiente [Ref.- 3]. También permite obtener una dirección de correo gratuita en el dominio "icloud.com".

Las transferencias de datos hacia los servidores de iCloud están cifradas. En el caso de los datos considerados confidenciales por parte de Apple (por ejemplo, el llavero de iCloud o las contraseñas de redes Wi-Fi), el cifrado es extremo a extremo por lo que, teóricamente, Apple no puede acceder a los mismos [Ref.- 38].

### 5.2.1 BLOQUEO DE ACTIVACIÓN

El denominado "Bloqueo de activación" es una medida de seguridad para evitar que un dispositivo pueda ser activado si no se dispone de las credenciales vinculadas al ID de Apple de su propietario [Ref.- 20]. Se activa de forma automática cuando se habilita la función "Buscar mi iPhone" en un dispositivo[8].

Al habilitar "Buscar", se establece un mapeo entre la cuenta de iCloud y el identificador *hardware* del dispositivo (*device ID*), que se guarda en los servidores de activación de Apple[9] [Ref.- 22].

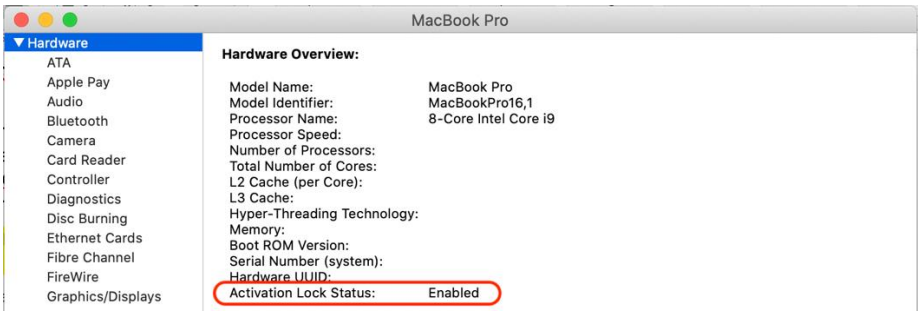



*Figura 27 - Estado del bloqueo de activación en un ordenador Mac (en inglés) con el chip de seguridad T2*

Cuando este bloqueo se encuentra activo, el dispositivo solicitará la contraseña vinculada al ID de Apple y/o el método de desbloqueo del dispositivo para activar o desactivar el servicio "Buscar", al cerrar la sesión de iCloud en el dispositivo, y al borrar los contenidos del dispositivo (restauración a fábrica) y volver a llevar a cabo su proceso de activación.

El bloqueo de activación puede gestionarse mediante entornos empresariales de gestión de dispositivos móviles y/o tradicionales (MDM, Mobile Device Management).

[7] Hasta hace un tiempo, el espacio gratuito era de 5 GB. Sin embargo, durante la elaboración de la presente guía, la creación de una nueva cuenta solo ofreció 1 GB de almacenamiento.

[8] Para macOS, el bloqueo de activación solo está disponible en los dispositivos que incorporan el chip de seguridad T2.

[9] "Everything You Wanted to Know about Activation Lock and iCloud Lock". https://blog.elcomsoft.com/2018/10/everything-you-wanted-to-know-about-activation-lock-and-icloud-lock/

### 5.2.2 GESTIÓN DE LA CUENTA DE ICLOUD

La gestión de la cuenta de iCloud se puede realizar a través de un interfaz web y desde el propio dispositivo.

#### 5.2.2.1 Interfaz web

Accediendo a la web "icloud.com" con las credenciales del ID de Apple, se presenta el interfaz de administración de la cuenta de usuario de Apple, desde el cual es posible:

- Acceder a los contenidos almacenados por algunas de las diferentes apps suministradas por defecto por Apple con iOS que almacenan sus datos en iCloud, pinchando sobre los correspondientes iconos de la <Figura 28>.
  No es posible acceder a los contenidos de las apps de terceros que utilizan el almacenamiento de iCloud, siendo éste gestionado internamente por cada una de las apps.
- Determinar la ubicación de los denominados "Amigos" (ver apartado "6.8. Servicio "Compartir mi ubicación"").
- Desde el menú "Ajustes de la cuenta", es posible:
  - Gestionar los dispositivos vinculados a la cuenta (los denominados "de confianza").
  - Restaurar copias de seguridad de determinados datos (ver apartado "12. Copias de seguridad y restauración en iCloud").
  - Cerrar la sesión en todos los navegadores web que la tengan activa.
  - Definir qué apps pueden buscar a un determinado usuario mediante su ID de Apple.
  - Consultar la lista de dispositivos pertenecientes al grupo "En familia" (si bien su gestión no puede realizarse a través del interfaz web; ver apartado "6.9. Grupo "Familia"").

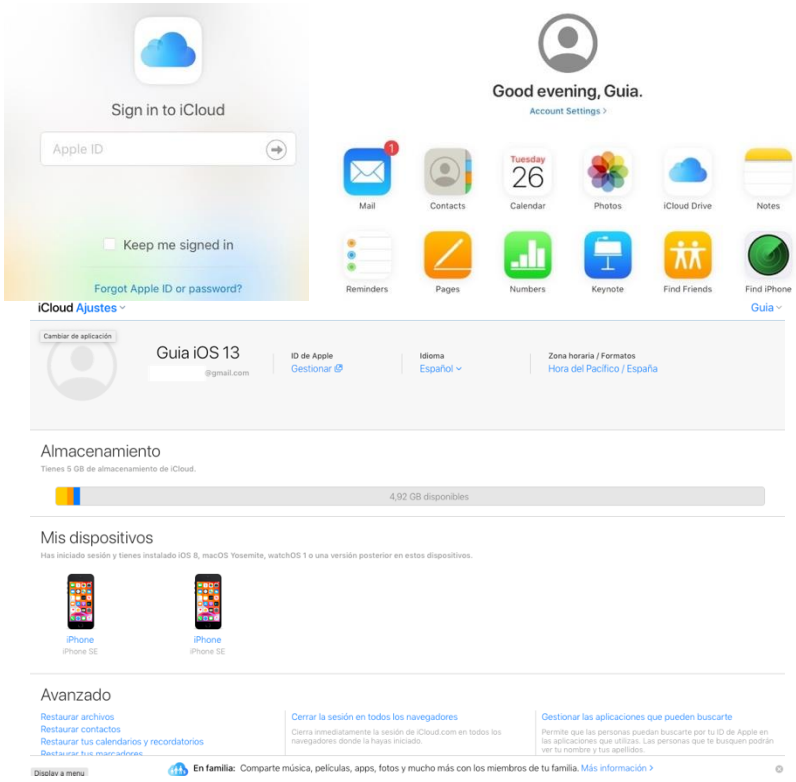



*Figura 28 - Gestión de la cuenta de iCloud vía web*

### 5.2.2.2 macOS

Los ajustes de iCloud de macOS en la versión 10.14 (Mojave) se encuentran en "Preferencias del sistema - iCloud". En la versión 10.15 (Catalina) se acceden desde el icono "ID de Apple" de la parte superior del menú "Preferencias del sistema".

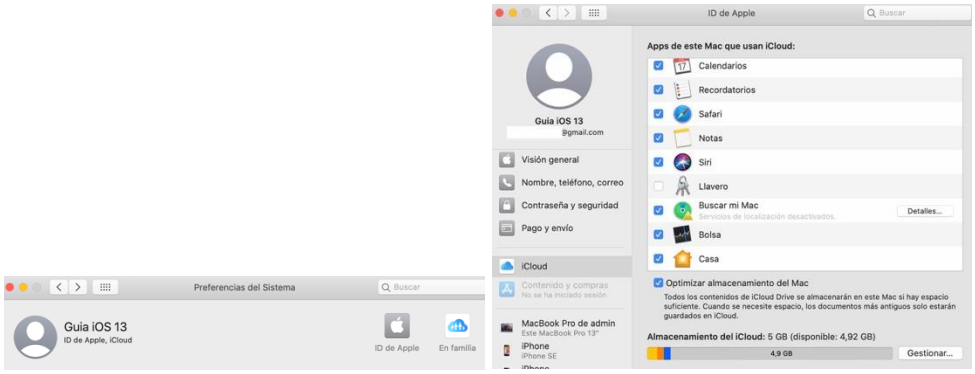



*Figura 29 - Ajustes de iCloud en macOS 10.15 Catalina*

Al dar de alta la cuenta de iCloud, la opción más conservadora (y recomendada desde el punto de vista de privacidad) es elegir "No fusionar" para los servicios propuestos y proceder posteriormente a deshabilitar otros servicios sobre los cuales el sistema no solicita autorización.

El proceso de alta de la cuenta de iCloud solicitará permiso de ubicación para la funcionalidad "Buscar mi Mac", que se recomienda conceder.

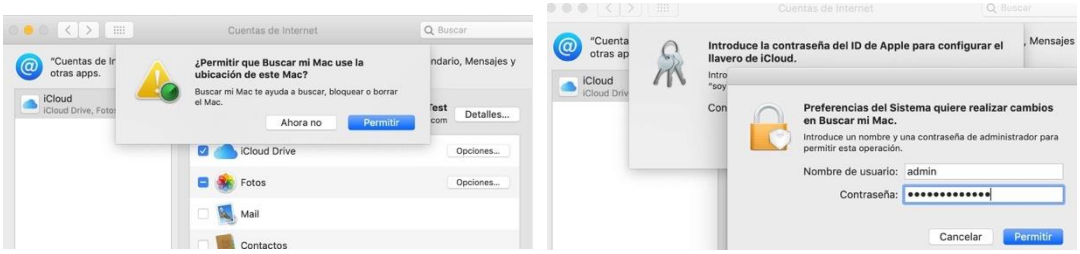



*Figura 30 - Permiso de ubicación para "Buscar mi Mac" mediante iCloud*

macOS solicitará de nuevo la contraseña asociada al ID de Apple para proceder a configurar el llavero de iCloud (ver apartado "8. Gestión de credenciales en iCloud"):




*Figura 31 - Solicitud de la contraseña del ID de Apple para configurar el llavero de iCloud*

Una vez configurada la cuenta de iCloud para el usuario, ***se recomienda***:

- ***Suprimir todas las apps que almacenen contenido sensible*** del menú o pestaña "Documentos" disponible desde el botón "Opciones..." de la categoría "iCloud Drive", accesible desde "Preferencias del sistema - iCloud".
- Desmarcar todas las opciones o categorías de sincronización salvo "Buscar mi Mac".

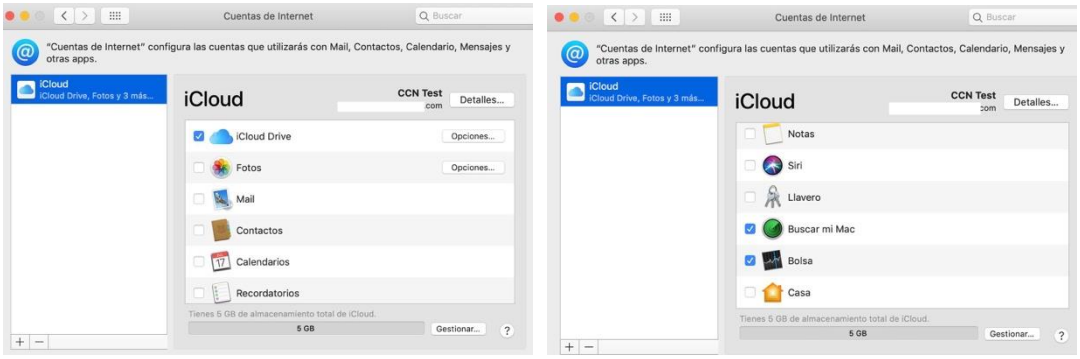



*Figura 32 - Selección de los elementos a gestionar a través de iCloud*

Además de por cuestiones de privacidad, las recomendaciones anteriormente expuestas se deben al enorme impacto de seguridad y privacidad que tendría que un tercero tomase control sobre la cuenta de iCloud del usuario.

Para cerrar sesión en iCloud, es necesario:

- macOS Mojave: seleccionar "Preferencias del sistema - iCloud - Cerrar sesión".
- macOS Catalina: seleccionar "Preferencias del sistema - ID de Apple - Visión General - Cerrar sesión".

#### 5.2.2.3 iOS

Una vez se da de alta la cuenta del ID de Apple en un iPhone, se iniciará sesión en iCloud, y los ajustes estarán disponibles en "Ajustes - [ID de Apple, iCloud, iTunes Store y App Store] - iCloud". Por defecto, se habilitará la sincronización en iCloud para buena parte de las apps proporcionadas por Apple por defecto con iOS. También las apps de terceros pueden almacenar contenido en la nube de Apple, de forma que esté disponible en todos los dispositivos vinculados a dicha cuenta de usuario que tienen instalada la app.




*Figura 33 - Ajustes de iCloud*

Para dejar de sincronizar con iCloud el contenido de una app concreta, se desactivará el interruptor de dicha app. Las apps para las que, en lugar de un interruptor, se muestra "Sí"/"No" (por ejemplo, "Fotos"), admiten otras opciones. Para esos casos, al desactivar la sincronización, se ofrecerá al usuario la posibilidad de guardar una copia en el almacenamiento

local. El contenido no se borrará de iCloud, sino que permanecerá accesible para las apps de otros dispositivos vinculados a la misma cuenta de usuario que sigan teniendo la sincronización activa.

La sección "Buscarme" identifica las apps que tiene permiso para desvelar el nombre y apellidos del usuario a otros usuarios de dicha app cuando le busquen por la dirección de correo asociada a su ID de Apple. ***Se recomienda revisar esta sección y eliminar de ella las apps para las que no se desea compartir dicha información siguiendo los pasos descritos en la*** [Ref.- 18]**.**




*Figura 34 - Desactivación de la sincronización en iCloud para las apps "Fotos", "Notas" y "Safari"*

Si se desea prescindir de los servicios de iCloud, es posible cerrar la sesión a través del menú "Ajustes - [ID de Apple] Cerrar sesión" (ver tercera imagen de la <Figura 23>).

***Se recomienda mantener la sesión de iCloud abierta permanentemente en el dispositivo a fin de poder disponer del servicio "***Buscar mi iPhone***".*** Sí se recomienda cerrar la sesión en iCloud si, por cualquier causa, fuese necesario permitir el acceso al dispositivo móvil a un tercero, incluido personal de soporte técnico del propio Apple.

### 5.2.3 ALIAS DE CORREO

El servicio de iCloud Mail permite la utilización de hasta tres alias de correo: un alias es una dirección de correo alternativa que permite ocultar a terceros la dirección principal de iCloud mail del destinatario, de modo que no coincida con la vinculada a su cuenta de iCloud.

El alias de iCloud mail no puede vincularse a otro ID de Apple, ni puede emplearse para iniciar sesión en la cuenta de iCloud; sin embargo, puede asociarse como alias del ID de Apple (ver apartado "5.1.5. Alias del ID de Apple") y ser empleado en servicios como iMessage y FaceTime.

Para crear un alias, se recomienda seguir el procedimiento descrito en la [Ref.- 39] e ilustrado en la <Figura 35>. Para dejar de utilizar un alias, se puede, bien desactivarlo (si cabe la posibilidad de volver a utilizarlo en el futuro), bien eliminarlo (esta acción es irreversible y el alias será suprimido de la cuenta de forma permanente).




*Figura 35 - Creación de un alias de iCloud (mail)*

***La utilización de un alias de correo está recomendada desde el punto de vista de seguridad y privacidad***, ya que permite ocultar el identificador de usuario de la cuenta de Apple, haciendo que sea más difícil para un atacante intentar obtener las credenciales asociadas.

### 5.2.4 USO DEL ALMACENAMIENTO EN iCLOUD POR APPS DE TERCEROS

Es posible configurar apps de terceros para que almacenen su información en la cuenta de iCloud [Ref.- 27]. En este caso, iOS permite el uso de contraseñas específicas para cada app (por ejemplo, Mozilla Thunderbird), de forma que no sea necesario que la app acceda a la contraseña asociada al ID de Apple del usuario. Estas contraseñas se obtienen iniciando sesión en la web "apple.appleid.com" desde el menú "Seguridad".

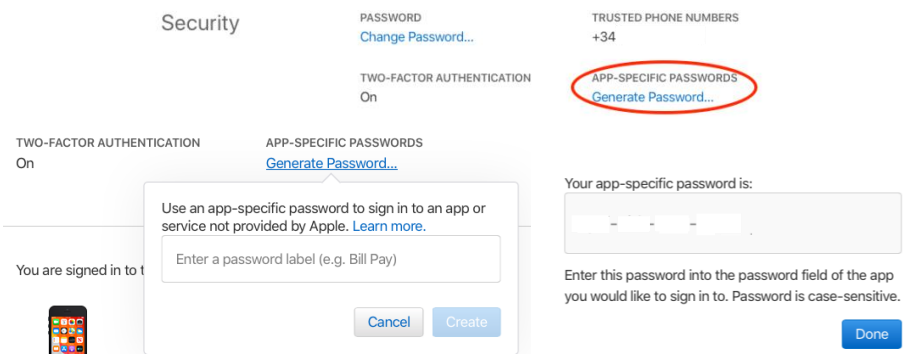



*Figura 36 - Uso de una contraseña específica de una app para acceder a iCloud*

La configuración de apps de terceros queda fuera del ámbito de la presente guía, pero se puede consultar algún ejemplo en la página web oficial de Apple [Ref.- 28].

Aquellas apps cuyo interruptor esté activo volcarán su contenido en iCloud, de forma que estará accesible para esas mismas apps cuando se utilicen desde otro dispositivo vinculado a la misma cuenta de iCloud (es decir, a un mismo ID de Apple).

## 5.3 CUENTA DE iTUNES/APP STORE

La cuenta utilizada para el almacén de contenidos en iTunes (Store) y para la tienda oficial de Apple (App Store) puede estar vinculada en iOS y en macOS con un ID de Apple diferente del empleado para la cuenta de iCloud. Este tipo de configuración es la recomendada desde el punto de vista de seguridad, ya que permite independizar los servicios de iCloud (potencialmente más críticos) del acceso y las compras de apps y contenidos en la App Store.

Esta cuenta es la que se empleará para la descarga de contenidos (multimedia, música, libros y apps).

En caso de disponer de cuentas independientes entre iCloud y la App Store en macOS 10.15, se debe añadir primero la cuenta vinculada a iCloud y posteriormente la vinculada a la App Store.

- En macOS, el botón "Preferencias del sistema - ID de Apple - Visión general - Cerrar sesión" cerrará sesión tanto en la cuenta de iCloud como en la cuenta vinculada a la App Store. Para cerrar sesión únicamente en cuenta vinculada a la App Store, debe utilizarse el menú "App Store - Tienda - Cerrar sesión".
- En iOS, a pesar de existir un único menú "Cerrar sesión" bajo "Ajustes - ID de Apple", su selección presenta un cuadro de diálogo que permite al usuario elegir en qué cuenta desea cerrar la sesión. Adicionalmente, existe un menú específico en "App Store - [Icono de usuario] - Cerrar sesión" para cerrar sesión solo en la App Store.

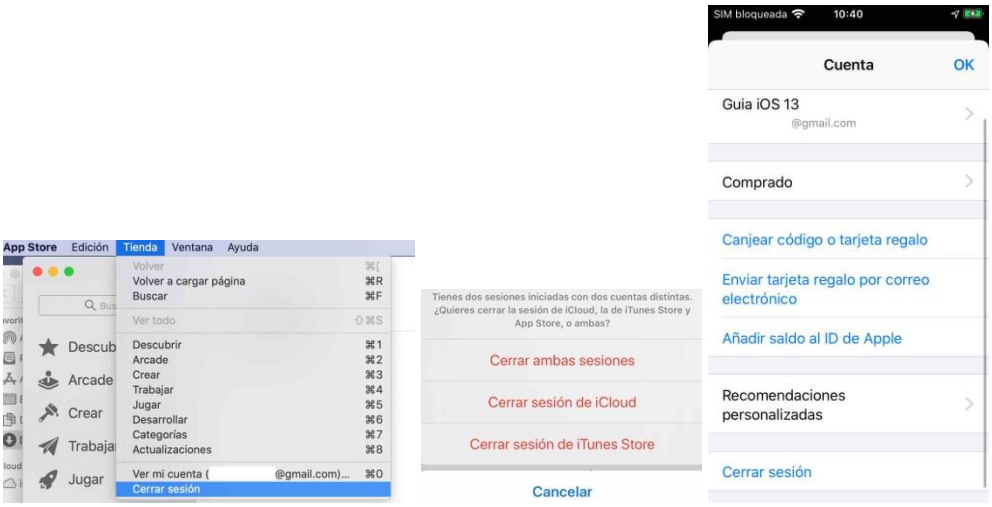



*Figura 37 - Cierre de sesión con cuentas de iCloud y App Store independientes*

Las recomendaciones de seguridad relativas al uso de la App Store se pueden consultar en las guías específicas de cada sistema operativo, iOS y macOS: "Configuración segura de iOS 13" [Ref.- 413] y "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412].

### 5.3.1 COMPRAS DEL GRUPO "FAMILIA"

Los miembros del grupo "Familia" (ver apartado "6.9. Grupo "Familia"") pueden compartir las compras de apps (quedan excluidas las compras realizadas dentro de las apps) que cualquier otro integrante del grupo haya realizado si:

- La opción "[Funciones compartidas] - Compartir compras" está activa.
- La app es compatible para compartición: para ello, es preciso abrir la "App Store", seleccionar la app en la sección "Comprado" y comprobar que "En familia" se incluye en el apartado "Compatibilidad" [Ref.- 26].

Sin embargo, puede ser recomendable ocultar la compra de determinadas apps para administrar su utilización granularmente, de forma que otros miembros no puedan consultarlas, ni descargarlas, siguiendo los procedimientos descritos en la [Ref.- 25], tanto en iOS como en macOS, desde la app "App Store".

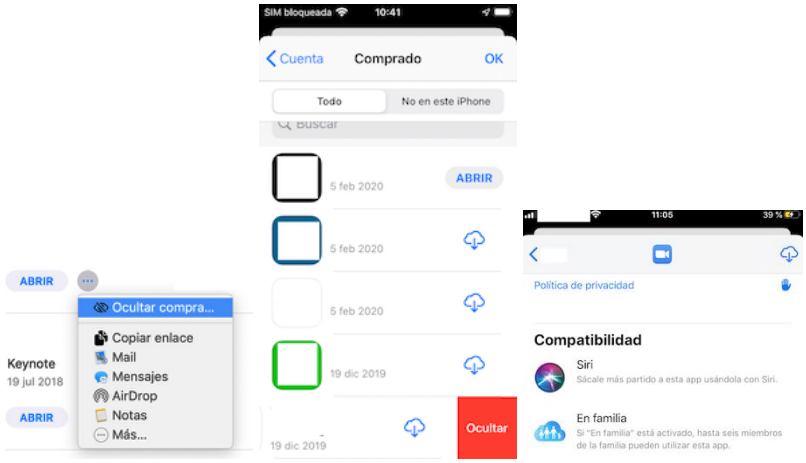



*Figura 38 - Ocultar compras realizadas en la App Store*

Las compras iniciadas por miembros del grupo "Familia" menores de edad se notificarán a los miembros con roles "Organizador" y "Padre/tutor", siendo precisa su aprobación expresa para que la app sea descargada en el dispositivo solicitante. En el caso del rol "Padre/tutor", se requiere que el organizador le haya otorgado permiso previamente para la aprobación de solicitudes de compra [Ref.- 32].

Es posible (y recomendable desde el punto de vista de privacidad), utilizar un ID de Apple específico para las compras compartidas con el grupo "Familia". Para ello, se dispone del menú:

- iOS: "Ajustes - [ID de Apple] - En familia - [Seleccionar el nombre] - [Música y compras]", desde el que se puede modificar el ID de Apple.
- macOS: "Preferencias del sistema - En familia - [Seleccionar el nombre] - [Música y compras] - Modificar".

Solo se permite modificar el ID de Apple asignado a "Familia" cada 90 días.

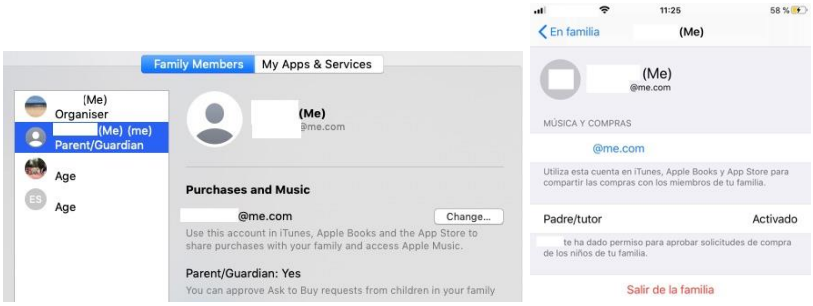



*Figura 39 - Uso de un ID de Apple específico para compras compartidas con el grupo "Familia"*

La función "Solicitar la compra" se habilita por defecto para los menores de 13 años, y el organizador deberá definirla explícitamente para las cuentas pertenecientes a menores de 18 años que se añadan al grupo familiar.

## 5.4 OTRAS CUENTAS VINCULADAS A LOS SERVICIOS DE APPLE

Existen diversos servicios de Apple que utilizan cuentas específicas. Habitualmente, estas cuentas coinciden con el ID de Apple que se configure en primera instancia en los ajustes del dispositivo.

### 5.4.1 CUENTA DE FACETIME

La utilización de FaceTime requiere disponer de un ID de Apple vinculado al uso de este servicio, que puede ser o no el mismo que se usa a nivel general en el dispositivo. Su configuración se encuentra en:

- iOS: "Ajustes - FaceTime - Usa tu ID de Apple para FaceTime".
- macOS: en el menú de la app FaceTime "Preferencias... - ID de Apple" (macOS).

Es posible cerrar sesión en la cuenta actual y definir una nueva cuenta, distinta a la del ID de Apple vinculado al resto de servicios. En caso de que ambas cuentas sean diferentes, si se cierra la sesión asociada al ID de Apple general, será posible seguir haciendo uso de los servicios de FaceTime.

Complementariamente, los alias vinculados al ID de Apple configurado en FaceTime (ver apartado "5.1.5. Alias del ID de Apple") se pueden utilizar para contactar con el usuario a través de FaceTime (campo "Forma de contacto por FaceTime") y como origen de las comunicaciones que el usuario inicie (campo "Identificación de llamada"), siendo posible definir cuáles se quieren emplear desde estos menús.

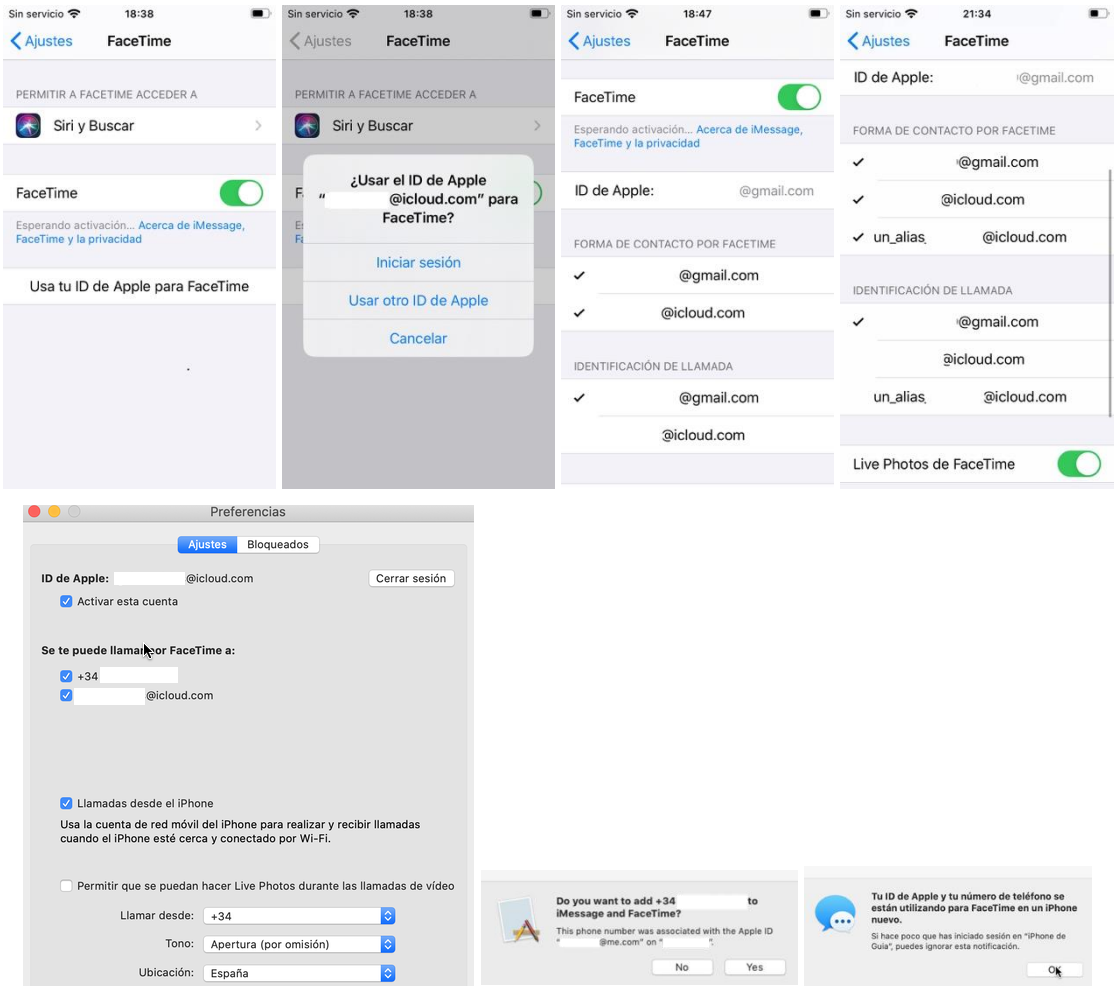



*Figura 40 - Configuración de las cuentas vinculadas a FaceTime*

***Desde el punto de vista de seguridad y privacidad***, se recomienda utilizar para FaceTime un ID de Apple distinto al de la cuenta general o, al menos, hacer uso de uno o varios alias, así como definir detalladamente cuáles se quieren permitir para recibir y para iniciar llamadas.

El ID de Apple de FaceTime es un requisito para poder hacer uso del servicio de llamadas a través de un iPhone desde otros dispositivos sin capacidades de telefonía, descrito en el apartado "7.1.4. Recepción de llamadas telefónicas".

El ID de Apple de FaceTime se mantiene aun cuando se cierra sesión en el ID de Apple general, y no cambia si se abre sesión con otro nuevo ID de Apple en el dispositivo.

Si el ID de Apple tiene vinculación con un número de teléfono, este número también puede utilizarse como origen y/o destino de comunicaciones vía FaceTime.

### 5.4.2 CUENTA DE iMESSAGE

Al igual que sucede con FaceTime, iMessage requiere disponer de un ID de Apple vinculado al uso de este servicio, que puede ser o no el mismo que se usa a nivel general en el dispositivo. Su configuración se encuentra en:

- iOS: "Ajustes - Mensajes - Enviar y recibir - ID de Apple".
- macOS: en el menú de la app Mensajes "Preferencias... - iMessage - ID de Apple" (macOS).

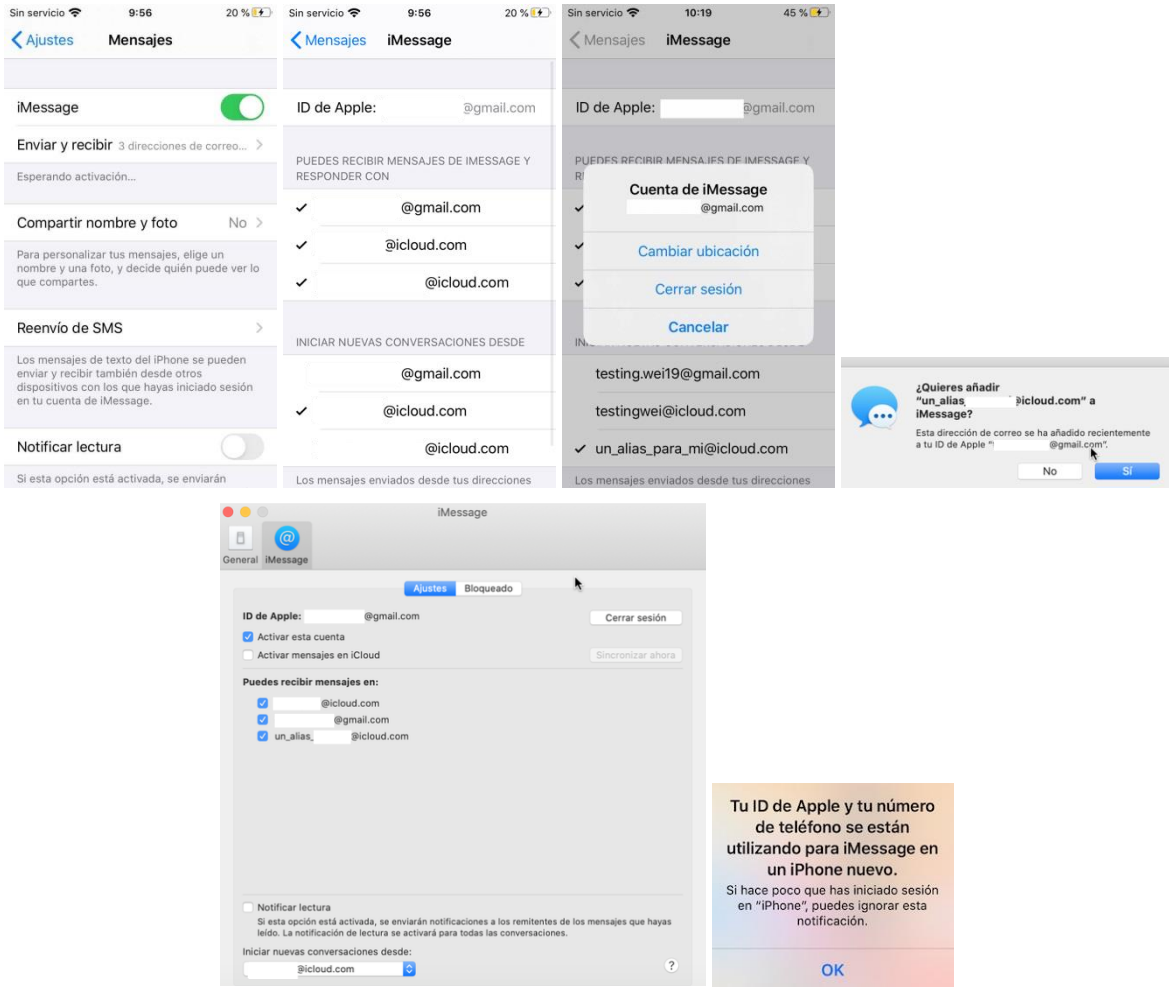



*Figura 41 - Configuración de las cuentas vinculadas a iMessage*

Es posible cerrar sesión en la cuenta actual de iMessage y definir una nueva cuenta distinta, independientemente del ID de Apple vinculado al resto de servicios. En caso de que ambas cuentas sean diferentes, si se cierra la sesión asociada al ID de Apple general, será posible seguir haciendo uso de los servicios de iMessage a través de la otra cuenta. La vinculación de un ID de Apple a un dispositivo como cuenta de iMessage se notificará al resto de dispositivos vinculados al ID de Apple, como ilustra la última imagen de la <Figura 41>.

Los dispositivos que hayan vinculado un determinado ID de Apple para iMessage se mostrarán en la sección "Dispositivos" del interfaz de gestión del ID de Apple https://appleid.apple.com/account/manage, pero este interfaz no indica expresamente que la sesión de un dispositivo concreto se limite al uso de iMessage, no siendo posible diferenciar los dispositivos que utilizan el ID de Apple como cuenta general del dispositivo de los que solo la utilizan para iMessage.

En caso de pérdida o robo de un dispositivo cuyo servicio iMessage está vinculado al ID de Apple, se recomienda ejecutar la acción "Eliminar de la cuenta" para evitar que el nuevo usuario disponga de acceso a los mensajes de iMessage pasados y futuros del usuario víctima.

Complementariamente, es posible designar los alias vinculados al ID de Apple (ver apartado "5.1.5. Alias del ID de Apple") que se desea utilizar para establecer comunicaciones a través de iMessage (campos "Puedes recibir mensajes de iMessage y responder con" e "Iniciar nuevas conversaciones desde").

***Desde el punto de vista de seguridad y privacidad***, se recomienda utilizar para iMessage un ID de Apple distinto al de la cuenta general o, al menos, hacer uso de uno o varios alias y cursar las comunicaciones a través de ellos, de modo que no sea necesario que terceras personas conozcan el ID de Apple real del usuario. Adicionalmente, se recomienda definir detalladamente cuáles de estos alias se quieren permitir para recibir y para iniciar conversaciones.

Los detalles de funcionamiento del protocolo subyacente al servicio iMessage se detallan en el apartado "7.2.2. iMessage".

## 6. GESTIÓN REMOTA DE DISPOSITIVOS: SERVICIO "BUSCAR"

Recomendaciones de seguridad:

- Ante la mínima sospecha de que el dispositivo haya sido sustraído, o que caiga en manos de terceros, se recomienda proceder al borrado remoto de sus contenidos si se considera que almacena datos confidenciales y estos priman sobre la recuperación del dispositivo.
- Habilitar la recepción de notificaciones cuando un dispositivo perdido se localice.

El servicio "Buscar" (Find my iPhone/Mac) nació con el objetivo de pode localizar un dispositivo extraviado, y, eventualmente, permitir su borrado remoto en caso de no ser posible su recuperación. Tanto en iOS como en macOS, Apple ha integrado este servicio dentro de la app "Buscar", que ofrece, además del servicio de localización del dispositivo, otras funcionalidades adicionales (descritas en los siguientes subapartados) [Ref.- 10] [Ref.- 13].

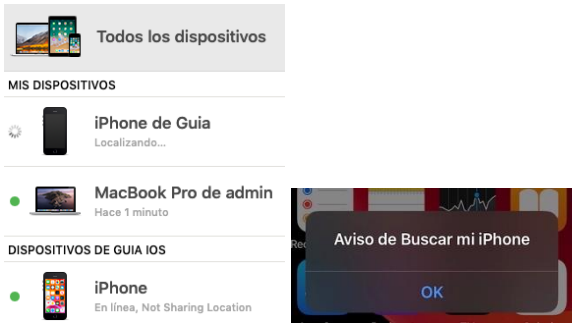



*Figura 42 - Lista de dispositivos propios y asociados a "Familia" y ejecución de "Reproducir un sonido"*

Al acceder al interfaz de "Buscar", se mostrará un mapa con la ubicación de los dispositivos propios, y el menú "Todos los dispositivos", desde el que se permite la gestión remota tanto de los dispositivos propios como los vinculados al grupo "Familia" (ver apartado "6.9. Grupo "Familia"").

Para el correcto funcionamiento de los servicios de búsqueda del dispositivo, se requiere:

- Que la sesión de iCloud esté **abierta** en el dispositivo a gestionar.
- Que el servicio "[ID de Apple] - iCloud - Buscar mi iPhone/mi Mac" esté **activo**: si no lo está, no podrá realizarse ninguna tarea de gestión remota sobre el dispositivo.
- Que el ajuste "Privacidad - Localización - Servicios del sistema - Buscar mi iPhone" o "Preferencias del sistema - Seguridad y Privacidad - Privacidad - Localización - Servicios del sistema - Detalles... - Buscar mi Mac" esté **habilitado**. En caso contrario, será posible realizar tareas de gestión, pero no determinar la ubicación del dispositivo en el mapa.
- En macOS, el ajuste "Localización" debe estar **habilitado** a nivel global. De lo contrario, no será posible mostrar en el mapa la ubicación del Mac, aunque sí se podrán iniciar otras labores de gestión remota, como reproducir un sonido o borrar sus contenidos (ver <Figura 43>). En iOS este el valor del ajuste global no es limitante, según se describe en el apartado "6.2. Modo perdido".
- Disponer de conexión de datos (a través de red o de datos móviles): en caso contrario, solo será posible localizarlo a través del servicio descrito en el apartado "6.7. Servicio "Encontrar sin conexión"".

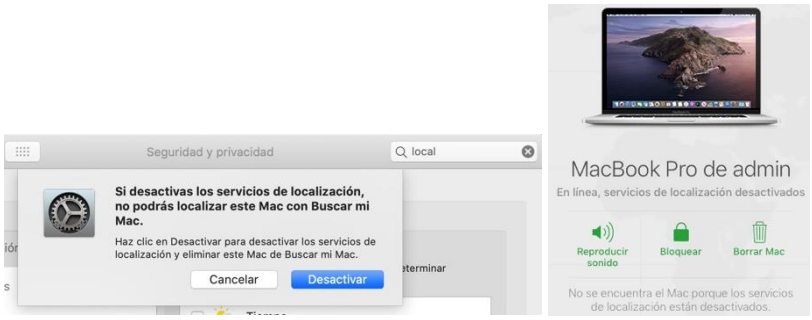



*Figura 43 - Mensaje de indisponibilidad de la función "Buscar" en macOS*

**NOTA:** si el dispositivo fuese reiniciado por parte de un tercero y no se introdujese el código de desbloqueo en el arranque, no es posible hacer uso de las capacidades del servicio "Buscar", ya que los contenidos estarían cifrados y no se habría iniciado sesión en iCloud.

Cuando se activa la funcionalidad "Buscar" en un dispositivo, el sistema solicitará:

- Las credenciales del ID de Apple.

- El método de bloqueo vigente en el propio dispositivo.
- El código de desbloqueo de otros dispositivos actualmente vinculados al mismo ID de Apple (ver <Figura 44>, en la que se ilustra cómo el código de desbloqueo del iPhone es solicitado en un Mac en el que se había cerrado sesión en la cuenta de iCloud y viceversa).




*Figura 44 - Solicitud del código de desbloqueo del iPhone al dar de alta su ID de Apple en un Mac*

En macOS, tras el arranque del sistema, el demonio FMM (*Find my Mac*) establece una conexión con el servidor de iCloud, enviándole los datos para la geolocalización del equipo cuando se le requieran y escuchando los comandos de gestión remota que dicho servidor le envíe. Si el equipo se reinicia y ningún usuario inicia sesión, "Buscar mi Mac" no podrá conectar con el equipo si el disco está cifrado con FileVault (opción recomendada desde el punto de vista de seguridad). Todas las acciones que se inicien desde el interfaz de "Buscar mi Mac" quedarán pendientes hasta que el disco sea desbloqueado mediante un inicio de sesión válido.

Las tareas de gestión remota asociadas al servicio "Buscar" están disponibles:

- Desde el interfaz web de iCloud: ver apartado "6.5. Interfaz web de "Buscar"".
- Desde la app "Buscar", existente tanto en iOS como en macOS.

Las tareas disponibles, aparte de la que permite localizar a los dispositivos en un mapa, son:

- "Bloquear"/"Modo perdido": ver apartado "6.2. Modo perdido". ***Se recomienda realizar esta acción como primera medida para asegurar que el dispositivo quede bloqueado y sus datos inaccesibles para un tercero***.
- "Reproducir sonido": genera una señal sonora en el dispositivo, incluso en modo no molestar, y presenta una notificación en pantalla, incluso aunque esté bloqueada. Esta opción solo debería utilizarse en caso de que se tenga la certeza de que el dispositivo está en un rango de distancia que permita al usuario escuchar la señal acústica, pero no si existen sospechas de que pueda estar en un lugar con acceso público alejado del propietario. En todo caso, antes de iniciar esta acción, se recomienda activar el "modo perdido" para que, si el sonido es oído por un tercero, el terminal se encuentre bloqueado.
- "Borrar iPhone/Mac": en última instancia, si existe la mínima sospecha de que el dispositivo está realmente perdido, se recomienda iniciar esta acción, que enviará una solicitud de reseteo a fábrica, con la que toda la información (incluida la vinculada al ID de Apple) será eliminada. En el apartado "6.1. Borrado remoto de dispositivos" se proporcionan más detalles sobre esta funcionalidad.

El "bloqueo de activación" (descrito en el apartado "5.2.1. Bloqueo de activación") seguirá vigente para el dispositivo, impidiendo su reinstalación por parte de terceros.

## 6.1 BORRADO REMOTO DE DISPOSITIVOS

**IMPORTANTE**: si se desea llevar a cabo pruebas de esta funcionalidad, se recomienda realizar previamente una copia de seguridad completa del dispositivo, que permita restaurarlo en caso de un fallo en el proceso de recuperación.

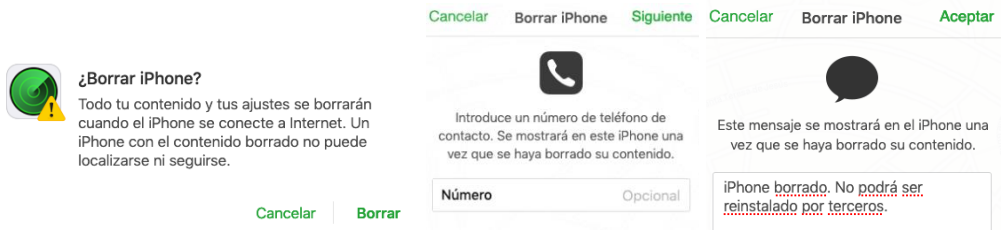
Los dispositivos borrados mediante esta funcionalidad dejan de pertenecer al grupo de dispositivos "de confianza", no pudiendo utilizarse como segundo factor de autentificación [Ref.- 33]. Una vez invocada esta operación, no será posible localizar en el mapa el dispositivo, ni invocar otras tareas de gestión remota.

**NOTA:** si el equipo se va a ceder a un tercero, se desaconseja borrar los contenidos mediante la funcionalidad de borrado remoto, ya que esta operación requiere que la sesión de iCloud esté abierta en el Mac y el borrado dejaría vigente el bloqueo de activación. Por tanto, el borrado de un dispositivo que se va a traspasar voluntariamente debe realizarse de forma local siguiendo los procedimientos descritos en la [Ref.- 34]. En este caso, tras completar la operación de borrado, se aconseja comprobar que el dispositivo ya no aparece de la cuenta de iCloud y, por tanto, ha dejado de ser de confianza (ver apartado "5.1.6. Dispositivos de confianza").

El borrado remoto se realiza de forma rápida, ya que no sobrescribe todos los contenidos de la unidad de almacenamiento, sino únicamente la denominada "*Media Key*" [Ref.- 21], que forma parte de la jerarquía de claves de cifrado de los dispositivos de Apple:

- En iOS, la "Media Key" envuelve los metadatos del volumen de datos, impidiendo por tanto el acceso a las claves de cifrado.
- En macOS, envuelve el material criptográfico, todos los metadatos y los datos de los volúmenes protegidos con FileVault (ver apartado "Cifrado de almacenamiento APFS con chip T2" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412]). Adicionalmente, tal como se detalla en el apartado "Cifrado del almacenamiento" de dicha guía [Ref.- 412], la cuenta de usuario de iCloud puede ser utilizada en macOS para desbloquear un disco cifrado con FileValut y para resetear la contraseña de cifrado (alternativamente a iCloud se puede hacer uso de una clave de recuperación local). Este servicio es conocido como *iCloud FileVault Recovery*.

Si el dispositivo no tiene conexión[10] en el momento de solicitarse el borrado, la petición quedará pendiente y se cursará cuando se recupere la conexión. Durante ese periodo, es posible cancelar la operación mediante el menú "Detener borrado", que solicitará la contraseña de iCloud:




[10] En el caso de iOS, puede emplearse una conexión de datos móviles o Wi-Fi. Para macOS, la conexión por defecto se establecerá vía Wi-Fi o Ethernet.

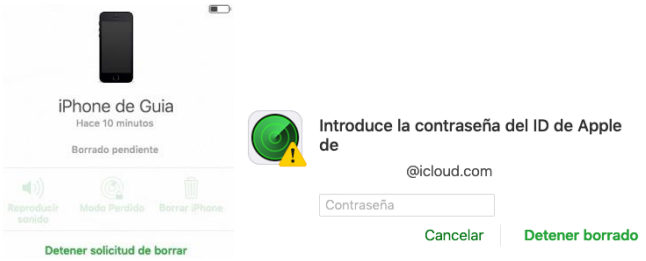



*Figura 45 - Operación de borrado remoto sobre un dispositivo iOS*

En el caso de macOS, la funcionalidad "Borrar" sobrescribe los bloques de disco que contienen la clave "*Media Key*" de FileVault: sin ella, no es posible descifrar la clave de cifrado del volumen, por lo que, aunque el disco fuese extraído y montado en otro equipo, los datos no podrían recuperarse. Únicamente se mantiene habilitada la partición de recuperación (*Recovery*), de forma que, al finalizar el proceso de borrado, el sistema entrará en modo de recuperación.




*Figura 46 - Operación de borrado remoto sobre un dispositivo macOS*

Los datos de las unidades de disco externas conectadas al Mac no serán eliminados.

La operación de borrado sobre un Mac requerirá que el usuario establezca una clave de seis dígitos, que será necesario introducir de nuevo en el modo de recuperación si se intenta volver a reinstalar el Mac (tras ser completada la operación de forma exitosa).

## 6.2 MODO PERDIDO

El "modo perdido" [Ref.- 24] es una funcionalidad del servicio "Buscar" que fuerza el bloqueo del dispositivo y que se muestre en él un mensaje personalizado. Este mensaje puede, por ejemplo, incluir un método e información de contacto que favorezca su devolución (no se recomienda que incluya datos personales del propietario, y, de ser posible, tampoco su número de teléfono personal).

La activación del "modo perdido" se notificará al usuario a través de un mensaje de correo electrónico remitido a la cuenta de correo de iCloud a la que el dispositivo se encuentre vinculado. Adicionalmente, el servicio Apple Pay quedará inhabilitado en el dispositivo.

Se recomienda activar las notificaciones que avisan de cuándo un dispositivo extraviado sea localizado mediante el interruptor "Notificaciones - Avisar cuando se encuentre".

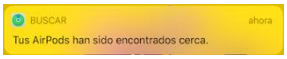



*Figura 47 - Notificación del servicio "Buscar" cuando se localiza un dispositivo extraviado*

### 6.2.1 MODO PERDIDO/BLOQUEAR EN MACOS

El "modo perdido" en macOS se puede iniciar:

- Desde el interfaz web "Buscar" de iCloud con la opción "Bloquear".
- Desde la app "Buscar" de otro dispositivo Apple, mediante el menú "Marcar como perdido - Activar".

El usuario tendrá que definir un código PIN de 6 dígitos, cuya introducción en el propio Mac será necesaria para desbloquear el modo perdido una vez ha sido encontrado.

Cuando el Mac perdido esté accesible a través de Internet, el servidor de iCloud enviará un comando "*lock*", que provoca que el equipo se reinicie en un modo especial de recuperación (en las pruebas realizadas existe un retardo efectivo de más de 10 segundos), y almacene en NVRAM los siguientes valores:

- "`good-samaritan-message`": corresponde al texto que se mostrará en la pantalla del equipo bloqueado, que incluye un texto fijo establecido por iCloud y el texto definido por el usuario durante la solicitud de bloqueo:

```
$ nvram -p -x | grep -i samaritan
good-samaritan-message    Este Mac se ha bloqueado con Buscar mi Mac.
¿No lo has bloqueado? Ve a www.icloud.com/find y obtén el PIN para
desbloquearlo. "Mac perdido"
```

*Figura 48 - Mensaje en macOS con el "modo perdido" activo*

- "`fmm-password-hash`": corresponde a un hash del PIN fijado en la acción "Bloquear" por parte del propietario de la cuenta de iCloud. Este valor se eliminará de la NVRAM una vez se desbloquee el equipo a través del PIN.
- "`security-pinType`": algoritmo de hash y cifrado del PIN.
- "`recovery-boot-mode=locked`": cuando el sistema arranca de la partición de recuperación o *recovery*, invoca a la app "Installer.app". Esta app comprueba el valor de la variable "`recovery-boot-mode`" y, si está "`locked`", invocará a la app "Lock.app", que muestra el PIN-Pad y el mensaje "`good-samaritan-message`" (ver imagen derecha de la <Figura 49>).

Los servicios asociados a FMM (*Find my Mac*) se definen en los archivos:

- `/System/Library/LaunchDaemons/com.apple.findmymac.plist`
- `/System/Library/LaunchAgents/com.apple.icloud.findmydeviced.findmydevice-user-agent.plist`

Aunque el interfaz web de "Buscar" ofrece la opción "Desbloquear", su funcionalidad se limita a mostrar al usuario en la pantalla de iCloud la contraseña de bloqueo, previa comprobación de su identidad mediante la solicitud de la contraseña del ID de Apple asociado a la cuenta de iCloud[11].

Si los servicios de localización estaban desactivados en el Mac, no será posible rastrear su ubicación.

Tras la validación del PIN del "Modo perdido", el Mac se reiniciará, presentando la pantalla estándar de desbloqueo y autentificación del proceso de arranque. De este modo, si el disco

[11] Si el ID de Apple no está configurado con 2FA, el usuario tendrá que responder dos de las preguntas de seguridad que definió cuando dio de alta dicha cuenta de usuario de Apple. Si el 2FA está activo, el usuario tendrá que haber iniciado sesión en el interfaz "Buscar" desde un dispositivo de confianza o un navegador web que haya sido autorizado desde uno de dichos dispositivos.

está cifrado con FileVault, se impide que un tercero que llegase a introducir el código de desbloqueo correcto del "modo perdido" obtuviera acceso directo a los datos.

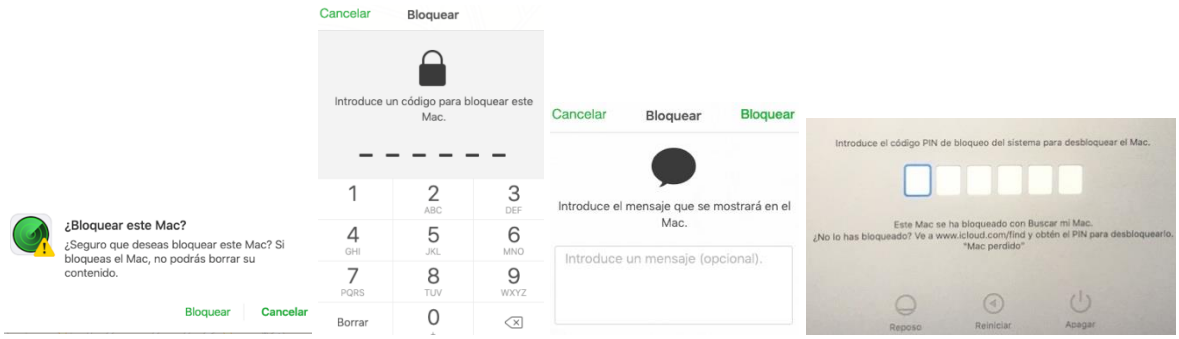



*Figura 49 - Configuración de la acción "Bloquear" para un Mac*




*Figura 50 - "Modo perdido" activo para un ordenador Mac con macOS 10.15 Catalina*

El "modo perdido" impide que sea posible arrancar en modo de restablecimiento de la NVRAM; si se intenta reiniciar el equipo en modo de recuperación de forma manual, aparecerá en pantalla un menú de introducción de contraseña, que corresponderá a:

- La contraseña de *firmware* si el equipo dispone de ella (opción recomendada desde el punto de vista de seguridad): ver imagen izquierda de la <Figura 50>. Una vez introducida la contraseña de *firmware*, se procedería al paso siguiente.
- El código de desbloqueo configurado al activar el "Modo perdido" si el Mac no dispone de contraseña de *firmware* (teóricamente, esto implica que la función "Bloquear" de "Buscar" está estableciendo como contraseña temporal de *firmware* el PIN de 6 dígitos definido en su menú): ver imagen derecha de la <Figura 49>.

En ambos casos, una vez validado el código de desbloqueo del "Modo perdido", se continuará con el proceso de arranque del modo de recuperación.

### 6.2.2 MODO PERDIDO EN iOS

El "modo perdido" en iOS se puede iniciar:

- Desde el interfaz web "Buscar" de iCloud con la opción "Modo perdido".
- Desde la app "Buscar" de otro dispositivo Apple, mediante el menú "Marcar como perdido - Activar".

Solo será necesario definir un código de desbloqueo si el dispositivo iOS, iPhone, no dispone de un código de acceso propio ya establecido. El iPhone no se reiniciará, sino que será bloqueado (si no lo estaba ya) y mostrará en pantalla el mensaje y/o el número de teléfono definidos en el menú de activación del "Modo perdido".

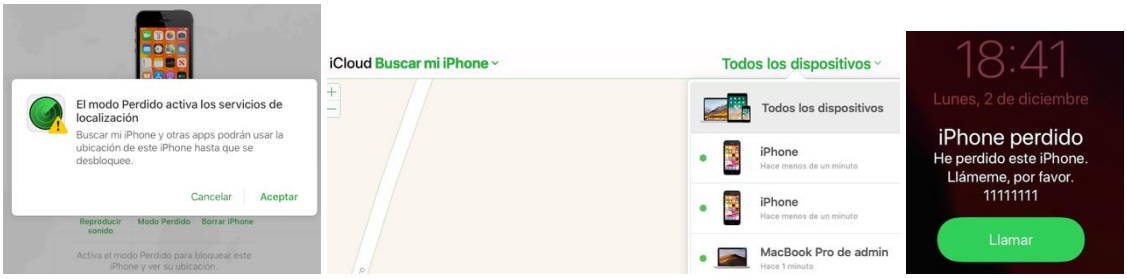



*Figura 51 - Funcionalidad "Modo perdido", con localización desactivada en el dispositivo, para iOS*

Es importante reseñar, que, aunque el ajuste global "Privacidad - Localización" esté desactivado, la activación del "modo perdido" permite que Apple active temporalmente la localización mientras el iPhone permanezca bloqueado, permitiendo su ubicación y presentación en el mapa. Los servicios de localización volverán a desactivarse cuando el dispositivo móvil salga del "modo perdido" (mediante la introducción del código de acceso correcto en el iPhone).

La vigencia del "modo perdido" se identifica por el símbolo "🔒" junto al nombre del dispositivo, y se puede desactivar en el iPhone tanto desde el interfaz de iCloud o de la app "Buscar" de otro dispositivo móvil (no está disponible desde la app "Buscar" de macOS), seleccionando el campo "[Marcar como perdido] Activado - Desactivar "Marcar como perdido"". El dispositivo se mantendrá con la pantalla bloqueada hasta que se introduzca el código de desbloqueo en el propio dispositivo.

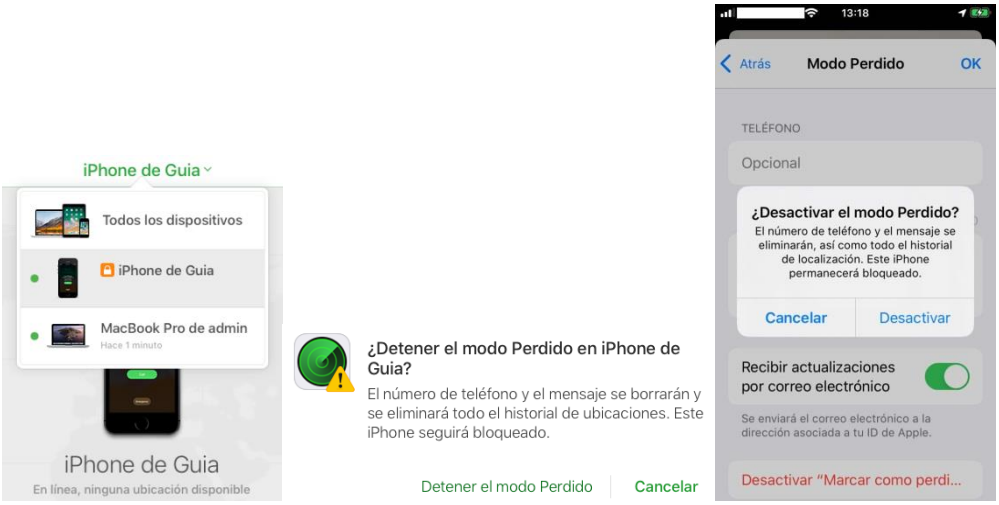



*Figura 52 - Desactivación del "modo perdido" para un iPhone*

## 6.3 AJUSTES VINCULADOS A "BUSCAR" EN IOS

Los ajustes del servicio "Buscar" en iOS se encuentran bajo "Ajustes - [ID de Apple] - Buscar":

- "Buscar mi iPhone": incorpora las opciones:
  - "Buscar mi iPhone": este interruptor **debe** estar activo para poder hacer uso del servicio de gestión remota del terminal.
  - "Encontrar sin conexión": ver apartado "6.7. Servicio "Encontrar sin conexión"".
  - "Enviar última ubicación": provoca que el dispositivo envíe a Apple su ubicación cuando el nivel de batería sea crítico. Apple almacenará esta ubicación en sus servidores durante 24 horas [Ref.- 10].




*Figura 53 - Ajustes requeridos para el servicio "Buscar" en iOS 13*

Se recomienda tener habilitados todos los servicios asociados a "Buscar", a fin de minimizar el riesgo de no poder hacer uso del servicio ante la pérdida o sustracción de un dispositivo.

Complementariamente, el ajuste "Ajustes - Privacidad - Localización - Servicios del sistema - Buscar mi iPhone" debe encontrarse habilitado.

## 6.4 AJUSTES VINCULADOS A "BUSCAR" EN macOS

El uso del servicio "Buscar" en macOS 10.15 requiere activar los siguientes ajustes:

- "Preferencias del sistema - Seguridad y privacidad - Privacidad - Localización - Activar los servicios de localización" y "Preferencias del sistema - Seguridad y privacidad - Privacidad - Localización - Servicios del sistema - Detalles… - Buscar mi Mac".
- "Preferencias del sistema - [ID de Apple] - Buscar mi Mac - [Opciones] Buscar mi Mac": adicionalmente, se recomienda habilitar "Encontrar sin conexión"; ver apartado "6.7. Servicio "Encontrar sin conexión"".

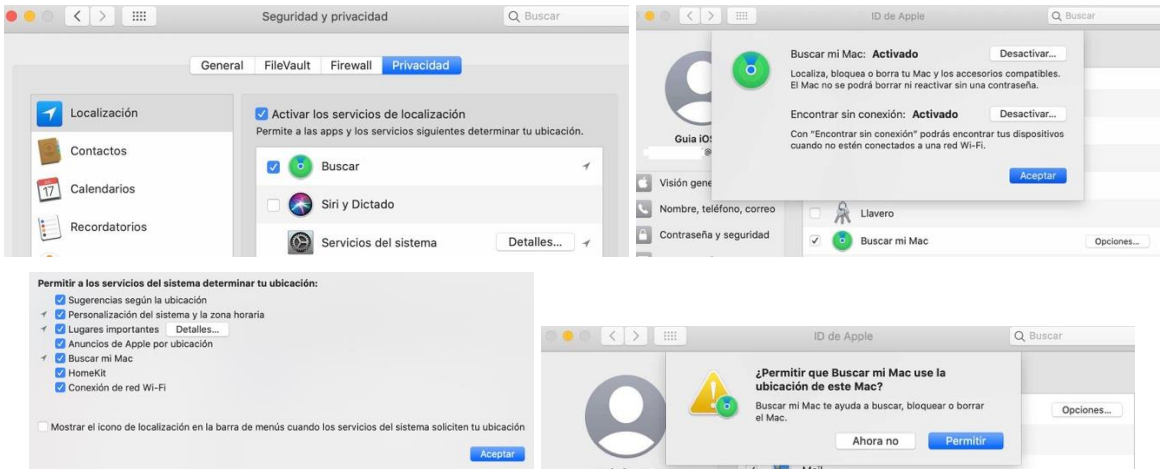



*Figura 54 - Ajustes requeridos para el servicio "Buscar" en macOS 10.15 Catalina*

La activación del servicio "Buscar" en macOS requiere privilegios de administración. Una vez habilitado, se creará un usuario en el sistema para gestionar el servicio FMM ("_findmydevice"), que se puede visualizar desde la "Utilidad de Directorios - Editor de

directorios" (ver apartado "Directorio de Servicios" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412]):

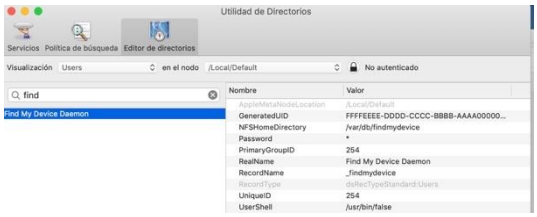



*Figura 55 - Usuario de sistema asignado a "Buscar mi Mac" (FMM) en macOS 10.14 y 10.15*

Si se intenta cerrar sesión en la cuenta de iCloud en el equipo, el sistema desactivará la funcionalidad "Buscar mi Mac", pero para ello solicitará la contraseña del ID de Apple, impidiendo que un tercero que desconozca la contraseña pueda deshabilitar la cuenta y/o este servicio. Si esta contraseña no es proporcionada, el sistema no cerrará la sesión de iCloud. El cierre de la sesión provocará que el campo "ID de Apple" de la sección "Usuarios y grupos - <Usuario> Opciones avanzadas" se restablezca, ya que el ID de Apple vinculado al usuario de sistema operativo corresponde al de la cuenta de iCloud (y no al ID de Apple que se puede usar en otros servicios adicionales de Apple, como iTunes o la App Store).

Es importante reseñar que la funcionalidad "Buscar mi Mac" permanece operativa aunque la pantalla esté bloqueada y aunque el usuario haya cerrado su sesión en el sistema. Sin embargo, si el equipo se reinicia y ningún usuario inicia sesión, "Buscar mi Mac" no podrá conectar con el equipo si el disco está cifrado con FileVault (opción recomendada desde el punto de vista de seguridad). Todas las acciones que se inicien desde el interfaz de "Buscar mi Mac" quedarán pendientes hasta que el disco sea desbloqueado mediante un inicio de sesión válido.

## 6.5 INTERFAZ WEB DE "BUSCAR"

Para hacer uso del servicio de localización del dispositivo, es preciso acreditarse con las credenciales asociadas al ID de Apple en la web de iCloud y seleccionar "Buscar" (o acceder directamente a través de https://www.icloud.com/#find). Se mostrará un mapa con la ubicación de todos los dispositivos asociados a la cuenta de iCloud, y, al seleccionar cualquiera de ellos, se detallará su última ubicación, el tiempo que ha transcurrido desde que ésta se obtuvo y un menú que permite realizar ciertas tareas de gestión remota dependientes del sistema operativo (descritas previamente) [Ref.- 8]. Los dispositivos cuya ubicación se conoce se marcarán con el símbolo "●" (verde), y con el símbolo "●" (gris) si la ubicación es desconocida.

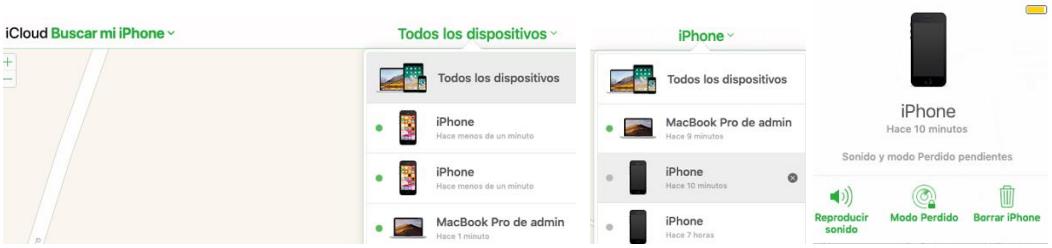



*Figura 56 - Interfaz web del servicio "Buscar"*

Si el dispositivo carece de conexión de datos (mediante una red cableada, Wi-Fi o móvil), las peticiones de gestión remota se encolarán, y se procesarán una vez que se recupere esta

conectividad (ver imagen derecha de la <Figura 56>). Si se opta por realizar una operación "Borrar" sobre un dispositivo de confianza (ver apartado "5.1.6. Dispositivos de confianza"), el dispositivo dejará de pertenecer a ese grupo.

Es posible dar de baja de la cuenta un dispositivo extraviado seleccionando la opción "⊗" (ver tercera imagen de la <Figura 56>). Si se habían invocado operaciones de gestión remota para este dispositivo mediante la funcionalidad "Buscar" que hubiesen sido encoladas por encontrarse el dispositivo inaccesible vía Internet cuando se solicitaron, estas operaciones se desestimarán, y no tendrán efecto.

Para desactivar la funcionalidad "Buscar" en un dispositivo es necesario introducir la contraseña asociada al ID de Apple.

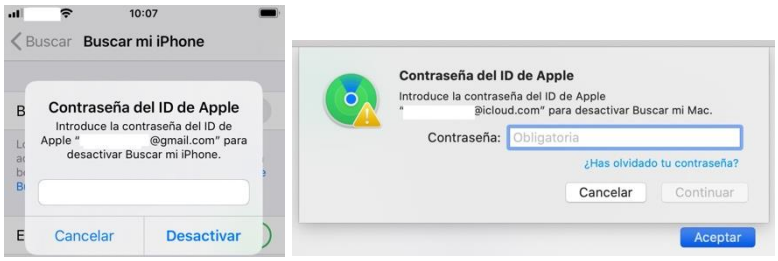



*Figura 57 - Desactivación de la función "Buscar" en iOS 13 y macOS 10.15*

En el año 2019 Apple introdujo en iOS 13 y macOS 10.15 Catalina la opción "Encontrar sin conexión" dentro de los servicios asociados a "Buscar" (ver apartado "6.7. Servicio "Encontrar sin conexión""), que permite la localización de un dispositivo aunque éste no disponga de conexión a una red de datos (cableada, Wi-Fi o móvil).

## 6.6 APP "BUSCAR"

La app "Buscar" está disponible tanto para iOS como para macOS. Ambas incluyen un menú y un mapa sobre el que se posicionarán las ubicaciones correspondientes a cada elemento de una categoría. Las categorías disponibles varían ligeramente entre iOS y macOS:

- Sección "Dispositivos": muestra la lista de los dispositivos de confianza (ver apartado ""5.1.6. Dispositivos de confianza""). Para acceder a las acciones disponibles sobre un dispositivo, basta con seleccionarlo en iOS. En macOS, es preciso pinchar en el icono "ⓘ" que aparece junto al dispositivo en el mapa de ubicación.
- Sección "Personas": muestra el menú desde el que es posible ver con qué contactos se está compartiendo actualmente la ubicación y quiénes la están compartiendo con el propietario de la cuenta de iCloud.
- Sección "Yo" (solo en iOS): su equivalente en macOS se encuentra dentro de la sección "Personas", y alberga los ajustes para la compartición de ubicación y la consulta de su estado (ver apartado "6.8. Servicio "Compartir mi ubicación"").

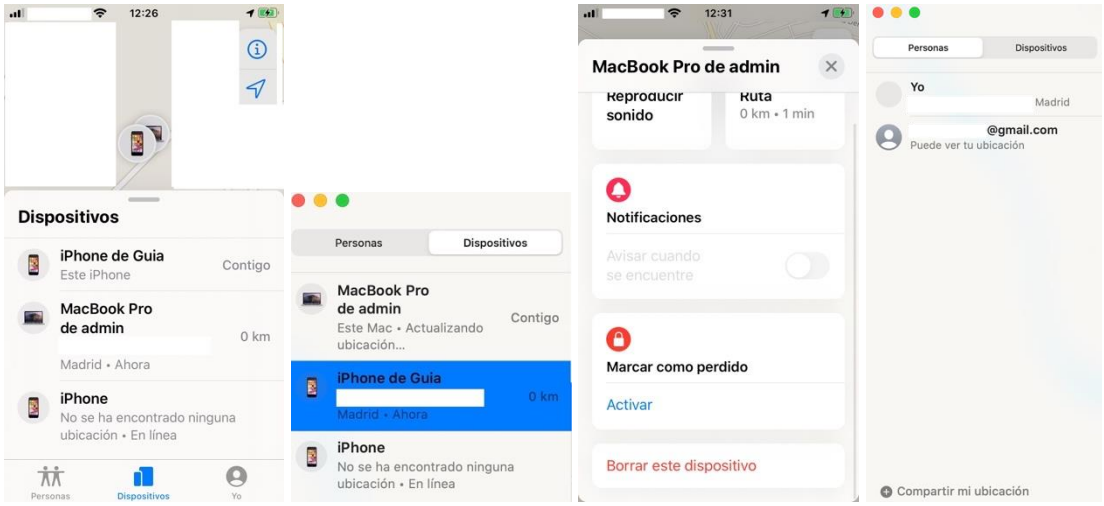



*Figura 58 - Interfaz gráfico de la app "Buscar"*

## 6.7 SERVICIO "ENCONTRAR SIN CONEXIÓN"

El servicio "Encontrar sin conexión" ("*Offline finding*"; ver apartado "Find My" de la [Ref.- 21]) permite a un usuario localizar un dispositivo (iPhone, Mac, iPad o Apple Watch) extraviado o sustraído que no disponga de conectividad hacia Internet, pero que sí tiene activo el interfaz Bluetooth. Los requisitos para el uso de este servicio son:

- Que la opción "Encontrar sin conexión" bajo "Ajustes - [ID de Apple] Buscar - Buscar mi iPhone" (iOS) o "Ajustes - [ID de Apple] Buscar mi Mac" (macOS) esté habilitada.
- Disponer de un segundo dispositivo vinculado al mismo ID de Apple desde el que se procederá a la localización del dispositivo perdido.
- Para que un dispositivo de Apple de un tercero pueda intervenir en la localización de otros dispositivos perdidos, también debe de tener esta opción activa.

Para que el servicio funcione respetando la privacidad del usuario y evitando que cualquiera (incluido Apple) pudiera utilizarlo para rastrear su localización [Ref.- 11], se utiliza un nuevo sistema criptográfico que se apoya en los siguientes mecanismos[12]:

- Cuando se habilita el ajuste "Encontrar sin conexión", el dispositivo (1) genera un par de claves pública y privada que se compartirán entre todos los dispositivos vinculados al mismo ID de Apple mediante comunicaciones cifradas (empleando el llavero de iCloud).
- Adicionalmente, el dispositivo (1) deriva un par de claves efímeras a partir del par de claves previo, que rota periódicamente (aproximadamente cada 15 minutos), y cuya clave pública asociada será emitida mediante mensajes de *broadcast* a través de Bluetooth (de forma similar a un *beacon*), siendo recibida por otros dispositivos Apple de terceros que se encuentren en rango. Este dispositivo ajeno (en adelante, "cooperante") obtendrá su propia ubicación (correspondiente a la ubicación aproximada del dispositivo perdido), la cifrará con la clave pública obtenida a través de Bluetooth, y enviará a Apple este dato de ubicación cifrado, junto a un *hash* de la clave pública, que actúa de identificador de los datos remitidos.

[12] https://www.wired.com/story/apple-find-my-cryptography-bluetooth/

- Cuando el propietario del dispositivo extraviado (1) intenta localizarlo mediante la app "Buscar" desde otro dispositivo (2) vinculado al mismo ID de Apple, el dispositivo (2) enviará a Apple los *hashes* de las últimas claves públicas que se hayan generado (y compartido entre los dispositivos asociados al mismo ID de Apple). Apple buscará entre todos los *hashes* almacenados hasta dar con el (o los) coincidente(s) que recibió por parte del dispositivo "cooperante" para el dispositivo (1).
- Cuando localice el *hash* coincidente, enviará al dispositivo (2) los datos de localización cifrados que se recibieron junto a ese *hash*, y que corresponderán a la ubicación aproximada de (1). De hecho, se podrían recibir diferentes localizaciones cercanas proporcionadas por múltiples dispositivos "cooperantes" que vieron la señal de Bluetooth emitida por el dispositivo perdido (1), mejorando así la precisión de su ubicación real. Como (2) posee la misma clave privada que (1), podrá descifrar los datos de ubicación cifrados con la clave pública asociada. La clave privada es compartida entre los diferentes dispositivos con el mismo ID de Apple mediante un canal cifrado extremo a extremo implementado a través del llavero de iCloud (y un mecanismo de derivación de claves).

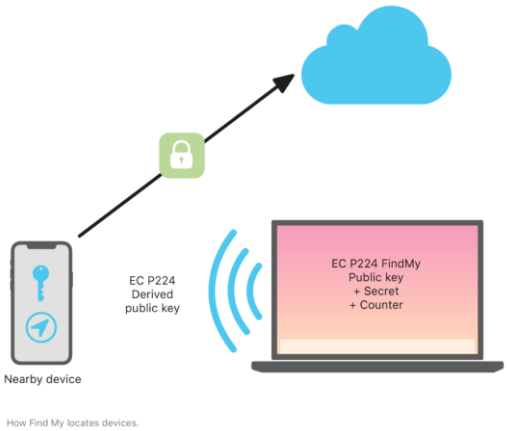



*Figura 59 - Esquema de funcionamiento de "Encontrar sin conexión" [Ref.- 21]*

Apple afirma que solo se almacena una ubicación para cada dispositivo marcado como extraviado. La identidad de los propietarios de las cuentas de iCloud involucradas (tanto de los dispositivos "cooperantes" como del extraviado) no se conocerá por parte de Apple, ya que el tráfico que se envía a sus servidores como parte de este servicio carece de información de autenticación o identificación en sus cabeceras.

Un dispositivo que se ha localizado mediante "Encontrar sin conexión" solo se mostrará en el mapa de la app "Buscar" de los dispositivos vinculados a su misma cuenta de iCloud. Como ilustra la imagen derecha de la <Figura 60>, el interfaz web de "Buscar" (en la parte inferior) solo es capaz de mostrar la "Ubicación anterior" obtenida hace una hora, mientras que la app "Buscar" de un Mac perteneciente a la misma cuenta de usuario de Apple puede dar la ubicación con unos minutos de retardo.

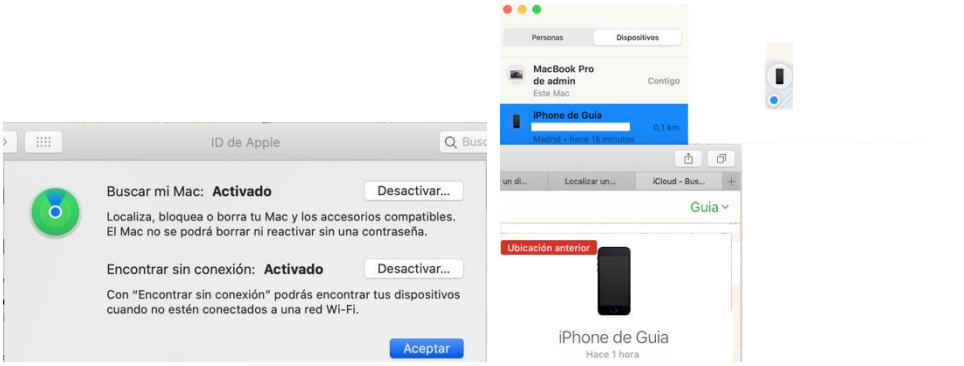



*Figura 60 - Localización de un dispositivo mediante "Encontrar sin conexión"*

## 6.8 SERVICIO "COMPARTIR MI UBICACIÓN"

Apple proporciona el servicio "Compartir mi ubicación" para favorecer la compartición de la ubicación (o el rastreo) de dispositivos vinculados a cuentas de iCloud diferentes a la propia (se requiere que el dispositivo móvil disponga de conexión a Internet para reportar su ubicación).

En versiones de iOS hasta la 12, el servicio se proporcionaba mediante una app independiente disponible en la App Store como "Buscar a mis amigos". En iOS 13 y macOS 10.15 Catalina, este servicio se incorpora a la app "Buscar", dentro de la categoría "Personas", y también a iCloud mediante el servicio "Amigos" (accesible a través del icono "🧍"). En esta categoría se puede consultar con quiénes se está compartiendo actualmente la ubicación y quiénes la están compartiendo con la cuenta de iCloud del usuario.

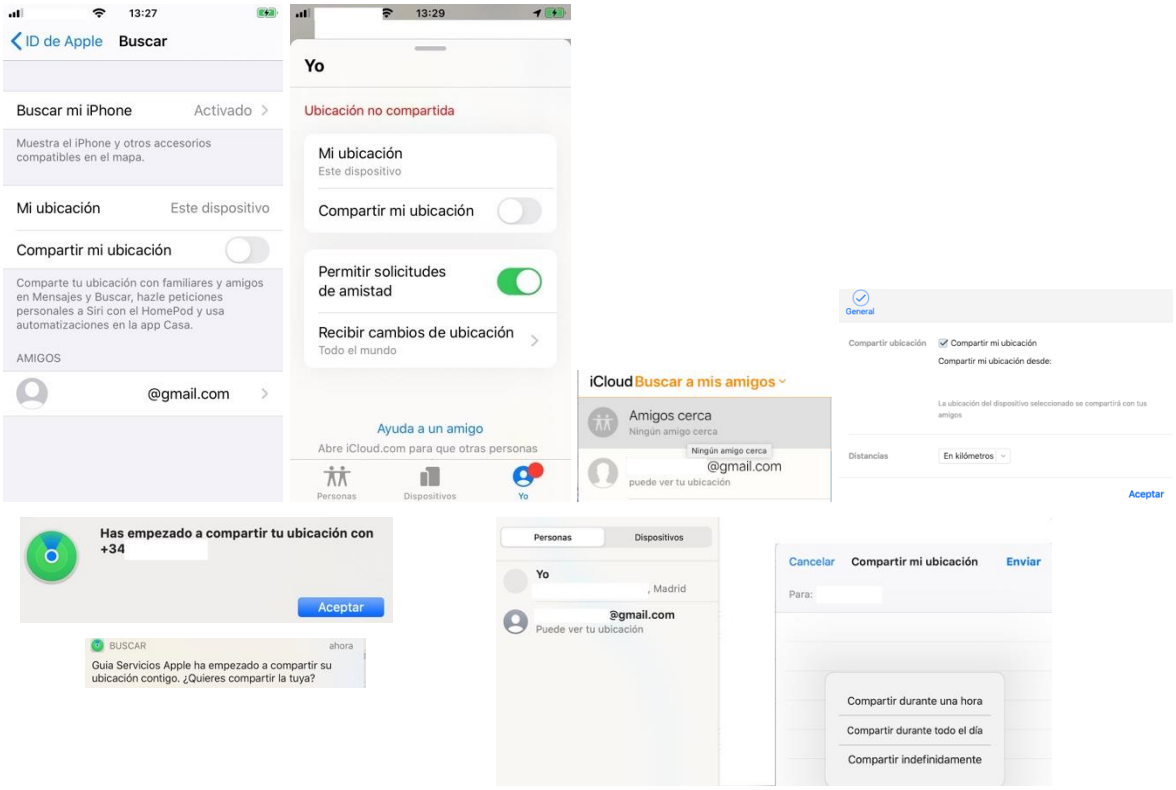



*Figura 61 - Ajustes para "Compartir mi ubicación" en iOS, interfaz web de iCloud y macOS*

En iOS, si se modifica el interruptor "ID de Apple - Buscar - Compartir ubicación" (primera imagen de la <Figura 61>), se cambiará también el de la app "Buscar", y viceversa.

La solicitud de compartición de ubicación del dispositivo se cursa a través de la app "Mensajes". El dispositivo externo recibirá una notificación, que, al abrirse, consultará a su propietario si desea que la compartición de ubicación sea recíproca:

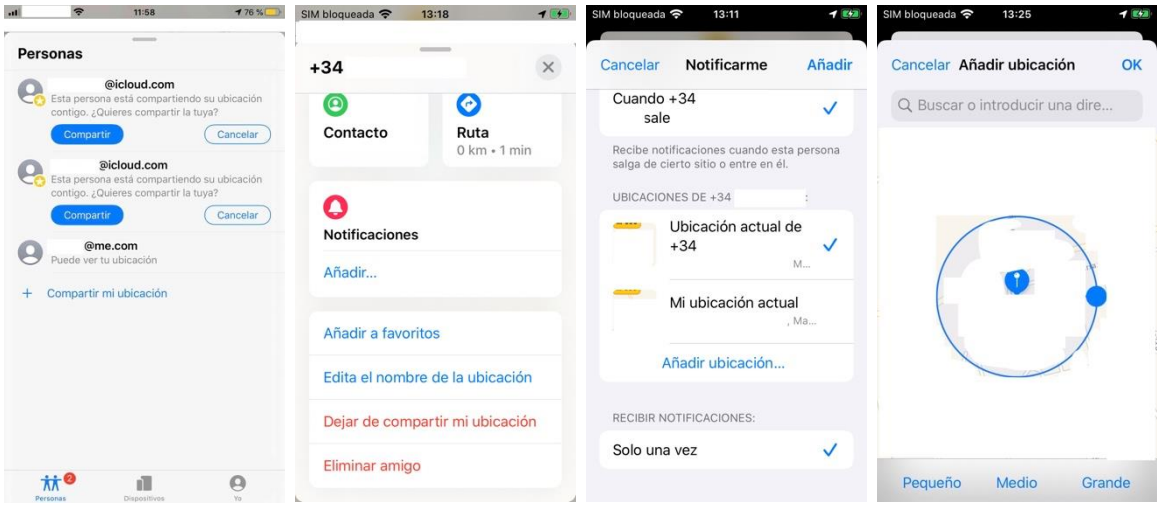



*Figura 62 - Compartición de ubicación a través de iCloud*

Se puede detener la compartición de ubicación tanto a nivel global (desactivando el interruptor "Compartir mi ubicación") como de forma discrecional, accediendo a la app "Buscar" y seleccionando al contacto con el que ya no se desea compartir la ubicación en el menú "Personas - Dejar de compartir mi ubicación".

El menú "Notificaciones" permite configurar ante qué eventos de ubicación del contacto que la comparte se desea recibir un aviso, o viceversa, es decir, qué eventos de ubicación propia se enviarán al contacto con el que se está compartiendo. Se ofrecen por defecto la llegada a o salida de la ubicación actual, pero se permite definir ubicaciones precisas y el radio de proximidad a las mismas que disparará la notificación (ver <Figura 62>).

Si no se desea que terceros puedan iniciar la compartición de ubicación con la cuenta de iCloud propia, se puede desactivar el interruptor "Permitir solicitudes de amistad".

Este servicio puede resultar interesante como medida de control parental sobre dispositivos de menores, especialmente para los miembros de una familia en iCloud (ver apartado "6.9. Grupo "Familia""). Desde el punto de vista del usuario adulto, también es interesante si se debe visitar un lugar que entrañe peligro. Desde el punto de vista de privacidad, la activación del ajuste debería ser solo puntual, y eliminarse tan pronto finalice la necesidad de usarlo.

La funcionalidad "Atajos" ofrece un atajo predefinido para iniciar la compartición de ubicación (ver apartado "Atajos (shortcuts): automatización en iOS 13" de la guía "Configuración segura de iOS 13" [Ref.- 413]).

## 6.9 GRUPO "FAMILIA"

"En Familia" es un servicio de Apple que permite agregar diferentes cuentas de iCloud (hasta un máximo de seis) dentro de un grupo especial con el objetivo de compartir contenidos y

otros servicios entre todos sus miembros. La configuración detallada de este servicio puede consultarse en la documentación oficial de Apple [Ref.- 29].

Un ID de Apple únicamente puede pertenecer a un grupo "Familia", y se establece como limitación un solo cambio de familia al año.

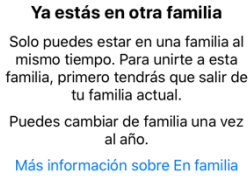



*Figura 63 - Limitación de pertenencia a más de un grupo "Familia"*

**NOTA:** para poder disolver un grupo "Familia", las cuentas de iCloud de los menores de 13 años tienen que trasladarse a otro grupo familia siguiendo las indicaciones de la [Ref.- 31].

Uno de los principales servicios disponibles para "Familia" es la gestión remota de los dispositivos vinculados al grupo, que permite acceder a toda la funcionalidad de "Buscar" (ver apartado "6. Gestión remota de dispositivos: Servicio "Buscar"") desde cualquier cuenta de iCloud del grupo, incluidas las de los menores.

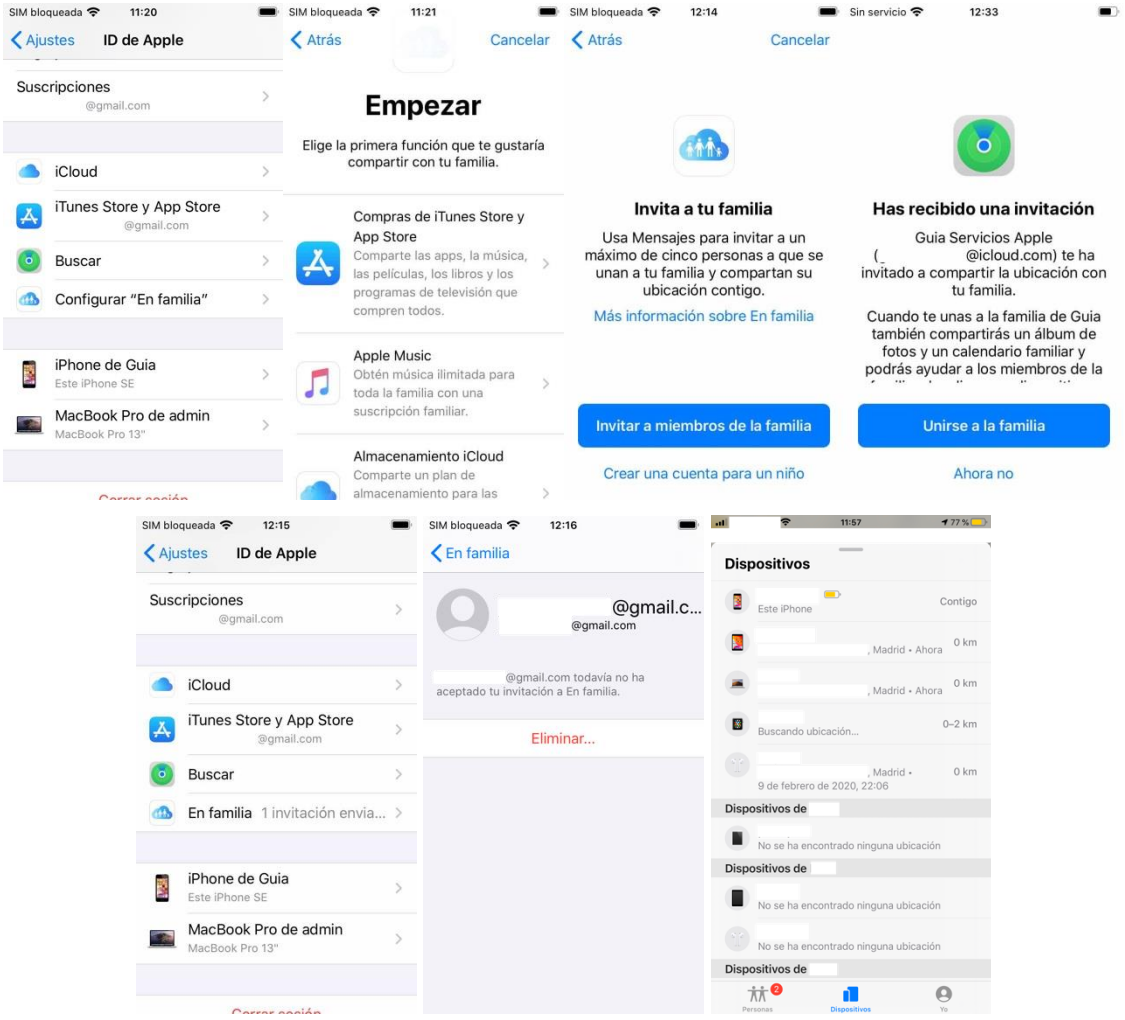



*Figura 64 - Configuración del grupo "Familia" en iOS 13 (1)*

Los mensajes de invitación al grupo "Familia" en iOS se pueden cursar mediante:

- iMessage: en este caso, puede ocurrir (si la dirección asociada al ID de Apple invitado no pertenece al dominio icloud.com o me.com) que el mensaje se curse por SMS, por lo que pueden conllevar un coste asociado.
- "En persona": en ese escenario, se presentará en el dispositivo un menú en el que el invitado tendrá que introducir las credenciales asociadas a su ID de Apple.
- Creación de una cuenta para un menor.

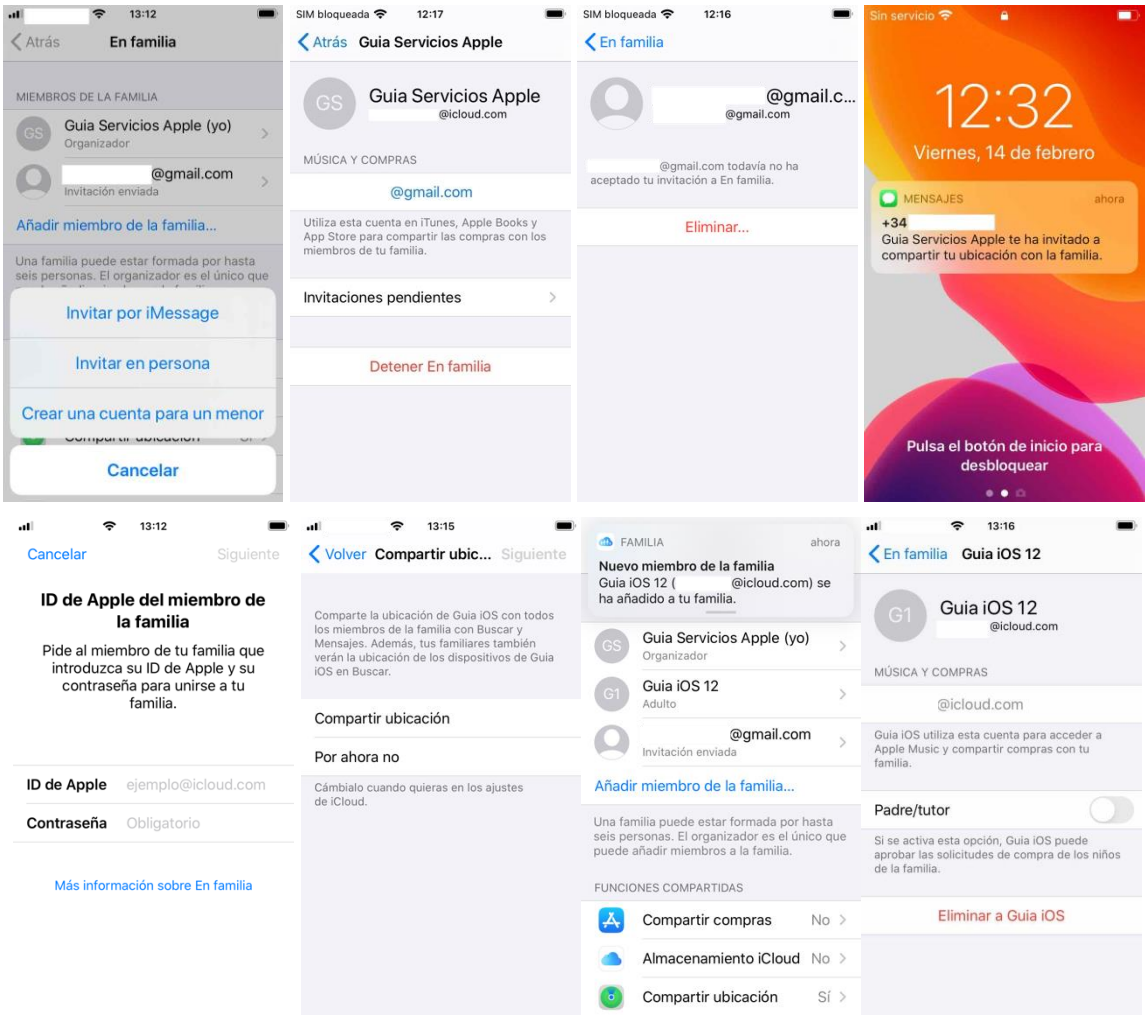



*Figura 65 - Configuración del grupo "Familia" en iOS 13 (2)*

Una vez aceptadas las invitaciones por parte de los ID de Apple invitados, la app "Buscar" mostrará en la sección "Personas" la lista de dispositivos propios (en la parte superior) y las de los dispositivos de otros miembros de la familia en secciones sucesivas.

Los servicios disponibles para compartición entre miembros del grupo "Familia" se describen en los siguientes apartados.

### 6.9.1 ROLES DE "EN FAMILIA"

Los diferentes roles de cada miembro del grupo "Familia" se pueden consultar en "ID de Apple - En familia - Miembros de la familia":

- Miembros de la familia: muestra el listado de integrantes, junto a su rol (organizador, padre/tutor, adulto) o la edad (para los menores de 18 años). Cada rol lleva asignada una serie de capacidades, y todos - a excepción de los menores - pueden abandonar el grupo mediante la opción "Salir de la familia":
  - Organizador: es el creador del grupo "Familia", y el único con capacidades para disolverlo (a través de la opción "Detener En familia"), conceder/revocar el rol "Padre/tutor" y añadir otros miembros a la familia (mediante el menú "Añadir miembro de la familia"). Tiene potestad para gestionar todas las funciones compartidas (descritas a continuación).
  - Padre/tutor: las cuentas configuradas con este rol pueden aprobar/denegar solicitudes de compra por parte de los miembros menores. Pueden asimismo gestionar todas las funciones compartidas, a excepción de "Compartir ubicación".
  - Adulto: pueden contratar un plan para almacenamiento en iCloud y activar/desactivar la compartición de su propia ubicación. Puede abandonar voluntariamente el grupo.
  - Menor: a este grupo se añadirán las cuentas de iCloud de los menores de 18 años. No obstante, los mayores de 14[13] años pueden abandonar el grupo "Familia".
  - La función "Solicitar la compra" de la App Store se habilita por defecto para los menores de 13 años, y el organizador deberá definirla explícitamente para las cuentas pertenecientes a menores de 18 años que se añadan al grupo familiar.

### 6.9.2 FUNCIONES COMPARTIDAS ENTRE EL GRUPO "FAMILIA"

La configuración de las funciones compartidas por los integrantes del grupo "Familia" está disponible en "ID de Apple - En familia - Funciones compartidas", algunas de las cuales solo pueden ser activadas/desactivadas por parte del miembro "organizador".

- "Compartir compras": si la compartición de compras se habilita por parte del organizador, cada miembro adulto de la familia puede definir si desea compartir su cuenta de la App Store propia con el resto de integrantes (ver apartado "5.3. Cuenta de iTunes/App Store"). Para poder hacer uso del servicio de compartición de compras, se requiere tener configurado algún método de pago en los ajustes correspondientes a la "App Store" (ver apartado "5.3.1. Compras del grupo "Familia"").
  La descarga de contenidos puede compartirse con hasta 10 dispositivos por cada cuenta, y con un máximo de cinco ordenadores [Ref.- 26].
  La selección de un componente en el menú "Familia" permite consultar su ID de Apple, y ver qué configuración tiene para la función de compartición de compras.

  **NOTA**: en las pruebas realizadas durante la elaboración de la presente guía, se constata que, en macOS, incluso aunque no se seleccione la opción de compartición de compras, Apple requiere que exista un método de pago vigente para el ID de Apple que se configura como organizador, tal como ilustra la <Figura 66>. No se observa esta limitación en iOS 13.

- "Almacenamiento iCloud": Apple permite el uso de un almacenamiento compartido para los miembros de la familia si se dispone de un plan de pago de 200 GB o 2 TB, no siendo posible compartir el que se proporciona de forma gratuita con la cuenta de iCloud individual.

[13] Esta edad puede variar en función de la zona geográfica. Para España, la edad para poder abandonar el grupo familia es de 14 años, mientras que en EEUU es de 13 años.

- "Compartir ubicación": solo el organizador puede activar esta funcionalidad; una vez habilitada, cada miembro mayor de edad puede optar por compartir o no su ubicación con el resto de integrantes desde este menú. La ubicación de los miembros que la comparten se puede obtener a través de la app "Buscar" en la sección "Personas".

**IMPORTANTE:** durante las pruebas realizadas en la elaboración de la presente guía, se constata que, una vez habilitada la compartición de ubicación, no se dispone, ni en iOS ni en macOS, ni en el interfaz web de administración de iCloud, de opción alguna para deshabilitarla. Únicamente se dispone de un interruptor para gestionar la propia compartición de ubicación.

- "Tiempo de uso" (*Screen Time*): esta funcionalidad permite establecer controles parentales sobre el uso del dispositivo (por ejemplo, apps permitidas y tiempo máximo de uso de las mismas) sobre los menores de 18 años. Se recomienda consultar el apartado "Tiempo de uso" de la guía "Configuración segura de iOS 13" [Ref.- 413] para obtener detalles sobre su funcionalidad.
  Cuando se alcance alguna restricción establecida, el dispositivo del menor le mostrará una notificación, desde la que se puede iniciar una solicitud para ampliar el límite. Los miembros del grupo con rol organizador y padre/tutor recibirán a su vez otra notificación, desde la que se puede ampliar o denegar la extensión del límite.
- "Apple Music", "Canales de TV" y "Apple Arcade": estos ajustes permiten configurar la compartición de suscripciones a cada uno de estos servicios.




*Figura 66 - Configuración del grupo "Familia" en macOS*

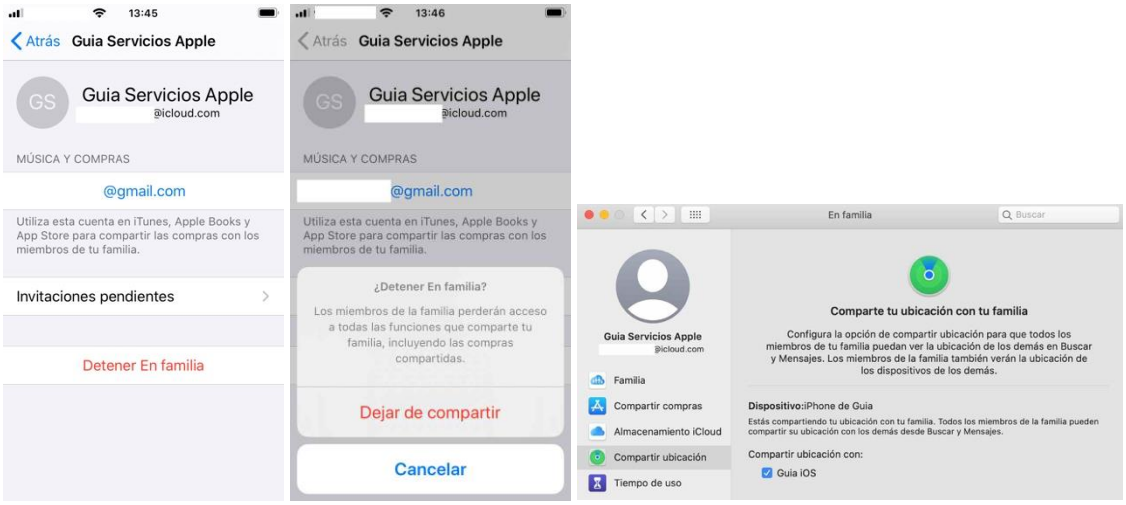



*Figura 67 - Configuración de funciones compartidas para "Familia"*

Existen otros servicios adicionales, descritos a continuación, que se configuran fuera de esta sección. Dado que estos servicios están accesibles a través de iCloud y, por tanto, albergados en los servidores de Apple, se recomienda valorar su necesidad y, en caso de ser innecesarios, prescindir de ellos.

#### 6.9.2.1 Compartir Internet con "Familia"

iOS permite compartición de los puntos de acceso personales entre los dispositivos vinculados a las cuentas de iCloud del grupo "Familia". Para ello, se dispone del menú "Ajustes - Datos móviles - Punto de acceso personal - En familia". Este menú permite habilitar la compartición del punto de acceso y definir, para cada integrante del grupo, si podrá conectarse de forma automática o si se requerirá aprobación por parte del propietario del *hotspot* (***recomendado desde el punto de vista de seguridad***), no siendo posible denegar la conexión de forma particular para un integrante.

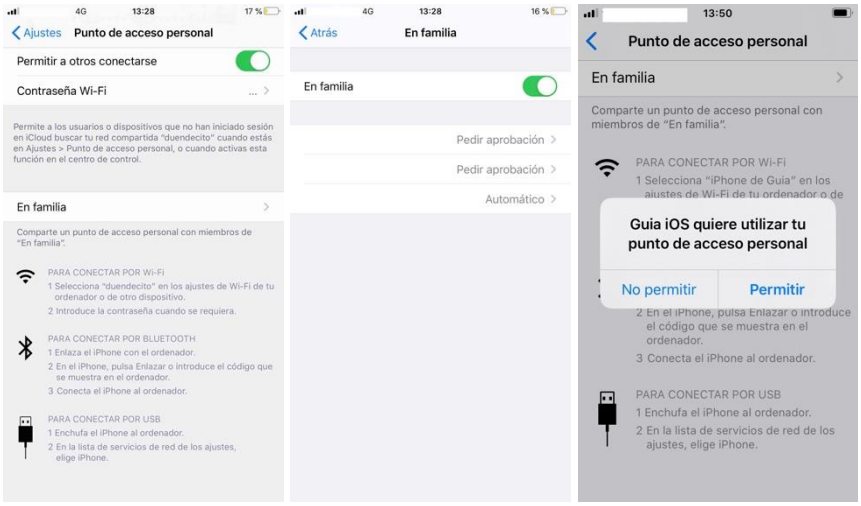



*Figura 68 - Compartición del punto de acceso personal con los miembros del grupo "Familia"*

Con esta compartición habilitada, no se precisa introducir la contraseña del punto de acceso en los dispositivos vinculados a las cuentas de iCloud del grupo "Familia".

Este servicio requiere que el interfaz Bluetooth de los dispositivos implicados en la conexión esté habilitado en el menú "Ajustes - Bluetooth", ya que, como se describe en el apartado "7.1.6. Instant Hotspot", el interés de conexión al *hotspot* por parte de un dispositivo se emite como anuncio BLE. Es importante reseñar que la operación de deshabilitar las conexiones Bluetooth desde el icono "" del Centro de control (pasando a un estado de semi-activación de color blanco) no impide el funcionamiento de la compartición del punto de acceso personal.

**IMPORTANTE:** el mecanismo para la compartición del punto de acceso personal entre miembros de la familia no requiere que el ajuste "Datos móviles - Punto de acceso personal - Permitir a otros conectarse" esté habilitado.

**IMPORTANTE:** durante las pruebas realizadas durante la elaboración de la presente guía, se constata que el interruptor "Permitir a otros conectarse" se habilita automáticamente si un dispositivo vinculado al grupo "Familia" se conecta al *hotspot*. Si durante el intervalo en que dura la conexión se recibe una solicitud de conexión por parte de otro dispositivo que conoce la contraseña, se permitirá también su conexión sin informar al usuario.

El interruptor "Permitir a otros conectarse" no se deshabilita inmediatamente cuando finaliza la conexión del dispositivo "familia" (se ha constatado que pueden transcurrir más de 30 segundos), por lo que otras conexiones al *hotspot* por parte de dispositivos que conozcan la contraseña serán cursadas desde ese momento.

Si un dispositivo de la familia está conectado al *hotspot* y un tercero entra en el rango de alcance y solicita conectarse a él, se recibirá una solicitud de compartición de la contraseña Wi-Fi en el dispositivo invitado (vinculado al familiar), no en el que ofrece el *hotspot*. Esto tiene importantes implicaciones desde el punto de vista de seguridad, porque la contraseña de la red Wi-Fi podría ser compartida sin que el propietario del dispositivo que ofrece el *hotspot* tenga conocimiento de ello.

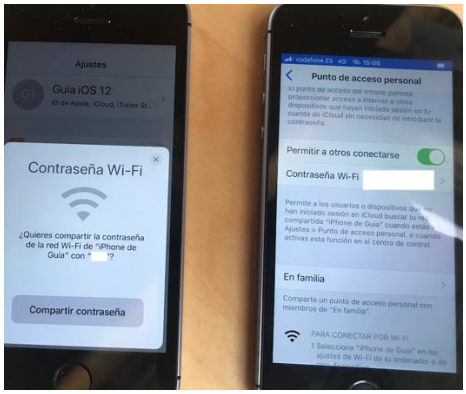



*Figura 69 - Compartición de punto de acceso personal activa con un miembro del grupo "Familia" y notificación en el dispositivo cliente para compartir la contraseña de la red Wi-Fi con un tercero ajeno al grupo*

Los detalles sobre el uso de *hotspot* en iOS 13 pueden consultarse en el apartado "Personal hotspot" de la guía "Configuración segura de iOS 13" [Ref.- 413], y ***se recomienda aplicar las recomendaciones de seguridad en él descritas***.

#### 6.9.2.2 Álbum de fotos compartido con "Familia"

La configuración del servicio "En familia", o creación del grupo "Familia", lleva implícita la creación de un álbum compartido en la app "Fotos", en el que los miembros del grupo quedan automáticamente añadidos como "suscriptores", con capacidad para añadir y editar contenidos. La adición de contenidos se notificará a todos los suscriptores, de forma análoga a la de cualquier otro álbum compartido.

Se recomienda eliminar este álbum si no se desea hacer uso de este servicio. En todo caso, se aconseja desactivar la opción "Sitio web público", que permitiría que el álbum quede accesible a través de un enlace público en iCloud.




*Figura 70 - Álbum de fotos compartido asociado al grupo "Familia"*

La compartición de fotografías se describe en el apartado "11.7. Fotografías y vídeos".

### 6.9.2.3 Calendario compartido con "Familia"

La configuración del servicio "En familia" conlleva la creación de un calendario compartido, al que todos los miembros se añaden como suscriptores, pudiendo consultar y añadir eventos, y recibir notificaciones en todos sus dispositivos con las actualizaciones realizadas sobre dicho calendario por parte del resto de integrantes del grupo.

Se recomienda eliminar este calendario salvo necesidad expresa. El ajuste "Calendario público" debe mantenerse deshabilitado para impedir su acceso por parte de terceros a través de un enlace "webcal".

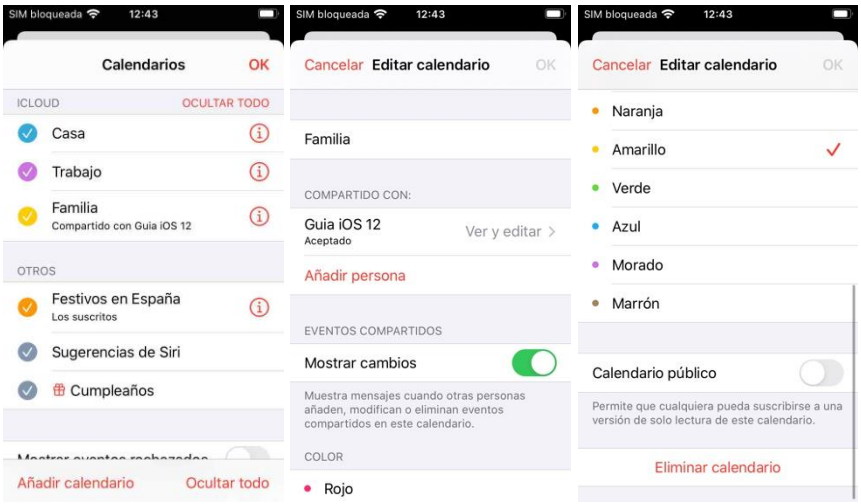



*Figura 71 - Calendario compartido asociado al grupo "Familia"*

La compartición de calendarios se describe en el apartado "11.5. Calendarios".

#### 6.9.2.4 Recordatorios compartidos con "Familia"

La creación del grupo "Familia" añade a la app "Recordatorios" la lista compartida "Familia", integrada por defecto por todos los miembros del grupo, y cuyo propietario es la cuenta de iCloud asignada al rol organizador.

Es posible eliminar por completo esta lista (opción "Eliminar lista"), dejar de compartirla temporalmente (opción "Dejar de compartir") y revocar el acceso a ella para ciertos integrantes del grupo (opción "[Miembro del grupo] - Eliminar acceso"). Se recomienda limitar el uso de la lista a lo mínimo que se requiera.




*Figura 72 - Recordatorio asignado al grupo "Familia"*

En el apartado "11.1. Recordatorios" se proporciona información sobre esta funcionalidad.

# 7. SERVICIOS PROPIETARIOS DE APPLE

## 7.1 CONTINUIDAD

Recomendaciones de seguridad:

- Desactivar los servicios de continuidad cuando no se requiera hacer uso de los mismos, en especial, *handoff* y el portapapeles universal.
- Evitar hacer uso del desbloqueo automático del Mac con el Apple Watch.

"Continuidad" (*Continuity*) es un conjunto de servicios que Apple proporciona con el propósito de simplificar tareas cotidianas del usuario, por ejemplo:

- Utilización indistinta de los dispositivos vinculados a una misma cuenta de iCloud para realizar una labor determinada, que puede ser iniciada en cualquiera de ellos y retomada en otro.
- Establecimiento de relaciones de confianza entre dispositivos vinculados a la misma cuenta de iCloud, por ejemplo, para desbloquear un Mac con un Apple Watch.
- Copiar y pegar contenidos de un dispositivo a otro.
- Compartición de Internet entre dispositivos.

En la [Ref.- 35] se proporciona el recurso oficial de Apple para la configuración de los servicios de Continuidad, y en la [Ref.- 36] la lista con los dispositivos Apple para los cuales está soportada esta funcionalidad.

Los servicios de continuidad requieren que los dispositivos tengan habilitados los interfaces Wi-Fi y Bluetooth, lo cual contrapone la recomendación general de seguridad de no mantener permanentemente activos estos interfaces. Adicionalmente, el uso de estos servicios requiere que la mayoría de los contenidos que se intercambian pasen por los servidores de iCloud de Apple, por lo que debe sopesarse las implicaciones desde el punto de vista de la privacidad. Por tanto, ***se aconseja desactivar los interfaces Wi-Fi y Bluetooth cuando no se esté haciendo uso de los servicios de continuidad***.




*Figura 73 - Opción "Handoff" para servicios de "Continuidad"*

### 7.1.1 APNs (APPLE PUSH NOTIFICATION SERVICE)

El servicio APNs (Apple Push Notification service) [Ref.- 37] proporciona una arquitectura para propagar información entre las apps y los dispositivos Apple mediante el envío de notificaciones remotas de tipo *push*.

Cuando una app o servicio que hace uso de esta funcionalidad se inicia, se establece una conexión TCP/IP persistente, autenticada y cifrada entre la app y el servicio APNs de Apple, que se empleará para que la app se registre como receptora de notificaciones.

Los denominados "proveedores" (servidores que el desarrollador de la app configura para usar APNs) envían sus notificaciones al servicio APNs mediante peticiones HTTP/2 a través de un canal seguro, de forma que el servicio APNs las distribuya a las apps destinatarias de los dispositivos receptores.

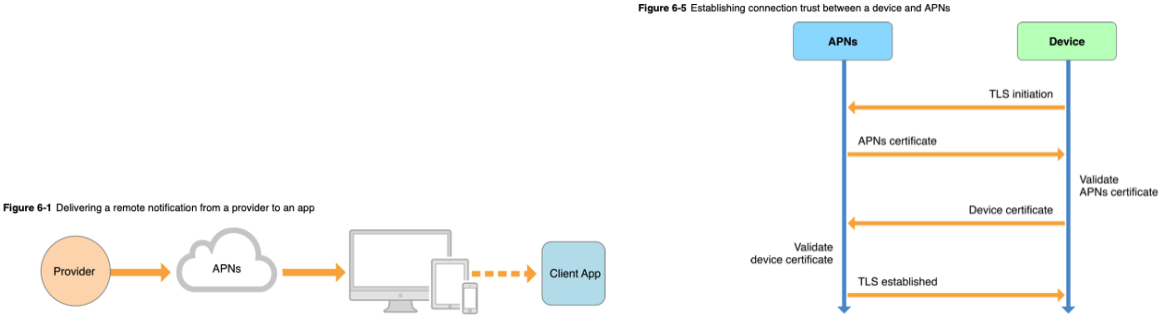



*Figura 74 - Arquitectura del Apple Push Notification service (APNs) [Ref.- 37]*

El proveedor puede determinar qué instancias de su app están en ejecución a través de un *token* (que asigna Apple) único y específico para una app y un dispositivo. Cada instancia de la app recibe su *token* cuando se registra en el APNs, y este *token* se traslada al proveedor, quien debe incluirlo como parte de la notificación *push* para que ésta pueda cursarse hacia el dispositivo y la app legítimos.

Por su parte, la comunicación entre el APNs y un dispositivo se realiza a través de una conexión TLS que utiliza:

- El certificado criptográfico y la clave privada del dispositivo que el sistema operativo le asigna durante su activación inicial.
- El certificado del APNs.

De este modo se pretende que ninguna notificación *push* pueda llegar a un dispositivo ilegítimo.

### 7.1.2 HANDOFF

"Handoff" permite iniciar una actividad en un dispositivo y retomarla en otro dispositivo Apple vinculado a la misma cuenta de iCloud que se encuentre en el rango de Bluetooth. Entre las tareas que se pueden continuar entre dispositivos y los intercambios que permite este servicio, se encuentran [Ref.- 71]:

- De app nativa a app nativa: por ejemplo, entre las apps Mail de iOS y Mail de macOS, o Safari de iOS y Safari de macOS.
- De app nativa a navegador web.
- De navegador web a app nativa.
- De app de Apple Watch a app de iOS.

Para poder hacer uso del servicio, se requiere:

- Tener el ajuste "Handoff" activado: para evitar el uso accidental de "Handoff", ***se aconseja mantener el ajuste desmarcado y proceder a su activación cuando sea preciso***:
  - macOS: "Preferencias del Sistema - General - Permitir Handoff entre este Mac y tus dispositivos con iCloud".
  - iOS: "Ajustes - General - AirPlay y Handoff".

  Cuando se activa el ajuste de "Handoff", el sistema añade unas claves de cifrado en la categoría "Contraseñas" del llavero "Inicio de sesión" (ver apartado "8.2. Gestión de las contraseñas almacenadas en el llavero").
- Que los dispositivos implicados tengan Bluetooth y Wi-Fi activos.

Los dispositivos implicados en una operación de "Handoff" se emparejan mediante *Bluetooth Low Energy* (BLE) 4.2 a través del servicio APNs (ver apartado "7.1.1. APNs (Apple Push Notification service)"). Cada dispositivo genera (y almacena en su llavero o *Keychain*) una clave simétrica AES de 256 bits, que se emplea para cifrar y autenticar los anuncios sobre las tareas que actualmente están en curso, los cuales se recibirán en el resto de dispositivos emparejados. Los anuncios emplean AES-256 en modo GCM (Galois/Counter Mode)[14] con medidas para protección ante ataques de *replay* [Ref.- 21].

Cuando un dispositivo recibe por primera vez un anuncio asociado a una nueva clave, inicia una conexión (cifrada con los mecanismos de cifrado BLE 4.2) con el dispositivo que la envió, y

[14] https://en.wikipedia.org/wiki/Galois/Counter_Mode

realiza un intercambio de claves de cifrado que se utilizarán para proteger los mensajes. Las claves de "Handoff" se incluyen en el llavero (en macOS, se incluyen en el llavero de inicio de sesión, "handoff-own-encryption-key", y son accesibles para el demonio "`sharingd`").

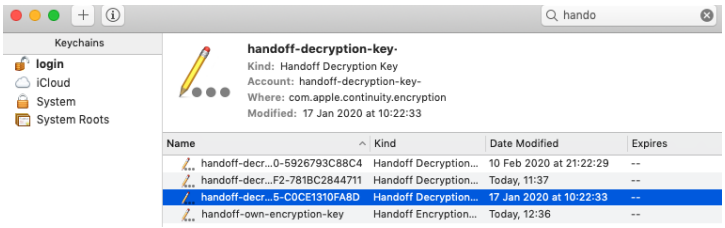



*Figura 75 - Clave de cifrado de "Handoff" almacenada en el llavero de macOS*

**NOTA:** otras aplicaciones de terceros de macOS también pueden añadir al llavero sus propias entradas relacionadas con "Handoff", tal como muestra la imagen superior (tres entradas).

La operación de "Handoff" se lanza de forma automática en macOS en la esquina izquierda del "Dock", y, posicionándose sobre la app, se obtendrán los detalles de la app del dispositivo origen. En iOS, es preciso iniciar el selector de tareas (mediante doble pulsación en el botón de inicio) para que se muestre el icono correspondiente a "Handoff" y a la tarea a continuar.

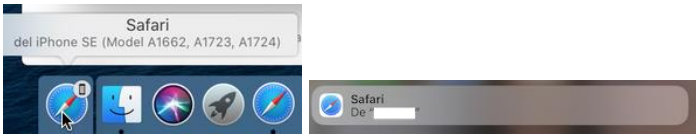



*Figura 76 - Ejemplo de uso de "Handoff" entre navegadores web Safari de dos dispositivos Apple*




*Figura 77 - Ejemplo de "Handoff" entre una app y un navegador web*

Las ventanas de navegación privada de Safari no son susceptibles de transferirse vía "Handoff".

### MECANISMO DE "HANDOFF" ENTRE APPS Y SITIOS WEB

Mediante "Handoff", una app puede:

- Retomar en otro dispositivo de confianza (2) la actividad que el usuario estuviera llevando a cabo en el navegador web de un dispositivo (1) para una página web de los dominios propiedad del desarrollador de la app. Ambos (app y navegador web) han de implementar las APIs de "Handoff":
  - Para evitar que las apps puedan reanudar actividades de sitios web fuera del control del desarrollador de la app, el sistema utiliza el mecanismo de credenciales web compartidas basado en el recurso "`/.well-known/apple-app-site-association`" del sitio web, en el que se declaran los identificadores de las apps permitidas para el sitio web (`applinks`) y las URLs concretas dentro del sitio web (`paths`) (este mecanismo es similar al descrito en el apartado "8.2.4. Autorrelleno de contraseñas y de códigos de seguridad").

- Cuando el usuario esté navegando en el dispositivo (1) y el dispositivo (2) esté en rango de Bluetooth, el sistema operativo iOS/macOS de (1) enviará un anuncio de "Handoff" cifrado en el que se indica el dominio de la página web visitada. El sistema operativo de (2) recibirá el anuncio y, si detecta que tiene una app instalada que ha declarado en sus *entitlements*[15] aceptar "Handoff" para ese dominio, mostrará su icono en el área de "Handoff". Si el usuario lo selecciona, el sistema abrirá la app con la URL completa y el título de la página.

**NOTA:** en las pruebas realizadas durante la elaboración de la presente guía, no se ha conseguido mostrar un ejemplo real de este escenario, ya que, cualquier intento de transferencia desde un navegador web en el dispositivo (1) a una app nativa que soporte "Handoff" en el dispositivo (2) es interceptada por Safari, sin que ni iOS ni macOS ofrezcan el icono de la app de forma adicional (Safari tiene prioridad sobre las apps).

- Trasladar al navegador web de (2) la actividad que la app nativa estuviese realizando en (1) si (2) no dispone de dicha app nativa: para ello, la app de (1) puede enviar una URL de *fallback*, que el sistema operativo de (2) abrirá en el navegador web por defecto (siempre que soporte "Handoff") si el usuario selecciona el icono correspondiente a la tarea a continuar. En este caso, no es obligatorio que la URL de *fallback* se incluya en los dominios del desarrollador de la app nativa.
  En la <Figura 77> se proporciona un ejemplo de este escenario. Como se puede observar, el navegador web mostrará brevemente una indicación (en la barra de navegación) de que está abriendo una página mediante "Handoff", y a la derecha se observa la URL de *fallback*.

Es importante reseñar que, si el usuario dispone de una sesión autentificada, "Handoff" únicamente pasará las referencias al recurso del sitio web, sin incluir información de la sesión.

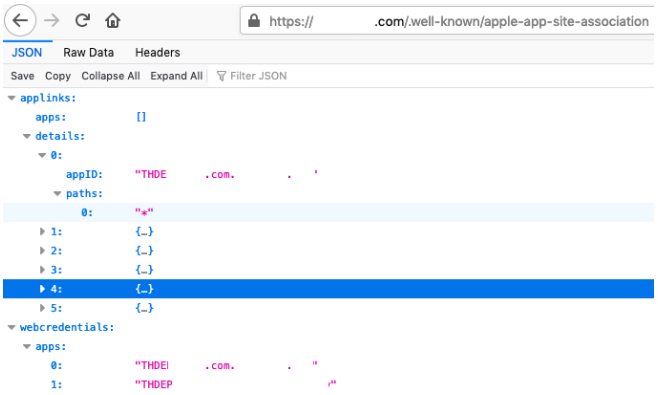



*Figura 78 - Recurso "/.well-known/apple-app-site-association" para un sitio web*

### "HANDOFF" A TRAVÉS DE CONEXIONES WI-FI "PEER-TO-PEER"

Cuando la operación de "Handoff" requiere un intercambio de datos mayor (por ejemplo, una app de correo que puede incluir adjuntos de gran tamaño), la app puede utilizar conexiones Wi-Fi "*peer-to-peer*" (el mecanismo es similar al de AirDrop, cuyos detalles pueden consultarse en el apartado "AirDrop" de la guía "Configuración segura de iOS 13" [Ref.- 413]).

- El intercambio inicial utiliza BLE, al igual que las conexiones "Handoff" típicas.

[15] Consultar el enlace de Apple sobre "Supporting Associated Domains in Your App" en https://developer.apple.com/documentation/safariservices/supporting_associated_domains_in_your_app para más información.

- Posteriormente, se intercambian los certificados de identidad de iCloud a través de una conexión TLS vía Wi-Fi, cuya identidad se compara con la del usuario.
- Si las identidades coinciden, se procede al envío del resto de los datos sobre la conexión TLS cifrada.

### 7.1.3 PORTAPAPELES UNIVERSAL

Este servicio permite que los contenidos que se copian en un dispositivo Apple se trasladen al portapapeles de otro dispositivo Apple cercano, desde el que se pueden pegar hasta que sean reemplazados por otro contenido o transcurra cierto tiempo. Esta funcionalidad requiere que "Handoff" esté habilitado en ambos dispositivos, y los desarrolladores de apps disponen de mecanismos para que el contenido que se copie en su app no se comparta a través del portapapeles.

Todas las apps del dispositivo cercano tienen acceso al portapapeles universal, y no se requiere por parte del usuario confirmación sobre el contenido a pegar, siendo transparente para él el dispositivo de procedencia, a diferencia de lo que ocurre con la funcionalidad estándar de "Handoff".

### 7.1.4 RECEPCIÓN DE LLAMADAS TELEFÓNICAS

Este servicio de continuidad permite cursar y responder las llamadas telefónicas de un iPhone desde otro dispositivo Apple compatible que se encuentre en su misma red Wi-Fi. Se desaconseja su utilización en entornos laborales, ya que podría ocurrir que el usuario se ausente brevemente de su puesto de trabajo y que un tercero pueda responder desde el Mac a la llamada que está siendo recibida en el teléfono del usuario.

Los requisitos para el correcto funcionamiento de este servicio son:

- Los dispositivos deben estar vinculados a la misma cuenta de iCloud.
- Los dispositivos deben haber iniciado sesión en FaceTime utilizando el mismo ID de Apple que el vinculado a la cuenta de iCloud (ver apartado "5.4.1. Cuenta de FaceTime").
- El ajuste del iPhone "Datos móviles - Llamadas en otros dispositivos - Permitir en otros dispositivos" debe estar activo, así como el correspondiente al dispositivo para el que se desea utilizar el servicio.

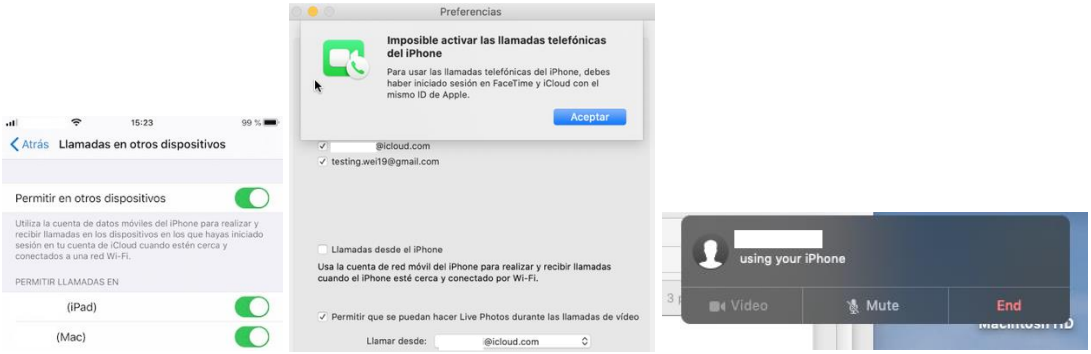



*Figura 79 - Configuración de iOS y macOS para cursar llamadas telefónicas mediante Continuidad y ejemplo de llamada en macOS*

Las notificaciones de llamada entrante se cursan a través del APNs, y los datos de audio se transmiten desde el iPhone al dispositivo en el que se descuelgue la llamada a través de una conexión extremo a extremo cifrada. Si existe más de un dispositivo que pueda aceptar la

llamada, cuando uno de ellos responda, los demás serán notificados mediante un anuncio BLE cifrado.

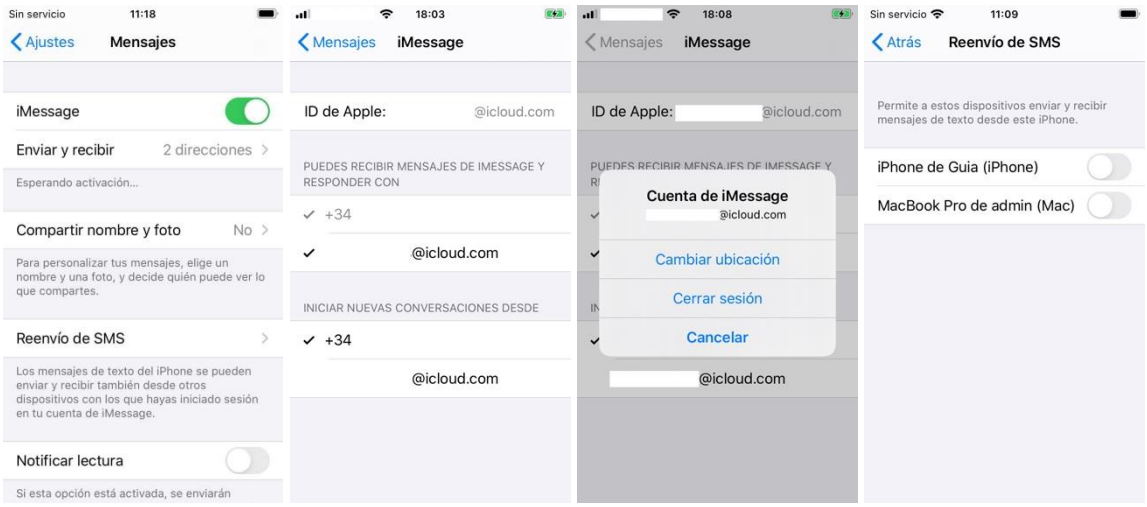
### 7.1.5 REENVÍO DE MENSAJES

Esta funcionalidad permite el envío, recepción y sincronización de mensajes (iMessages y SMS) desde cualquier dispositivo que comparta la cuenta de iCloud, siempre que el iPhone disponga de conexión de red (vía Wi-Fi o de datos móviles). Los requisitos para su correcta utilización son:

- Que el interruptor "iMessage" esté habilitado en el menú de la app "Mensajes" (iOS).
- Que la opción "Activar mensajes en iCloud" esté habilitada en el menú "iMessage" (macOS).
- Que los dispositivos hayan iniciado sesión en el servicio "iMessage" utilizando el mismo ID de Apple (ver apartado "5.4.2. Cuenta de iMessage"). En caso contrario, como ilustra la <Figura 80>, no se realizará la sincronización con los mensajes de otros dispositivos.
- Que se realice la inscripción en el servicio por parte de los dispositivos receptores:
  - Esta inscripción es automática para los dispositivos de confianza si el ID de Apple tiene habilitado segundo factor de autentificación (2FA).
  - La inscripción requerirá introducir un código de 6 dígitos generado por el iPhone en los dispositivos receptores si el ID de Apple no dispone de 2FA.

  Para determinar qué dispositivos de los vinculados a iMessage con el mismo ID de Apple que el iPhone pueden enviar y recibir los mensajes de texto cursados a través de dicho iPhone, se dispone del menú "Reenvío de SMS", con un interruptor por cada dispositivo que habilita/deshabilita el envío y la recepción. En macOS, al inhabilitar la opción "Activar mensajes en iCloud", se solicitará confirmación al usuario sobre si desea deshabilitar la recepción de mensajes únicamente en el propio Mac o en todos los dispositivos vinculados a la cuenta [Ref.- 40].

El intercambio de mensajes entre el iPhone y los dispositivos enlazados utiliza los mecanismos de cifrado propios de iMessage (descritos en el apartado "7.2.2. iMessage").



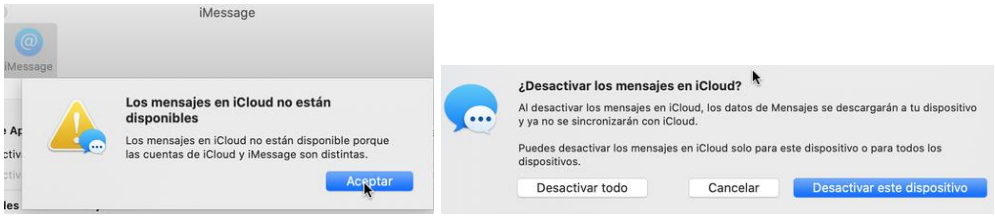



*Figura 80 - Uso de iMessage para la funcionalidad de reenvío de mensajes de texto*

La funcionalidad de reenvío de mensajes de texto permite el uso de la función de autorrellenar códigos de un solo uso en el navegador Safari (ver apartado "8.2.4. Autorrelleno de contraseñas y de códigos de seguridad").

### 7.1.6 INSTANT HOTSPOT

Este servicio habilita la utilización del *hotspot* Wi-Fi ofrecido por un dispositivo móvil Apple (iPhone o iPad) que disponga de conexión de datos móviles para su compartición con otros dispositivos vinculados a la misma cuenta de iCloud, sin necesidad de introducción expresa de la contraseña por parte del dispositivo cliente, ni de habilitar expresamente el *hotspot* Wi-Fi en el dispositivo móvil que ofrece su conexión a Internet. Desde iOS 13, también las cuentas vinculadas al grupo "Familia" pueden hacer uso del servicio si la opción "Punto de acceso personal - En familia - En familia" se encuentra habilitada (ver apartado "6.9. Grupo "Familia"").

A diferencia de otros servicios de Continuidad, como "Handoff", esta funcionalidad no exige ninguna acción expresa por parte del usuario, sino que está habilitada automáticamente por el mero hecho de tener ambos dispositivos una sesión iniciada en la misma cuenta de iCloud y los interfaces Wi-Fi y Bluetooth activos.

A nivel técnico, el servicio se implementa:

- Cuando el dispositivo cliente accede al menú de configuración Wi-Fi, emite un anuncio BLE con un identificador conocido por todos los dispositivos vinculados a la cuenta de iCloud, anunciando su interés de conectarse a una red Wi-Fi.
- Este identificador se genera a partir del denominado "DSID" (*Destination Signaling Identifier*) de la cuenta de iCloud, que rota periódicamente.
- Los dispositivos en rango BLE que reconocen el identificador y pueden ofrecer el servicio de punto de acceso personal, detectan la señal y responden indicando su disponibilidad y ofreciendo su servicio "Instant Hotspot".
- Para las cuentas que pertenecen al grupo "Familia" que tienen el servicio de compartición del *hotspot* habilitado, la sincronización se lleva a cabo mediante claves públicas Ed25519 y el servicio IDS (Apple *Identity Service*). El intercambio de claves efímeras utiliza ECDH (Curve25519) y la autenticación emplea las claves públicas Ed25519 [Ref.- 21].
  Para más detalles sobre la compartición del *hotspot* con miembros de la familia, se recomienda consultar el apartado "6.9.2.1. Compartir Internet con "Familia"".
- Cuando un dispositivo no vinculado al grupo "Familia" desea conectarse al punto de acceso personal (ej. iPhone), le envía una solicitud para activar el *hotspot* mediante un mensaje protegido por cifrado BLE, similar al empleado por iMessage. El iPhone responderá a través del mismo enlace BLE cifrado con la información de la conexión al *hotspot*. El mecanismo criptográfico es el mismo que el empleado para dispositivos HomeKit.

### 7.1.7 DESBLOQUEO AUTOMÁTICO, INICIO DE SESIÓN Y ACCESO A FUNCIONES ADMINISTRATIVAS CON UN APPLE WATCH

La vinculación entre un Apple Watch y un Mac al mismo ID de Apple (configurado con 2FA) ofrece las siguientes funcionalidades, cuya configuración se detalla en la [Ref.- 42]:

#### 7.1.7.1 Desbloqueo automático del Mac

Esta funcionalidad permite que el Mac salga del estado de reposo y sea desbloqueado de forma automática (no sirve para iniciar sesión por primera vez tras un reinicio del sistema) si el Apple Watch vinculado a su mismo ID de Apple se encuentra en un rango de distancia determinado. Para ello, basta con pulsar una tecla o levantar la tapa de la pantalla.

Para confirmar si el Mac es compatible con esta funcionalidad, hay que comprobar el campo "Desbloqueo automático" del menú "" - Acerca de este Mac - Informe del sistema - Red - Wi-Fi - [Interfaces]".

Cuando la opción "Preferencias del Sistema - Seguridad y privacidad - General - Permitir que el Apple Watch desbloquee el Mac" se habilita, se establece un enlace seguro basado en unas claves denominadas "Identidades de desbloqueo automático" ("*Auto Unlock Identities*"). El sistema operativo macOS deriva un secreto de un solo uso que se transmite al Apple Watch a través de dicho enlace, y que solo está accesible cuando el reloj está desbloqueado [Ref.- 21].

Cuando la función de desbloqueo automático se inicia, el Mac establece una conexión BLE con el Apple Watch, y se establece un canal seguro entre ambos mediante las claves compartidas previamente.

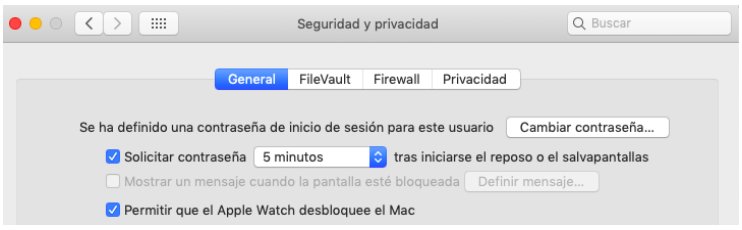
Mediante una conexión Wi-Fi extremo a extremo se determina la distancia entre el Mac y el Apple Watch y, si esta distancia cumple el rango establecido, el Apple Watch transferirá el secreto al Mac mediante el enlace seguro.

**NOTA:** no se ha encontrado ninguna documentación oficial de Apple que indique cuál es la distancia máxima entre el Apple Watch y el Mac para que el desbloqueo automático tenga efecto. Durante las pruebas realizadas en la elaboración de la presente guía, se ha observado que la máxima distancia está en torno a 1,2 metros. Superado ese umbral, el Mac mostrará el último mensaje de la <Figura 81>.

El secreto se regenera tras haber sido usado una vez, y el Mac lo transmitirá de nuevo al Apple Watch para el siguiente desbloqueo.

Esta funcionalidad no tiene efecto si el dispositivo está actualmente conectado a un proyector de pantalla o a un monitor externo, lo cual evita que contenidos confidenciales se hagan accesibles a terceros de forma accidental.

***Esta funcionalidad se desaconseja desde el punto de vista de seguridad*** debido al riesgo de que el usuario se aproxime al Mac de forma accidental y lo desbloquee de forma inconsciente.





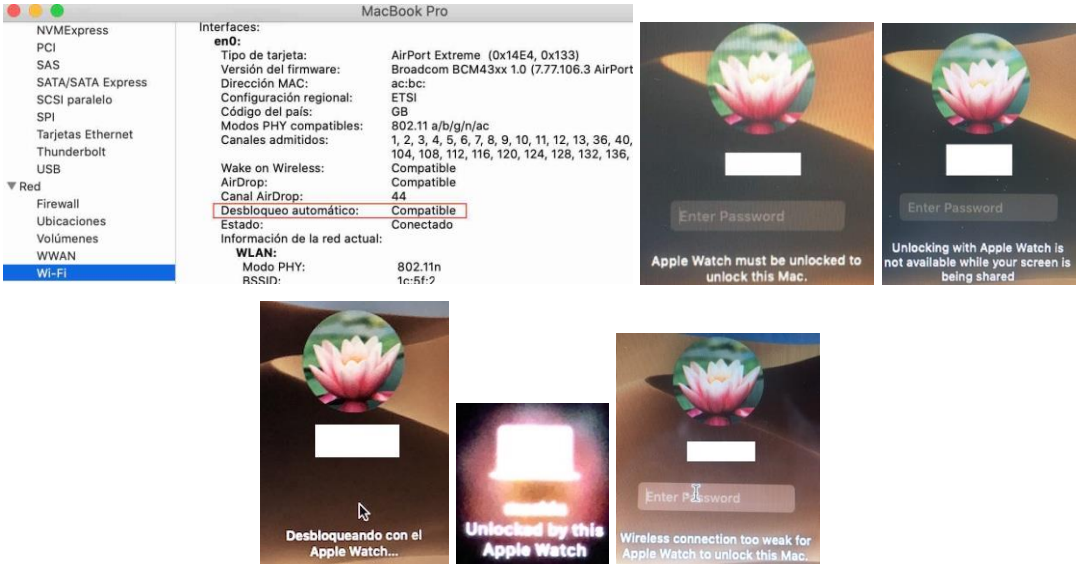




*Figura 81 - Desbloqueo automático de macOS con Apple Watch*

#### 7.1.7.2 Autorizar operaciones con el Apple Watch

Desde macOS 10.15 Catalina y WatchOS 6, si la opción de desbloqueo automático descrita previamente está activa, es posible utilizar el Apple Watch en lugar de introducir la contraseña de administrador del Mac para:

- Sustituir la introducción de la contraseña de administración del Mac al modificar ajustes de "Preferencias del sistema" que requieren de máximos privilegios, por una doble pulsación en el botón del reloj.
- Autorizar operaciones del sistema operativo y de las apps propias de Apple (por ejemplo, aprobar la instalación de apps).
- Autentificación del usuario en apps de terceros.
- Acceso a notas bloqueadas.
- Acceso a las contraseñas almacenadas en Safari.

### 7.1.8 CONTINUIDAD DE CÁMARA

Este servicio permite incorporar en las apps compatibles de macOS (a fecha de publicación de la presente guía, Finder, Keynote, Mail, Notas, Numbers, Pages, TextEdit y Mensajes) documentos escaneados y fotos tomadas desde un dispositivo móvil (se requiere al menos disponer de la versión iOS 12). Cuando el usuario selecciona el menú "Archivo - Insertar desde iPhone" en la app correspondiente, la app "Cámara" se abrirá sin necesidad de interacción por parte del usuario, incluso aunque el iPhone se encuentre bloqueado.

Este servicio de continuidad requiere que el ID de Apple disponga de doble factor de autentificación (2FA).

Para hacer uso del servicio, se recomienda consultar la [Ref.- 41]. La <Figura 82> ilustra el uso de la app "Notas" de macOS, tanto para inserción de fotografías como para el escaneo de documentos.




*Figura 82 - Uso de la funcionalidad "Continuidad de cámara"*

### 7.1.9 DIBUJO Y MARCACIÓN

Esta funcionalidad está disponible desde iOS 13 y macOS 10.15 Catalina (siendo necesario que el ID de Apple disponga de 2FA), y permite la inserción de dibujos en macOS (ordenador Mac) creados en el dispositivo iOS (iPhone) y la marcación de documentos respectivamente [Ref.-42]:

- Dibujo: al iniciar en el Mac una app compatible y seleccionar el menú "Archivo - Insertar desde [dispositivo] - Añadir dibujo" se abrirá en el iPhone una ventana de dibujo, que se transferirá y aparecerá en el Mac cuando el usuario pulse "OK" en el iPhone.
  Es importante reseñar que, aunque el iPhone se encuentre bloqueado, la ventana de dibujo se abrirá en él, volviendo al estado de bloqueo al salvar el dibujo mediante "OK".
- Marcación: desde la app "Finder" del Mac, debe accederse al menú de marcación (bien desde un menú de vista previa, bien desde el menú "Marcación" de las funciones rápidas) y elegir el botón de anotación, aparecerá en el iPhone el menú con las herramientas de dibujo. Los cambios se propagan al Mac de forma instantánea.
  Al igual que con la funcionalidad de dibujo, el menú se abrirá en el iPhone aunque éste se encuentre bloqueado. El estado de bloqueo se reanudará al pulsar "OK" para finalizar la edición o desde el menú de anotación, seleccionado "Desconectarse del [Nombre del iPhone]".

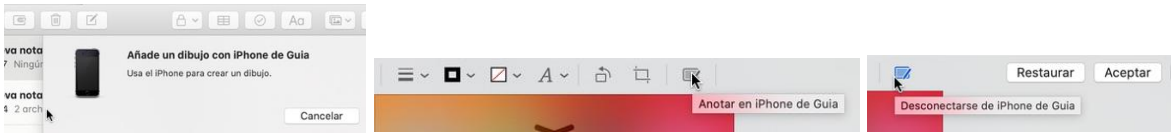



*Figura 83 - Uso de continuidad en dibujo y marcación*

## 7.2 COMUNICACIONES PROPIETARIAS DE APPLE

### 7.2.1 AIRDROP

**Recomendaciones de seguridad:**

- Mantener AirDrop desactivado.
- En caso de requerirse el uso de AirDrop, deshabilitarlo tan pronto finalice la necesidad.
- Al hacer uso de AirDrop evitar habilitar el modo "Todos", especialmente en lugares concurridos, y hacer únicamente uso del modo "Solo Contactos".
- Cuando se desee enviar un fichero vía AirDrop, utilizar el menú de compartición, no los accesos directos.
- Prestar atención a las categorías del panel de compartición para evitar enviar contenidos a usuarios no deseados, especialmente en lugares concurridos.

AirDrop es un servicio empleado para la compartición de contenidos entre dispositivos Apple que se encuentran en un rango de alcance de Bluetooth (el interfaz Bluetooth debe estar habilitado, así como el interfaz Wi-Fi). El intercambio requiere que ambos dispositivos estén desbloqueados[16] (si bien para la detección de dispositivos receptores es suficiente con que la pantalla no esté suspendida). AirDrop también utiliza la tecnología "Bonjour" (ver apartado "7.2.4. Bonjour (macOS)") para el descubrimiento de servicios.

A nivel técnico, AirDrop hace uso de diversos protocolos y mecanismos de cifrado, que se pueden consultar en la [Ref.- 21]:

- Protocolo AWDL (*Apple Wireless Direct Link*)[17], que integra:
  - Bluetooth Low Energy (BLE) para el descubrimiento de dispositivos que soporten el servicio y para la implementación de los mecanismos de autentificación.
  - Una conexión Wi-Fi punto a punto (es decir, entre dispositivos cliente y que no requiere de un punto de acceso Wi-Fi) para la transmisión cifrada de datos entre los dispositivos implicados en la comunicación, empleando un túnel TLS con certificados digitales en ambos extremos. La conexión Wi-Fi también hace uso del servicio Bonjour (DNS) de resolución de nombres para el descubrimiento de servicios, en concreto, el servicio de AirDrop. Apple hace uso de direcciones MAC aleatorias para las comunicaciones Wi-Fi punto a punto asociadas a AirDrop (y a AirPlay).
- Un mecanismo de autentificación basado en un certificado de identidad RSA de 2.048 bits que se almacena en el dispositivo cuando el usuario inicia sesión en iCloud.
- Un conjunto de *hashes* o identidades cortas (generadas a partir de los hashes SHA256) que se utilizan como mecanismo de autentificación en las conexiones AirDrop, y que se crean en el dispositivo a partir del ID de Apple, los números de teléfono y las direcciones de correo del usuario (hasta un máximo de 4) cuando se habilita AirDrop. Adicionalmente, se hace uso posteriormente de una identidad larga correspondiente al hash SHA256 completo de la información de contacto del usuario.

#### 7.2.1.1 Mecanismo de funcionamiento de AirDrop

La secuencia de pasos para el correcto establecimiento de un intercambio de datos a través de AirDrop es:

- El dispositivo emisor desea realizar un envío de información mediante AirDrop y emite un anuncio BLE que incluye su identidad corta de AirDrop (mediante un *hash* corto).
- Los dispositivos cercanos que tienen AirDrop activo (y, por tanto, son potenciales receptores) detectan la señal y comparan la identidad recibida con los *hashes* de las identidades que tienen en su app "Contactos":
  - Si la recepción AirDrop está en modo "Solo Contactos", solo se responde si la identidad recibida está presente en sus contactos.
  - Si la recepción AirDrop está en modo "Todos", el potencial receptor responde independientemente de si conoce o no la identidad del emisor.

[16] Existe una excepción a este comportamiento: si emisor y receptor comparten la cuenta de iCloud, la transferencia puede efectuarse aunque el receptor esté bloqueado. Dependiendo de la app receptora del contenido, la transferencia podrá hacerse completamente efectiva o no de manera automática.
[17] https://owlink.org/wiki/#what-is-apple-wireless-direct-link-awdl

- La respuesta del receptor se envía a través de una conexión Wi-Fi punto a punto, y contiene la identidad corta de AirDrop del potencial receptor (mediante un *hash* corto), que el emisor también compara con la información de su app Contactos, y en base a la cual crea el panel de compartición de AirDrop (en adelante, "panel"). El panel puede contener las siguientes categorías y, dentro de ellas, albergar iconos por cada identidad recibida para que el emisor seleccione el/los destinatarios (<Figura 87>):
  - "Personas": si se encontró coincidencia para la identidad del receptor de AirDrop en los contactos del emisor, éste envía a través de una conexión Wi-Fi punto a punto su identidad larga para iniciar el intercambio de datos vía AirDrop.
    - Si el receptor valida la identidad larga del emisor recibida mediante Wi-Fi en su app Contactos, también responde con su identidad larga. El emisor buscará esta identidad larga en su app "Contactos" y, si encuentra coincidencia, mostrará en su panel el nombre del contacto (y su foto, si existe) bajo la categoría "Personas".
  - "Dispositivos": esta categoría recoge los dispositivos receptores de AirDrop vinculados a la misma cuenta de iCloud que el emisor de AirDrop.
  - "Otras personas": si no se encontró coincidencia para la identidad del receptor de AirDrop en los contactos del emisor, el emisor mostrará en el panel un icono genérico con el valor del ajuste "General - Información - Nombre" del potencial dispositivo receptor.

***Esta organización en categorías en el nuevo panel de AirDrop de iOS 13 es muy importante desde el punto de vista de seguridad***, ya que puede ayudar a impedir ataques de suplantación como el descrito en la vulnerabilidad Man-in-the-Middle (MitM) detallada posteriormente sobre el protocolo AWDL[18]: si se está enviando un fichero a un contacto y el nombre esperado no aparece en la categoría correcta, se puede sospechar que un tercero esté intentando hacerse pasar por el legítimo receptor. Por este motivo, ***se recomienda no utilizar el menú de compartición directa de iOS***, ya que dificulta la identificación del receptor, ***y utilizar en su lugar el panel de*** **AirDrop**. Únicamente las categorías "Personas" y "Dispositivos" reflejan que el otro usuario o contacto ha sido verificado o autentificado.




*Figura 84 - Panel de compartición de AirDrop*

[18] https://www.youtube.com/watch?v=5T7Qatoh0Vo

- Cuando el usuario emisor realiza la selección del destinatario (o usuario receptor) en el panel de AirDrop, el dispositivo emisor inicia una conexión TLS con el receptor, en la que se intercambian sus certificados de identidad (RSA) de iCloud.
  - Si la validación de identidades tiene éxito, el receptor mostrará en la pantalla un mensaje solicitando al usuario confirmación para formalizar la transferencia.

**NOTA:** Durante las pruebas realizadas en la elaboración de la presente guía, se ha constatado que, aunque el usuario emisor cierre sesión en su cuenta de iCloud, es posible realizar transferencias vía AirDrop. Esto representa un potencial problema de seguridad ya que, en caso de que el cierre de la sesión se haya realizado por sospechas de compromiso de la cuenta de iCloud, los dispositivos que aún tengan en sus contactos al emisor seguirán creyendo que la conexión proviene de un contacto legítimo.

#### 7.2.1.2 Uso de AirDrop

Las capacidades de comunicación de AirDrop se gestionan desde:

- iOS 13:
  - El "Centro de Control": desplegando el menú contextual asociado al grupo "Ajustes de red" realizando una pulsación larga sobre cualquiera de los iconos asociados a las comunicaciones y seleccionando el icono "AirDrop" (ver <Figura 67>). Por defecto, se encuentra habilitado solo para los contactos.
  - El ajuste "General - Airdrop".
- macOS:
  - El menú de AirDrop está disponible por defecto en la barra lateral izquierda de la app "Finder", dentro de la sección "Favoritos". En el menú inferior central "Permitirme ser visible para:" se controla qué orígenes están autorizados para iniciar transferencias.

Para iniciar una comunicación mediante AirDrop, tanto el dispositivo emisor como el receptor requieren tener activos los interfaces de Bluetooth y Wi-Fi, y que la pantalla no esté suspendida. Desde el contenido a compartir, el emisor debe pulsar el icono ""[19] y:

a) Seleccionar el icono genérico de AirDrop "" (iOS) / "

" (macOS) del menú de compartición (parte inferior de la cuarta imagen de la <Figura 87>): ésta es la opción recomendada desde el punto de vista de seguridad, porque facilita la identificación de ataques de suplantación (ver apartado "7.2.1.1. Mecanismo de funcionamiento de AirDrop").

b) En iOS, el menú de compartición permite seleccionar un acceso directo a un contacto mediante su icono concreto (parte superior de la cuarta imagen de la <Figura 87>). Desde el punto de vista de seguridad, ***se debe prestar especial atención a los iconos mostrados por el interfaz gráfico de usuario de*** iOS de cara a confirmar si un usuario ha sido autentificado en el proceso: si se muestra la foto del contacto, su identidad ha sido validada, al igual que si se muestran sus iniciales (cuando el contacto no tiene una foto asociada en la app Contactos). Sin embargo, si se muestra el icono genérico con la silueta de una persona en color gris y blanco, la identidad del otro usuario no ha sido verificada, pudiendo ser potencialmente víctima de ataques MitM.

[19] Algunas apps disponen del menú "Pulsa para compartir con AirDrop".

**NOTA:** Durante las pruebas realizadas durante la elaboración de la presente guía, se ha observado que, si el dispositivo tiene activo el punto de acceso personal, las comunicaciones a través de AirDrop no pueden cursarse, incluso aunque no exista ningún dispositivo conectado al punto de acceso personal o *Personal Hotspot*.




*Figura 85 - Configuración de AirDrop y error generado durante el uso de un punto de acceso personal en iOS 13*




*Figura 86 - Configuración de AirDrop en macOS 10.15*

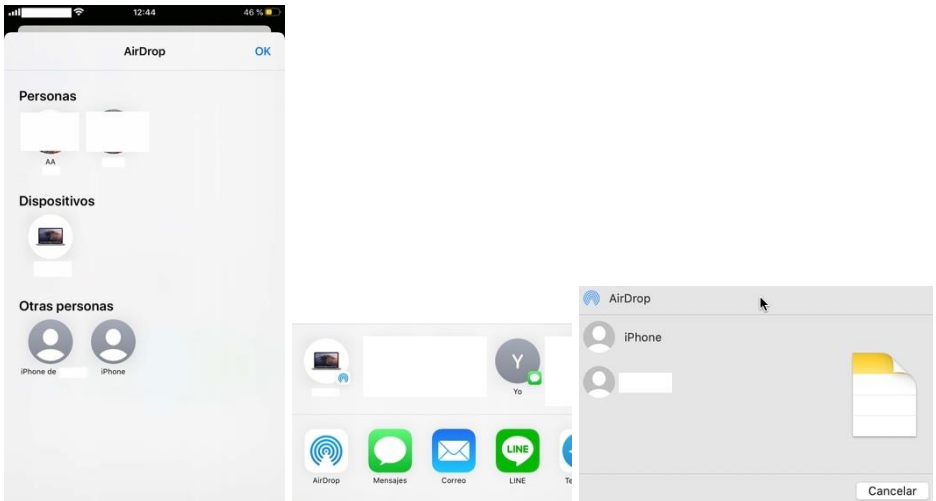



*Figura 87 - Compartición de contenidos vía AirDrop en iOS (parte izquierda) y macOS (parte derecha)*

**NOTA:** Un dispositivo que sale del modo de pantalla suspendida, aunque esté con la pantalla bloqueada, aparece como potencial receptor tan pronto activa su pantalla. Ello implica que en dicho estado monitoriza los anuncios BLE de otros dispositivos AirDrop y comienza a divulgar su identidad de AirDrop incluso con la pantalla bloqueada.

El dispositivo receptor mostrará un mensaje solicitando confirmación al usuario. Si la emisión proviene de un contacto conocido, iOS mostrará una previsualización del contenido a enviar (primera y segunda imagen de la <Figura 88>). En caso contrario, solo se mostrará una notificación (tercera imagen). En macOS la previsualización del contenido se presenta independientemente del origen de la comunicación.

Si el dispositivo receptor está bloqueado, se informará al usuario a través de una notificación desde la pantalla de bloqueo que, si se despliega, solicitará el método de desbloqueo (cuarta imagen)[20]:

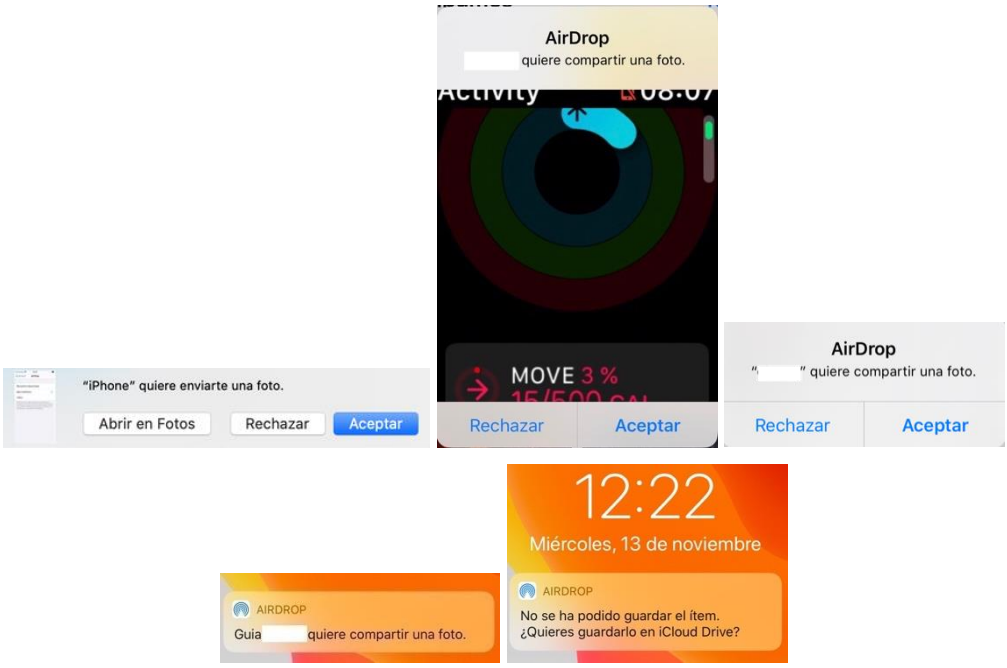



*Figura 88 - Solicitud de aceptación de recepción de contenido vía AirDrop*

En macOS, el menú de aceptación incluye la posibilidad de abrir el fichero recibido en una app concreta o descargarlo (si se selecciona "Aceptar", los archivos recibidos se almacenan en la carpeta "`Descargas`" ("`Downloads`") del usuario receptor).

El proceso encargado de la transmisión vía AirDrop es "`/System/Library/PrivateFrameworks/FinderKit.framework/Versions/A/PlugIns/AirDrop.appex/Contents/MacOS/AirDrop`", que se lanza al solicitarse la transferencia y finaliza cuando esta concluye, haya tenido éxito o no.

Los atributos de cuarentena de los archivos asociados al fichero trasmitido en el ordenador origen son propagados a través de la transferencia AirDrop hacia el ordenador destino. Adicionalmente, se añaden nuevos atributos para reflejar el nombre del equipo desde el que

[20] Si emisor y receptor comparten cuenta de iCloud, la transferencia puede efectuarse aunque el receptor esté bloqueado. El receptor emitirá una señal sonora y, dependiendo de la app receptora del contenido, la transferencia podrá hacerse completamente efectiva (por ejemplo, para la app "Notas") o no (por ejemplo, para la app "Fotos").

se ha recibido el fichero ("`com.apple.metadata:kMDItemWhereFrom`") y la asignación de una etiqueta ("`com.apple.metadata:kMDLabel_<etiqueta>`").

Desde el punto de vista de seguridad, se recomienda mantener deshabilitado el servicio AirDrop, y, en caso de requerirse utilizar las capacidades de transmisión de datos de AirDrop, habilitarlo solo para los contactos y solo mientras se lleve a cabo el intercambio de datos.

Dado que el servicio AirDrop emplea un identificador que se almacena en el dispositivo, y cifra los contenidos en base a un certificado ligado a la identidad de las cuentas de iCloud involucradas, podría considerarse más seguro de cara a la transferencia de información que otros mecanismos, como el correo electrónico. Pese a ello, adolece de los riesgos de seguridad asociados a la necesidad de mantener los interfaces Bluetooth y Wi-Fi activos para su operativa, y a las debilidades descubiertas para el protocolo AWDL (consultar la [Ref.- 44] para más información).

En iOS 13 es posible establecer una restricción sobre AirDrop (ver apartado "Restricciones" de la guía "Configuración segura de iOS 13" [Ref.- 413]).

### 7.2.2 iMessage

iMessages es el servicio propietario de Apple para el envío de mensajes instantáneos (a través de redes Wi-Fi o redes de datos de telefonía móvil), junto a imágenes, vídeos, contactos, localizaciones, etc. A través del servicio de continuidad descrito en el apartado "7.1.5. Reenvío de mensajes", iMessage permite la sincronización entre todos los dispositivos vinculados al mismo ID de Apple de los mensajes cuyo origen o destino sea cualquiera de estos dispositivos.

iMessage define dos pares de claves únicas para cada dispositivo, una para firma y otra para cifrado, ya que iMessage emplea cifrado extremo a extremo entre los dispositivos Apple involucrados en una comunicación (las partes privadas de las claves se almacenan en el llavero del dispositivo y solo son accesibles cuando éste se desbloquea tras un reinicio) [Ref.- 21]:

- Las claves de firma emplean ECDSA 256-bits.
- Las claves de cifrado son dos:
  - Una clave RSA de 1.280-bits.
  - Una clave de curva elíptica (EC) de 256 bits empleando la curva NIST P-256.

Las claves de cifrado y de firma que se emplean en las comunicaciones de iMessage se almacenan en el llavero de inicio de sesión del usuario (dentro de la categoría "Claves"):

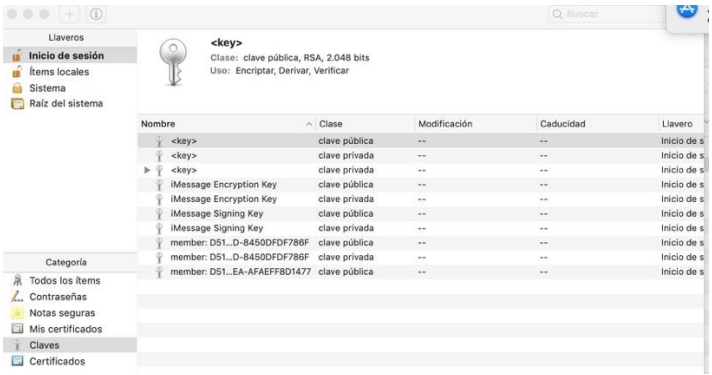



*Figura 89 - Claves de cifrado y firma de iMessage en el llavero de macOS*

Cada nuevo dispositivo que un usuario incorpora a iMessage se añadirá al directorio de servicios de Apple (IDS, Apple *Identity Service*). Este directorio almacena:

- El número de teléfono (si procede) de la tarjeta SIM del dispositivo, previa comprobación de su autenticidad a través de un SMS que se cursa mediante el operador de telefonía.
- La dirección de correo electrónico del usuario, previa verificación mediante un e-mail de confirmación.
- La dirección APNs del dispositivo (ver apartado "7.1.1. APNs (Apple Push Notification service)").
- Las partes públicas de las claves a utilizar por iMessage.

El flujo de información asociado a una nueva conversación de iMessage entre el usuario origen [1] y el destinatario [2] es:

1. El usuario [1] introduce los datos del destinatario [2]:
   - Si los datos son un número de teléfono o un e-mail, el dispositivo [1] consulta al IDS para obtener las claves públicas y las direcciones APNs de todos los dispositivos vinculados a [2].
   - Si los datos son un nombre, el dispositivo [1] accede a su app "Contactos" para obtener los números de teléfono y las direcciones de correo de [2], y procede como en el punto previo.
2. A partir de las claves obtenidas del IDS en el paso 1, los contenidos del mensaje se cifran para cada dispositivo receptor mediante un mecanismo que asegura la confidencialidad e integridad del texto intercambiado. Cada mensaje resultante incluye el texto cifrado, la clave de cifrado y la firma del emisor.
3. Los mensajes se envían al servicio APNs mediante un túnel TLS cifrado. Si su longitud excede los 16 KB (o 4 KB, según la versión de iOS), los contenidos se cifran con una clave aleatoria AES de 256 bits y se suben a iCloud. Esta clave, un identificador URI (*Uniform Resource Identifier*) del contenido y un *hash* SHA-1 se envían al destinatario como si fueran el contenido del mensaje, protegidos con los mecanismos de cifrado propios de iMessage.
4. El servicio APNs enruta el mensaje a cada dispositivo receptor mediante notificaciones *push*. Si el mensaje excedía el límite anteriormente comentado, el contenido adjunto subido a iCloud se descargará en base al URI que acompaña al mensaje. En caso de que el teléfono o e-mail de [1] figuren en los contactos de [2], se mostrará el nombre del emisor.
5. Los mensajes pueden encolarse en el servicio APNs hasta un máximo de 30 días para permitir su recepción en dispositivos que no estén en línea en el momento del envío. Una vez se complete la recepción, el mensaje se borrará del servicio APNs, al igual que ocurre con cualquier otra notificación *push*.

Cuando el mensaje se dirige a un grupo, el flujo anteriormente descrito se lleva a cabo para cada dispositivo receptor.

Complementariamente, Apple ofrece un servicio de mensajería para negocios (*Business Chat*), a modo de "chat" para clientes, que presenta como peculiaridad que el origen de la conversación solo puede ser el usuario particular, y no el negocio. En el caso del chat de Apple, el ID del chat está vinculado al ID de Apple del cliente. El resto de chats de negocios no reciben información del ID de Apple del cliente o usuario [Ref.- 21].

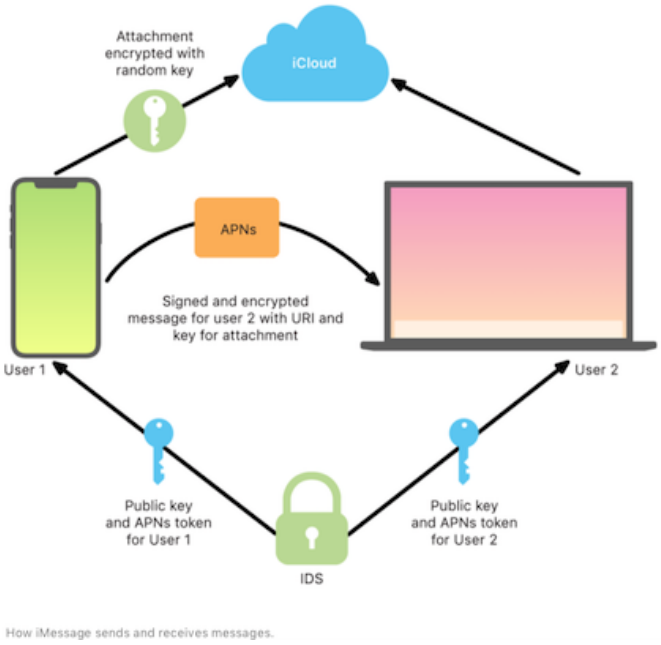



*Figura 90 - Esquema de una comunicación de iMessage [Ref.- 21]*

### 7.2.2.1 App Mensajes

La aplicación de acceso al servicio de mensajería (iMessage) disponible por defecto en iOS y macOS se denomina "Mensajes", también empleada para el envío y recepción de mensajes de texto (SMS o MMS).

Los mensajes se clasifican en base al otro interlocutor en lo que se denominan "conversaciones", de modo que todos los mensajes intercambiados con un mismo número de teléfono o un e-mail de un mismo contacto (o de un número que no pertenezca a la lista de contactos) se muestran agrupados. La app "Mensajes" permite eliminar una conversación, así como silenciarla, deslizando el dedo de izquierda a derecha mientras se pulsa la conversación. Ninguna de estas acciones implica que se bloquee el contacto (en el caso de chats de negocios, la eliminación de la conversación sí es equivalente a bloquear el contacto, ya que solo podrán volverse a recibir mensajes de este chat en caso de que el cliente inicie una nueva conversación).




*Figura 91 - Gestión de una conversación de iMessage*

La configuración de iMessages se realiza desde el menú "Ajustes - Mensajes" (iOS) y "Preferencias" de la app "Mensajes" (macOS):

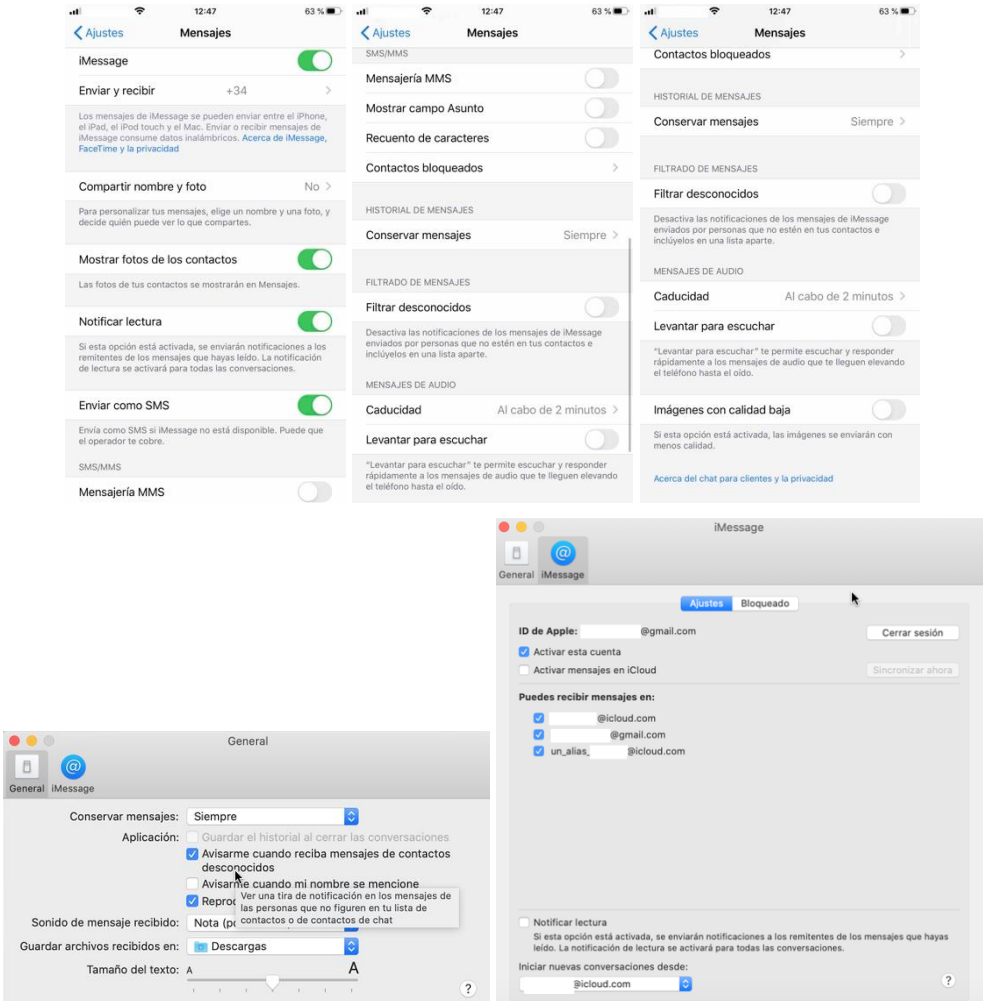



*Figura 92 - Configuración de iMessage*

Desde el punto de vista de seguridad y/o privacidad, ***se recomienda la siguiente configuración***:

- "Notificar lectura": ***desactivado***. De este modo no se enviará acuse de recibo de la lectura de los mensajes al emisor.
- "Enviar como SMS": ***activado***. Para asegurar las posibilidades de recepción del mensaje de texto, en formato de SMS, por parte del destinatario, sin limitarlo al propio servicio de iMessage[21].
- "Enviar y recibir": determina las direcciones que pueden ser empleadas como origen y destino de mensajes en el dispositivo móvil (ver apartado "5.4.2. Cuenta de iMessage"). Se recomienda ***eliminar*** aquellas direcciones que no se desea publicar para este servicio. No es posible eliminar el número de teléfono vinculado a la tarjeta SIM en un iPhone (de ahí que aparezca sombreado en gris).
- "Contactos bloqueados": determina qué contactos no podrán iniciar conversaciones con el usuario, y corresponden a la misma lista que está descrita en la sección "Ajustes del módulo de telefonía" de la guía "Configuración segura de iOS 13" [Ref.- 413].

[21] Esta recomendación depende de las tarifas de telefonía móvil: el servicio de envío de mensajes SMS puede conllevar costes adicionales que el usuario debe evaluar.

- "[Mensajes de audio] Levantar para escuchar": ***desactivado***. Para impedir que un mensaje pueda ser escuchado indebidamente por un tercero.
- "Filtrar desconocidos": al activar este ajuste, los mensajes de números que no aparezcan en la lista de contactos se agruparán en la categoría "Remitentes desconocidos", y no se emitirá ninguna notificación cuando se reciban. Esta característica es útil para evitar *spam*.
- "Reenvío de SMS": esta opción, asociada a los servicios de continuidad, solo está disponible si se ha dado de alta un ID de Apple para uso de iMessage en el dispositivo. Consultar el apartado "7.1.5. Reenvío de mensajes" para más información.

Adicionalmente, el servicio iMessage soporta el "Reenvío de SMS", que permite que los mensajes de texto (SMS) recibidos en el número de teléfono asociado al dispositivo móvil se reciban también en aquellos dispositivos vinculados al mismo ID de Apple y, que dispositivos que carecen de capacidades de telefonía móvil puedan utilizar las capacidades del iPhone como pasarela de mensajes.

Si se habilita esta funcionalidad de reenvío de SMS con un ordenador macOS, la función de autorrellenar códigos de un solo uso se propagará al navegador web Safari de dicho ordenador tan pronto se reciba el mensaje que contenga el código asociado a un segundo factor (2FA) vía SMS en el iPhone (ver apartado "8.2.4. Autorrelleno de contraseñas y de códigos de seguridad").

La app "Mensajes" permite en macOS acceder a la compartición de pantalla del Mac (ver apartado "Compartir pantalla" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412]).

### 7.2.3 FaceTime

El servicio FaceTime ofrece llamadas de audio y videollamadas cuyo contenido está cifrado extremo a extremo entre el dispositivo del usuario y otros dispositivos, incluyendo llamadas de grupo de hasta 33 dispositivos. Es preciso disponer de un ID de Apple habilitado para el uso del servicio (ver apartado "5.4.1. Cuenta de FaceTime").

Su mecanismo de funcionamiento es el siguiente:

- Cuando se inicia una conexión, se utilizan notificaciones del servicio APNs y mensajes STUN (*Session Transversal Utilities for* NAT) que permiten verificar las identidades de los dispositivos implicados y generar una clave secreta de sesión.
- La clave secreta permite derivar claves de sesión para los distintos canales (audio y vídeo) en base a SRTP (*Secure Real-time Transport Protocol*), cuyos paquetes se cifran con AES-256.
- Una vez inicializada la sesión, la conexión entre los dispositivos es extremo a extremo.

Las llamadas de grupo también se cifran extremo a extremo, pero emplean un mecanismo de generación de claves que asegura que el compromiso de un dispositivo no revelará clos ontenidos de llamadas pasadas (*forward secrecy*). Las claves de sesión se envuelven con AES-SIV y se distribuyen entre los participantes mediante ECIES con claves ECDH de curva elíptica P-256 efímeras. Si algún nuevo participante se incorpora a una llamada en curso, las claves se regeneran para todos los dispositivos.

A diferencia del servicio iMessage, FaceTime no almacena claves de cifrado en el llavero del dispositivo en macOS, únicamente una contraseña de aplicación:

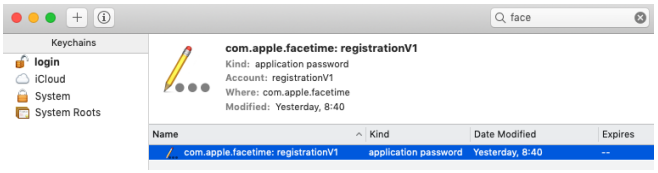



*Figura 93 - Elementos del llavero asociados a FaceTime*

La configuración de FaceTime se realiza a través del menú "Ajustes - FaceTime" (en iOS) y del menú "Preferencias" de la app FaceTime. Se recomienda hacer uso de alias para evitar revelar a terceros el ID de Apple del usuario, así como cerrar la app FaceTime (en macOS, utilizar el menú "Salir de FaceTime") para evitar que la app quede de fondo y puedan establecerse comunicaciones accidentales (especialmente en macOS).

### 7.2.4 BONJOUR (macOS)

"Bonjour" (también conocido como "Rendezvous") es una implementación desarrollada por Apple para las denominadas tecnologías "Zeroconf" (*zero-configuration networking*) [Ref.- 45] [Ref.- 46], basadas en establecer una red de ordenadores mediante el uso de direccionamiento a nivel local y del uso de paquetes DNS y mDNS (multicast DNS) para el nombrado e identificación de servicios. Su objetivo es el descubrimiento de servicios basados en TCP/IP dentro de una misma subred, sin que sea necesario ningún tipo de configuración previa.

Los servicios descubiertos mediante el uso de este protocolo se muestran bajo la sección "Compartido" (Shared) de la ventana de la app "Finder".

A nivel de sistema, los ficheros de configuración asociados a Bonjour en macOS son:

- "`/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist`": corresponde al proceso principal de mDNS, "`/usr/sbin/mDNSResponder`".
- "`/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist`".

Por defecto, los distintos nombres de equipo asignados por macOS tras el proceso de configuración inicial son "`MacBook-Pro-de-<usuario>.local`", donde "`<usuario>`" es el nombre de la cuenta de usuario creada inicialmente durante este proceso inicial (en el ejemplo, "Administrador").

Se recomienda modificar los diferentes nombres del equipo de forma que no desvelen detalles ni del tipo de equipo, ni del sistema operativo empleado, ni del propietario u organización, ni de la cuenta de usuario. Tras esta operación, se recomienda limpiar la caché de DNS mediante el comando "`dscacheutil -flushcache`".




```
$ hostname
MacBook-Pro-de-Administrador.local

$ sudo hostname portatil
$ hostname
portatil
```

*Figura 94 - Modificación de los diferentes nombres del equipo en macOS*

## 7.3 COMPARTICIÓN DE CONTRASEÑAS DE REDES WI-FI

El servicio de compartición de contraseñas de redes Wi-Fi (*Wi-Fi password sharing*) permite a un dispositivo iOS [1] enviar (de forma inalámbrica) la contraseña de acceso de una red Wi-Fi a la que está conectado a (o que es conocida por) otro dispositivo iOS [2], sin revelar directamente al otro usuario las credenciales de la red[22] (sección "Wi-Fi password sharing" de la [Ref.- 21]).

El procedimiento requiere:

- Que el interfaz Bluetooth esté activo en ambos dispositivos.
- Que el dispositivo [1] esté desbloqueado.
- Que [1] tenga en sus contactos el ID de Apple (u otro identificador de contacto) de [2].

El mecanismo de actuación de este servicio está basado en la siguiente secuencia:

- El dispositivo [2] entra en el menú de configuración de redes Wi-Fi y se le solicita introducir la contraseña de la red.
- [2] emite un anuncio BLE avisando de que quiere conocer la contraseña de la red Wi-Fi.
- Los dispositivos Apple cercanos que conocen la contraseña de la red Wi-Fi, se conectan a [2] por BLE y le solicitan su información de contacto.
- [2] debe proporcionar su identidad, utilizando un procedimiento similar al empleado por AirDrop (ver apartado "7.2.1. AirDrop").
- Si [1] valida la identidad proporcionada por [2], solicitará al usuario, mediante la ventana de diálogo de la <Figura 95> autorización para compartir la contraseña de la red Wi-Fi con [2].
- Si el usuario del dispositivo [1] acepta:
  - [1] enviará a [2] la contraseña de la red Wi-Fi cifrada con AES 256[23].
  - [2] almacenará esta contraseña en su llavero o *Keychain*, por lo que la contraseña en claro no podrá conocerse directamente por el usuario del dispositivo [2].

La principal ventaja de este mecanismo es que evita tener que proporcionar directamente a un tercero (aunque sea de confianza) las credenciales de acceso a una red Wi-Fi propia. Como principal inconveniente, sucede que, mientras [2] no olvide voluntariamente la red, tendrá la contraseña almacenada, y podrá a su vez aceptar peticiones de compartición de otros dispositivos que cumplan los requisitos expuestos anteriormente.

Desde el punto de vista de seguridad, si se va a hacer uso de este mecanismo, la recomendación es renovar la contraseña de la red Wi-Fi regularmente, de forma que los dispositivos con los que se haya compartido no dispongan de ella permanentemente.

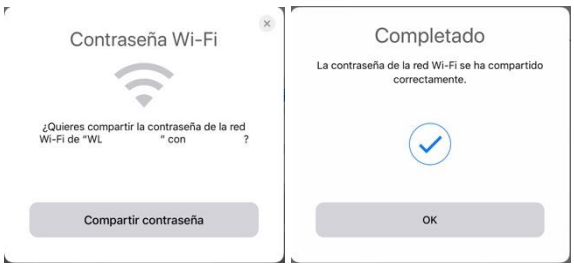



*Figura 95 - Compartición de contraseñas de redes Wi-Fi*

[22] Este procedimiento no es de aplicación en redes Wi-Fi que emplean filtros por dirección MAC.
[23] El cifrado mediante AES 256 se introdujo en iOS 11. Hasta entonces, este procedimiento utilizaba un cifrado más inseguro.

**NOTA:** El servicio de compartición de contraseñas Wi-Fi puede deshabilitarse mediante políticas de gestión de dispositivos empresariales (MDM).

## 8. GESTIÓN DE CREDENCIALES EN iCLOUD

Recomendaciones de seguridad en el uso del llavero de iCloud como gestor de contraseñas:

- Mantener las contraseñas más sensibles fuera del llavero, en especial, la de la cuenta de usuario vinculada al ID de Apple y el servicio iCloud, correo electrónico, servicios corporativos, servicios de banca on-line y servicios relacionados con la salud.

El llavero de iCloud proporciona un servicio de gestión de credenciales, al cual se pueden añadir elementos tanto por parte del usuario como del navegador web Safari y de las apps, y que se almacena y custodia en la nube de iCloud, protegidas con cifrado AES-256 bits.

Una de las principales características del llavero de iCloud es que permite al usuario compartición de credenciales entre sus diferentes dispositivos (tanto móviles como tradicionales).

Un dispositivo vinculado a una cuenta de iCloud podrá acceder a todos los contenidos del llavero de iCloud en cuanto active el llavero. La activación del llavero implica el establecimiento de un círculo de confianza entre los dispositivos vinculados, basado en las siguientes premisas:

- El primer dispositivo crea una identidad de sincronización (par de claves pública y privada). La clave pública se introduce en el círculo de confianza [Ref.- 21].
- El círculo de confianza se firma por duplicado por parte de:
  - La clave privada de la nueva identidad de sincronización.
  - Una clave asimétrica derivada de la contraseña de la cuenta de usuario de iCloud generada mediante curva elíptica P-256.
- El círculo incluye, por tanto:
  - La clave pública de la identidad de sincronización.
  - La semilla y el número de iteraciones (parámetros) empleados para crear la clave asimétrica derivada de la contraseña de la cuenta de usuario de iCloud.
- El círculo firmado se añade al área de almacenamiento de pares "clave-valor" (*key-value*) de iCloud del usuario, no pudiendo leerse sin conocer la contraseña de iCloud. Su integridad está asegurada por la firma, no pudiendo modificarse sin la clave privada de la identidad de sincronización.
- Cuando se activa el llavero de iCloud en otro dispositivo vinculado a la misma cuenta de usuario, se identifica que ya existe un círculo de confianza (del cuál no se forma parte), y el dispositivo genera su par de claves de identidad de sincronización.
- El dispositivo solicita su ingreso en el círculo de confianza mediante la creación de un ticket de aplicación que incluye la clave pública de la identidad de sincronización del dispositivo. El usuario del dispositivo debe introducir la contraseña de la cuenta de iCloud, lo que permite recuperar los parámetros de la generación de la clave asimétrica y generar la clave empleada para firmar el ticket.
- El ticket de aplicación se almacena en iCloud y, cuando el primer dispositivo que se añadió al círculo lo ve, solicita al usuario consentimiento para añadir el nuevo dispositivo al círculo, mediante la introducción de su contraseña de iCloud.

- Si el usuario acepta el ingreso del nuevo dispositivo, el primer dispositivo añade la clave pública del nuevo dispositivo al círculo de confianza, el cual se firma nuevamente por parte del primer dispositivo, se almacena de nuevo en iCloud, y también se firma por el nuevo dispositivo.
- Como cada integrante del círculo posee la clave pública del resto, pueden añadir e intercambiar elementos a través del llavero de iCloud empleando el almacenamiento de pares "clave-valor" de iCloud o CloudKit. Si un elemento existe en más de un dispositivo, el que haya sido modificado más recientemente se sincroniza para todos.
- Los elementos sincronizados solo pueden ser descifrados por dispositivos del círculo de confianza.
- Para la incorporación de sucesivos dispositivos al llavero de iCloud, la aprobación del ticket puede llevarse a cabo desde cualquier dispositivo que ya forme parte del círculo.

El llavero de iCloud únicamente sincroniza aquellos elementos del llavero o *Keychain* del usuario que presentan el atributo "exportable" (`kSecAttrSynchronizable`) y, por tanto, no son específicos de un dispositivo. Por ejemplo, las identidades de redes VPN no son sincronizadas ni compartidas, mientras que las credenciales empleadas por Mobile Safari o las contraseñas de redes Wi-Fi sí lo son. Por defecto, los elementos añadidos al llavero por las apps de terceros están identificados como no sincronizables, debiendo el desarrollador de la app modificar el atributo si desea que sea compartido entre diferentes dispositivos.

La activación del llavero de iCloud implica que los ítems exportables ya existentes del llavero local se traspasen a la nube, no siendo posible para el usuario elegir a nivel de cada elemento en qué llavero desea alojarlo[24]. Complementariamente, si se desactiva el llavero de iCloud, se ofrecerá al usuario la posibilidad de guardar una copia de los elementos existentes en iCloud en el llavero local (ver <Figura 99>).

**NOTA:** los datos del llavero de iCloud no se incluyen en la copia de seguridad del dispositivo, sino que se guardan en la nube de iCloud y están accesibles mientras al menos uno de los dispositivos vinculados a la cuenta de usuario de Apple tenga activo el llavero. Los datos se eliminan de la nube cuando ningún dispositivo de la cuenta tiene habilitado el llavero de iCloud.

El uso del llavero de iCloud debe de evaluarse minuciosamente, ya que el compromiso de un dispositivo podría exponer todas las credenciales, además de que implica asumir plena confianza en la custodia que Apple hace de estos datos tan sensibles.

Para hacer uso del llavero de iCloud, es preciso habilitarlo en:

- iOS: "Ajustes - ID de Apple - iCloud - Llavero".
- macOS: "Preferencias del sistema - ID de Apple - iCloud - Llavero".

El sistema operativo almacena dentro del llavero elementos específicos para controlar el acceso al propio llavero:

[24] Los ítems de sistema sí se siguen almacenando en el llavero local, de forma transparente para el usuario, por parte del sistema operativo.

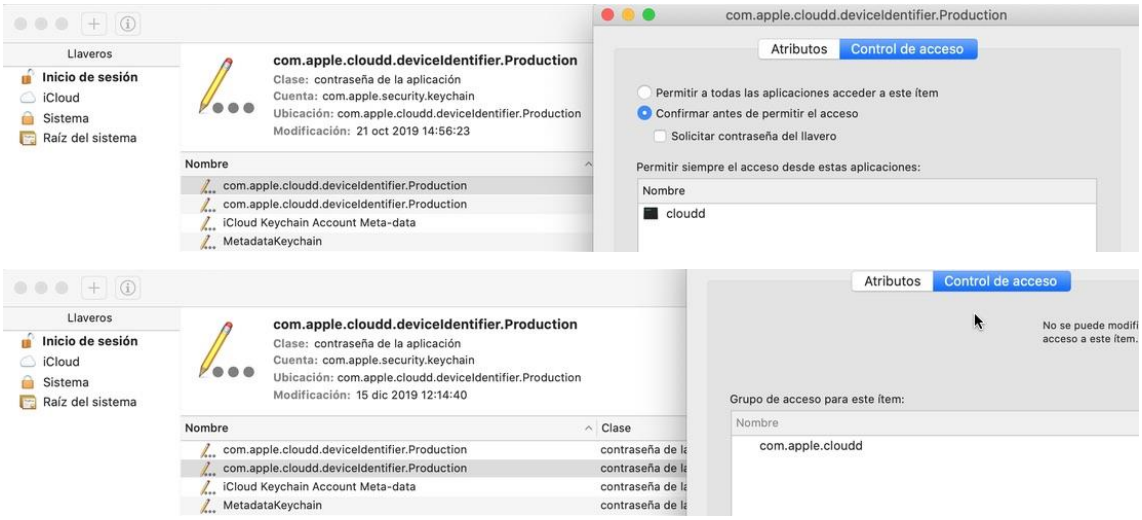



*Figura 96 - Elementos de gestión del llavero almacenados en el dispositivo*

## 8.1 MECANISMO DE DEPÓSITO DEL LLAVERO DE ICLOUD

Apple ofrece al usuario un mecanismo de depósito o custodia del llavero de iCloud (*escrow service*), transparente para el usuario, como respaldo para evitar que todas las contraseñas se pierdan, que se custodia en *clusters* HSM (*Hardware Security Module*). Este servicio requiere disponer de un segundo método de autentificación para cifrar el llavero y proporcionar una copia si se cumplen las condiciones de seguridad requeridas por Apple.

Es importante reseñar que el usuario no dispone de opciones para decidir si se guardará este depósito o no, que se creará incluso si sólo se dispone de un dispositivo con el llavero de iCloud activo.

La copia del llavero debe protegerse mediante un código de seguridad (iCloud *Security Code*, ISC), que corresponde al código de acceso al dispositivo (iOS) o la contraseña del usuario administrador (macOS).

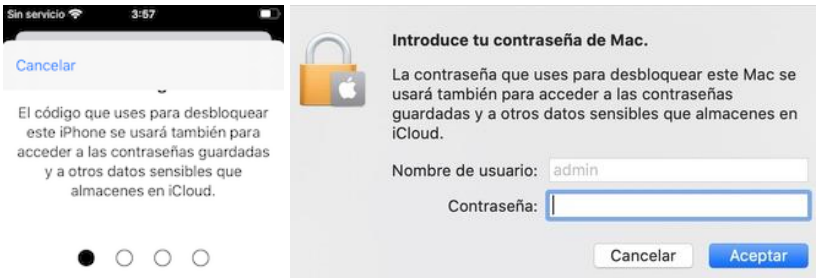



*Figura 97 - Alta del iCloud Security Code*

**IMPORTANTE:** aunque en la guía oficial de seguridad de Apple [Ref.- 21] se indica que el depósito del llavero de iCloud puede obtenerse sin que la cuenta disponga de 2FA, y que, en este caso, el ICS podrá ser determinado por el usuario, bien usando un código de seguridad de 6 dígitos, bien uno propio, o bien uno generado aleatoriamente por parte de sus dispositivos, durante las pruebas realizadas en la elaboración de la presente guía se constata que **no** es posible habilitar el llavero de iCloud si la cuenta no dispone de 2FA.

Al habilitar el llavero de iCloud en una cuenta que no disponga de 2FA, se solicitará al usuario revisar su configuración de seguridad para habilitar el 2FA. En macOS, si se intenta habilitar el

llavero de iCloud en una cuenta que no dispone de 2FA, el proceso de activación se quedará permanentemente en estado "Configurando" (ver siguiente imagen).

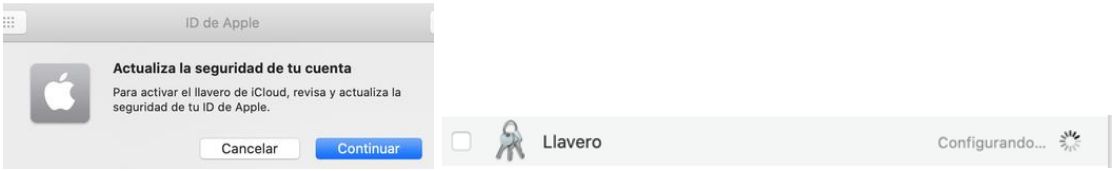



*Figura 98 - Prueba de la obligatoriedad de disponer de 2FA para habilitar el llavero de iCloud*

Para realizar el depósito del llavero en los servidores de Apple, se requiere generar el denominado "iCloud *Escrow Record*" (registro de depósito o custodia de iCloud), para lo cual:

- El dispositivo debe exportar una copia del llavero de iCloud del usuario, cifrarlo con las claves en una bolsa de claves (*keybag*) asimétrica y subirlo al área de almacenamiento de pares "clave-valor" de iCloud.
- La bolsa de claves se envuelve con el código de seguridad de iCloud (ISC) y con la clave pública del módulo HSM de Apple que lo almacena.

### 8.1.1 RECUPERACIÓN DE LA COPIA DEL LLAVERO EN DEPÓSITO

Para que el usuario pueda recuperar un llavero de iCloud (apartado "Escrow security for iCloud Keychain" de la [Ref.- 21]) debe:

- Autenticarse con las credenciales de su cuenta de usuario de iCloud.
- Responder al SMS que Apple envía al número de teléfono que registró como respaldo.
- Introducir el "iCloud *Security Code*" (ISC) que se configuró al crear el depósito. Este código no se envía propiamente a Apple, sino que se verifica su conocimiento mediante el protocolo SRP[25] (*Secure Remote Password*). Este código permite desenvolver la clave aleatoria de cifrado del llavero, que se recuperará desde el almacenamiento de pares "clave-valor" de iCloud y se restaurará en el dispositivo.

Se dispone de un máximo de 10 intentos para introducir el código de seguridad, tras los cuales la copia en depósito se bloquea (es posible en este punto contactar con el soporte de Apple para obtener intentos adicionales). Para evitar ataques de fuerza bruta, tras el décimo intento fallido de introducción del código, el *cluster* de HSMs de Apple destruirá el registro, y no será posible recuperar la copia del llavero de iCloud.

**NOTA:** dado que hay varios sistemas que forman parte del *cluster* de HSMs, el número máximo de intentos fallidos comprende la suma de todos los intentos erróneos procesados por cada sistema individual.

Según Apple, el acceso de administración a estos sistemas es imposible, al haberse destruido las tarjetas de acceso de administración (que permiten cambiar el *firmware* de los HSMs). Complementariamente, cualquier intento de modificar el *firmware* o acceder a la clave privada provocarán que ésta sea destruida, y los propietarios de los registros de custodia serán notificados de la pérdida de dichos registros.

[25] https://es.wikipedia.org/wiki/Secure_Remote_Password

## 8.2 GESTIÓN DE LAS CONTRASEÑAS ALMACENADAS EN EL LLAVERO

### 8.2.1 iOS

Desde el punto de vista del usuario, los elementos almacenados por él en el llavero se pueden gestionar desde la sección "Contraseñas y cuentas - Contraseñas de webs y apps", no siendo posible en este menú diferenciar entre elementos almacenados en local o en el llavero de iCloud.

Para más información sobre la gestión de los elementos del llavero, se recomienda consultar el apartado "Gestión de los elementos del llavero" de la guía "Configuración segura de iOS 13" [Ref.- 413].

### 8.2.2 macOS

Cuando se habilita el uso del llavero de iCloud en macOS, se añade un nuevo llavero "iCloud" a los tres existentes por defecto ("Inicio de sesión", "Ítems locales" y "Sistema"). Los contenidos de este llavero se pueden consultar desde la app "Acceso a llaveros" pinchando sobre la entrada "iCloud" (se recomienda revisar el apartado "Llavero (Keychain)"" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.- 412] para una descripción detallada del uso de los llaveros en macOS).

Complementariamente, las contraseñas almacenadas en el llavero se pueden acceder a través de la app "Safari" (ver apartado "8.2.3. Uso del llavero por parte de Safari").

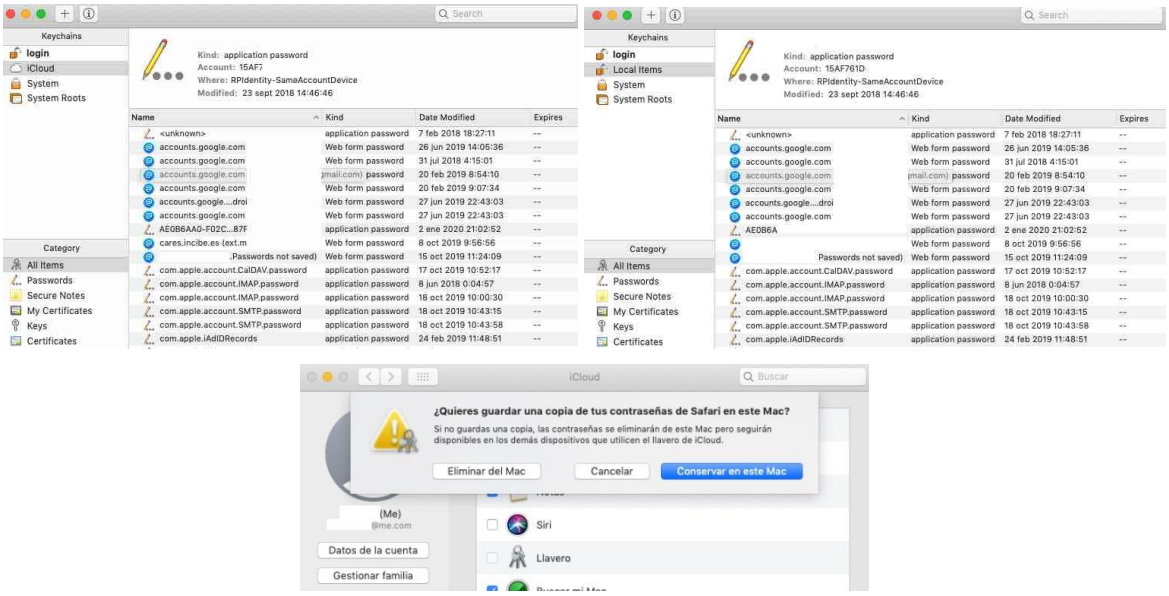



*Figura 99 - Gestión del llavero de iCloud*

### 8.2.3 USO DEL LLAVERO POR PARTE DE SAFARI

Tanto la versión de Mobile Safari disponible en iOS como la versión de Safari de macOS se integran directamente con el llavero de iCloud, permitiendo el almacenamiento de credenciales y tarjetas de crédito, su reutilización, e incluso la generación y almacenamiento de nuevas contraseñas (a través de un generador de contraseñas aleatorias robustas). Esta

funcionalidad de Safari se complementa con capacidades para autocompletar formularios web.

Desde el menú de Safari "Preferencias - [Contraseñas]", previa introducción de la contraseña del usuario administrador, se accede a los contenidos del llavero. Seleccionando una entrada concreta, además de ver los datos de la credencial, se puede compartir vía AirDrop con los contactos dados de alta en el Mac.

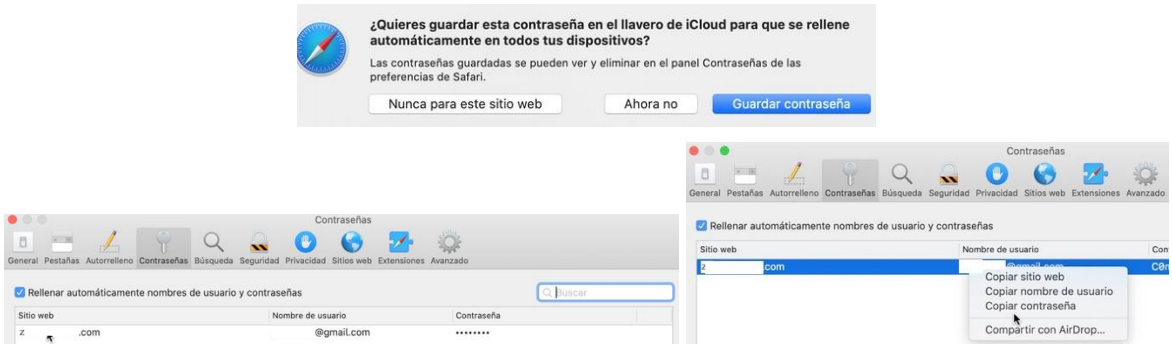



*Figura 100 - Compartición de contraseñas del llavero de iCloud*

Safari puede añadir nuevos elementos al llavero cuando se introducen las credenciales en un sitio web para el cual no existen entradas, a excepción de cuando se navega de forma privada. Algunos sitios web imponen el no almacenamiento de credenciales, en cuyo caso Safari no guardará datos para ellos.

### 8.2.4 AUTORRELLENO DE CONTRASEÑAS Y DE CÓDIGOS DE SEGURIDAD

Los contenidos del llavero de iCloud son accesibles por parte de la funcionalidad de autorrelleno (para más información, consultar los apartados "Autorrellenar contraseñas" y "Ajustes de Safari" de la "Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 13)" [Ref.- 413]).

La principal funcionalidad de este servicio es la de rellenar las credenciales tanto en apps como en sitios webs, sin que el usuario deba teclearlas activamente. Complementariamente, permite:

- La compartición de contraseñas con los contactos del usuario.
- La generación automática de contraseñas seguras.
- Proporcionar la contraseña a un dispositivo Apple TV cercano que la solicite.

La función de autorrelleno permite al usuario compartir las credenciales almacenadas por Safari con otras apps, siempre que el usuario dé su consentimiento, presentando la lista de credenciales fuera del proceso asociado a la app. De forma equivalente, las credenciales que un usuario introduce en una app de confianza pueden almacenarse en el llavero para su uso por la función de autorrelleno.

Para que una app pueda consultar las credenciales almacenadas para un sitio web, es necesario:

- Que haya declarado un "*entitlement*" solicitando acceso a las contraseñas almacenadas por Safari en el llavero. El "*entitlement*" debe incluir los FQDN (*Fully Qualified Domain Names*) de los sitios cuyas credenciales puede solicitar.
- Que el servidor web del sitio incluya en su recurso "`/.well-known/apple-app-site-association`" los identificadores únicos de la app autorizados por Apple.

- Adicionalmente, el usuario debe aprobar la consulta mediante el menú de diálogo.

Complementariamente, el denominado "relleno automático de códigos de seguridad" (*security code autofill*), permite que los mensajes SMS asociados a contraseñas o códigos de un solo uso (OTP, *One Time Password*, empleados habitualmente como segundo factor de autentificación, 2FA) puedan ser autorrellenados, tanto en el dispositivo iOS que los recibe como en ordenadores con macOS vinculados a la cuenta de iCloud. El código OTP se mostrará en la app destinataria a través de la barra "QuickType" (disponible en la parte superior del teclado en iOS) o como un menú flotante cercano al campo destinado al OTP (en macOS), requiriendo simplemente realizar una pulsación sobre él para que el código se inserte automáticamente en el campo correspondiente. El autorrelleno de códigos en macOS forma parte de las funciones de continuidad, y requiere que el menú "Mensajes - Reenvío de SMS" del iPhone incluya al Mac.

Esta función pretende simplificar de cara al usuario la introducción de credenciales asociadas a 2FA. Para detectar cuándo un SMS puede corresponder a un código, se utilizan elementos heurísticos como la detección de las palabras "código" o "contraseña".

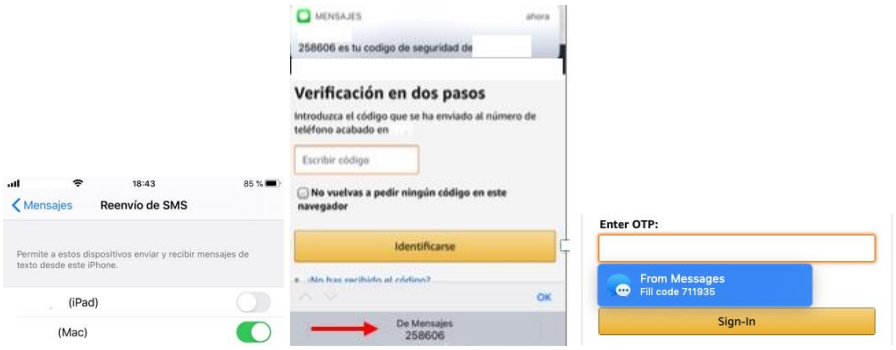



*Figura 101 - Autorrelleno de códigos de seguridad por SMS en iOS y macOS*

## 9. APPLE PAY

Apple Pay es un conjunto de funcionalidades que Apple proporciona para realizar pagos electrónicos en diferentes servicios:

- Tiendas físicas: permite efectuar pagos sin contacto (*contactless*) en establecimientos comerciales, máquinas expendedoras, taxis, etc.
- Sitios web: en los comercios on-line que dispongan del símbolo "Comprar con Pay" desde el navegador web Safari. Si se utiliza un Mac, es preciso que disponga de "Touch ID" o, en su defecto, que esté vinculado a una cuenta de iCloud existente en un iPhone o un Apple Watch (en este último caso, el pago se hará efectivo desde el iPhone o desde el reloj).
- Compras en apps: para apps que dispongan de la opción "Comprar con Pay".
- Transporte público: solo disponible en determinadas regiones, no incluyéndose España.
- En EEUU, permite el envío y la recepción de dinero a través de la app "Mensajes".

El uso de Apple Pay requiere que el dispositivo soporte autentificación basada en biometría (Face ID o Touch ID) o que tenga definido un código de acceso. La información relativa a Apple Pay se vincula con el ID de Apple con el que se haya abierto sesión en el dispositivo, y es posible deshabilitar el servicio accediendo al interfaz appleid.apple.com.

Para habilitar el servicio es necesario configurar al menos una tarjeta de crédito/débito/prepago dentro de la app Wallet[26]. Se recomienda consultar la [Ref.- 48] para obtener más detalles sobre el uso de Wallet, que queda fuera del ámbito de la presente guía.

Con Apple Pay el número real de la tarjeta no se comparte con la entidad receptora del pago. Cuando una tarjeta se añade a Wallet:

- Sus datos se envían cifrados a Apple, donde se descifran para determinar la red de pago de la tarjeta, y se vuelven a cifrar mediante una clave propia de dicha red de pago.
- La entidad emisora de la tarjeta asocia un número de cuenta al dispositivo, lo cifra y lo envía a Apple, incluyendo una clave para generar códigos de seguridad dinámicos exclusivos de cada transacción.
- El número de cuenta del dispositivo se almacena en el "*Secure Element*" del dispositivo (un chip diseñado para almacenar información de pago de forma segura[27]). Este número no se incluye en la copia de seguridad de iCloud.

Según afirma Apple, "Apple Pay solo almacena una parte del número de cada tarjeta y una parte de cada número de cuenta de dispositivo, junto con una descripción de la tarjeta" [Ref.- 48].

Si el usuario cierra sesión en su cuenta de iCloud, las tarjetas configuradas en Apple Pay se eliminan del dispositivo, siendo preciso volverlas a añadir si se inicia sesión de nuevo. Complementariamente, es posible eliminar las tarjetas configuradas en un dispositivo desde otro dispositivo vinculado al mismo ID de Apple, lo cual resulta útil en caso de robo o pérdida [Ref.- 70].

## 10. ASISTENTE PERSONAL "SIRI"

Recomendaciones de seguridad:

- Desactivar el uso de Siri en la pantalla de bloqueo.
- Inhabilitar a Siri para analizar el uso que se hace de las apps sensibles.
- Evitar el uso de atajos de Siri que impliquen acciones sensibles.

Siri es el asistente personal digital introducido por Apple en iOS 5.x, basado en un sistema de reconocimiento de voz y lenguaje natural, que permite al usuario realizar multitud de tareas a través de comandos de voz, entre otras [Ref.- 66] [Ref.- 68]:

- Hacer llamadas o enviar mensajes.
- Iniciar aplicaciones.
- Acceder a recordatorios cuando el usuario llega a una ubicación concreta.
- Proporcionar información detallada sobre ubicaciones cercanas en base a la localización actual del usuario.
- Ejecutar atajos.
- Desde iOS 13, para leer las notificaciones entrantes asociadas a aplicaciones de mensajería a través de los AirPods y auriculares compatibles[28].

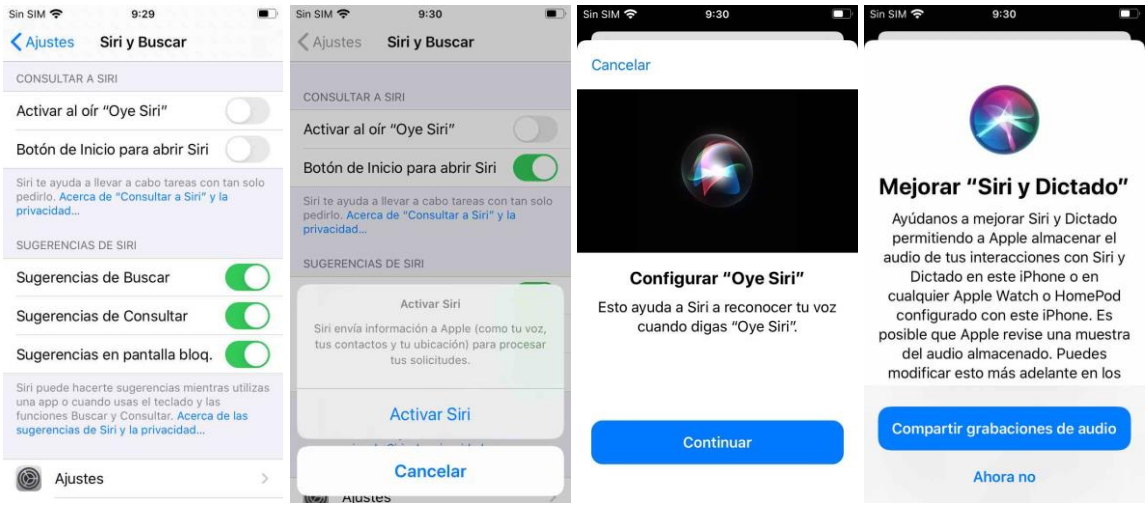
[26] La entidad emisora de la tarjeta debe permitir su configuración como medio de pago en Wallet, para lo cual puede solicitar mecanismos de verificación adicionales.
[27] https://www.kaspersky.es/blog/secure-element/16189/

Siri precisa de acceso a Internet y está disponible para todos los dispositivos del ecosistema Apple, incluido el Apple Watch, CarPlay, Apple TV y HomePod. Debido a que la información procesada por Siri es enviada a Apple (incluida la localización si el ajuste "Privacidad - Localización - Siri y Dictado" está activo), y a que, a lo largo de la historia, se han identificado numerosas vulnerabilidades en este servicio[29], la recomendación de seguridad y privacidad ***es evitar el uso de Siri en la medida de lo posible***. No obstante, en el presente apartado se proporcionan las recomendaciones para la utilización del servicio buscando el equilibrio entre seguridad y funcionalidad.

**NOTA:** Apple ha reconocido en varias ocasiones que fragmentos de grabaciones recibidas en base al uso de Siri han sido accedidos por personal externo, sin que los usuarios afectados fueran conscientes de haber invocado la funcionalidad del asistente[30].

La activación de Siri se lleva a cabo desde el menú:

- iOS: "Ajustes - Siri y Buscar" (iOS), habilitando cualquiera de los interruptores "Activar al oír "Oye Siri"" o "Botón de Inicio para abrir Siri". Durante el proceso de activación, el asistente guiará al usuario a través del proceso de reconocimiento de voz. ***La primera recomendación es denegar la funcionalidad*** "Mejorar "Siri y Dictado"", para evitar que las grabaciones de audio sean enviadas y analizadas por Apple:




[28] https://support.apple.com/es-es/HT210406

[29] https://www.cvedetails.com/cve/CVE-2018-4252/, https://www.cvedetails.com/cve/CVE-2018-4244/, https://www.cvedetails.com/cve/CVE-2016-7597/, https://www.theverge.com/2019/9/13/20863993/ios-13-exploit-lockscreen-bypass-security

[30] https://www.forbes.com/sites/kateoflahertyuk/2019/07/28/apple-siri-eavesdropping-puts-millions-of-users-at-risk/#1adaf516a530, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings




*Figura 102 - Proceso de activación de Siri en iOS 13*

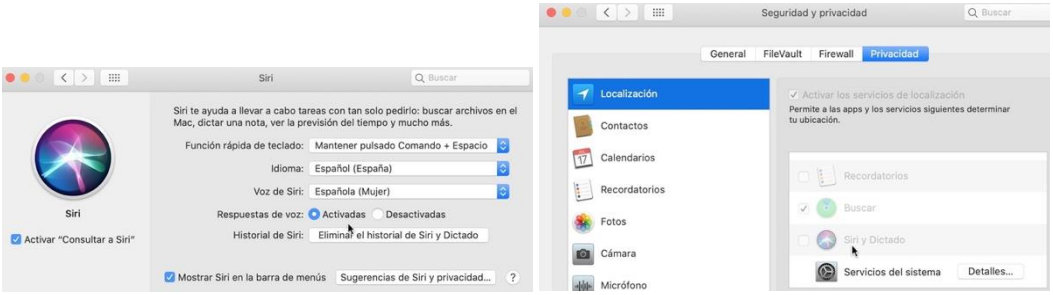



*Figura 103 - Proceso de activación de Siri y ajustes del asistente en macOS 10.15 Catalina*

- macOS: "Preferencias del sistema - Siri - Activar "Consultar a Siri"".

Complementariamente, el usuario puede determinar si desea que la información de Siri se comparta entre todos sus dispositivos o no activando/desactivando el ajuste "ID de Apple - iCloud - Siri".

Las <Figura 102> y <Figura 103> ilustran el proceso de activación y los ajustes relativos a Siri que quedan por defecto en el sistema iOS 13 y macOS 10.15 Catalina (respectivamente) tras completarse dicho proceso. Se aconseja actualizar la configuración por defecto para minimizar los riesgos de seguridad y privacidad derivados del uso de Siri:

- ***Desactivar*** "Siri con pantalla bloqueada" (iOS): esta recomendación se basa en el historial de vulnerabilidades que han afectado a Siri en la pantalla de bloqueo. Adicionalmente, se evita que sea posible acceder a contenidos de mensajes, de eventos del calendario, etc. que pueden estar siendo atendidos por terceros de forma accidental. Este ajuste es equivalente a "Ajustes - Touch ID y código - Permitir acceso al estar bloqueado: Siri", y la modificación de uno conduce automáticamente a la modificación del otro.
- ***Cambiar el ajuste*** "Respuestas de voz": seleccionar "Controlar con el botón de tono" o "Manos libres" (iOS) y "Desactivadas" (macOS) para impedir que Siri proporcione respuestas en voz alta en cualquier situación.
- ***Eliminar*** el "Historial de "Siri y Dictado"" cuando se considere que se han realizado interacciones con Siri que involucren contenido sensible, tanto del usuario como de su actividad personal y o profesional.

- ***Desactivar*** "Sugerencias en pantalla bloqueada" (iOS): se considera que la condición de bloqueo del dispositivo es un elemento que debe preservarse por encima de cualquier funcionalidad. Estando activa, Siri puede emitir sugerencias que desvelen información sensible, por ejemplo, al aproximarse el dispositivo a un lugar determinado, puede sugerir enviar un mensaje a un contacto. Por otro lado, a lo largo de la historia Siri a introducido numerosas vulnerabilidades en la pantalla de bloqueo de iOS [Ref.- 30].
- Para cada app individual, el usuario debe valorar los siguientes ajustes relacionados con las sugerencias de Siri, ya que, aunque Apple indica que el procesamiento de los datos por parte de Siri se realiza a nivel local y que en ningún caso está vinculado a información personal del usuario, los elementos recabados se envían (además de a iCloud para la sincronización de Siri en todos los dispositivos vinculados al mismo ID de Apple) al propio Apple, para mejoras en sus productos y en otros motores de búsqueda [Ref.- 67]:
  - "Aprender de esta app": se recomienda desactivar el interruptor para las apps que manejen contenido sensible, evitando así que sus datos puedan ser enviados a Apple y procesados por éste o sus filiales de cara a análisis de uso del producto.
  - "Mostrar en Buscar" (iOS): de este modo se impide que la propia app aparezca en los resultados del servicio "Buscar".
  - "Sugerencias de Siri en la app" (disponible solo para algunas apps, como "Calendario" o "Recordatorios"): con esta opción se controla si Siri podrá interferir en el uso de la app para ofrecer sugerencias.
  - "Sugerir atajos" (iOS): ver apartado "10.2. Atajos de Siri".
- ***Desactivar*** "Ajustes - Privacidad - Localización - Servicios del sistema - Sugerencias según ubicación" (iOS) o "Preferencias del sistema - Seguridad y privacidad - Privacidad - Localización - Servicios del sistema - Detalles… - Sugerencias según la ubicación" (macOS) para impedir que Siri envíe a Apple la localización exacta del dispositivo mientras opera en segundo plano. Pese a ello, Apple sí podrá utilizar la dirección IP del dispositivo para determinar una ubicación aproximada.
- ***Seleccionar*** "Ajustes - Privacidad - Localización - Siri y Dictado: Nunca" (iOS) para impedir que la localización se envíe a Apple durante las búsquedas de Siri.
- ***Desactivar*** "Ajustes - Notificaciones - Avisar de los mensajes con Siri" para evitar que Siri lea el contenido de los mensajes recibidos con la pantalla bloqueada si el usuario lleva puestos auriculares compatibles[31], ya que no existe ningún mecanismo para detectar que el portador de los auriculares sea el propietario del dispositivo. Aunque este ajuste permite filtrar los contactos para los cuales se habilitará esta funcionalidad, debido a que no es posible determinar qué contenidos pueden ser recibidos, se aconseja desactivar la opción global.

Es posible bloquear las búsquedas web a través de Siri estableciendo una restricción en el menú "Ajustes - Tiempo de uso - [Restricciones de contenido] - [Siri] Contenido de búsquedas web" (consultar el apartado "Restricciones" de la guía "Configuración segura de iOS 13" [Ref.- 413] para más información sobre el establecimiento de restricciones en el dispositivo móvil).

## 10.1 FUNCIONAMIENTO DE SIRI

**NOTA**: el alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de Siri ni de sus protocolos de comunicaciones.

[31] https://support.apple.com/es-es/HT210406

Cuando el usuario pronuncia "Oye Siri" o pulsa el botón de inicio (iOS), o el botón de Siri del Touch Bar o el atajo de teclado (macOS) o utiliza la búsqueda de "Spotlight" (dependiendo de los ajustes del dispositivo), Siri comienza a procesar la entrada (ya sea la voz del usuario o el texto introducido en el campo de búsqueda) e intenta resolver la consulta de forma local. En caso negativo, traslada la consulta a los servidores Siri de Apple utilizando unos identificadores aleatorios generados por el dispositivo durante la activación Siri. Los contenidos de la consulta y la respuesta se intercambian cifrados, impidiendo su intercepción por parte de terceros. Si se desactiva Siri y vuelve a ser activado de nuevo, estos identificadores aleatorios cambiarán por lo que, teóricamente, sería posible eliminar toda la información que Siri hubiera almacenado previamente sobre el usuario desactivando el servicio.

Siri es capaz de resolver expresiones del lenguaje natural y trasladar los resultados a otras apps del dispositivo que implementan el SiriKit: por ejemplo, la indicación "Telefonear a <nombre>" accederá a la información de "Contactos" del usuario para encontrar correspondencias con "<nombre>" y ejecutar la acción específicamente sobre el resultado. Siri comprueba si la app que solicita la resolución tiene permiso de acceso (concedido por el usuario) a la información concreta. En caso negativo, en lugar del resultado, pasará a la app la expresión de lenguaje natural tal cual ha sido reconocida.

## 10.2 ATAJOS DE SIRI

Desde iOS 13 la app "Atajos" se ofrece como app de sistema y se integra completamente con los "Atajos de Siri". En el apartado "Atajos (Shortcuts): Automatización en iOS 13" de la guía "Configuración segura de iOS 13" [Ref.- 413] puede consultarse más información sobre el uso de atajos de forma local.

A través de esta integración, Siri puede ejecutar un atajo en cuanto el usuario inicie el asistente y pronuncie el nombre asignado al atajo. Complementariamente, Siri analiza el uso que el propietario hace del dispositivo y de sus apps y, en base a sus heurísticas, crea patrones de comportamiento y realiza sugerencias para iniciar tareas. Por ejemplo, el uso de una app de una cadena de restaurantes puede llevar a que, si se detecta un establecimiento en una localización cercana, se sugiera al usuario pedir comida.

Los atajos derivados por parte de Siri se incorporan al menú "Ajustes - Siri y Buscar - Atajos Sugeridos", y el usuario puede añadirlos a su galería mediante el botón "+", para lo cual debe grabar un patrón de voz que, al ser identificado por Siri, lanzará la automatización [Ref.- 69].

Las apps de terceros compatibles con los atajos de Siri ofrecen el botón "Añadir a Siri" en los atajos que implementan (la ubicación de estos atajos depende de la app); por medio de este botón, el usuario puede incorporar un atajo a Siri para que éste lo procese al escuchar el patrón de voz asociado al atajo. En la <Figura 104> se ofrece el ejemplo de integración con los atajos de Siri de la app "Gmail", a cuya configuración se accede desde el menú " ≡ - ⚙ Ajustes ".

La propia app "Atajos" incorpora en su sección "Galería" una serie de atajos titulados "Genial con Siri", que vienen pre-configurados con acciones habituales para ser usados desde el asistente.

Desde el punto de vista de seguridad, se recomienda no ejecutar atajos que impliquen acciones potencialmente sensibles a través de Siri, debido al riesgo de que un tercero pueda grabar una locución del propietario del dispositivo invocando el atajo y pueda posteriormente tratar de reproducirlo.




*Figura 104 - Configuración de un atajo de Siri desde la app Gmail*

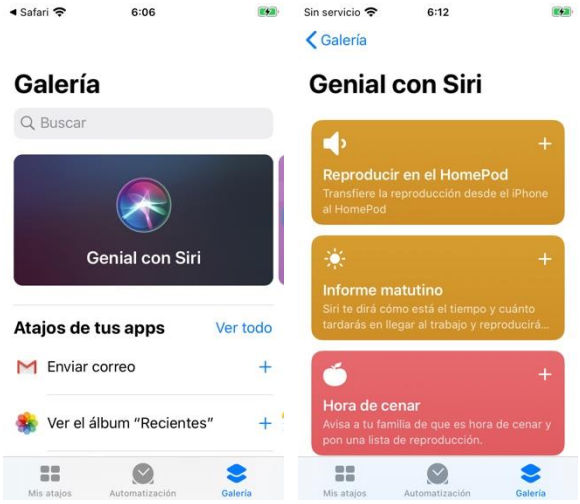



*Figura 105 - Galería de atajos de Siri en la app "Atajos"*

## 11. APPS CON FUNCIONALIDAD LIGADA A LA CUENTA DE ICLOUD

Recomendaciones de seguridad:

- Evaluar la necesidad de sincronizar los contenidos de las apps entre distintos dispositivos, ya que puede ocurrir que el uso que el propietario hace de ellas no lo justifique.
- Evitar la compartición de elementos con terceros y, especialmente, la compartición mediante URLs de índole pública.

### 11.1 RECORDATORIOS

El servicio "Recordatorios" se ha modificado sustancialmente desde iOS 13, y los recordatorios almacenados en iCloud no son accesibles desde dispositivos que no dispongan de iOS 13 o macOS 10.15 Catalina [Ref.- 50]. Se han añadido diversas funcionalidades vinculadas a la compartición de recordatorios vía iCloud.

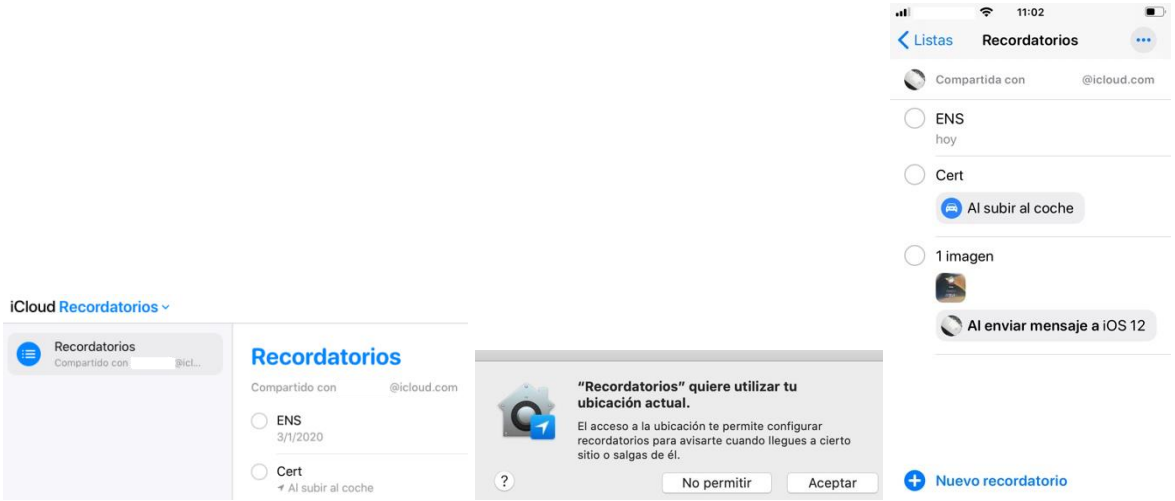
El acceso a los datos de “Recordatorios” está disponible tanto desde los dispositivos vinculados al mismo ID de Apple como desde el interfaz de iCloud, y estos datos se incluyen en las copias de seguridad de iCloud (ver apartado "12. Copias de seguridad y restauración en iCloud").

Las capacidades vinculadas al uso de "Recordatorios" en iCloud permiten al usuario:

- Compartir tareas y consultar las que otros usuarios han compartido con él/ella a través de las listas compartidas. Para ello, se debe seleccionar el menú "..." dentro de una lista concreta y elegir la opción "Añadir personas". Se mostrará la lista de apps a través de las cuales se podrá enviar al destinatario la URL de iCloud que da acceso al recordatorio. Si se opta por compartir un recordatorio mediante la app "Mail", el usuario invitado deberá aceptarlo a través del enlace "Unirme" incluido en el contenido del mensaje de invitación.
  Es importante identificar en el menú principal de la app "Recordatorios" las listas que están siendo compartidas, a fin de determinar cuándo la compartición deja de ser necesaria. Cuando cese el motivo por el cual se compartió un recordatorio con un tercero, se aconseja eliminarlo de la lista de personas con acceso mediante el menú "... - Ver participantes - Dejar de compartir".
  Asimismo, los integrantes del grupo con roles diferentes al de organizador pueden abandonar la lista de forma activa a través del menú "Ver participantes - [Seleccionar el ID de Apple propio] Eliminar acceso" (ver <Figura 72>).
- Crear listas de compartición con el grupo "Familia" (ver apartado "6.9.2.4. Recordatorios compartidos con "Familia"").

La app "Recordatorios" se integra con otras apps para ofrecer funcionalidades adicionales:

- Incluir recordatorios basados en la ubicación del dispositivo[32], para lo cual la app "Recordatorios" solicitará al usuario permiso de ubicación.
- Activar un recordatorio cuando se esté enviando un mensaje a un contacto concreto.
- Permitir que se añada un recordatorio cuando se programen eventos en otra app (por ejemplo, una app de planificación de viajes). Se desaconseja autorizar el acceso a "Recordatorios" a apps que no sean de total confianza y especialmente, si no se requiere que incluyan elementos de este carácter.
- Insertar ficheros adjuntos, incluyendo fotografías.




[32] "How to Create a Location-Based Reminder on Your iPhone". https://www.macrumors.com/how-to/create-location-based-reminder-ios/

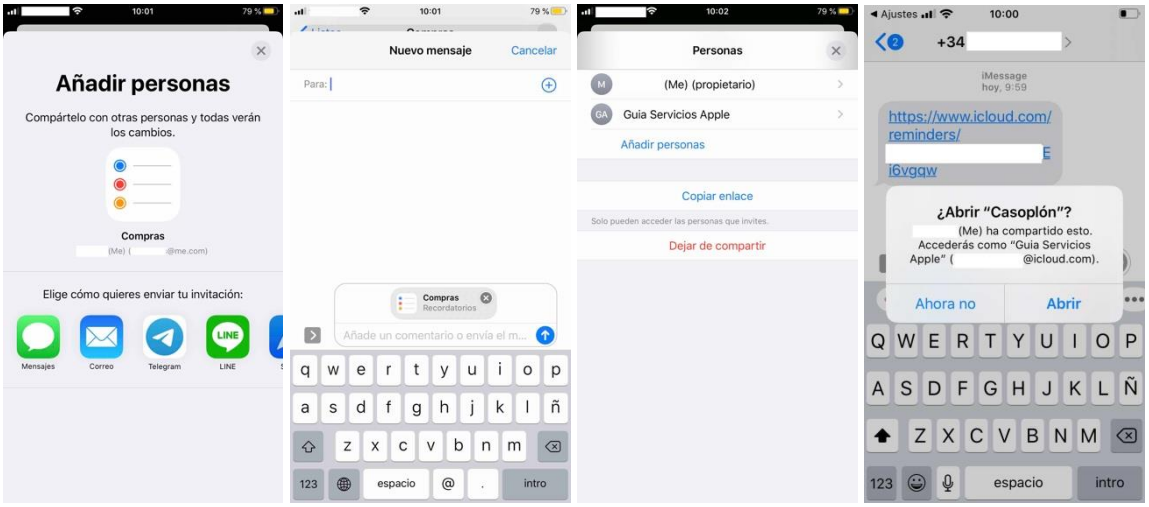



*Figura 106 - Uso de "Recordatorios" en iCloud en iOS 13*

Para obtener una descripción detallada sobre el uso de este servicio, se recomienda consultar la documentación oficial de Apple [Ref.- 51], [Ref.- 52] y [Ref.- 61].

## 11.2 ICLOUD DRIVE

iCloud Drive es un servicio de almacenamiento de archivos en la nube que permite la compartición de información tanto entre los dispositivos vinculados a una misma cuenta de iCloud como con otros usuarios. Los archivos modificados en un dispositivo sin conexión se sincronizarán con el almacenamiento de iCloud Drive cuando se disponga de acceso a Internet. A fecha de elaboración de la presente guía, Apple ofrece de forma gratuita 5 GB de almacenamiento en Drive, disponiendo de diversos planes de ampliación[33].

A través de la app "Archivos", se pueden crear carpetas compartidas en iCloud Drive a las que se puede incluso otorgar permiso para poder añadir nuevos archivos.

Desde macOS 10.15 Catalina, para que una app pueda acceder a iCloud Drive deberá solicitar el permiso expreso del usuario. Para inhabilitar el permiso de acceso a iCloud Drive una vez concedido, se dispone del menú "Preferencias del sistema - iCloud - iCloud Drive - Opciones... - Documentos". Si la opción "Carpeta Escritorio y Documentos" se habilita, todos los documentos del Mac almacenados en las carpetas "Escritorio" y "Documentos" se trasladarán a iCloud[34], desde donde estarán accesibles por parte de todos los dispositivos vinculados a la cuenta. En el "Finder" de macOS ambas carpetas se mostrarán en la rama "iCloud" (ver <Figura 107>).

**NOTA:** si se desactiva la opción "Carpeta Escritorio y Documentos", los archivos se conservarán en iCloud Drive, y se crean sendas carpetas "Escritorio" y "Documentos" en el directorio "Home" (`/Users/<usuario>`) del usuario en macOS sin contenido. El usuario deberá trasladar manualmente desde iCloud Drive los archivos que desee que estén disponibles localmente.

Por su parte, en iOS todas las apps suministradas de fábrica tienen concedido el permiso de acceso de iCloud Drive una vez el usuario inicia sesión en iCloud. Para alterar este comportamiento, cada app dispone de un interruptor bajo "Ajustes - ID de Apple - [Apps que

[33] "Precios y planes de almacenamiento de iCloud". https://support.apple.com/es-es/HT201238

[34] Es importante diferenciar entre el "Escritorio" de macOS (único) y los "Espacios" del escritorio (las múltiples vistas que el usuario puede crear para organizar el espacio de trabajo).

usan iCloud]". En la sección "Ajustes - ID de Apple - Almacenamiento - iCloud - Gestionar almacenamiento" se puede consultar el uso que cada app hace del espacio en la nube.

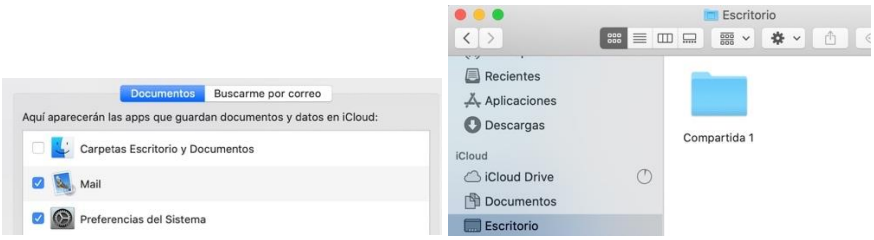



*Figura 107 - Control del acceso a iCloud Drive por parte de las apps en macOS 10.15 Catalina*

El acceso a los contenidos almacenados en iCloud Drive desde iOS se realiza a través de la app "Archivos" (descrita en el apartado "App "Archivos"" de la guía "Configuración segura de iOS 13" [Ref.- 413]). Como se indica en dicho apartado, la opción "Añadir personas" del menú "Compartir" permite compartir ficheros mediante los enlaces a su ubicación en iCloud. La modificación del archivo (si está permitida por el usuario que comparte) implicará que todos los usuarios vean reflejados los cambios.

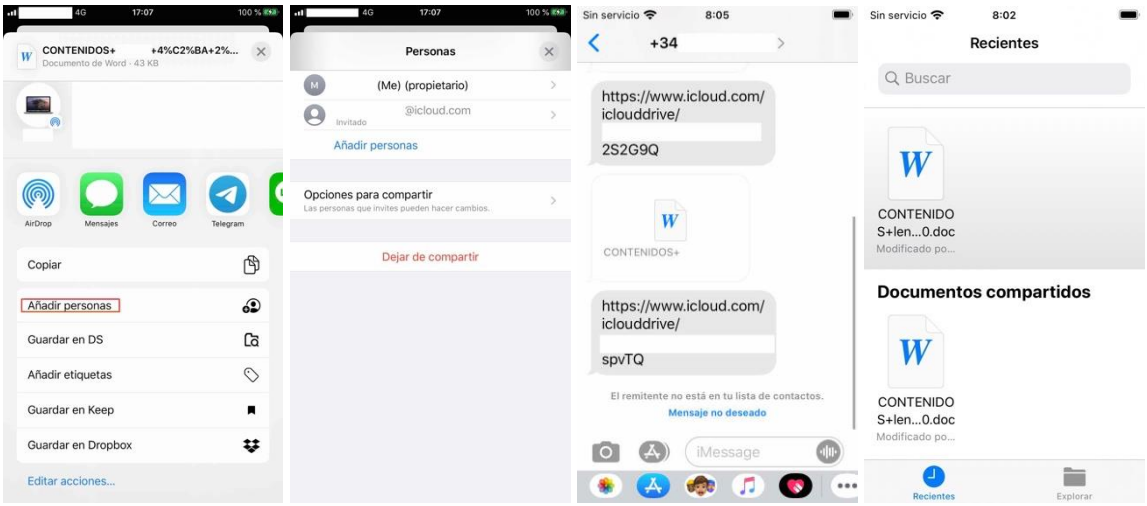



*Figura 108 - Uso de la app "Archivos" en iOS 13 para compartición de ficheros de iCloud Drive*

Según la [Ref.- 38], el tránsito de los datos que se intercambian con iCloud Drive incorpora cifrado extremo a extremo, y también se cifra el contenido de los propios datos almacenados en los servidores de iCloud. Sin embargo, si un atacante tuviera acceso a cualquier dispositivo vinculado a la cuenta de usuario podría comprometer la información de todos los dispositivos, lo cual lleva a desaconsejar el uso del almacenamiento en iCloud Drive para los contenidos sensibles.

Consultar el apartado "12.2.2.1. Restauración de archivos de iCloud Drive" para obtener información sobre cómo recuperar elementos que se han borrado de iCloud Drive.

## 11.3 MAIL

"Mail" es la app cliente de correo electrónico proporcionada por Apple en las distribuciones de sus sistemas operativos iOS y macOS. Puede ser configurada para acceder tanto al servicio de correo de iCloud como a servidores de correo externo, y soporta cifrado y firma mediante GPG a través de extensiones de terceros.

La app "Mail" utiliza una base de datos cifrada (incluyendo los adjuntos) mediante unas claves protegidas por el código de acceso al dispositivo.

Las cuentas de correo del dominio "icloud.com" pueden obtenerse al dar de alta un nuevo ID de Apple o activando el interruptor "Ajustes - [ID de Apple] - iCloud - Mail" en iOS (ver <Figura 109>).

Los ajustes vinculados a la app "Mail" están disponibles en:

- iOS: "Ajustes - Correo".
- macOS: desde el menú "Preferencias" de la app "Mail".
- iCloud: desde el menú "Mail" accediendo a la configuración disponible en el icono " - Preferencias".

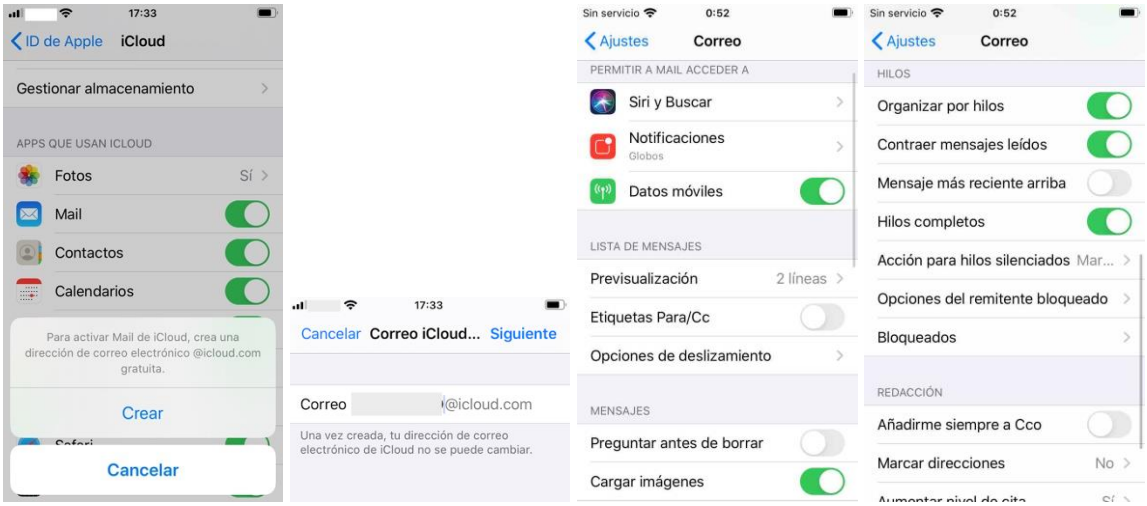



*Figura 109 - Creación de una cuenta de correo en el dominio icloud.com y ajustes de correo en iOS 13*

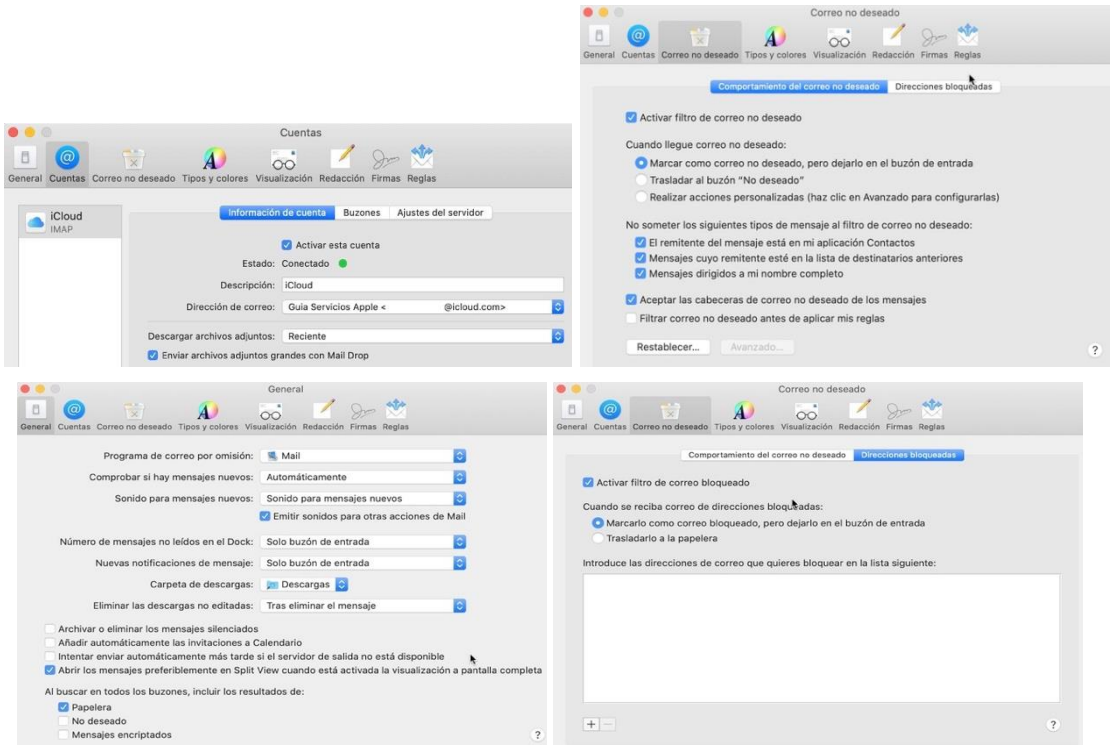



*Figura 110 - Ajustes de la app "Mail" en macOS 10.15 Catalina*

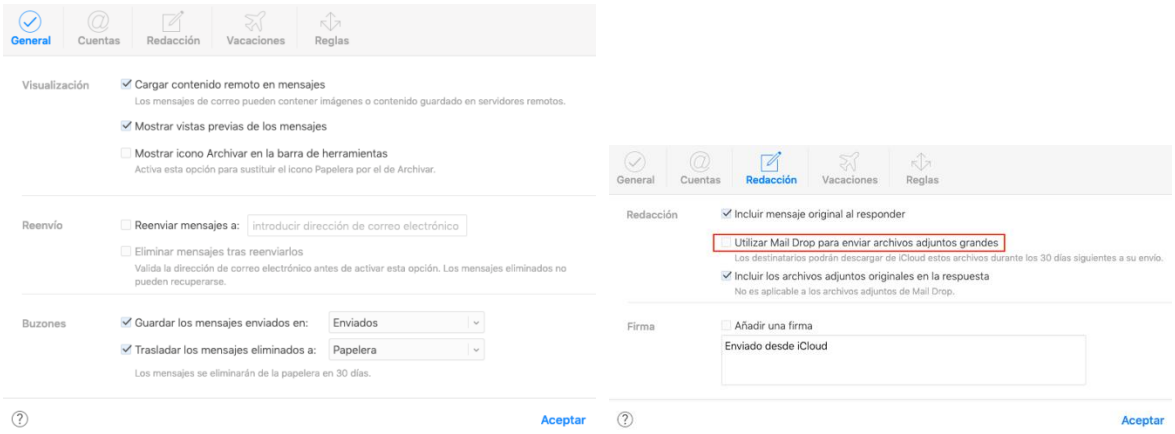



*Figura 111 - Ajustes de Mail en icloud.com*

Desde el punto de vista de seguridad y privacidad, ***se recomienda establecer los siguientes ajustes***:

- [Cuentas] - Información de cuenta - Descargar archivos adjuntos" (macOS): fijar a "Nada" para evitar que "Mail" descargue de forma automática archivos con un formato que no corresponda a contenido multimedia[35]. Aunque macOS dispone de mecanismos de protección contra *malware* (consultar el apartado "Mecanismos de protección y tecnologías de seguridad en macOS" de la "Guía práctica de seguridad de macOS 10.14 Mojave" [Ref.-412] para más información), se recomienda en todo caso no seleccionar ningún archivo cuyo remitente no sea de confianza, y no abrir contenido que resulte sospechoso.
- [Visualización] Cargar contenido remoto en mensajes" (macOS): desactivar.
- "Firma" (iOS): eliminar el texto "Enviado desde mi iPhone" para no desvelar el tipo de dispositivo.
- Suprimir de la pantalla de bloqueo el contenido de los mensajes de "Mail" para evitar que el acceso visual por parte de terceros pueda revelar contenido sensible:
  - iOS: "Ajustes - Mail - Notificaciones - Mostrar previsualizaciones - Si está desbloqueado/Nunca".
  - macOS: "Preferencias del sistema - Notificaciones - Mail - Mostrar previsualizaciones de notificaciones - Al desbloquear".

### 11.3.1 CORREO CIFRADO (macOS)

La app "Mail" soporta el envío de mensajes cifrados y firmados si se dispone de una *smart-card* con un *token* PIV (*Personal Identity Verification*) o de una extensión como OpenPGP[36]. Si la cuenta de correo configurada en el Mac se corresponde con el certificado del *token*, "Mail" mostrará el icono "", que representa la opción para firmar el mensaje; si se pulsa dicha opción, el mensaje mostrará el icono "" indicando que lleva incorporada la firma digital del emisor.

Para el cifrado del mensaje, si "Mail" dispone del certificado asociado a la dirección del destinatario o bien puede obtenerlo de un GAL (Microsoft Exchange *Global Address List*), presentará un botón "" en la barra de herramientas del mensaje y, al pulsarlo, el mensaje se

[35] Las imágenes, archivos PDF y archivos de vídeo y/o audio siempre se descargan de forma automática, de acuerdo con lo descrito en el "Manual del usuario de Mail" que se despliega desde el icono "?".
[36] https://www.openpgp.org/software/ y https://gpgtools.org

cifrará con la clave pública del receptor y la barra mostrará el icono "" indicando que se enviará cifrado.

### 11.3.2 CORREO NO DESEADO

La app "Mail" permite bloquear remitentes, de forma que sus mensajes se procesen como bloqueados en todos los dispositivos vinculados al mismo ID de Apple y se apliquen las reglas definidas para ellos. Para ello el remitente debe figurar en los contactos del usuario.

- iOS:
  - "[Hilos] - Opciones del remitente bloqueado": permite determinar si los mensajes bloqueados se mostrarán en el buzón de entrada o se trasladarán a la papelera.
  - "[Hilos] - Bloqueados": desde este menú se permite seleccionar los contactos que se desea bloquear.
- macOS:
  - El bloqueo de remitentes se configura desde el menú "Correo no deseado - Direcciones bloqueadas", pudiéndose optar por enviar los mensajes a la Papelera o dejarlos en la carpeta de entrada como bloqueados.

Desde el mensaje bloqueado es posible acceder al menú de preferencias (en caso de que se desee, por ejemplo, eliminar al remitente de la lista de bloqueados o cambiar algún otro ajuste).

Los mensajes bloqueados se identifican en la app "Mail" por el símbolo " " (en gris en iOS).

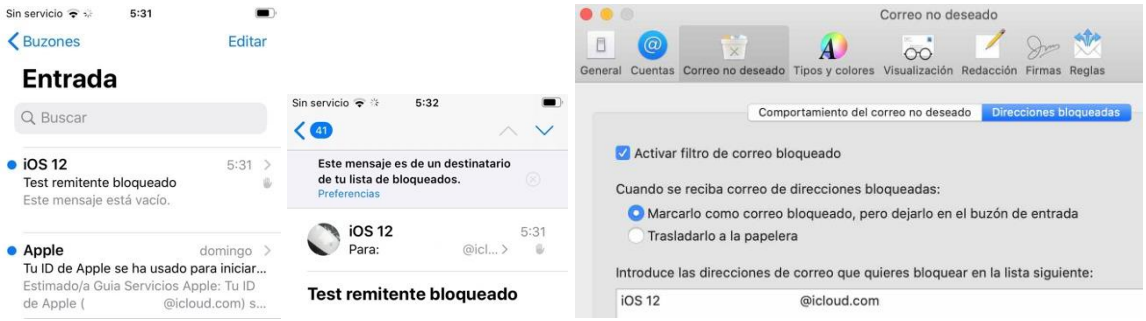



*Figura 112 - Bloqueo de remitentes en la app "Mail"*

Complementariamente al bloqueo de remitentes, la app "Mail" ofrece la opción "silenciar", mediante la cual es posible suprimir las notificaciones y los avisos sonoros en todos los dispositivos vinculados a la misma cuenta de iCloud para todos los mensajes de correo que formen parte de un mismo hilo. Las acciones para silenciar un hilo son:

- iOS:
  - Realizar una pulsación prolongada "*haptic touch*" en uno de los mensajes del hilo hasta que se muestre el menú de la primera imagen de la <Figura 113>, y elegir la opción "Silenciar". De forma equivalente, un hilo silenciado puede reactivarse mediante otra pulsación "*haptic touch*" sobre él y la opción "Dejar de silenciar".
  - Elegir la opción "" del mensaje para que se muestre el menú de la tercera imagen de la <Figura 113> y proceder a "Silenciar".

  La acción a realizar con los mensajes silenciados depende del valor "Ajustes - Mail - [Hilos] - Acción para hilos silenciados".

- macOS:
  - Obtener el menú contextual secundario (el gesto dependerá de la configuración del *trackpad* del usuario) y marcar "Silenciar".

  La acción a realizar con los mensajes silenciados depende del valor "Preferencias de la app Mail - General - Archivar o eliminar los mensajes silenciados".

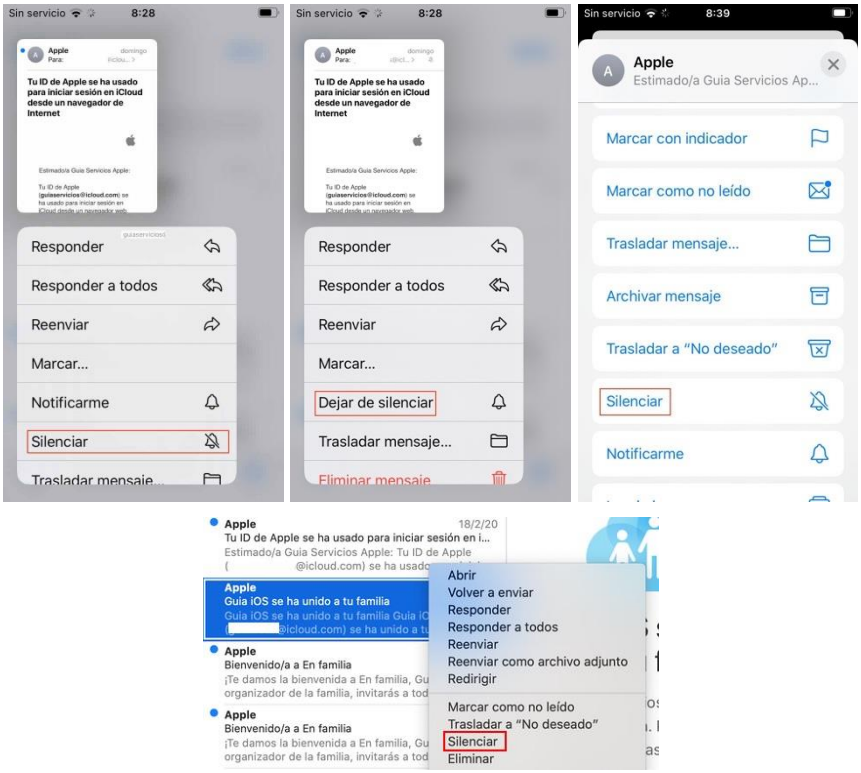



*Figura 113 - Acción para silenciar un hilo de correo electrónico*

### 11.3.3 MAIL DROP

"Mail Drop" es un servicio (deshabilitado por defecto) proporcionado por Apple para el envío y recepción de ficheros adjuntos de correo electrónico cuyo tamaño exceda el tamaño máximo permitido por el proveedor de la cuenta de e-mail del remitente (para cuentas de iCloud el máximo tamaño permitido son 20 MB), y siempre que no supere los 5 GB [Ref.- 54]. Si se habilita, el adjunto se sube a la nube de Apple, donde se almacenará cifrado, y el destinatario recibirá en su lugar un enlace desde el que puede proceder a su descarga en un plazo de 30 días.

Para habilitar el servicio se requiere:

- icloud.com: marcar el ajuste " - Preferencias - Redacción - Utilizar Mail Drop para enviar archivos adjuntos grandes" (ver <Figura 111>).
- macOS: activar la opción "Cuentas - Enviar archivos adjuntos grandes con Mail Drop" del menú "Preferencias" de la app "Mail" (ver <Figura 110>).
- iOS: seleccionar la opción "Usar Mail Drop" del menú de diálogo que el sistema desplegará cuando detecte un tamaño de archivo superior a 20 MB.

Como ilustra la <Figura 114>, el adjunto se reemplaza por un enlace que se enviará al destinatario (en función del tamaño puede ocurrir que tarde un tiempo en estar disponible), y

la app "Mail" iniciará automáticamente la descarga al directorio "`Descargas`" (en macOS se puede especificar otro directorio a través de la opción "General - Carpeta de descargas") tan pronto se selecciona el fichero, sin solicitar confirmación por parte del usuario:

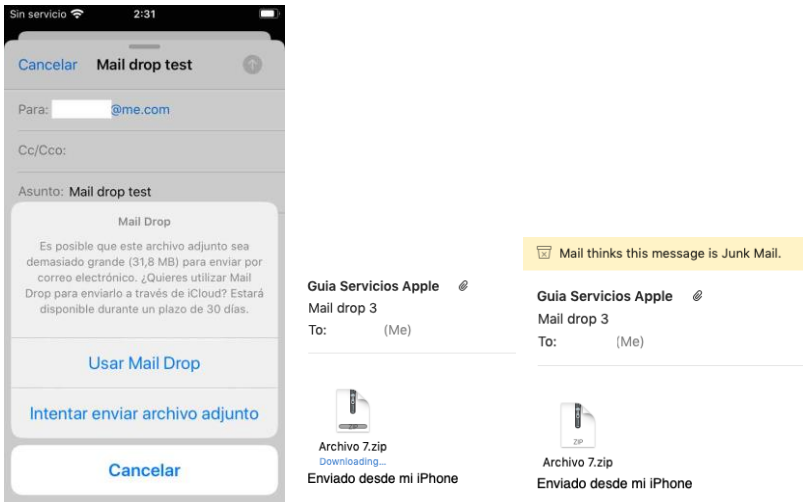



*Figura 114 - Envío de adjuntos de gran tamaño vía Mail Drop*

**NOTA:** durante las pruebas realizadas en la elaboración de la presente guía, se ha observado que la app "Mail" de macOS considera algunos mensajes de Mail Drop como *spam*, y los ubica en el buzón "No deseado" (ver última imagen de la <Figura 114>).

## 11.4 NOTAS

Recomendaciones de seguridad:

- Limitar el uso de notas o carpetas de notas compartidas.
- Limitar el acceso de escritura por parte de terceros.
- Desactivar la compartición cuando cese la razón que dio lugar a ella.

En iOS 13 y macOS 10.15 Catalina, la app "Notas" puede almacenar sus contenidos, además de en el propio dispositivo, en la cuenta de iCloud vinculada a él (siendo éste el valor por defecto mientras no se cambie el parámetro "Ajustes - Notas - Cuenta por omisión" (iOS) y "Notas - Preferencias - Cuenta por omisión" (macOS)), permitiendo así editar y sincronizar carpetas y notas individuales entre todos los dispositivos de la cuenta.

**NOTA:** para poder disponer de notas en el Mac, es preciso seleccionar la opción "Activar la cuenta en mi Mac" [Ref.- 53]. macOS permite además incorporar cuentas que almacenen notas desde otros servicios, por ejemplo, la cuenta de usuario de Google.

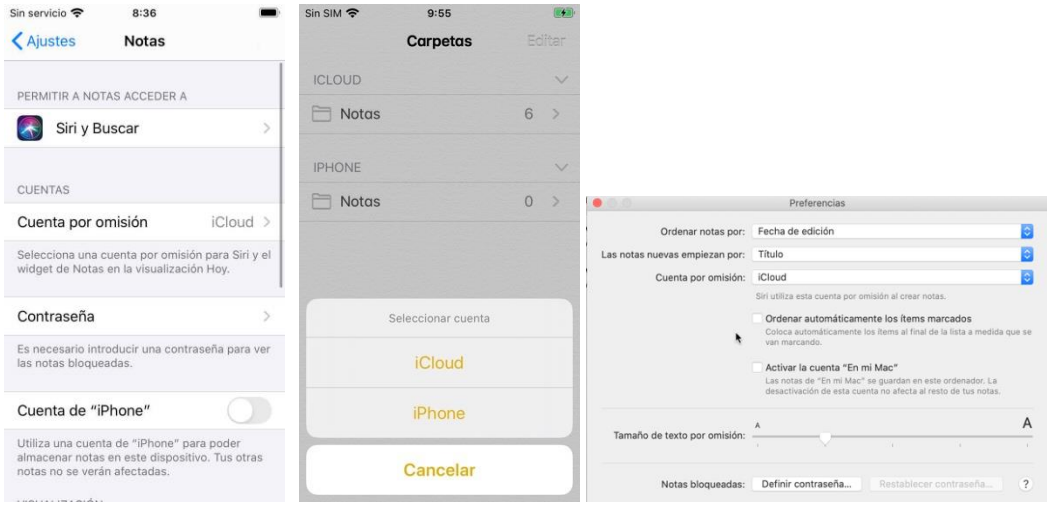



*Figura 115 - Ajustes de "Notas" y selección de cuenta para "Notas" en iOS 13 y macOS 10.15 Catalina*

Adicionalmente, "Notas" ofrece la posibilidad de compartir con otros usuarios de iCloud:

- Carpetas de notas:
  - iOS: accediendo al contenido de una carpeta, desde el menú "" que se muestra en la parte superior (ver <Figura 116>) se desplegará el menú "Añadir personas", desde el cual es posible determinar el método de compartición y las opciones ("Solo lectura" o "Puede hacer cambios").
  - Las carpetas de notas compartidas se muestran con el icono "" a la izquierda de su entrada, y el texto "Compartido con <ID de Apple>" bajo el nombre de la carpeta.

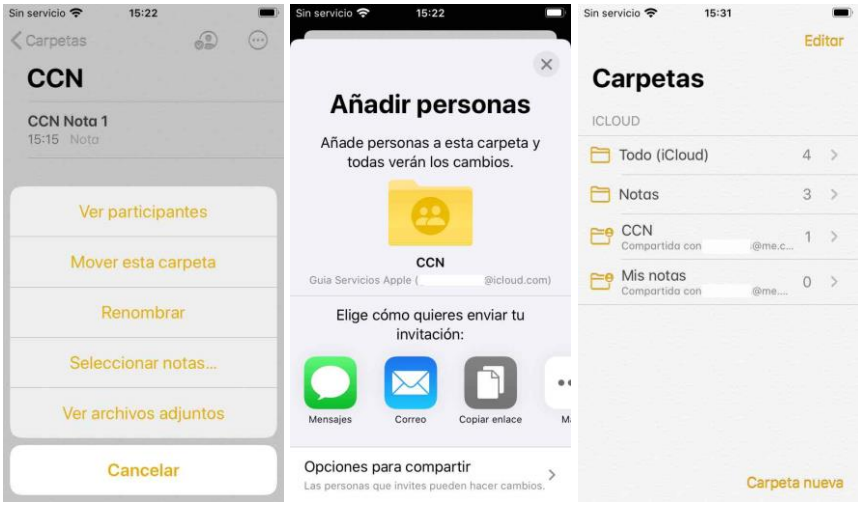



*Figura 116 - Compartición de carpetas de notas y visualización de una carpeta de notas en iOS 13*

  - macOS: desde el menú "" situado a la derecha del nombre de la carpeta se muestra el asistente "Añadir personas", que incluye, como en el caso de iOS, el método de compartición y los permisos de modificación.

- Las carpetas compartidas incluyen el icono "" a la derecha del nombre. En el menú que aparece en la parte superior tras seleccionar una carpeta de notas, se ofrece el icono "" que, además de indicar que la carpeta está siendo compartida, permite obtener los detalles de usuarios y opciones de edición actuales, así como modificarlos (tanto para añadir/suprimir el acceso a todos o ciertos usuarios, como para cambiar los permisos).

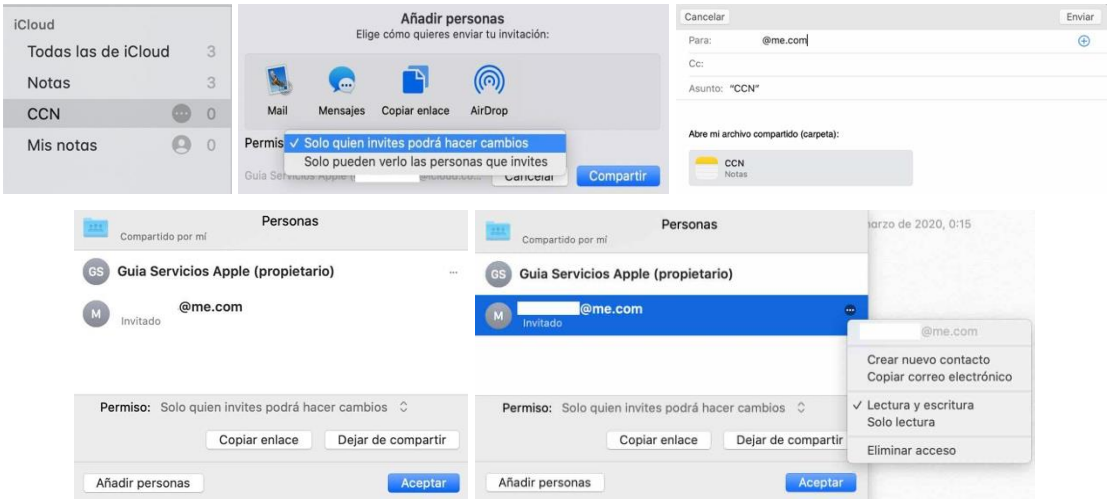


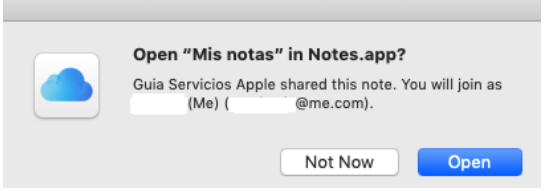

*Figura 117 - Compartición de carpeta de notas en macOS 10.15 Catalina*

- Notas individuales:
  - iOS: tras seleccionar la nota a compartir, se pinchará el menú "", que incluye el menú "Añadir personas", desde el cual es posible determinar el método de compartición y las opciones ("Solo lectura" o "Puede hacer cambios").
  - macOS: tras seleccionar la nota a compartir, se mostrará el menú "" (si la nota no está siendo compartida actualmente) que, al pincharlo, mostrará la opción "Nota <nombre de la nota>"[37]; si la nota ya está siendo compartida, en lugar del menú "" se mostrará el menú "", desde el cual se obtiene el mismo menú descrito anteriormente para la compartición de carpetas, ilustrado en la <Figura 117>.




*Figura 118 - Compartición de nota individual en macOS 10.15 Catalina*

Cuando el receptor de la nota/carpeta recibe, a través del medio seleccionado en el dispositivo origen, el elemento, se solicitará al usuario consentimiento para unirse a su compartición.




[37] En la versión de macOS empleada en la elaboración de la presente guía, parece existir un *bug* por el cual el menú "Añadir personas" aparece sombreado, debiéndose cursar la compartición mediante el menú "Nota <nombre nota>".

*Figura 119 - Solicitud de permiso para abrir en la app "Notas" un elemento compartido*

Las denominadas "notas bloqueadas", que son notas protegidas con contraseña (y aparecen con el símbolo "🔒" a su izquierda), no pueden ser compartidas con otros usuarios de iCloud. La contraseña se define desde el menú "Ajustes - Notas - Contraseña", y se recomienda establecer contraseñas distintas para las notas almacenadas en iCloud y las almacenadas en el iPhone.

En el apartado "App "Notas"" de la guía "Configuración segura de iOS 13" [Ref.- 413] se dispone de información adicional sobre el uso de notas en dispositivos móviles.

## 11.5 CALENDARIOS

Recomendaciones de seguridad:

- Evitar el uso de calendarios compartidos de carácter público.
- Revisar el estado de compartición de los calendarios privados (suscriptores y contenidos) y suprimir los que puedan comprometer la privacidad del usuario.
- Si únicamente se dispone de un dispositivo Apple (o solo se consulta el calendario en un dispositivo concreto), elegir el calendario local frente al calendario de iCloud.

Tanto macOS como iOS permiten la utilización del calendario de iCloud, de forma que los eventos incluidos en él se sincronicen entre todos los dispositivos vinculados al mismo ID de Apple y que sus datos estén accesibles desde el interfaz https://www.icloud.com/calendar/. Para ello, es preciso que el interruptor "[ID de Apple] - iCloud - Calendarios" se encuentre activo. iCloud conserva los eventos de calendario con antigüedad inferior a 6 meses y hasta 3 años vista.

La app "Calendario" permite la gestión de distintos calendarios, asociados a cuentas diferentes. La gestión de las cuentas vinculadas a calendarios está disponible en el menú "Ajustes - Contraseñas y cuentas". Los eventos que se creen se asignarán al calendario por omisión si el usuario no especifica uno en particular. Para establecer el calendario por defecto, se dispone de la opción "Ajustes - Calendario - Calendario por omisión".

La copia de seguridad de los datos de calendario se incluye en iCloud, pudiendo volcarse una versión antigua desde el menú "Avanzado - Restaurar calendarios". Adicionalmente, se puede (y se recomienda desde el punto de vista de seguridad) descargar un archivo de extensión "`.ics`" y salvaguardarlo localmente (ver apartado "12.1. Copia de seguridad").

La utilización de calendarios en iCloud conlleva el mismo riesgo que el resto de servicios asociados a la cuenta del usuario, principalmente ante el compromiso de la cuenta por parte de un tercero.

Para trasladar el calendario de iCloud a otra app cliente de calendario, se aconseja descargar el calendario de iCloud al dispositivo local siguiendo el procedimiento descrito en la documentación oficial de Apple "Descargar un calendario de iCloud.com"[38].

### 11.5.1 COMPARTICIÓN DE CALENDARIOS

El servicio "Calendarios" de iCloud permite la compartición de calendarios con otros usuarios desde el interfaz de iCloud https://www.icloud.com/calendar/, seleccionando el calendario

[38] https://support.apple.com/es-es/HT204055#calendars

concreto y el botón "" situado a la derecha de su nombre (los calendarios que no están compartidos actualmente tienen el icono en gris claro, frente a los ya compartidos, que lo tienen en gris más intenso ""). Se distinguen dos tipos de compartición:

- Privada: únicamente otros usuarios que dispongan de un ID de Apple y utilicen los servicios de iCloud pueden acceder al calendario compartido. El destinatario recibirá una notificación con la invitación al calendario, desde la que puede unirse o rechazar la compartición. Si se une, el propietario del calendario será asimismo notificado.
  Si el invitado acepta, el calendario aparecerá tanto en la app "Calendario" de sus dispositivos como en su interfaz de iCloud https://www.icloud.com/calendar/. El invitado podrá ver las direcciones del propietario y de otros miembros del calendario, pero no podrá a su vez compartirlo con otros usuarios (únicamente puede abandonar el grupo si lo desea).
- Pública: se crea un enlace público en iCloud, de forma que, cualquier persona con acceso al enlace, puede incorporar el calendario a su entorno. La invitación puede cursarse directamente desde el interfaz de iCloud (vía correo electrónico), bien enviando el enlace webcal por cualquier medio. ***El uso de calendarios compartidos, especialmente públicos, se desaconseja desde el punto de vista de seguridad/privacidad, y debe observarse mucha precaución con los eventos que se añaden a dicho calendario.***

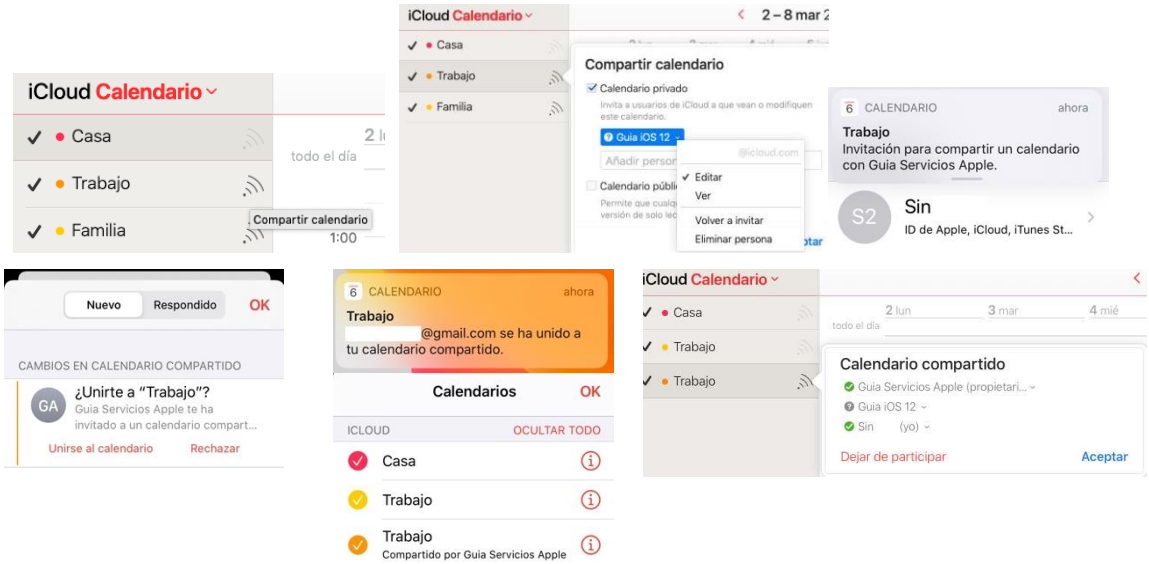



*Figura 120 - Compartición de un calendario privado de iCloud*

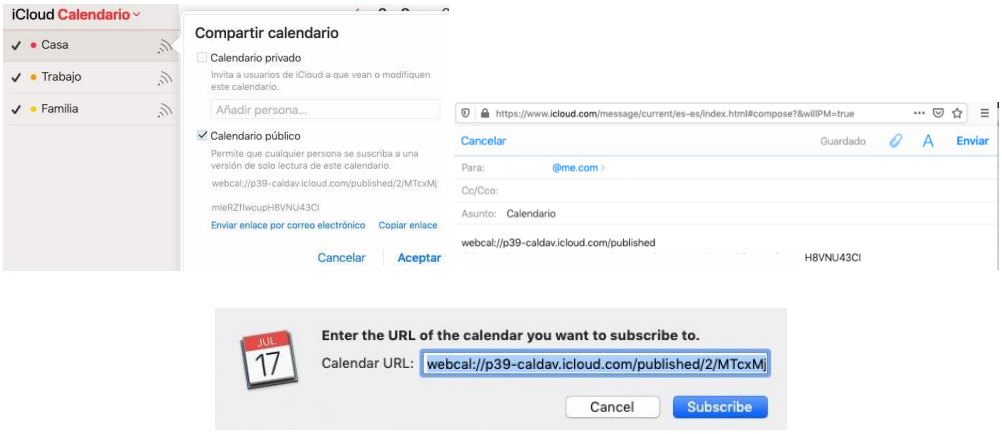



*Figura 121 - Compartición de un calendario público de iCloud*

La existencia del grupo "Familia" añade a iCloud un calendario compartido específico para los miembros del grupo (ver apartado "6.9.2.3. Calendario compartido con "Familia"").

## 11.6 ATAJOS

Recomendaciones de seguridad:

- Evitar la importación de atajos de iCloud que no procedan de fuentes fiables.
- Antes de importar un atajo obtenido de un tercero, revisar concienzudamente las acciones que ejecuta.

"Atajos" es una funcionalidad de automatización que Apple ha integrado en iOS 13 a nivel de sistema operativo, que permite, en base a elementos "disparador", iniciar una secuencia de acciones sin intervención (o con intervención parcial) por parte del usuario. La descripción exhaustiva de esta funcionalidad se describe en el apartado "Atajos (Shortcuts): Automatización en iOS 13" de la guía "Configuración segura de iOS 13" [Ref.- 413].

Para que los atajos creados en un dispositivo iOS estén disponibles en todos los dispositivos de este tipo, es preciso habilitar la opción "Ajustes - Atajos - Sincronizar con iCloud", "Sincronizar el orden" o ambas [Ref.- 59].

La compartición de atajos con otros usuarios se realiza desde la app "Atajos", seleccionando el atajo concreto y pinchando en el botón "". Se creará un enlace https://www.icloud.com/shortcuts/<identificador_del_atajo> accesible por todo aquel que lo conozca, independientemente del medio empleado para la compartición.

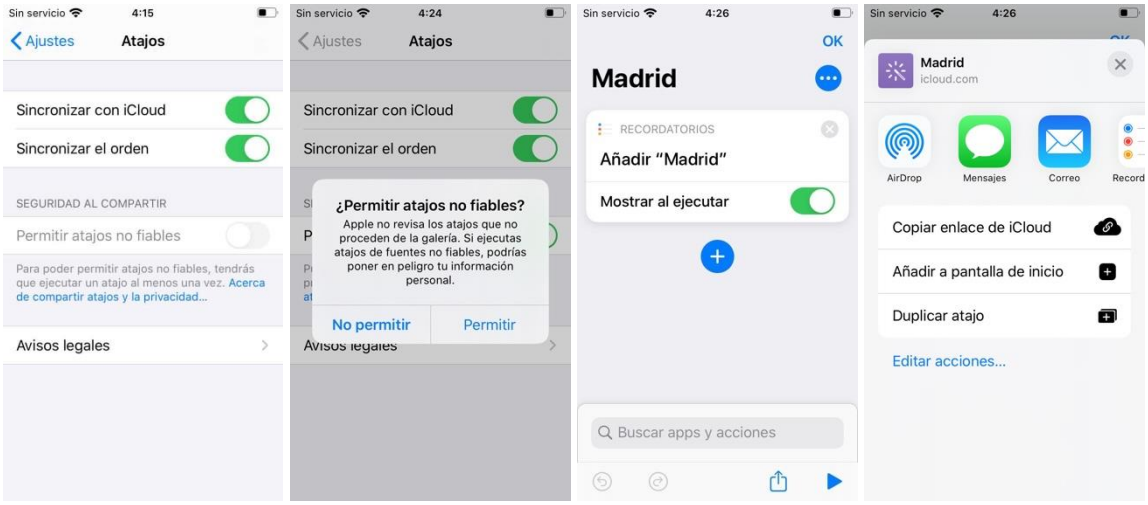



*Figura 122 - Sincronización de atajos con iCloud*

Es posible compartir los atajos creados en el propio dispositivo con otros usuarios de iCloud, e importar los que otros usuarios hayan compartido, mediante la opción "Permitir atajos no fiables" (que requiere la introducción del código de acceso del dispositivo). Dado que los atajos pueden ejecutar tareas y acceder a configuración sensible del dispositivo, ***se desaconseja su importación desde otras fuentes***[39], especialmente si no se dispone de conocimientos técnicos

[39] Existen diversos recursos en Internet que incluyen los enlaces a atajos que se han añadido a iCloud por parte de otros usuarios.

para la evaluación del comportamiento del atajo, o si no se tiene plena confianza en el creador del atajo.

En el dispositivo receptor de un atajo compartido, al accederse a su enlace, se abrirá la app "Atajos" solicitando confirmación del usuario para añadirlo a su repositorio local.

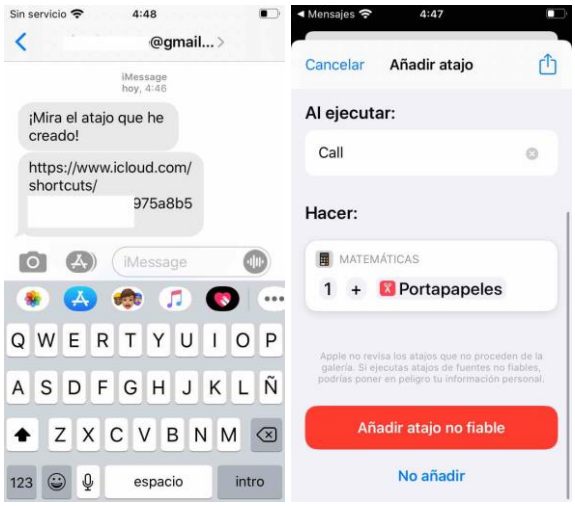



*Figura 123 - Importación de un atajo compartido por una fuente externa*

En el apartado "10.2. Atajos de Siri" se proporciona información sobre el uso de atajos por parte del asistente personal de Apple.

## 11.7 FOTOGRAFÍAS Y VÍDEOS

Recomendaciones de seguridad y privacidad:

- Asegurarse de que las fotografías y vídeos compartidos no contienen información de la ubicación en las que fueron tomados.
- Evitar el uso de álbumes compartidos de libre acceso.
- Evitar añadir elementos de contenido sensible a álbumes compartidos.
- Evitar etiquetar rostros de personas en las fotografías.

Apple ofrece el servicio de almacenamiento de fotografías y vídeos dentro del espacio de iCloud del usuario, permitiendo la sincronización de elementos en todos los dispositivos, tanto para la adición como para su edición y eliminación. El uso del servicio se habilita desde "Ajustes - ID de Apple - iCloud - Fotos en iCloud" (iOS) o su ajuste equivalente bajo "Preferencias del sistema" (macOS). Los archivos se guardan en iCloud con la resolución que fueron tomados, puesto que la opción "Optimizar almacenamiento" de iOS solo aplica a la reducción de tamaño de los archivos para minimizar el consumo de espacio en el propio dispositivo.

Con el servicio activo, las fotos y vídeos se sincronizarán con la nube de Apple cuando el dispositivo esté conectado a la corriente y a una red Wi-Fi (si el ajuste "Datos móviles - Fotos" está activo, la transferencia también podrá realizarse a través de una conexión de datos móvil. En función del plan de datos contratado con el operador de telefonía, el usuario deberá valorar la desactivación de este ajuste).

Si la app "Cámara" dispone de permisos de localización, iOS añadirá a la cabecera EXIF de los archivos de fotografías las coordenadas GPS correspondientes a la ubicación en la que fueron

obtenidas. Debido a la sensibilidad de esta información, se aconseja elegir la opción "No permitir" en el menú de solicitud de permiso que iOS mostrará la primera vez que se inicie la app "Cámara" y, en caso de haberse concedido previamente, inhabilitarlo mediante el interruptor "Ajustes - Privacidad - Localización - Cámara". La información de geolocalización de una fotografía no está disponible a través de la app "Fotos", pero sí lo está si la fotografía se copia a la app "Archivos" y, desde el menú contextual asociado a su fichero, se selecciona "Información - Mostrar más".

En caso de que una fotografía haya sido tomada con permisos de ubicación, la app "Fotos" dispone de una medida de preservación de la privacidad del usuario a través de su opción de compartición "Incluir - Ubicación", que se aconseja sea desactivado si se va a distribuir la foto en Internet (redes sociales, etc.).

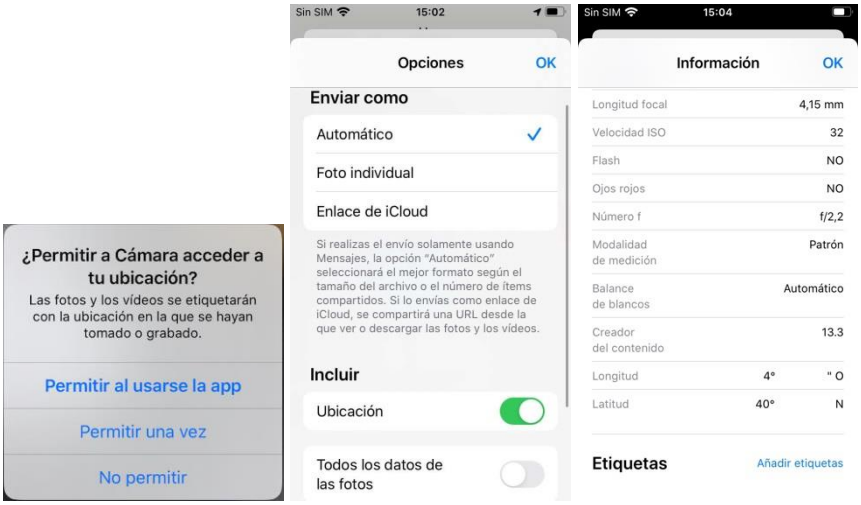



*Figura 124 - Permiso de ubicación "Cámara" y supresión de la información de localización del menú de compartición*

Como mecanismos de protección de los contenidos de fotografías, Apple afirma que los ficheros asociados a ellas se dividen en porciones que se cifran de forma individual con AES-128 y una clave derivada de los contenidos de cada porción, haciendo también uso de *hashes* SHA-256. Estas claves y los metadatos del fichero se almacenan en la cuenta de iCloud del usuario sin que exista ninguna vinculación con la identidad del usuario[40].

La app "Fotos" de macOS permite asignar palabras clave a las fotografías, que pueden ser utilizadas para buscar contenido concreto [Ref.- 65]. Se aconseja seleccionar términos que, aunque tengan sentido para el usuario, no revelen información sensible sobre el potencial contenido de las fotografías.

### 11.7.1 COMPARTICIÓN DE FOTOGRAFÍAS Y VÍDEOS

Además de la compartición aislada de elementos mediante el menú de compartición de la app "Fotos", el servicio de fotos de iCloud ofrece la posibilidad de compartir el contenido subido al almacenamiento del usuario de dos formas:

[40] https://support.apple.com/en-us/HT202303 (https://www.imore.com/icloud-photo-library-and-security-what-you-need-know)

- Álbumes compartidos: esta funcionalidad está orientada a la compartición permanente y bidireccional de fotografías y vídeos. El carácter de "compartido" se asigna a un álbum durante su creación desde el menú de "Fotos", no siendo posible transformar en álbum compartido un álbum que no se creó con esa condición. Desde el menú "Fotos Personas" disponible tras seleccionar un álbum compartido, se puede consultar qué usuarios están actualmente suscritos al álbum, añadir usuarios adicionales o revocar el acceso al álbum de un suscriptor concreto mediante la opción "Eliminar suscriptor", que se muestra pinchando sobre dicho usuario. La compartición puede ser:
  - Circunscrita a usuarios de iCloud: el propietario añade suscriptores que deben disponer de una cuenta de iCloud, y que recibirán una notificación para unirse al álbum. Un ejemplo particular de este uso es el álbum compartido que se crea de forma automática cuando se configura la funcionalidad "Familia" (ver apartado "6.9. Grupo "Familia"").
  - Pública: se crea un enlace al álbum de libre acceso. El uso de esta opción debe sopesarse cuidadosamente, evitando compartir cualquier contenido sensible a través de este medio, ya que, aunque el álbum se elimine pasado un tiempo, el propietario no tendrá control de la distribución que cualquier tercero pueda hacer de los elementos publicados.

**NOTA:** paradójicamente, los contenidos de álbumes compartidos no se contabilizan para el límite de almacenamiento de iCloud del propietario, sino que se limitan a 5.000 elementos, independientemente del tamaño que ocupen. Por el contrario, los contenidos de álbumes no compartidos están limitados por el espacio disponible para su propietario.

- Compartición puntual de contenido sugerido por Apple: la activación de "Fotos" en iCloud lleva implícita la creación de la sección "Sugerencias para compartir" dentro de la sección "Para ti" de la app "Fotos". Esta sección agrupa contenidos en base a la ubicación y la fecha en que fueron tomados, permitiendo su compartición mediante la app "Mensajes" con otros usuarios de iCloud, que, una vez reciban el enlace y añadan los contenidos a su fototeca, podrán a su vez compartir los que Apple haya identificado como relacionados con los recibidos. El uso detallado de este servicio queda fuera del ámbito de la presente guía, disponiéndose de información exhaustiva en la documentación oficial de Apple [Ref.- 23].




*Figura 125 - Uso de álbumes compartidos de iCloud*

### 11.7.2 ETIQUETADO DE PERSONAS EN "FOTOS"

Apple escanea las fotografías que incluyen rostros de personas para agruparlas dentro del álbum "Personas" de la app "Fotos", y puede sugerir (en base a la información obtenida de la app "Contactos"), nombres para asignar a un rostro concreto [Ref.- 64]. Esta funcionalidad no puede ser deshabilitada, aunque Apple afirma que el reconocimiento facial se realiza de forma local en el dispositivo y nunca se carga en los servidores de iCloud.

## 12. COPIAS DE SEGURIDAD Y RESTAURACIÓN EN ICLOUD

Recomendaciones de seguridad:

- Si se hace uso de almacenamiento de elementos en iCloud, se recomienda activar la copia de seguridad en iCloud para poder proceder a la recuperación de datos en caso necesario.
- Verificar de forma habitual que las copias de seguridad han sido exitosas.
- Comprobar el espacio libre en iCloud para que quede capacidad para albergar las copias.

iCloud ofrece un servicio de copias de seguridad para iPhone, iPad y iPod Touch, complementario a la funcionalidad de copia de seguridad en un ordenador propio a través de una conexión USB, que permite al usuario salvaguardar sus datos en la nube de Apple y, en caso necesario, proceder a restaurarlos. Desde el punto de vista de privacidad, aunque las copias están cifradas, se recomienda realizar copias de seguridad locales frente al uso de los servidores de Apple.

El espacio físico disponible para las copias de seguridad es el asociado a la cuenta de iCloud del usuario (en la actualidad, Apple proporciona 5GB de espacio de almacenamiento gratuito en iCloud, pudiendo ampliarse dicha capacidad mediante varias opciones de pago).

Estas copias no incluyen los datos que el usuario ya tenga almacenados en iCloud (entre otros, Contactos, Calendarios, Fotos de iCloud, iMessages, y mensajes SMS y MMS), que Apple custodia de forma independiente, ni los de otros servicios de la nube (como Microsoft One Drive). La lista completa de los elementos salvaguardados en la copia de iCloud está disponible en la [Ref.- 56]. El usuario dispone de otros mecanismos para salvaguardar los elementos que quedan fuera de las copias de seguridad de iCloud (y se recomienda emplearlos desde el punto de vista de seguridad), como se detallará en los siguientes subapartados.

La información de metadatos de los ficheros almacenados en iCloud, junto a las claves de cifrado, se almacenan por Apple en la cuenta de iCloud del usuario. Los contenidos de los ficheros son almacenados por Apple sin que se establezca ninguna vinculación con el usuario.

### 12.1 COPIA DE SEGURIDAD

Para activar esta funcionalidad, en iOS se dispone del menú "Ajustes - [ID de Apple] - iCloud - Copia en iCloud", desde el cual:

- El interruptor "Copia en iCloud" activa la copia de seguridad automática, que se iniciará cuando se den las condiciones descritas en dicho menú (ver <Figura 126>).
- Alternativamente, desde el botón "Realizar copia de seguridad ahora", el usuario puede iniciar un *backup* instantáneo si el dispositivo móvil se encuentra conectado a Internet mediante una red Wi-Fi.

- Este menú mostrará la información sobre la fecha de la última copia de seguridad exitosa.




*Figura 126 - Realización de copias de seguridad en iCloud desde iOS*

Las copias de seguridad de iCloud son de tipo incremental, es decir, solo se transfieren los datos que cambiaron desde la última copia realizada con éxito.

### 12.1.1 COPIA DE SEGURIDAD DE ARCHIVOS

Se recomienda mantener copias de respaldo en almacenamiento propio de los archivos importantes hospedados en iCloud, tanto ante posible indisponibilidad del servicio como de problemas con el acceso a Internet.

En macOS es posible copiar los archivos almacenados en iCloud a otra unidad (de disco interno, externo o de almacenamiento en red) utilizando la app "Finder", como para cualquier otro fichero.

En iOS, para poder realizar la copia de los archivos hospedados en iCloud Drive, es preciso abrir la app "Archivos" y seleccionar mediante una pulsación prolongada "*haptic touch*" el archivo o carpeta que se quiere salvar en otra ubicación. Desde el menú emergente, la opción "Copiar" permitirá hacer una copia del elemento y, mediante la navegación dentro de la propia app "Archivos", llegar hasta la ruta destino, para elegir "Pegar".

Complementariamente, el interfaz de iCloud Drive dispone de la opción "☁", para proceder a la descarga de los elementos que el usuario haya seleccionado.

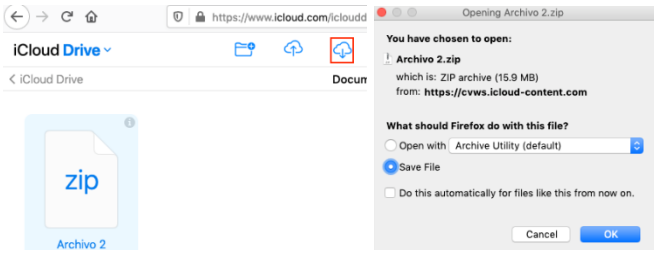



*Figura 127 - Salvaguarda de archivos de iCloud Drive*

### 12.1.2 COPIA DE SEGURIDAD DE CALENDARIOS

Para guardar una copia de respaldo de un calendario, es posible:

- Exportarlo en macOS desde el menú "Archivo - Exportar" de la app "Calendario". Se creará en la ubicación indicada por el usuario un fichero con extensión "`.ics`" que puede importarse posteriormente en cualquier aplicación que soporte el formato, incluidas las de Windows.
- Descargar el calendario directamente desde iCloud, siguiendo el proceso descrito en la documentación oficial de Apple de la [Ref.- 60].




*Figura 128 - Copia de seguridad local de un calendario*

### 12.1.3 COPIA DE SEGURIDAD DE RECORDATORIOS

Las diferentes listas que componen los recordatorios se pueden exportar utilizando macOS versión 10.14 Mojave o anterior. Para ello, tras seleccionar la lista concreta desde la app "Recordatorios", se utilizará la opción "Archivo - Exportar", proporcionando el nombre y la ubicación de la copia. En macOS 10.15 Catalina, el rediseño completo del servicio no incluye esta posibilidad.

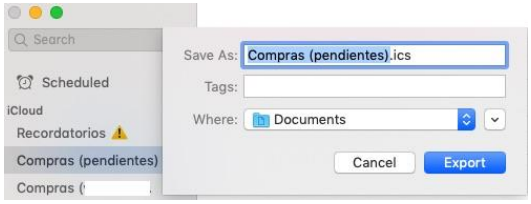



*Figura 129 - Copia de seguridad en fichero de una lista de recordatorios (macOS 10.14 Mojave)*

### 12.1.4 COPIA DE SEGURIDAD DE "FOTOS"

Se recomienda mantener copias de seguridad de los archivos de fotografías y vídeos, ya que no se incluyen en la copia de seguridad de iCloud. El proceso está completamente detallado en las secciones "Hacer una copia de seguridad de las fotos y los vídeos" y "Descargar tus fotos y vídeos" de la documentación oficial de Apple [Ref.- 62].

### 12.1.5 COPIA DE SEGURIDAD DE LOS MARCADORES DE SAFARI

Para poder obtener una copia de seguridad de los marcadores de Safari debe utilizarse macOS. Desde el menú de Safari "Archivo - Exportar marcadores..." es posible indicar la ubicación y el nombre del archivo de extensión "`.html`" que albergará la copia.

Desde el menú "Archivo - Importar desde - Archivo HTML de marcadores..." es posible restaurar una copia obtenida anteriormente.

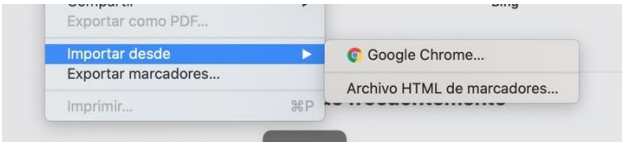



*Figura 130 - Exportación / Importación de marcadores en Safari desde macOS*

## 12.2 RESTAURACIÓN DE DATOS DESDE ICLOUD

Se contemplan dos tipos de restauración a partir de la información disponible en iCloud para el dispositivo:

- Completa: la copia de seguridad realizada según el procedimiento descrito en el apartado anterior puede ser restaurada en el dispositivo.
- Parcial: el interfaz web de iCloud dispone de capacidad para restaurar contactos, calendarios y los marcadores del navegador web Safari si el usuario sincroniza estos elementos en iCloud, mediante el interruptor correspondiente del apartado "Ajustes - ID de Apple - iCloud" (iOS) o "Preferencias del sistema - ID de Apple - iCloud" (macOS).
  Adicionalmente, es posible restaurar archivos eliminados recientemente de iCloud Drive.

### 12.2.1 RESTAURACIÓN COMPLETA DESDE COPIA DE SEGURIDAD EN iCLOUD

Para poder volcar en el dispositivo móvil una copia de seguridad desde iCloud, es preciso restablecerlo previamente a fábrica [Ref.- 57] (ver apartado "Eliminación de datos de usuario manteniendo la versión de iOS" de la guía "Configuración segura de iOS 13" [Ref.- 413]). Se recomienda realizar una copia de seguridad antes de proceder a la eliminación de los contenidos del iPhone.

Tras el reinicio, se lanzará el proceso de activación del dispositivo, en el que deberá establecerse conexión con una red Wi-Fi y seleccionar la opción "Restaurar con copia de iCloud". El proceso solicitará iniciar sesión utilizando el ID de Apple asociado a la cuenta de iCloud. Si la sesión se inicia correctamente, se mostrarán las copias disponibles, de entre las cuales se elegirá la deseada. El menú de restauración guiará al usuario durante el proceso.




*Figura 131 - Restauración completa en iOS desde copia de seguridad de iCloud*

### 12.2.2 RESTAURACIÓN DE ELEMENTOS INDIVIDUALES DE iCLOUD

Accediendo al menú "Ajustes de la cuenta - Avanzado" del interfaz web icloud.com es posible recuperar la información de contactos, calendarios, marcadores y ciertos archivos.

La opción "Restaurar archivos" permite recuperar archivos eliminados por parte de apps que guardan ficheros en iCloud. Los contenidos que el usuario almacene en su espacio de iCloud Drive y sean eliminados de dicha unidad, deben recuperarse desde el menú de "iCloud Drive".

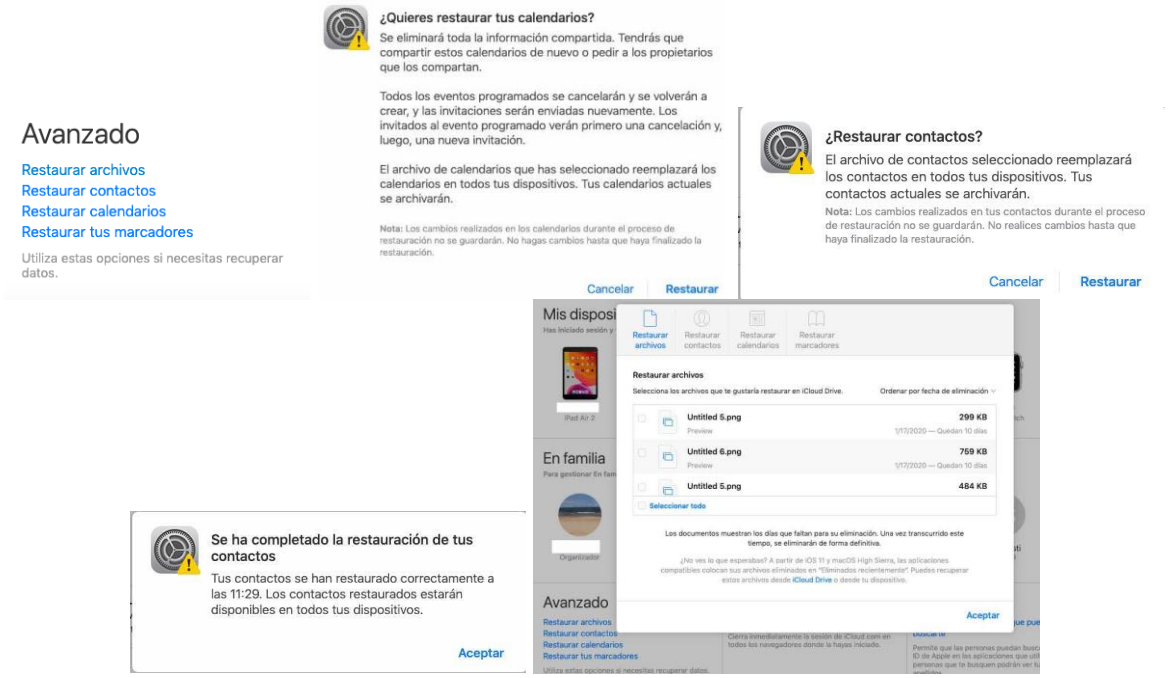



*Figura 132 - Restauración parcial desde iCloud.com*

### 12.2.2.1 Restauración de archivos de iCloud Drive

Los archivos que hayan sido eliminados de iCloud Drive en los últimos 30 días se encuentran disponibles para su restauración desde la sección de "iCloud Drive". En la parte inferior de la página web de dicha sección, se presenta el enlace "Eliminados recientemente (n)", donde "(n)" indica el número de archivos que se eliminaron de iCloud Drive en los 30 días anteriores al momento presente.

Al seleccionar "Eliminados recientemente (n)", aparecen los archivos disponibles para su restauración.

Complementariamente, la app "Archivos" de iOS también ofrece la sección "Recién eliminado", en la que se indica, para cada elemento, su procedencia (el propio dispositivo o el almacenamiento en iCloud Drive) y, bien desde la opción "Seleccionar - <marcar elementos> Recuperar", bien desde el menú "Recuperar" que se despliega con una pulsación "*haptic touch*" sobre un elemento, es posible restaurarlos de nuevo en iCloud Drive.




*Figura 133 - Restauración de ficheros de iCloud Drive desde el interfaz web de icloud.com*

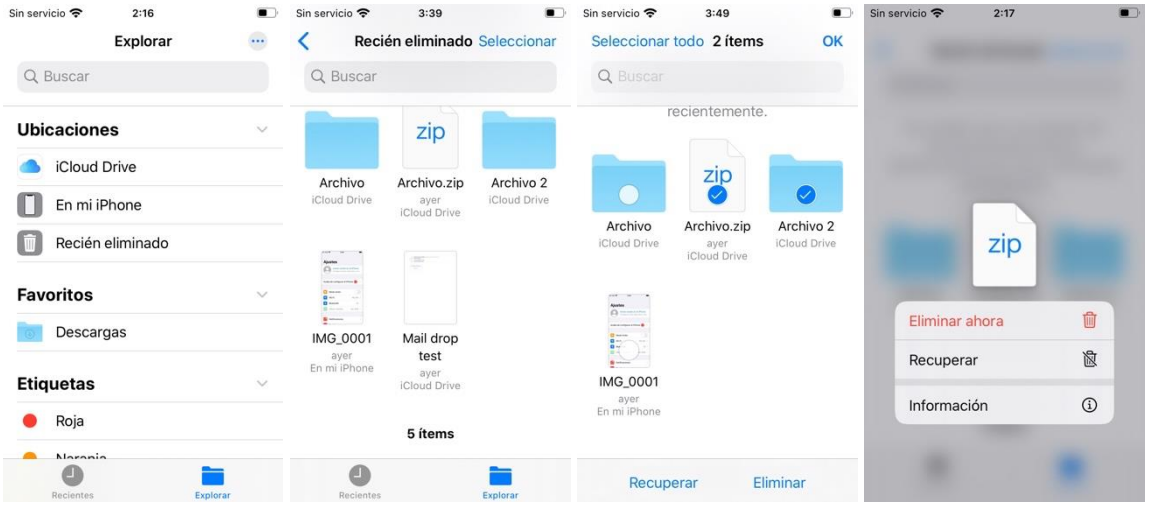



*Figura 134 - Restauración de ficheros de iCloud Drive desde la app "Archivos" de iOS 13*

# 13. RESUMEN DE LAS RECOMENDACIONES DE SEGURIDAD DE LOS SERVICIOS DE APPLE

| Decálogo de seguridad para el uso de los servicios de Apple | |
|---|---|
| 1 | Elegir una contraseña robusta para el ID de Apple, preferiblemente de tipo *passphrase*, que no coincida con la de ningún otro servicio ni código de acceso de ningún dispositivo u ordenador. |
| 2 | Habilitar el segundo factor de autentificación (2FA) para el ID de Apple, prestando especial atención a las alertas de seguridad que se recibirán en los dispositivos vinculados a la cuenta de usuario de Apple y en la dirección de correo electrónico correspondiente. |
| 3 | Hacer uso de "alias" para las cuentas de iMessage y FaceTime, a fin de preservar el ID de Apple y evitar que sea conocido por terceros. |
| 4 | Utilizar las capacidades de gestión remota del dispositivo vinculadas al servicio "Buscar" en caso de extravío o sustracción. Hacer uso del "Modo perdido" y, si se sospecha que no habrá posibilidad de recuperarlo, proceder a eliminar su contenido remotamente.<br>Asegurarse de que el modo "Encontrar sin conexión" se encuentra habilitado. |
| 5 | Evaluar el uso de servicios de continuidad y desactivar aquellos que no se utilicen. En todo caso, procurar realizar activaciones puntuales únicamente cuando estos servicios sean requeridos. |
| 6 | Habilitar AirDrop únicamente cuando se requiera hacer uso del servicio, y no utilizar nunca el modo de recepción "Todos". |
| 7 | Utilizar la ocultación del correo electrónico mediante el servicio "Sign-in with Apple" para evitar el seguimiento del usuario por parte de apps y servicios web de terceros. |
| 8 | Deshabilitar el uso de los servicios de localización para todas las apps que no proporcionen funcionalidad expresa de ubicación, incluidas las fotografías. Asimismo, deshabilitar el envío de información de ubicación a Apple a través de Siri, en caso de utilizarse este asistente digital personal. |
| 9 | Desactivar el uso de Siri en la pantalla de bloqueo, y revisar los ajustes de "Sugerencias de Siri y Buscar" para cada app individualmente, especialmente para las aplicaciones más delicadas, en caso de utilizarse este asistente digital personal. |
| 10 | No utilizar los servicios de compartición de contenidos de las apps vinculadas a iCloud en modo "público". Desactivar la compartición privada tan pronto deje de ser precisa. |

## 14. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:


| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 1] | "iOS 13". Apple.<br>URL: https://www.apple.com/ios/ios-13/ |
| [Ref.- 2] | "iPhone". Apple.<br>URL: https://www.apple.com/iphone/ |
| [Ref.- 3] | Comprar más almacenamiento en iCloud. Apple.<br>URL: https://support.apple.com/es-es/HT201318 |
| [Ref.- 4] | "Estado del sistema". Apple.<br>URL: https://www.apple.com/es/support/systemstatus/ |
| [Ref.- 5] | "Autenticación de doble factor para el ID de Apple". Apple.<br>URL: https://support.apple.com/es-es/HT204915 |
| [Ref.- 6] | "iCloud". Apple.<br>URL: https://www.apple.com/es/icloud/ |
| [Ref.- 7] | "Si has olvidado la contraseña de tu ID de Apple". Apple.<br>URL: https://support.apple.com/es-es/HT201487 |
| [Ref.- 8] | "Configurar Buscar mi iPhone". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmfc0f0c67/1.0/icloud/1.0 |
| [Ref.- 9] | "Comprobar la lista de dispositivos de tu ID de Apple para ver en cuáles has iniciado sesión". Apple. URL: https://support.apple.com/es-es/HT205064 |
| [Ref.- 10] | "Localizar un dispositivo con Buscar mi iPhone en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmfc0f2442/icloud<br>"Amigos y dispositivos. Encuéntralos aquí". Apple.<br>URL: https://www.apple.com/es/icloud/find-my/ |
| [Ref.- 11] | "Designing for Privacy". Apple WWDC 2019.<br>URL: https://developer.apple.com/videos/play/wwdc2019/708/?time=1919 |
| [Ref.- 12] | "Configurar y usar Buscar a mis amigos". Apple.<br>URL: https://support.apple.com/es-es/HT201493<br>"Configurar Buscar en el iPhone, en el Mac y en otros dispositivos". Apple.<br>URL: https://support.apple.com/es-es/HT210400 |
| [Ref.- 13] | "Find my iPhone: Borrar tu dispositivo". Apple.<br>URL: https://support.apple.com/kb/PH19300?locale=en_US&viewlocale=es_ES |
| [Ref.- 14] | "El ID de Apple y la privacidad". Apple.<br>URL: https://support.apple.com/es-es/HT208650 |
| [Ref.- 15] | "Cómo se utiliza Iniciar sesión con Apple". Apple.<br>URL: https://support.apple.com/es-es/HT210318 |
| [Ref.- 16] | "Ocultar mi Correo Electrónico en Iniciar sesión con Apple". Apple.<br>URL: https://support.apple.com/es-es/HT210425 |
| [Ref.- 17] | "What is "Sign In with Apple": Challenges and way Forward with WSO2 Identity Server". Junio 2019. Ishara Karunarathna. URL: https://medium.com/@isharaaruna/what-is-apple-sign-in-challenges-and-way-forward-with-wso2-identity-server-f1faa1b715cc |
| [Ref.- 18] | "Evitar que las aplicaciones muestren tu nombre". Manual del usuario de iCloud. Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmbffe88bb42/icloud |
| [Ref.- 19] | "Crear una dirección de correo electrónico en iCloud Mail". CCN-CERT. Mayo 2018.<br>URL: https://support.apple.com/es-es/guide/icloud/mmdd8d1c5c/1.0/icloud/1.0 |

| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 20] | "Bloqueo de activación para iPhone, iPad y iPod touch". Apple.<br>URL: https://support.apple.com/es-es/HT201365<br>"Acerca del Bloqueo de activación en tu Mac". Apple.<br>URL: https://support.apple.com/es-es/HT208987<br>"Acerca del Bloqueo de activación en el Apple Watch". Apple.<br>URL: https://support.apple.com/es-es/HT205009 |
| [Ref.- 21] | "Apple Platform Security". Otoño 2019. Apple.<br>URL: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf |
| [Ref.- 22] | "Bloqueo de activación en Buscar mi iPhone". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmb2460cabcf/icloud |
| [Ref.- 23] | "Usar Sugerencias para compartir en Fotos". Apple.<br>URL: https://support.apple.com/es-es/HT209035 |
| [Ref.- 24] | "Usar el modo Perdido en Buscar mi iPhone en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmfc0f0165/icloud |
| [Ref.- 25] | "Ocultar las compras de la App Store". Apple.<br>URL: https://support.apple.com/es-es/HT201322 |
| [Ref.- 26] | "¿Qué tipos de contenido puedo compartir con mi familia mediante las compras compartidas?". Apple. URL: https://support.apple.com/es-es/HT203046 |
| [Ref.- 27] | "Usar contraseñas específicas para apps". Apple.<br>URL: https://support.apple.com/es-es/HT204397 |
| [Ref.- 28] | "Ajustes de servidor de correo para clientes de correo electrónico de iCloud". Apple.<br>URL: https://support.apple.com/es-es/HT202304 |
| [Ref.- 29] | "Configurar en familia". Apple.<br>URL: https://support.apple.com/es-es/HT201088<br>"En familia". Apple.<br>URL: https://support.apple.com/es-es/HT201060 |
| [Ref.- 30] | "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Sep 2014 - Mar 2020. URL: https://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html |
| [Ref.- 31] | "Trasladar un niño o una niña a otro grupo con En Familia". Apple.<br>URL: https://support.apple.com/es-es/HT201080 |
| [Ref.- 32] | "Solicitar y hacer compras con Solicitar la compra". Apple.<br>URL: https://support.apple.com/es-es/HT201089 |
| [Ref.- 33] | "Borrar un dispositivo en Buscar mi iPhone en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmfc0ef36f/icloud |
| [Ref.- 34] | "Qué debes hacer antes de vender, regalar o renovar tu iPhone, iPad o iPod touch". Apple.<br>URL: https://support.apple.com/es-es/HT201351<br>"Qué hacer antes de vender, regalar o renovar tu Mac". Apple.<br>URL: https://support.apple.com/es-es/HT201065 |
| [Ref.- 35] | "Usar Continuidad para conectar tu Mac, iPhone, iPad, iPod touch y Apple Watch". Apple.<br>URL: https://support.apple.com/es-es/HT204681 |
| [Ref.- 36] | "Requisitos de sistema de Mac, iPhone, iPad, iPod touch y Apple Watch para el uso de las funciones de Continuidad". Apple. URL: https://support.apple.com/es-es/HT204689 |
| [Ref.- 37] | "APNs Overview". Apple developers. URL: https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html#//apple_ref/doc/uid/TP40008194-CH8-SW1 |
| [Ref.- 38] | "Información general sobre la seguridad de iCloud". Apple.<br>URL: https://support.apple.com/es-es/HT202303 |
| [Ref.- 39] | "Usar alias de correo electrónico en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mm6b1a490a/icloud |
| [Ref.- 40] | "Usar mensajes en iCloud en el Mac". Apple.<br>URL: https://support.apple.com/es-es/guide/messages/icht5b5d1e63/13.0/mac/10.15 |

| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 41] | "Usar Continuidad de cámara en el Mac". Apple.<br>URL: https://support.apple.com/es-es/HT209037 |
| [Ref.- 42] | "Cómo desbloquear un Mac con el Apple Watch". Apple.<br>URL: https://support.apple.com/es-es/HT206995 |
| [Ref.- 43] | "Utilizar el iPad, iPhone o iPod touch para dibujar o marcar documentos del Mac". Apple.<br>URL: https://support.apple.com/es-es/HT204975#sketch |
| [Ref.- 44] | "A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link". Technical University of Darmstadt & Northeastern University. Aug 2019.<br>URL: https://www.usenix.org/conference/usenixsecurity19/presentation/stute<br>URL: https://news.northeastern.edu/2019/08/19/airdrop-is-making-your-iphone-vulnerable-to-attackers/ |
| [Ref.- 45] | Bonjour Overview. Apple Developers. URL: https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Articles/domainnames.html#//apple_ref/doc/uid/TP40002460-SW1 |
| [Ref.- 46] | Zero Configuration Networking.<br>URL: http://www.zeroconf.org |
| [Ref.- 47] | "Obtener ayuda para usar el llavero de iCloud". Apple.<br>URL: https://support.apple.com/es-es/HT203783 |
| [Ref.- 48] | "Configurar Apple Pay en Wallet en el iPhone". Apple.<br>URL: https://support.apple.com/es-es/guide/iphone/iph9b7f53382/ios |
| [Ref.- 49] | "Descripción general de la seguridad y la privacidad de Apple Pay". Apple.<br>URL: https://support.apple.com/es-es/HT203027 |
| [Ref.- 50] | "Prepararse para la nueva app Recordatorios". Apple.<br>URL: https://support.apple.com/es-es/HT210220 |
| [Ref.- 51] | "Utilizar Recordatorios en el iPhone, el iPad o el iPod touch". Apple.<br>URL: https://support.apple.com/es-es/HT205890#share |
| [Ref.- 52] | "Manual del usuario de iCloud". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmc0cd794a/1.0/icloud/1.0 |
| [Ref.- 53] | "Añadir o eliminar cuentas de Notas en el Mac". Apple.<br>URL: https://support.apple.com/es-es/guide/notes/not85d6f7b58/mac |
| [Ref.- 54] | "Añadir archivos adjuntos a correos electrónicos en Mail en el Mac". Apple.<br>URL: https://support.apple.com/es-es/guide/mail/mlhlp1050/mac<br>"Límites de Mail Drop". Apple.<br>URL: https://support.apple.com/es-es/HT203093 |
| [Ref.- 55] | "Añadir un archivo adjunto de correo electrónico en Mail en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mm6b1a7a10/icloud |
| [Ref.- 56] | "¿De qué hace copias de seguridad iCloud?". Apple.<br>URL: https://support.apple.com/es-es/HT207428 |
| [Ref.- 57] | "Restaurar el iPhone, iPad o iPod touch desde una copia de seguridad". Apple.<br>URL: https://support.apple.com/es-es/HT204184#icloud |
| [Ref.- 58] | "Recuperar archivos eliminados en iCloud.com". Apple.<br>URL: https://support.apple.com/es-es/guide/icloud/mmae56ea1ca5/icloud |
| [Ref.- 59] | "Sincronizar atajos". Apple. URL: https://support.apple.com/es-es/guide/shortcuts/apdb3a4240b0/3.2/ios/13.2#apd2618c521f |
| [Ref.- 60] | "Archivar o realizar copias de la información que guardas en iCloud". Apple.<br>URL: https://support.apple.com/es-es/HT204055 |
| [Ref.- 61] | "Manual del usuario de Recordatorios". Apple.<br>URL: https://support.apple.com/es-es/guide/reminders/remnda262a43/mac |
| [Ref.- 62] | "Cómo configurar y usar Fotos de iCloud". Apple.<br>URL: https://support.apple.com/es-es/HT204264 |
| [Ref.- 63] | "Usar Álbumes compartidos en Fotos". Apple.<br>URL: https://support.apple.com/es-es/HT202786 |

| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 64] | "Acerca de las personas en Fotos del iPhone, iPad o iPod touch". Apple. URL: https://support.apple.com/es-es/HT207103 "Buscar e identificar fotos de personas con Fotos en el Mac". Apple. URL: https://support.apple.com/es-es/guide/photos/phtad9d981ab/mac |
| [Ref.- 65] | "Buscar fotos por palabra clave en Fotos en el Mac". Apple. URL: https://support.apple.com/es-es/guide/photos/pht8d0ad5198/5.0/mac/10.15 |
| [Ref.- 66] | "Siri". Apple. URL: https://www.apple.com/es/siri/ |
| [Ref.- 67] | "Sugerencias de Siri, Buscar y la privacidad". Apple. URL: https://support.apple.com/es-es/HT210658 |
| [Ref.- 68] | "Acerca de las sugerencias de Siri en el iPhone". Apple. URL: https://support.apple.com/es-es/guide/iphone/iph6f94af287/ios |
| [Ref.- 69] | "Usar atajos de Siri". Apple. URL: https://support.apple.com/es-es/HT209055 |
| [Ref.- 70] | "Gestionar la actividad y las tarjetas Apple Pay en el iPhone". Apple. URL: https://support.apple.com/es-es/guide/iphone/iph7b666943a/ios |
| [Ref.- 71] | "Adopting Handoff". Handoff programming guide. Apple developers. URL: https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/Handoff/AdoptingHandoff/AdoptingHandoff.html#//apple_ref/doc/uid/TP40014338-CH2-SW21 |


La siguiente tabla muestra las referencias documentales asociadas directamente a las publicaciones del CCN-CERT:


| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 400] | "Guía CCN-STIC-450: Seguridad de dispositivos móviles". CCN-CERT. Marzo 2013. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html |
| [Ref.- 401] | "CCN-STIC-457: Gestión de dispositivos móviles: MDM (Mobile Device Management)". CCN-CERT. Noviembre 2013. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-de-dispositivos-moviles-mdm/file.html |
| [Ref.- 402] | "CCN-CERT BP-03/16. Buenas Prácticas: Dispositivos móviles". CCN-CERT. Octubre 2016. URL: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html |
| [Ref.- 403] | "Guía CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x". CCN-CERT. Junio 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2901-ccn-stic-453d-seguridad-de-dispositivos-moviles-android-6-x/file.html |
| [Ref.- 404] | "Guía CCN-STIC-453E: Seguridad de dispositivos móviles: Android 7.x". CCN-CERT. Septiembre 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3040-ccn-stic-453e-seguridad-de-dispositivos-moviles-android-7-x.html |
| [Ref.- 405] | "CCN-STIC-456: Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android". CCN-CERT. Septiembre 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3043-ccn-stic-456-cuenta-de-usuario-servicios-aplicaciones-google-para-dispositivos-moviles-android/file.html |
| [Ref.- 406] | "Guía CCN-STIC-454: Seguridad en iPad". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/12-ccn-stic-454-seguridad-en-ipad.html |

| Referencia | Título, autor y ubicación |
|---|---|
| [Ref.- 407] | "Guía CCN-STIC-455: Seguridad en iPhone". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/13-ccn-stic-455-seguridad-en-iphone.html |
| [Ref.- 408] | "CCN-STIC-455C: Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 11.x)". CCN-CERT. Octubre 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3161-ccn-stic-455c-guia-practica-de-seguridad-en-dispositivos-moviles-iphone-ios-11x-1/file.html |
| [Ref.- 409] | "CCN-STIC-455D: Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 12.x)". CCN-CERT. Octubre 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12/file.html |
| [Ref.- 410] | "CCN-STIC-453F: Guía práctica de seguridad en dispositivos móviles Android 8". CCN-CERT. Marzo 2019. URL: https://www.ccn-cert.cni.es/gl/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3579-ccn-stic-453f-guia-practica-de-seguridad-en-dispositvos-moviles-android-8/file.html |
| [Ref.- 411] | "CCN-STIC-453G: Guía práctica de seguridad en dispositivos móviles Android 9". CCN-CERT. Marzo 2019. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3588-ccn-stic-453g-guia-practica-de-seguridad-en-dispositvos-moviles-android-9/file.html |
| [Ref.- 412] | "CCN-STIC-458: Guía práctica de seguridad de macOS 10.14 Mojave". CCN-CERT. Julio 2019. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3845-ccn-stic-458-seguridad-macos-mojave/file.html |
| [Ref.- 413] | "CCN-STIC-455E: Configuración segura de iOS 13". CCN-CERT. Febrero 2020. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/4569-ccn-stic-455e-configuracion-segura-de-ios-13.html |
| [Ref.- 414] | "CCN-CERT IA-03/20: Informe de amenazas: Dispositivos y comunicaciones móviles". CCN-CERT. Marzo 2020. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html |