

Guía de Seguridad de las TIC CCN-STIC 455E

Guía práctica de seguridad en dispositivos móviles iOS 13



Febrero 2020

Edita:



© Centro Criptológico Nacional, 2020
NIPO: 083-20-057-0

Fecha de Edición: Febrero de 2020

Mónica Salas y Raúl Siles (DinoSec) han colaborado en la elaboración de la presente guía.

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.....	6
2. INTRODUCCIÓN	7
3. OBJETO.....	7
4. ENTORNO DE APLICACIÓN DE ESTA GUÍA.....	8
5. IOS 13.....	8
6. DISPOSITIVO MÓVIL EMPLEADO.....	11
7. PROCESO DE ACTIVACIÓN DEL DISPOSITIVO MÓVIL.....	11
7.1 ESTADO DEL DISPOSITIVO TRAS LA ACTIVACIÓN INICIAL.....	17
8. ACCESO FÍSICO AL DISPOSITIVO MÓVIL.....	18
8.1 PROTECCIÓN DE ACCESO AL DISPOSITIVO.....	18
8.1.1 CÓDIGO DE ACCESO A LA TARJETA SIM	19
8.1.2 MÉTODO DE BLOQUEO DEL DISPOSITIVO MÓVIL.....	20
8.2 MEDICAL ID (EMERGENCIA SOS).....	26
8.2.1 APP "SALUD".....	28
8.3 AJUSTES ADICIONALES DE "TOUCH ID Y CÓDIGO"	28
8.4 ACCESOS RESTRINGIDOS AL DISPOSITIVO	29
9. PANTALLA DE INICIO ("HOME")	29
9.1 BARRA SUPERIOR DE ESTADO	30
9.2 CENTRO DE CONTROL	31
9.2.1 PERSONALIZACIÓN DEL CENTRO DE CONTROL.....	33
9.3 BÚSQUEDA MEDIANTE TEXTO Y VOZ.....	34
9.3.1 FUNCIÓN DICTADO.....	36
9.4 TODAY VIEW (VISTA DE HOY).....	37
9.4.1 ATAJOS (SHORTCUTS): AUTOMATIZACIÓN EN IOS 13	38
9.5 CENTRO DE NOTIFICACIONES	42
9.6 MODO "NO MOLESTAR"	44
9.7 MENÚS CONTEXTUALES.....	45
10. CONFIGURACIÓN DEL DISPOSITIVO MÓVIL: MENÚ "AJUSTES"	46
11. CUENTAS ASOCIADAS AL DISPOSITIVO MÓVIL	49
11.1 ID DE APPLE	49
11.1.1 INICIAR SESIÓN CON APPLE.....	50
11.2 CUENTA DE ICLOUD	50
11.3 CUENTA DE ITUNES & APP STORE.....	50
11.4 SECCIÓN "CONTRASEÑAS Y CUENTAS"	52
11.4.1 CUENTAS.....	52
11.5 DISPOSITIVOS ASOCIADOS A LA CUENTA	53
12. COMUNICACIONES DEL DISPOSITIVO MÓVIL	53
12.1 CONEXIONES INALÁMBRICAS Y REDES	53
12.1.1 MODO AVIÓN	53
12.1.2 BLUETOOTH.....	54
12.1.3 WI-FI	58
12.1.4 VOZ Y DATOS MÓVILES	64

12.1.5 PERSONAL HOTSPOT	68
12.2 COMUNICACIONES TCP/IP	70
12.3 COMUNICACIONES USB	71
12.3.1 PROCESO DE EMPAREJAMIENTO	71
12.3.2 MODO RESTRINGIDO USB	72
12.4 VPN	73
13. SERVICIOS PROPIETARIOS DE APPLE	75
13.1 AIRDROP	75
13.1.1 MECANISMO DE FUNCIONAMIENTO DE AIRDROP	76
13.1.2 USO DE AIRDROP	77
13.2 AIRPLAY	80
13.3 COMPARTIR	80
13.3.1 PANEL DE COMPARTICIÓN	80
14. SERVICIOS DE LOCALIZACIÓN	82
14.1 PERMISOS DE LOCALIZACIÓN DE LAS APPS	83
14.2 PERMISOS DE LOCALIZACIÓN PARA SERVICIOS DEL SISTEMA	84
14.2.1 SERVICIO "COMPARTIR MI UBICACIÓN"	85
14.2.2 PERMISO DE LOCALIZACIÓN EN FOTOGRAFÍAS	85
15. GESTIÓN DE CONTRASEÑAS	86
15.1 LLAVEROS - KEYCHAIN	87
15.2 GESTIÓN DE LOS ELEMENTOS DEL LLAVERO	87
15.3 LLAVERO DE ICLOUD	89
15.3.1 GENERACIÓN AUTOMÁTICA DE CONTRASEÑAS	90
15.4 AUTORRELLENAR CONTRASEÑAS	90
15.4.1 RELLENO AUTOMÁTICO DE CÓDIGOS DE SEGURIDAD RECIBIDOS POR SMS ..	92
16. NAVEGADOR WEB MOBILE SAFARI	93
16.1 NUEVAS FUNCIONALIDADES DE IOS 13 PARA SAFARI	93
16.1.1 INTERFAZ DE USUARIO DE SAFARI	94
16.1.2 AJUSTES DE PRIVACIDAD SELECTIVOS	95
16.1.3 GESTOR DE DESCARGAS	95
16.2 AJUSTES DE SAFARI	96
17. CERTIFICADOS DIGITALES	97
17.1 CERTIFICADOS RAÍZ	98
17.2 CERTIFICADOS CLIENTE	99
17.3 INSTALACIÓN DE CERTIFICADOS TRANSFERIDOS VÍA AIRDROP	100
17.4 GESTIÓN DE CERTIFICADOS EN MOBILE SAFARI	101
18. GESTIÓN DE LAS APPS	103
18.1 ACTUALIZACIÓN Y ELIMINACIÓN DE APPS	104
18.2 APPS RELEVANTES DESDE EL PUNTO DE VISTA DE SEGURIDAD	105
18.2.1 APP "ARCHIVOS"	105
18.2.2 APP "NOTAS"	107
18.3 AJUSTES DE PRIVACIDAD: PERMISOS DE LAS APPS	111
18.4 TIEMPO DE USO	112
18.4.1 CÓDIGO DE ACCESO PARA "TIEMPO DE USO"	113
18.4.2 RESTRICCIONES	114

18.5 ACCESO GUIADO	116
19. CIFRADO DEL DISPOSITIVO MÓVIL.....	117
20. COPIAS DE SEGURIDAD Y RESTAURACIÓN.....	118
20.1 COPIA DE SEGURIDAD EN UN ORDENADOR	118
20.2 RESTAURACIÓN DEL DISPOSITIVO DESDE UNA COPIA DE SEGURIDAD	119
20.3 ACTUALIZACIÓN VÍA WI-FI	120
20.4 ACTUALIZACIÓN MEDIANTE CONEXIÓN A UN ORDENADOR.....	122
21. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL.....	122
21.1 ELIMINACIÓN DE DATOS DE USUARIO MANTENIENDO LA VERSIÓN DE IOS	123
21.2 RESTABLECIMIENTO DE LOS AJUSTES DEL DISPOSITIVO A LOS AJUSTES DE FÁBRICA	124
21.3 PROCEDIMIENTO PARA ELIMINAR LOS DATOS DE UN DISPOSITIVO DEL QUE YA NO SE DISPONE	124
22. RESUMEN DE RECOMENDACIONES DE SEGURIDAD DE IOS 13.....	125
23. ANEXO A - CUENTA DE ICLOUD	126
23.1 GESTIÓN DE LA CUENTA DE ICLOUD	126
23.1.1 INTERFAZ WEB.....	126
23.1.2 INTERFAZ MÓVIL	127
23.2 USO DEL ALMACENAMIENTO EN ICLOUD POR APPS DE TERCEROS.....	128
23.3 SERVICIOS "BUSCAR" PARA LOCALIZACIÓN DE DISPOSITIVOS	129
23.3.1 TAREAS DE GESTIÓN REMOTA EN IOS	130
24. REFERENCIAS	133

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

La actual utilización de dispositivos móviles y sus múltiples servicios asociados, tanto en el plano profesional como personal, unida al constante incremento en el número y tipo de amenazas que recaen sobre ellos, requiere poner en marcha todos los mecanismos disponibles para garantizar la protección de la información que se transfiere y almacena en estos dispositivos, cada vez mayor y más sensible.

Se considera dispositivo móvil aquel dispositivo electrónico de uso personal o profesional, de reducido tamaño que permite la gestión de información (almacenamiento, intercambio y procesamiento de información) y el acceso a redes de comunicaciones y servicios remotos, tanto de voz como de datos, y que, habitualmente, dispone de capacidades de telefonía: teléfonos móviles, *smartphones*, *tablets* y agendas electrónicas (PDAs, *Personal Digital Assistants*), independientemente de si disponen de teclado físico o pantalla táctil.

La concienciación, el sentido común y las buenas prácticas en la configuración y el uso de los dispositivos móviles constituyen una de las mejores defensas para prevenir y detectar este tipo de incidentes y amenazas de seguridad [Ref.- 402].

3. OBJETO

El propósito del presente documento es realizar un análisis general de los mecanismos y la configuración de seguridad destinado a proporcionar una lista de recomendaciones de seguridad para la protección de los datos, comunicaciones e información que almacenan los dispositivos móviles basados en el sistema operativo iOS versión 13.x de Apple®, liberada en septiembre de 2019, y disponible para dispositivos móviles iPhone y iPod Touch listados en la [Ref.- 1], con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

El presente informe 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 basados en iOS 13.x en la actualidad, y se ha redactado considerando como requisito el equilibrio entre seguridad y funcionalidad de los dispositivos móviles a proteger.

Adicionalmente, se recomienda la lectura de las guías CCN-CERT asociadas a otros sistemas operativos y versiones de plataformas móviles, en caso de ser necesaria su aplicación en otros terminales, y a la gestión empresarial de dispositivos móviles (MDM):

- CCN-CERT BP-03/16 - Buenas Prácticas. Dispositivos móviles [Ref.- 402]
- CCN-STIC-450 - Seguridad de dispositivos móviles [Ref.- 400]
- CCN-STIC-454(A) - Seguridad de dispositivos móviles: iPad (iOS 7.x) [Ref.- 406]
- CCN-STIC-455(A) - Seguridad de dispositivos móviles: iPhone (iOS 7.x) [Ref.- 407]
- 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-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management) [Ref.- 401]
- CCN-STIC-458 - Guía práctica de seguridad de macOS 10.14 Mojave [Ref.- 412]
- CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x [Ref.- 403]
- CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x [Ref.- 404]
- CCN-STIC-453F - Guía práctica de seguridad en dispositivos móviles Android 8 [Ref.- 410]
- CCN-STIC-453G - Guía práctica de seguridad en dispositivos móviles Android 9 [Ref.- 411]

- CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android [Ref.- 405]

4. ENTORNO DE APLICACIÓN DE ESTA GUÍA

El iPhone es un dispositivo móvil de tipo *smartphone* con pantalla táctil capacitiva que ejecuta el sistema operativo iOS, diseñado y fabricado por Apple; proporciona capacidades de telefonía móvil, además de acceso a redes de datos como Internet. La primera versión o generación del iPhone (2G) se distribuyó en EEUU en junio de 2007, comercializándose desde entonces y hasta la fecha, posteriores generaciones del iPhone cada año.

Las principales diferencias entre las distintas generaciones de iPhone residen fundamentalmente en el tipo de *hardware* disponible, la funcionalidad proporcionada por el mismo y las mejoras de la versión de iOS asociada. Entre otras características *hardware*, los modelos más recientes ya cuentan con pantalla Retina, GPS y servicios de geolocalización, múltiples sensores (brújula digital, acelerómetro, giroscopio, barómetro, etc., varias cámaras (traseras y frontales)), chip A13 Bionic, capacidades Wi-Fi multi-frecuencia en 2,4 y 5 GHz (802.11a/b/g/n/ac/ax), soporte de telefonía móvil o celular 4G/LTE empleando una tarjeta nano SIM, VoLTE, soporte para Bluetooth 5.x, tecnología "Touch ID" (un lector biométrico de huella dactilar descrito en el apartado "8.1.2.2. Touch ID"), tecnología "Face ID" (un sistema de autenticación biométrica mediante reconocimiento facial que ha sido integrado en la cámara frontal del dispositivo móvil; ver apartado "8.1.2.3. Face ID"), conector *Lightning*, capacidades de carga inalámbrica y módulo NFC, entre otros.

iOS 13.x, a diferencia de su predecesor, iOS 12.x, no está soportado en dispositivos móviles iPad de tipo tableta, para los cuales Apple ha desarrollado en paralelo el sistema operativo iPadOS¹ (fuera del alcance de la presente guía), diferenciando por primera vez el sistema operativo de dispositivos móviles iPhone y iPad. El principal objetivo de Apple independizándolos es transformar el iPad en una alternativa a los portátiles, con un enfoque más profesional.

iOS 13.x está soportado en el iPhone SE, 6S y modelos superiores, quedando sin soporte el iPhone 5S, 6 y 6 Plus.

5. IOS 13

iOS (originalmente conocido como *iPhone Operating System*) es un sistema operativo Unix propietario de Apple, basado en Darwin BSD y heredado de macOS (anteriormente OS X), diseñado para dispositivos móviles.

Las nuevas versiones de iOS suelen acompañar al lanzamiento comercial de las nuevas versiones hardware de los dispositivos de Apple (normalmente del iPhone, liberándose nuevas subversiones de iOS, ahora de iPadOS, en el caso de nuevas versiones hardware del iPad). Así, la versión iOS 1.0 acompañó a la primera generación de iPhone (2G) en junio de 2007, mientras que la versión iOS 13.0 se liberó en septiembre de 2019 junto a los iPhone 11 Pro, 11 Max y 11.

¹ <https://www.apple.com/ipados/>

A fecha de elaboración de la presente guía (enero de 2020), la tasa de adopción de iOS 13 en dispositivos móviles de Apple es del 77%².

NOTA: Apple libera subversiones de sus sistemas operativos bajo soporte cada cierto tiempo, tanto para resolver fallos detectados como para añadir funcionalidades nuevas. Estas subversiones pueden contener soluciones a problemas de seguridad encontrados, los cuales se identifican mediante un "CVE"³. Los detalles sobre las vulnerabilidades solucionadas por una actualización concreta se proporcionan en la entrada de la tabla de la [Ref.- 30] correspondiente al sistema operativo en cuestión. Las correspondientes a iOS 13.3 (versión empleada en la elaboración de la presente guía) pueden consultarse en la [Ref.- 4].

Las principales funcionalidades introducidas por iOS 13 [Ref.- 29] son:

- Modo oscuro, que introduce un fondo negro tanto al sistema operativo como a las apps, pensado para entornos con escasa luminosidad, y cuya activación puede iniciarse desde el "Centro de Control".
- Rediseño de las apps "Fotos" y "Mapas", que incorporan nuevas prestaciones.
- Opciones de automatización basadas en la funcionalidad "Atajos" (ver apartado "9.4.1. Atajos (Shortcuts): automatización en iOS 13").
- Nuevas opciones en la app "Salud", incluyendo "Ciclos", una funcionalidad específica de "Salud menstrual", que se integra con watchOS 6.x.
- Se agiliza el tiempo de inicio de las apps (ver apartado "18. Gestión de las apps").
- Se permite enlazar dos pares de AirPods a un mismo iPhone y escuchar en ambas parejas de auriculares el mismo audio.
- Se incorpora la funcionalidad "QuickPath", que ofrece escritura predictiva sin levantar el dedo del teclado basada en técnicas de aprendizaje automático.
- Se añade la app "Recordatorios", que permite añadir avisos desde la barra de herramientas, y que se integra con iCloud para compartición de recordatorios entre dispositivos vinculados a la misma cuenta.
- La funcionalidad "Control por Voz" permite acceder a los servicios del iPhone con comandos de voz y gestos.
- Optimización de carga de la batería: para disminuir el deterioro de la batería, se reduce el tiempo en el que el iPhone se carga por encima del 80%. Para ello se analiza la rutina de carga mediante técnicas de aprendizaje automático.
- Posibilidad de añadir adjuntos a eventos de calendario.
- La opción "No molestar al conducir" detecta si se está viajando en transporte público y no se activa en tal caso.
- Se añade la funcionalidad "Inscripción de Usuario" para gestión de dispositivos de uso empresarial, cuyo objeto es independizar el uso del dispositivo separando los datos personales de los profesionales. Esta funcionalidad queda fuera del ámbito de la presente guía, pero puede consultarse la [Ref.- 59] para obtener más información.
- Se permite elegir el idioma de cada app de forma independiente del idioma del sistema.
- Modo de "Datos Reducidos" permite reducir el consumo de datos de las apps.
- Se incorporan los denominados "Menús contextuales" (ver apartado "9.7. Menús contextuales").

² <https://developer.apple.com/support/app-store/>

³ <http://cve.mitre.org/about/>

- El mecanismo "3D Touch" (solo disponible para dispositivos con *hardware* específico) se sustituye por "*Haptic Touch*" en todos los dispositivos⁴ (ver apartado "9.7. Menús contextuales").
- Características relevantes desde el punto de vista de la seguridad y/o privacidad:
 - Se proporciona al usuario un sistema de control más granular sobre los permisos y datos de localización (ver apartado "14. Servicios de localización").
 - Los nuevos controles de las API evitan que las apps puedan acceder a la ubicación mediante Wi-Fi o Bluetooth sin consentimiento del usuario.
 - Se incorpora la funcionalidad "Iniciar sesión con ID de Apple" para sitios webs y apps (ver apartado "11.1.1. Iniciar sesión con Apple").
 - Se incorporan prestaciones de "transparencia" para evitar actividades de rastreo sin consentimiento del usuario, como el permiso de Bluetooth (ver apartado "12.1.2. Bluetooth").
 - Se incorpora la funcionalidad "Acceso guiado", que permite fijar la pantalla de una app para que la sesión del usuario se limite al uso de dicha app (ver apartado "18.5. Acceso guiado").
 - Se añaden controles de localización para la compartición de fotos (ver apartado "14.2.2. Permiso de localización en fotografías").
 - Inclusión de nuevos controles en el "Centro de Control" para edición de Notas (ver apartado "9.2. Centro de Control").
 - La app "Notas" incorpora una funcionalidad de "carpetas compartidas" para su uso por parte de diferentes personas. Se permite definir colaboración de solo lectura (ver apartado "18.2.2. App "Notas"").
 - Nuevas funcionalidades de la app "Archivos" (ver apartado "18.2.1. App "Archivos""), tanto para almacenamiento local como en iCloud Drive.
 - Funcionalidad "Buscar":
 - "Buscar a mis Amigos" se combina con la tradicional "Buscar mi iPhone", dando lugar a una sola app "Buscar".
 - Se añade la funcionalidad "Búsqueda de dispositivos sin conexión", que permite la localización de dispositivos sin conexión de datos a través de la detección de su señal Bluetooth por parte de otros dispositivos Apple que entran en su radio de cercanía. Esta funcionalidad se describe en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413].
 - La app "Teléfono" incorpora un ajuste para silenciar llamadas de números desconocidos y muestra si han sido verificadas por el operador.
 - Navegador web Mobile Safari (ver apartado "16. Navegador web Mobile Safari"):
 - Incorpora ajustes selectivos por sitio web para la cámara, el micrófono y el acceso a la ubicación.
 - Analiza la robustez de la contraseña elegida al crear una cuenta nueva en un sitio web y avisa al usuario en caso de que no sea suficientemente segura.
 - El historial de Safari y las pestañas que se hayan sincronizado con iCloud se cifran punto a punto.
 - La funcionalidad "Tiempo de uso" incorpora ajustes para permitir a los padres restringir las comunicaciones de sus hijos durante el "Tiempo de Inactividad", así como para que gestionar los contactos disponibles para ellos (ver apartado "18.4. Tiempo de uso").

⁴ <https://www.ipadizate.es/2019/09/11/iphone-11-3d-touch/>

- Funcionalidad "Compartir" (ver apartado "13.3. Compartir"):
 - o Permite limitar opciones del contenido a enviar, como eliminar los datos de ubicación de una foto antes de mandarla.
 - o Determina de forma automática los dispositivos a los que se puede enviar información vía "AirDrop" y los incorpora al menú de compartición.
 - o Permite enviar contenido con un solo toque a contactos concretos de ciertas apps.
- La app de correo electrónico "Mail" permite bloquear a un remitente particular y hacer extensivo el bloqueo a todos los dispositivos vinculados a la misma cuenta de iCloud. También permite silenciar las notificaciones de hilos concretos (ver apartado "0. App "Mail""").
- El "Centro de Control" permite seleccionar redes Wi-Fi y dispositivos Bluetooth directamente, sin necesidad de entrar en el menú de ajustes correspondiente.
- Se incorpora soporte para cifrado WPA3 en comunicaciones Wi-Fi (ver apartado "12.1.3. Wi-Fi").
- En ausencia de conexión a una red Wi-Fi conocida, iOS 13 examinará las redes que estén en rango y avisa de la disponibilidad de las que estén siendo utilizadas.
- Las conexiones a puntos de acceso personal han sido rediseñadas, incorporando compartición persistente y automática (ver apartado "12.1.5. Personal Hotspot").

6. DISPOSITIVO MÓVIL EMPLEADO

El dispositivo móvil empleado en la elaboración del presente informe es el iPhone SE, que comparte muchas de las prestaciones de modelos de gama más alta, con pantalla de 4", procesador Apple A9 (y coprocesador de movimiento M9), cámara trasera de 12MP con capacidades de grabación de vídeo en 4K y tecnología Touch ID, entre otros.

La mayor parte de las recomendaciones de seguridad proporcionadas son aplicables al resto de dispositivos móviles iPhone que soporten la versión iOS 13, pero puede que algunas de ellas no sean de aplicación directa en modelos que no dispongan de los componentes hardware implicados.

Las versiones de iOS empleadas en la elaboración del presente informe son la 13.2.2, disponible desde noviembre de 2019, y la 13.3, liberada en diciembre de 2019.

NOTA: Consultar apartado "0. Actualización del sistema operativo iOS" para ver el mecanismo de actualizaciones.

7. PROCESO DE ACTIVACIÓN DEL DISPOSITIVO MÓVIL

Tras arrancar el dispositivo móvil por primera vez (o después de un reseteo a fábrica) mediante la pulsación del botón de encendido, es preciso realizar el denominado "proceso de activación", que establecerá una configuración por defecto con los valores fijados por Apple (y/o seleccionados por el usuario durante este proceso). Si se ha insertado adicionalmente una tarjeta SIM, se realizarán también los ajustes del operador de telefonía móvil en función del perfil de configuración móvil de iOS asociado a dicha tarjeta SIM y al operador.

El proceso de activación mostrará un saludo en varios idiomas (mediante el icono " ⓘ" se puede obtener información específica del dispositivo) y se iniciará al pulsar el botón "Inicio" ("Home"):

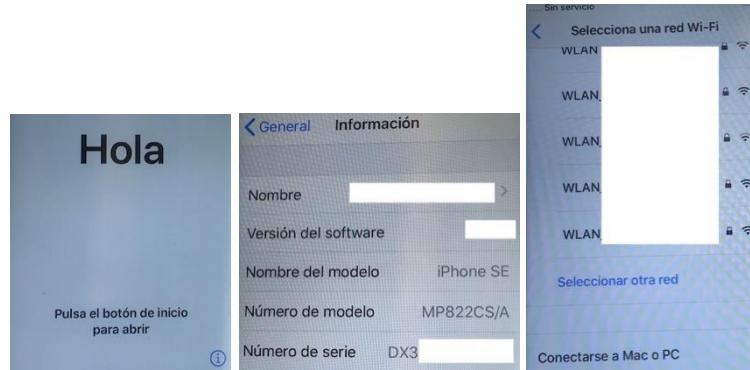


Figura 1 - Activación inicial de un dispositivo iOS

- Si se introdujo una tarjeta SIM: aparecerá una pantalla con identificadores en la que se muestra información sobre el número de serie y el IMEI del dispositivo móvil, y el ICCID de la tarjeta SIM, entre otros. Se indicará que la tarjeta SIM está bloqueada y, al pulsar en "Unlock" ("Desbloquear"), se solicitará el PIN correspondiente. La correcta introducción del PIN de la tarjeta SIM activa la vinculación del dispositivo móvil a dicha tarjeta y número de teléfono, y a sus capacidades de comunicación de datos móviles, y permite continuar con la activación.
- Si no se introdujo tarjeta SIM, el proceso de activación se iniciará directamente con la selección de idioma y región.

NOTA: El iPhone no ofrece la posibilidad de tomar capturas de pantalla durante el proceso de activación, por lo que algunas de las imágenes asociadas a este proceso se omitirán.

El proceso de activación puede llevarse a cabo de las siguientes formas:

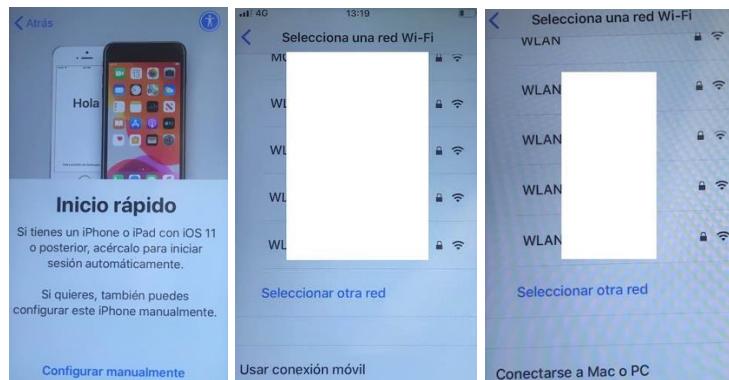


Figura 2 - Menú de configuración inicial de iOS 13

- A través de la funcionalidad "Inicio rápido"⁵: transfiere la configuración desde otro dispositivo móvil de Apple:
 - iPhone, iPad o iPod Touch con versión posterior a iOS 11: se transfieren los ajustes básicos y el resto se puede restaurar desde una copia de seguridad de iCloud.
 - iPhone con versión posterior a iOS 12.4: permite realizar una migración, bien de forma inalámbrica, bien mediante conexión directa desde un cable *Lighting*⁶.

Los detalles de esta configuración quedan fuera del ámbito de la presente guía.

⁵ <https://support.apple.com/es-es/HT210216>

⁶ <https://support.apple.com/es-es/HT210216#migrationhowto>

- A través del menú "Configurar manualmente", se activará el interfaz Wi-Fi, se escanearán las redes Wi-Fi cercanas y se mostrará una lista con las redes encontradas, ordenada alfabéticamente, para facilitar la conexión a una red Wi-Fi. Desde este menú se dispone de tres alternativas para realizar la activación inicial:
 - Al final de la lista se dispone de la opción para configurar una red Wi-Fi manualmente (opción "Seleccionar otra red")⁷ (ver imágenes izquierda y central de la <Figura 3>).
 - Configuración a través de iTunes desde un ordenador Mac o un PC conectado mediante un cable USB (ver imagen derecha de la <Figura 3>), cuyos detalles quedan fuera del ámbito de la presente guía).
 - Configuración a través de la conexión de datos móviles (botón "Usar conexión móvil"). Para que aparezca dicho botón, es preciso haber elegido la opción "Seleccionar otra red".

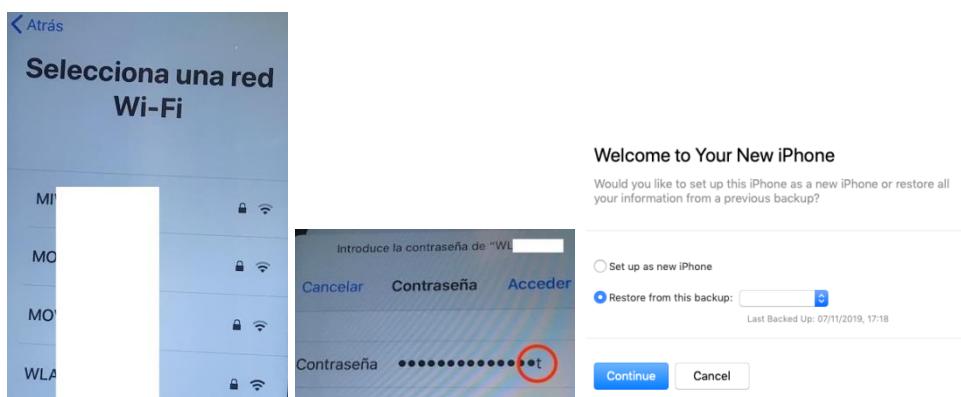


Figura 3 - Selección de red Wi-Fi durante el proceso de activación y activación del iPhone mediante un backup procedente de otro iPhone

La introducción de la contraseña de la red Wi-Fi debe realizarse de forma que se impida el acceso visual a la pantalla por parte de terceros no autorizados, ya que (como ilustra la imagen derecha de la <Figura 3>) los caracteres se muestran momentáneamente en claro durante su introducción. Una vez se verifica la contraseña, se reflejará que se ha establecido una conexión a esa red Wi-Fi mediante un símbolo de validación ("√") a la izquierda de su nombre. Al pulsar "Siguiente", se mostrará un mensaje informando de que el proceso de activación está en curso.

CONFIGURACIÓN DE TOUCH ID / CÓDIGO DE ACCESO

La siguiente pantalla informa al usuario de que se va a obtener información personal, junto a los aspectos de privacidad asociados, y propone la activación de la función "Touch ID" (identificación por huella). Se recomienda configurar dicha funcionalidad con posterioridad a completar el proceso de activación (ver apartado "8.1.2.2. Touch ID"), seleccionando "No usar".

⁷ A través de "Seleccionar otra red" se puede escoger una red Wi-Fi oculta, aunque el uso de este tipo de redes se desaconseja desde el punto de vista de seguridad.



Figura 4 - Activación inicial - Touch ID

Si se opta por "No usar" (opción recomendada), se presentará la pantalla de configuración de bloqueo de la pantalla, que, por defecto, solicita la introducción de un código de acceso (o PIN) de 6 dígitos, pero que también ofrece el menú "Opciones de código" (ver apartado "8.1.2. Método de bloqueo del dispositivo móvil") con otras alternativas. Desde el punto de vista de seguridad, se recomienda seleccionar, bien un código "alfanumérico personalizado" de al menos 8 caracteres, bien un código "numérico personalizado" de al menos 8 dígitos. Si se optase por "No usar código" (opción totalmente desaconsejada desde el punto de vista de seguridad), se mostrará un mensaje de aviso.

CONFIGURACIÓN DEL APPLE ID

El siguiente paso consiste en seleccionar si se desea realizar la configuración inicial a partir de una copia de seguridad (desde iCloud o iTunes; consultar el apartado "20. Copias de seguridad y restauración"), transferir los datos desde un dispositivo móvil Android o configurar como un nuevo iPhone (opción documentada en el presente informe), para la cual se ofrece la posibilidad de utilizar un identificador de usuario o ID de Apple (*Apple ID*) ya existente o crear uno nuevo, en cuyo caso se solicitará la fecha de nacimiento para permitir o inhabilitar el acceso a determinados servicios.

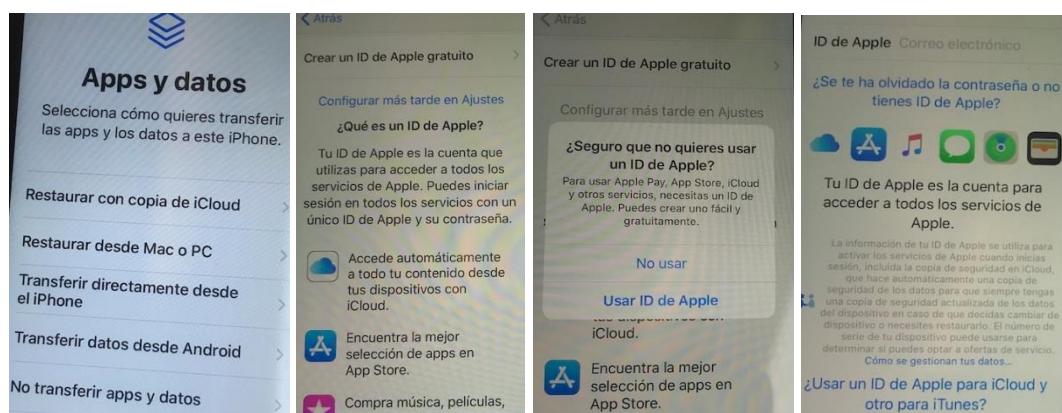


Figura 5 - Activación inicial: Apple ID

Para indicar el ID de Apple, se solicitará la introducción de una dirección de correo electrónico o la creación de una nueva cuenta de usuario en iCloud, que se utilizará como ID de Apple:

- En caso de no desear asociar el dispositivo móvil a un ID de Apple, se empleará la opción "Configurar más tarde en Ajustes". La asociación entre el dispositivo móvil y un ID de Apple es necesaria para la utilización de ciertos servicios de Apple, como "Buscar mi iPhone" (ver apartado "11. Cuentas asociadas al dispositivo móvil").

- En caso de querer realizar la vinculación del dispositivo móvil con un ID de Apple (opción documentada a continuación), la misma cuenta de usuario se empleará tanto para acceder a los servicios de iCloud, como a la iTunes Store y a la App Store. La contraseña ha de teclearse en un lugar seguro y fuera del alcance visual de terceros, ya que los caracteres aparecen brevemente en claro en la pantalla durante su introducción.

NOTA: Es muy importante destacar que, pese a que se muestra un mensaje informando de que la vinculación entre la dirección de e-mail seleccionada como ID de Apple y el dispositivo móvil no puede cambiarse posteriormente, la realidad es que esto sí es posible, como se documenta en el apartado "11. Cuentas asociadas al dispositivo móvil".

La cuenta de usuario proporcionada en este paso se empleará por defecto tanto para los servicios de iCloud como para el acceso a la iTunes Store y a la App Store, tanto si se crea nueva como si se añade una ya existente, si bien es posible (**y recomendado desde el punto de vista de seguridad**) utilizar una cuenta independiente para iTunes, como muestra la imagen derecha de la <Figura 5>.

Para validar el ID de Apple durante el proceso de activación, si dicho ID de Apple dispone de un segundo factor de autentificación (2FA) configurado⁸, debe seleccionarse entre dos mecanismos para recibir el código de verificación: "SMS" (utilizado por defecto) o "Llamada telefónica" (en caso de no recibirse el SMS y seleccionar "¿No has recibido el código de verificación?"). En caso de emplearse "SMS", el código de verificación se rellenará automáticamente una vez recibido el mensaje si la SIM asociada al iPhone corresponde al número utilizado como 2FA (si no es así, se puede teclear manualmente). Finalmente, se deberán aceptar los términos y condiciones del servicio.

DEFINICIÓN DE LA POLÍTICA DE ACTUALIZACIONES DE IOS

El proceso de instalación instará al usuario a activar las actualizaciones automáticas de iOS. Desde el punto de vista de seguridad, se recomienda seleccionar la opción "Instalar las actualizaciones manualmente".

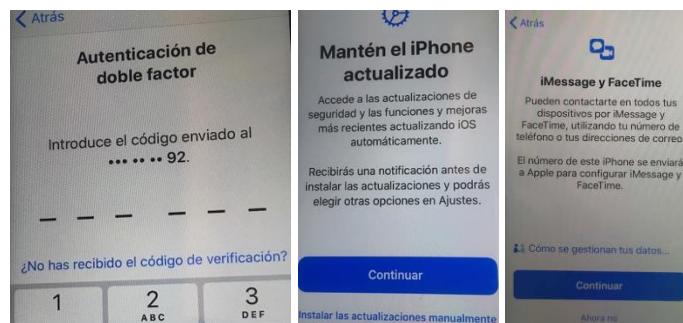


Figura 6 - Activación inicial: configuración del Apple ID e introducción del 2FA

SERVICIOS ADICIONALES

Se solicitará al usuario confirmación / permiso para:

- Enviar el número de teléfono a Apple para su uso en iMessage y FaceTime: desde el punto de vista de seguridad/privacidad, se recomienda seleccionar "Ahora no" (estos servicios se describen en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]).

⁸ Cuando se crea el ID de Apple durante la activación del dispositivo, como éste tiene que disponer de una tarjeta SIM, se activa automáticamente la cuenta de usuario con el segundo factor de autentificación.

- Activar los servicios de localización: **se recomienda seleccionar** "Desactivar localización" y seguir a posteriori las recomendaciones del apartado "14. Servicios de localización".
- Configurar los métodos de pago para el uso del servicio "Apple Pay": **se aconseja seleccionar** "Configurar más tarde en Wallet".
- Configurar el "Llavero de iCloud", un servicio de almacenamiento de credenciales y métodos de pago en la nube para su compartición entre los diferentes dispositivos móviles (iOS) y tradicionales (macOS) asociados a una misma cuenta de usuario de iCloud. Desde el punto de vista de seguridad y privacidad, **se desaconseja el uso del llavero de iCloud** hasta que se haya evaluado la conveniencia de su utilización (ver apartado "15.3. Llavero de iCloud").
- Activar el asistente personal digital Siri, **recomendándose desde el punto de vista de seguridad posponer su configuración** (el servicio "Siri" se describe en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]).
- Compartir con Apple la información sobre el uso y datos de los distintos servicios y productos asociados al dispositivo móvil y a la cuenta de iCloud. Desde el punto de vista de privacidad, **se recomienda seleccionar la opción** "No compartir".

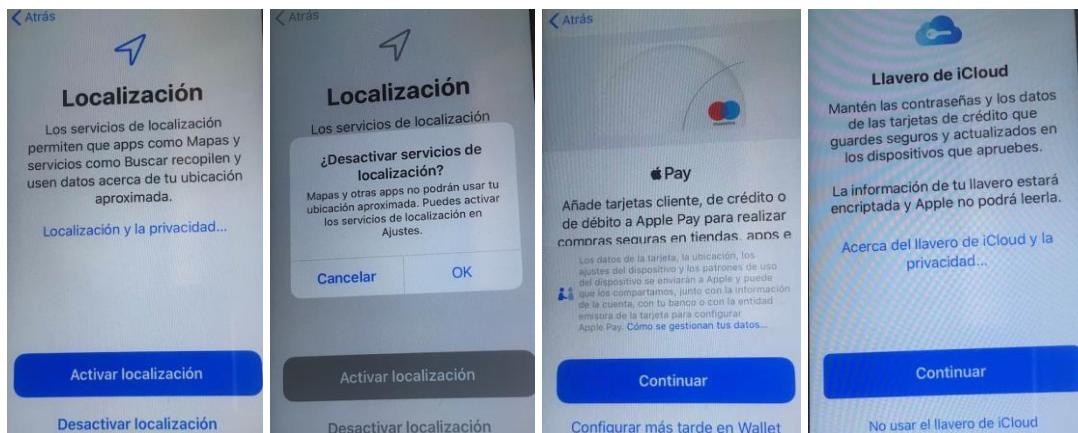


Figura 7 - Activación inicial: localización, Apple Pay y Llavero de iCloud



Figura 8 - Activación inicial: Siri, Tiempo de uso y Aspecto

TIEMPO DE USO Y ASPECTO

Por último, se invitará a configurar la funcionalidad "Tiempo de uso" (ver apartado "18.4. Tiempo de uso") y el "Aspecto", una funcionalidad introducida por iOS 13 que permite definir el fondo de pantalla (claro u oscuro). Desde el punto de vista de seguridad/privacidad, y con el objetivo de dificultar el acceso visual a la pantalla por parte de terceros, **se recomienda hacer**

uso del modo oscuro. El proceso de instalación concluye con un mensaje de bienvenida, tras el cual se mostrará la pantalla de inicio.

7.1 ESTADO DEL DISPOSITIVO TRAS LA ACTIVACIÓN INICIAL

Tras el proceso de activación, y asumiendo que se han aplicado las recomendaciones reflejadas en los apartados anteriores, el dispositivo móvil dispondrá de (ver menú "Ajustes - General - Información"):

- El nombre genérico "iPhone" (si no se dio de alta el Apple ID durante el proceso de activación).
- El nombre "iPhone de <Nombre>" (si se dio de alta el Apple ID para una cuenta para la que el propietario ha definido "<Nombre>" en el campo "Nombre").
- El interfaz Bluetooth activo (ver apartado "12.1.2. Bluetooth").
- El interfaz Wi-Fi activo (ver apartado "12.1.3. Wi-Fi").
- El "Centro de Control" disponible en la pantalla de bloqueo (ver apartado "9.2. Centro de Control").
- Si se dejó pendiente de activación/configuración alguna funcionalidad, se mostrará un menú "Acaba de configurar el iPhone 1" en el apartado "General". Si se selecciona esta entrada y se pulsa "Acaba de configurar", se lanzarán los correspondientes menús del proceso de activación.



Figura 9 - Estado del dispositivo tras el proceso de activación inicial.

Desde el punto de vista de seguridad, **se recomienda cambiar el nombre del dispositivo móvil** a través de "Ajustes - General - Información - Nombre - [nombre actual]" **por uno que no revele detalles ni del dispositivo móvil** (fabricante o modelo) **ni del usuario** (evitando tanto referencias al nombre de la persona como de la organización asociados al mismo), ya que este nombre se intercambia en múltiples comunicaciones, como las conexiones Bluetooth y el tráfico DHCP.

Una vez completada la activación, el dispositivo móvil abrirá la pantalla de inicio (o "Home"). En ese momento, dispondrá por un lado de los ajustes de configuración seleccionados por el usuario durante el proceso de activación, y por otro, de los ajustes por defecto fijados por Apple en función de otros parámetros, como la versión concreta de iOS o las características hardware del terminal. Se recomienda, a continuación, proceder a aplicar las recomendaciones ofrecidas en los sucesivos apartados del presente informe.

8. ACCESO FÍSICO AL DISPOSITIVO MÓVIL

Recomendaciones de seguridad:

- No dejar nunca el dispositivo desatendido, ni siquiera brevemente.
- Proteger la tarjeta SIM con un código de acceso robusto al menos 8 dígitos de longitud.
- No dejar nunca el dispositivo sin método de bloqueo.
- Proteger el acceso a los contenidos del dispositivo con un método robusto, que incluya un código alfanumérico de al menos 8 caracteres.
- Apagar el dispositivo cuando no se vaya a utilizar durante varias horas (por ejemplo, por la noche, o durante un viaje en transporte público).
- Establecer un bloqueo automático de pantalla que exija introducción del código.
- Establecer contactos de emergencia.
- En caso de requerirse forzosamente prestar el dispositivo a un tercero, hacer uso de la funcionalidad "Acceso guiado".

El acceso físico al dispositivo móvil debe limitarse todo lo posible, ya que un potencial atacante que consiga acceder, aunque sea brevemente, a él puede consultar contenidos disponibles en la pantalla de bloqueo, así como hacer uso de ciertos servicios de telefonía móvil (como descolgar llamadas entrantes). El dispositivo solo debe estar desbloqueado cuando esté en uso.

8.1 PROTECCIÓN DE ACCESO AL DISPOSITIVO

Se distinguen dos tipos de acceso al dispositivo:

- El asociado a las capacidades de telefonía disponibles: vinculado a la tarjeta SIM.
- El asociado a los contenidos del dispositivo: vinculado al método de acceso específico de iOS.

Ambos accesos deben estar protegidos mediante el método más robusto posible.

iOS proporciona mecanismos de cifrado para proteger los datos del usuario (ver apartado "19. Cifrado del dispositivo móvil"). Es importante tener en cuenta, sin embargo, que, a pesar de todos los mecanismos de cifrado y verificación, a lo largo de la historia de iOS se han descubierto diversas vulnerabilidades y procedimientos para saltarse la protección, que han permitido acceder a los datos del dispositivo móvil [Ref.- 16] [Ref.- 17]. Adicionalmente, en el pasado, se rumoreó que Apple disponía de capacidades para eliminar el código de acceso de un dispositivo móvil iOS sin conocer su valor disponiendo de acceso físico al mismo, y permitiendo acceso completo al dispositivo móvil y sus datos [Ref.- 18]. Apple ha negado este aspecto públicamente. A fecha de elaboración de la presente guía, existen empresas que ofrecen servicios y productos cuyo objetivo es obtener el código de acceso de un dispositivo móvil mediante técnicas de fuerza bruta y utilizando *exploits* no resueltos por Apple (algunos de los cuales se detallan en el informe publicado por CCN-CERT referenciado en [Ref.- 19]).

Por tanto, la mejor protección de los datos del dispositivo móvil se basa en incrementar la seguridad física, tanto del propio dispositivo como del ordenador al que se conecta (evitando accesos no autorizados), disponer de la última versión de iOS en el dispositivo móvil que resuelva la mayor parte de vulnerabilidades, elegir un código de acceso al dispositivo móvil robusto y difícilmente adivinable (al igual que para la contraseña de cifrado de las copias de

seguridad mediante iTunes), y no conectar el dispositivo móvil a ordenadores de terceros (para evitar la existencia de copias de seguridad y claves custodiadas en otros ordenadores).

8.1.1 CÓDIGO DE ACCESO A LA TARJETA SIM

Las tarjetas SIM soportan el establecimiento de un código PIN, cuya longitud puede ser de 4 a 8 dígitos (se aconseja utilizar 8), y **se recomienda encarecidamente hacer uso de él** para evitar que cualquier tercero que consiga sustraer la SIM del dispositivo pueda:

- Hacer uso de las capacidades de telefonía móvil asociadas a la SIM.
- Más importante, utilizar el número de teléfono asociado a la SIM para (entre otros):
 - Acceder a todos los servicios vinculados al número de teléfono de la SIM, muy sensibles, y entre los que se incluyen:
 - Códigos OTP (*One Time Password*) recibidos por SMS que se emplean como segundo factor de autenticación en multitud de servicios, como banca, comercio electrónico, autorización de acceso al ID de Apple desde otros dispositivos, etc.
 - Notificaciones sobre el uso de servicios, por ejemplo, realización de transacciones bancarias, o gastos de tarjetas de crédito superiores a una determinada cantidad.
 - Notificaciones de plataformas digitales de cualquier índole, entre las que se incluyen apps de ámbito sanitario, educativo, etc., que utilizan los SMS para informar al usuario de la disponibilidad de recursos (por ejemplo, recepción de una mercancía, recordatorios de citas o pruebas médicas, faltas de asistencia de un menor al centro escolar, etc.).
 - Suplantación del usuario en servicios y plataformas sensibles, como WhatsApp, donde el identificador de usuario está vinculado al número de teléfono de la SIM, que permitirían a un tercero que incorpore la SIM en un terminal propio trasladar la cuenta a dicho terminal, suplantando al usuario legítimo y accediendo a todos sus contenidos, incluso pertenecientes a fechas pasadas.
 - Recuperación de contraseñas de otros servicios haciendo uso de los servicios de "contraseña olvidada", por ejemplo, la cuenta de usuario de Apple o de Google (a fecha de elaboración de la presente guía), que típicamente solicitan y validan el número de teléfono vinculado a la cuenta como parte del proceso de recuperación.

Dado que las tarjetas SIM disponen de un PIN por defecto fijado por el operador de telefonía móvil, se recomienda **modificar el valor por defecto del PIN y emplear una secuencia numérica preferiblemente de 8 dígitos**, que no sea fácilmente adivinable y **que excluya** valores obvios como 0000, 1111, 1234, etc.

El PIN se solicita:

- Cuando se reinicia el dispositivo móvil.
- Al insertar la tarjeta SIM.

Se dispone de un máximo de tres intentos para el desbloqueo de la tarjeta SIM, mostrándose el número de intentos restantes en la pantalla de solicitud del PIN. Si se agotan, para poder desbloquear la tarjeta SIM, se requerirá introducir la contraseña de desbloqueo denominada PUK (*PIN Unlock Key*).

Aunque no se introduzca el PIN para la SIM, el acceso a contenidos del dispositivo móvil sigue estando disponible, incluso es posible consultar el registro de llamadas realizadas desde el dispositivo móvil iOS.

Para forzar la utilización del PIN de la SIM en dispositivos iOS 13 o para modificar el existente, se dispone de la opción "Cambiar PIN" del menú "Ajustes - Datos móviles - PIN de la SIM". iOS almacena en memoria el PIN de la tarjeta SIM, por lo que no lo solicitará al usuario cuando el dispositivo móvil salga del "Modo avión" (ver apartado "12.1. Conexiones inalámbricas y redes") para reactivar los servicios de telefonía móvil.



Figura 10 - Configuración del PIN de la tarjeta SIM

8.1.2 MÉTODO DE BLOQUEO DEL DISPOSITIVO MÓVIL

iOS incluye métodos de desbloqueo del dispositivo móvil basados en:

- El tradicional código de acceso, compuesto por un PIN por defecto de 4 ó 6 dígitos (en versiones más recientes de iOS) o por una contraseña alfanumérica.
- Mecanismos basados en biometría (reconocimiento de huella dactilar - "Touch ID" o reconocimiento facial - "Face ID").

Desde la aparición de los métodos de acceso basados en biometría, la comunidad de seguridad ha encontrado formas de saltarse esta protección (algunos ejemplos están disponibles en la [Ref.- 10]), lo que, en principio, parecería sugerir tener preferencia por el código de acceso como método de desbloqueo del dispositivo y de acceso a sus contenidos.

Sin embargo, existen también argumentos de seguridad a favor del uso de técnicas biométricas de desbloqueo:

- Riesgo de acceso visual no deseado a la pantalla del dispositivo (por parte de terceros o sistemas de grabación) que puede comprometer total o parcialmente el código.
- Riesgo de que el usuario prefiera la utilización de un código menos robusto, pero más usable (al tener que introducirlo decenas o cientos de veces al día).
- Imposibilidad de usar el código para autentificación en apps y servicios de terceros, si disponible para "Touch ID" y "Face ID", lo que también puede llevar a la reutilización de contraseñas entre servicios o el uso de contraseñas sencillas (este aspecto se refleja también en el apartado "15. Gestión de contraseñas").

Queda pues a criterio del usuario evaluar los factores anteriormente descritos a la hora de decidir el método de desbloqueo del dispositivo que mejor se ajustes a sus necesidades y a los potenciales vectores de ataque a los que pueda ser víctima, estableciéndose como una opción habitual hoy en día el uso de biometría junto a un código de acceso robusto.

8.1.2.1 Código de acceso

Recomendaciones de seguridad:

- Elegir un código de acceso de al menos 8 caracteres, preferiblemente alfanuméricos.
- No introducir nunca el código de forma que sea posible para un tercero visualizarlo total o parcialmente.
- Establecer un bloqueo automático de pantalla y exigir tras dicho bloqueo la introducción del código.
- Valorar el borrado automático de los contenidos del dispositivo tras 10 intentos fallidos de introducción del código.

El método de bloqueo del iPhone tiene como propósito bloquear cualquier tipo de acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones. iOS 13 ofrece diferentes métodos de bloqueo, descritos a continuación, si bien solo el código de acceso numérico está disponible en todos los modelos soportados, quedando Touch ID y Face ID excluidos de algunos de ellos.



Figura 11 - Pantalla de bloqueo de iOS 13

Desde el punto de vista de seguridad, **se deben seguir estas recomendaciones a la hora de establecer el código de acceso:**

- Fijarlo preferiblemente a un mínimo de 8 caracteres⁹ (los códigos numéricos de 4 y 6 dígitos revelan la longitud en la pantalla y se pueden romper con algunos de los medios técnicos disponibles actualmente).
- No debe coincidir con el PIN de la tarjeta SIM.
- No debe coincidir con ningún otro código empleado en cualquier otro servicio.
- Debe ser difícil de adivinar (si el nuevo código se considera demasiado sencillo, iOS mostrará el mensaje de la cuarta imagen de la <Figura 13>, pero permitirá al usuario utilizarlo si presiona "Usar de todos modos"):
 - No debe estar relacionado con datos (nombres de persona o animales, fechas, número de matrícula, etc.) fácilmente asociables al usuario del dispositivo¹⁰.

⁹ Guide to iOS estimated passcode cracking times (assumes random decimal passcode + an exploit that breaks SEP throttling): https://twitter.com/matthew_d_green/status/985885001542782978

- Se recomienda el uso de una *passphrase* (frase de paso) frente a palabras con sustituciones evidentes (4 por "a", 3 por "e", 1 por "i", 0 por "o", etc.).
- Cambiarlo periódicamente, sobre todo, si en algún momento ha sido preciso prestar el dispositivo a un tercero o ha podido estar expuesto, evitando reutilizar códigos antiguos.
- Evitar introducirlo de forma que permita su visión total o parcial por parte de terceros, dado que uno de los inconvenientes de iOS es que los caracteres pulsados aparecen iluminados durante un breve lapso de tiempo, suficiente para permitir a un tercero con acceso visual a la pantalla o a un sistema de grabación obtener o deducir el código. Por contra (como ilustra la segunda imagen de la <Figura 11>), si se trata de tomar una captura de pantalla durante la introducción del código, la imagen obtenida en iOS no mostrará ningún dígito.

La introducción del código de acceso es obligatoria, incluso aunque se haga uso de biometría:

- Tras reiniciar el dispositivo móvil o iniciararlo desde el estado apagado.
- Transcurridas 48 horas sin que haya sido desbloqueado.
- El código no se ha utilizado para el desbloqueo en las últimas 156 horas (6 días y medio) y "Face ID" no ha desbloqueado el dispositivo en las últimas 4 horas¹¹.
- Para cambiar el código vigente.
- Para registrar nuevas huellas en Touch ID o el rostro en Face ID.
- Tras 5 fallos en el reconocimiento de huella o facial (por parte de Touch ID o Face ID).
- Tras bloquearse el dispositivo móvil desde el interfaz "Buscar".
- Tras realizar una llamada de emergencia o acceder al ID médico.

CONFIGURACIÓN DEL CÓDIGO DE ACCESO

iOS 13 no exige disponer de un código de acceso para bloquear accesos no autorizados al terminal, pero incita a su configuración durante la activación (ver apartado "7. Proceso de activación del dispositivo móvil").



Figura 12 - Menú de configuración del código de acceso

¹⁰ La información publicada por el propietario de un dispositivo móvil en las redes sociales puede servir a un potencial atacante como punto de partida para adivinar el código de acceso al dispositivo móvil.

¹¹ <https://support.apple.com/es-es/HT208108>

Si el dispositivo carece de código de acceso, se recomienda establecerlo lo antes posible a través del menú "Ajustes - Touch ID y Código - Cambiar código". Si existe un código establecido, el acceso a este menú solicitará el vidente.

Un código de acceso vigente no se puede modificar de forma remota, pero es posible establecer uno si no lo está desde el servicio "Buscar" (apartado "23.3. Servicios "Buscar" para localización de dispositivos").

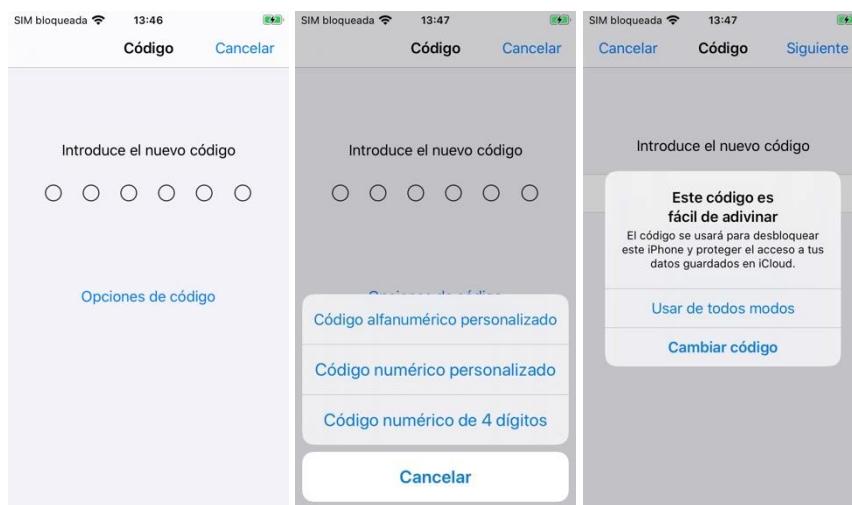


Figura 13 - Configuración de un nuevo código de acceso

PROTECCIONES EXTRA PARA EL DESBLOQUEO DEL DISPOSITIVO

A fin de proteger de la mejor forma posible el acceso ilegítimo al dispositivo, se recomienda utilizar los siguientes ajustes: para determinar cuándo es necesario introducir de nuevo el código de acceso al utilizar el dispositivo móvil:

- "Pantalla y Brillo - Bloqueo automático": determina cuándo se bloqueará (o suspenderá) la pantalla del dispositivo móvil tras un tiempo de inactividad (modo reposo). **Se recomienda fijarlo a un valor de entre 1 y 2 minutos** (imágenes 1 y 2 de la <Figura 14>). Si el modo de bajo consumo está activo, el dispositivo fijará este valor a 30 segundos, no siendo posible modificarlo.
- "Touch ID y código - Solicitar": determina cuándo se solicitará el código de acceso tras haber sido el dispositivo móvil bloqueado (o suspendido) por inactividad, en base al ajuste previo, o de forma manual por el usuario. **Se recomienda fijarlo a "De inmediato"** (imágenes 3 y 4 de la <Figura 14>). Esta es la única opción disponible si "Touch ID" está habilitado.
- "Touch ID y código - Borrar datos": fuerza la eliminación de los datos del dispositivo móvil al décimo intento erróneo de introducción del código (tercera imagen de la <Figura 14>). Estos datos no se borrarán de la cuenta asociada al ID de Apple del dispositivo, por lo que podrían ser recuperados por el usuario si dispone de una copia de seguridad (en iCloud o en iTunes).

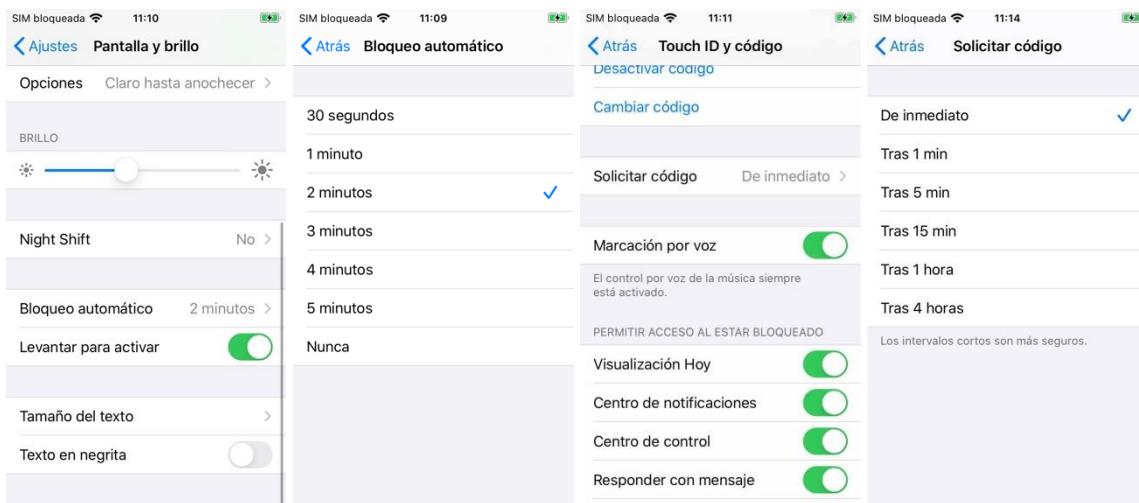


Figura 14 - Configuración del bloqueo automático de pantalla

INTRODUCCIÓN ERRÓNEA DEL CÓDIGO DE ACCESO

iOS incrementa la dificultad de adivinar el código por ensayo/error, forzando a que transcurra un tiempo entre intentos fallidos de introducción del código, tanto en la pantalla de bloqueo, como durante la configuración de un código nuevo o durante la configuración de "Restricciones": tras 5 intentos fallidos, deberá esperarse 1 minuto antes de poder volver a introducir el código (imagen derecha de la <Figura 15>); al sexto, se deberá esperar 5 minutos; al séptimo y octavo, 15 minutos, para cada intento. Tras el noveno intento y sucesivos, deberá esperarse una hora (60 minutos) por cada intento. El número de intentos fallidos no se indica si el error se produce en la pantalla de bloqueo (sí en los otros dos casos). Cada vez que se introduce un código de acceso erróneo, se emitirá un sonido acompañado de una vibración del dispositivo móvil.



Figura 15 - Intento fallido en el cambio de código de acceso

No existe ningún mecanismo para desbloquear un dispositivo bloqueado preservando sus datos si no se conoce el código de acceso. Es posible resetearlo siguiendo las indicaciones de la [Ref.- 7], y restaurar el dispositivo si se dispone de una copia de seguridad realizada en un ordenador local (para más información, consultar el apartado "20.2. Restauración del dispositivo desde una copia de seguridad").

8.1.2.2 Touch ID

"Touch ID" es un sistema biométrico de reconocimiento de huella dactilar mediante hardware para dispositivos móviles iOS¹², que se encuentra integrado en el botón de "Home", para facilitar su utilización. "Touch ID" puede ser empleado para desbloquear el dispositivo móvil, y permite tanto realizar compras en la App Store como validar al usuario en apps de terceros, en lugar de emplear las credenciales asociadas al login del servicio proporcionado por la app.

La habilitación de "Touch ID" requiere disponer de un código de acceso de respaldo, que es utilizado en caso de que no sea posible leer la huella dactilar, con el objetivo de proteger el dispositivo móvil frente a distintos escenarios de uso inapropiados. Tras cinco intentos fallidos, se requerirá introducir el código.

Si Touch ID está habilitado, el dispositivo móvil se bloqueará automáticamente al entrar en modo reposo o al suspenderse la pantalla, no aplicando el periodo de gracia definido en el ajuste "Solicitar código" disponible para el código de acceso (éste queda fijado a "De inmediato").

Para configurar Touch ID, se dispone del menú "Ajustes - Touch ID y código" (los detalles sobre cómo realizar este proceso se pueden consultar en la [Ref.- 8]). Se permite un máximo de cinco huellas en iOS 13. Una vez dada de alta una huella, se puede optar por utilizarla para:

- Desbloqueo del dispositivo móvil.
- Apple Pay.
- iTunes Store y App Store.
- Consultar las contraseñas almacenadas en el dispositivo (ver apartado "11.4. Sección "Contraseñas y cuentas"").

En caso se optarse por hacer uso de "Touch ID" para autentificación en apps o servicios de terceros, se aconseja comprobar que la app no permite reconocer una nueva huella añadida con posterioridad sin necesidad de revalidar las credenciales propias.

8.1.2.3 Face ID

"Face ID" es un sistema de biometría basado en reconocimiento facial adaptativo vía hardware, que se introdujo por primera vez en iPhone X, junto a iOS 11, reemplazando el acceso mediante huella ("Touch ID") en los dispositivos que lo soportan¹³. "Face ID" captura (a través de la cámara TrueDepth) los patrones faciales del usuario, y los transforma a una representación matemática que se almacena en un procesador denominado "*Secure Enclave Processor (SEP)*", que reside en los chips A11, A12 y A12X Bionic (iPhone XR, iPhone XS y XS Max) y en el A13 Bionic (iPhone 11, iPhone 11 Pro y iPhone 11 Pro Max).

NOTA: Debido a que el dispositivo empleado para la elaboración de la presente guía dispone únicamente de "Touch ID", otros modelos de iPhone y iPad con soporte para Face ID dispondrán del menú "Face ID y código" en lugar del menú "Touch ID y código".

Además de permitir el desbloqueo del terminal, "Face ID" (al igual que Touch ID) proporciona funcionalidades para el inicio de sesión y autentificación dentro de las apps, para la realización

¹² Touch ID está soportado para dispositivos iPhone 5s o posterior, iPad (5.ª generación y posterior), iPad Pro, iPad Air 2, y iPad mini 3 o posterior.

¹³ <https://support.apple.com/es-lamr/HT209183>

de pagos, y para el acceso al autorrelleno de contraseñas en Safari. La configuración de Face ID queda fuera del alcance de la presente guía, pero se puede consultar en la [Ref.- 9].

Desde el punto de vista de seguridad, aunque Apple afirma que la tecnología de reconocimiento facial es más segura que la de reconocimiento de huella dactilar (1:1.000.000 frente a 1:50.000 [Ref.- 39]), hay evidencias de que no es infalible ante, por ejemplo, gemelos o la creación de máscaras en tres dimensiones con los rasgos faciales del usuario [Ref.- 13].

Para deshabilitar el uso del reconocimiento facial permanentemente, se dispone del menú "Face ID y código". Para inhabilitarlo de forma temporal, por ejemplo, ante una situación de emergencia en la que se sospeche que un tercero puede tratar de sustraer y desbloquear el dispositivo móvil enfrentando la cara del usuario ante la cámara, se puede recurrir al procedimiento descrito en el apartado "8.2. Medical ID (Emergencia SOS)".

8.2 MEDICAL ID (EMERGENCIA SOS)

Una vez el dispositivo móvil está bloqueado, las únicas llamadas que se pueden cursar son las de emergencia (112 para España, consultar para otros países). Para cursar estas llamadas, hay dos opciones:

- En la pantalla de bloqueo, pulsar "SOS". El teclado permite introducir el número de emergencias local.
- Seguir las instrucciones de la [Ref.- 41] para el modelo concreto de dispositivo¹⁴ y deslizar el dedo a derechas sobre el botón "Emergencia SOS". Cuando se invoca esta opción:
 - El dispositivo llama a los servicios de emergencia, pudiendo incluirse la ubicación como parte de los datos que se faciliten (aunque no esté activa).
 - Tras concluir la llamada, se enviará a los contactos definidos en el campo "Contactos de emergencia" un mensaje informando de que el propietario del iPhone ha llamado a "Emergencias" y que incluye su ubicación actual. Si la ubicación cambia, se volverá a enviar a los contactos de emergencia un mensaje con la nueva ubicación.
 - Si el ajuste "Ver cuando está bloqueado" está activo, el menú también permite acceder a los "Datos médicos", disponibles en el menú "Ajustes - Salud - Datos médicos", que se pueden añadir o modificar también a través de la app "Salud". Desde el punto de vista de la privacidad, es importante tener en cuenta que la disponibilidad de estos datos aun con el dispositivo bloqueado puede permitir a terceros no autorizados obtener información delicada sobre el propietario.

La invocación del modo SOS tiene una importante característica desde el punto de vista de seguridad, ya que desactiva el desbloqueo al dispositivo mediante biometría, forzando la utilización del código de acceso vigente. Esta opción puede ser útil ante una situación de riesgo en la que el usuario tema verse obligado a desbloquear el terminal mediante estos medios (por ejemplo, en un control de aeropuerto).

La configuración detallada del "Medical ID" puede consultarse en la [Ref.- 20].

¹⁴ En el iPhone SE, empleado en la elaboración de la presente guía, pulsar 5 veces el botón de encendido.

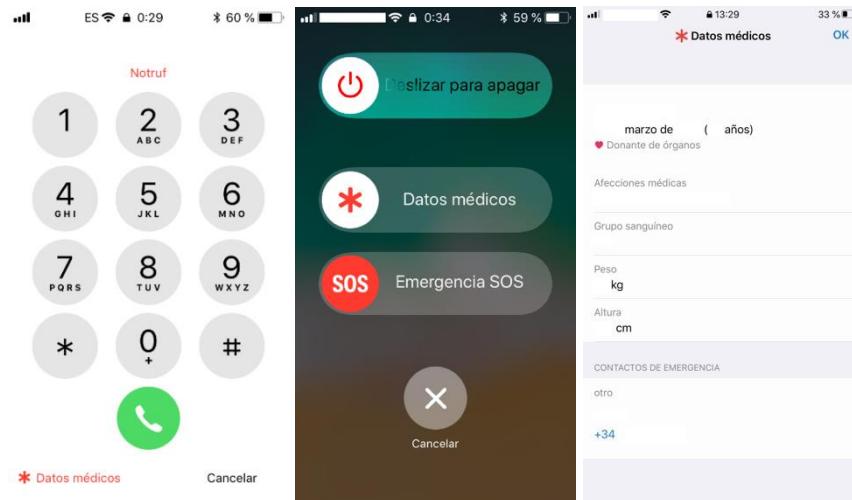


Figura 16 - Uso de la funcionalidad "Emergencia SOS" en la pantalla de bloqueo



Figura 17 - Menú "Ajustes - Salud"

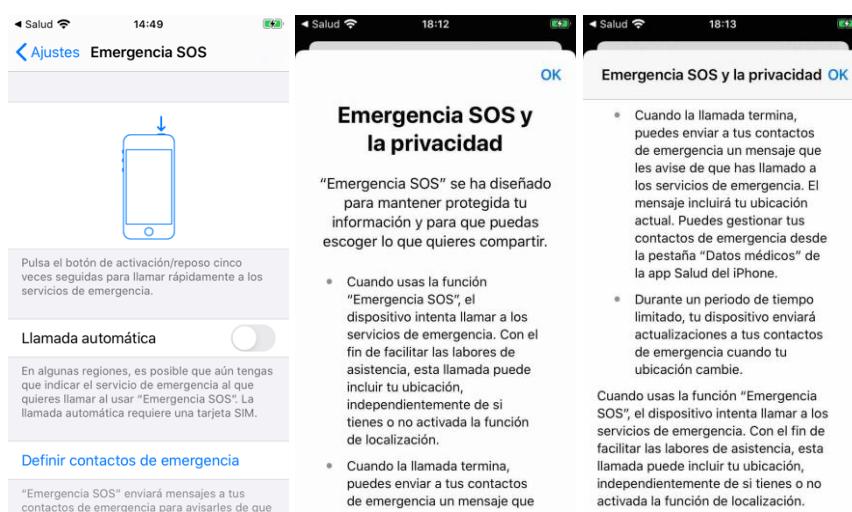


Figura 18 - Llamada de emergencia y datos médicos

8.2.1 APP "SALUD"

La app "Salud" ha sido rediseñada en iOS 13 para actuar como elemento central de gestión de datos relacionados con la salud recopilados por los dispositivos vinculados a una misma cuenta de iCloud (el propio iPhone, otros iPhone y Apple Watch) y apps de terceros que se integren con ella, incluidos ensayos clínicos. Los datos recopilados se almacenan en la cuenta de iCloud.

En iOS 13, se añade incluso una funcionalidad para control menstrual.

Los detalles de configuración de la app "Salud" pueden consultarse en la [Ref.- 42], y quedan fuera del ámbito de la presente guía. Desde el punto de vista de privacidad, los datos de salud se consideran extremadamente sensibles, por lo que debe valorarse muy concienzudamente su inclusión como parte de un dispositivo móvil.

En caso de quererse utilizar los servicios vinculados a "Salud", se debe verificar a través de "Ajustes - Privacidad - Salud" que no existe ninguna app con permisos de acceso a estos datos que no se deba tenerlos.

Para consultar los datos de salud obtenidos por la app "Salud" desde un dispositivo concreto, se ofrece el menú "Ajustes - Salud - [Datos] Acceso a datos y dispositivos". Desde el menú asociado a cada dispositivo, es posible eliminar todos los datos recabados de él.

8.3 AJUSTES ADICIONALES DE "TOUCH ID Y CÓDIGO"

Desde el punto de vista de seguridad, **se aconseja desactivar todas las opciones de la sección "Ajustes - Touch ID y código - Permitir acceso al estar bloqueado", incluyendo "Visualización hoy", "Marcación por voz", "Notificaciones recientes", "Centro de Control", "Siri", "Responder con mensaje", "Control de casa", "Wallet" y "Devolver las llamadas perdidas", para evitar que un tercero pueda realizar acciones indeseadas desde la pantalla de bloqueo.**

Se desaconseja habilitar la funcionalidad "Responder con mensaje" y "Devolver las llamadas perdidas", ya que pueden permitir a un tercero que acceda al dispositivo temporalmente enviar un mensaje, o responder a una llamada previa, suplantando al propietario.

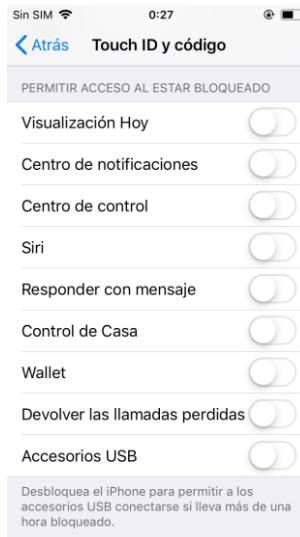


Figura 19 - Ajustes recomendados con la pantalla bloqueada

La opción "Accesos USB", estando deshabilitada (valor por defecto), evita que se pueda acceder mediante una conexión de datos vía USB al dispositivo móvil si éste ha permanecido

bloqueado durante más de una hora. Se recomienda consultar el apartado "12.3.2. Modo restringido USB" para más información sobre las medidas de protección de conexiones vía USB.

8.4 ACCESOS RESTRINGIDOS AL DISPOSITIVO

Además del acceso general que permite utilizar todas las funciones del iPhone, existen otros dos tipos de acceso restringido que bloquean ciertas funcionalidades del dispositivo y que son interesantes desde el punto de vista de seguridad:

- "Restricciones": permiten establecer límites tanto para las apps disponibles como para los ajustes del iPhone (ver apartado "18.4. Tiempo de uso").
- "Acceso guiado": interesante por ser un acceso tipo "quiosco" (ver apartado "18.5. Acceso guiado"), en el que se proporciona únicamente acceso a una app.

9. PANTALLA DE INICIO ("HOME")

La pantalla de inicio (o "Home") aparece al desbloquear el dispositivo móvil tras el proceso de arranque, y también al pulsar el botón "Home" desde cualquier otra pantalla. Consta de tantas subpantallas como puntos aparecen sobre la barra de iconos de acceso rápido (situada en la parte más inferior de la pantalla), entre las cuales es posible desplazarse desplazando el dedo a derecha o izquierda desde cualquier punto de la pantalla actual.

- La pantalla central y las situadas a la derecha contiene los iconos de las principales apps incluidas en iOS más las que haya instalado el usuario.
- La pantalla situada más a la izquierda incorpora:
 - La función de búsqueda mediante texto y voz (en la parte superior), descrita en el apartado "9.3. Búsqueda mediante texto y voz".
 - La "Vista de hoy" (ver apartado "9.4. Today View").
 - El área de "Widgets".
 - La sección correspondiente a "Tiempo de uso" (apartado "18.4. Tiempo de uso").



Figura 20 - Pantalla de "Inicio", "Centro de Notificaciones" y "Vista de Hoy" de iOS 13

9.1 BARRA SUPERIOR DE ESTADO

La barra de estado en iOS está compuesta por una serie de iconos de estado, que permiten obtener información relevante sobre el estado del dispositivo de forma rápida:

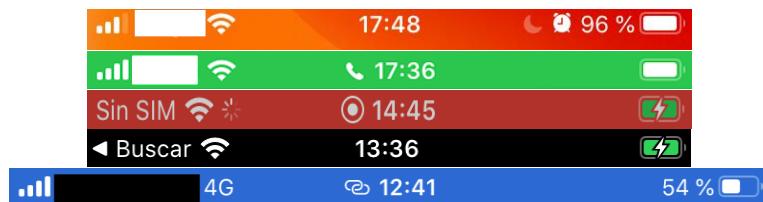


Figura 21 - Barra superior de estado

La lista completa de iconos disponibles puede consultarse en la página de soporte oficial de Apple [Ref.- 3]. Los principales son:

- En la parte izquierda de la barra se ofrece información sobre tráfico de red, entre otros:
 - El estado de la conectividad de datos móviles:
 - o el icono "■■■■" indica que se está dentro del alcance de una red móvil y el nivel de cobertura (a mayor número de barras marcadas, mejor cobertura), y viene acompañado del nombre del operador de la red y, eventualmente, del tipo de red disponible (GPRS, E, 3G, 4G, LTE). Si el iPhone dispone de SIM dual, las barras aparecen divididas en dos.
 - o El icono "◎" indica que se está haciendo uso de una conexión de datos compartida (ver apartado "12.1. Conexiones inalámbricas y redes").
 - El nombre del operador de telefonía móvil. Existen ocasiones en las que el nombre del operador se sustituye por el de algún servicio especial en ejecución, por ejemplo, la función "Buscar" (descrita en el apartado "23.3. Servicios "Buscar" para localización de dispositivos").
 - El icono "Wi-Fi" representa conexión a una red inalámbrica.
 - El icono "✖" indica que se está intercambiando tráfico de red.
 - La parte central de la barra de estado ofrecerá la hora si el dispositivo está desbloqueado, y mostrará "🔒" si se encuentra bloqueado.
 - En la parte derecha de la barra, por defecto se presenta solo el estado de la carga de la batería. Al igual que en su predecesor, iOS 12, el icono de Bluetooth no se muestra hasta que exista una conexión activa con otro dispositivo Bluetooth [Ref.- 4].

Adicionalmente, y según las funcionalidades activas, se podrá mostrar el símbolo de "No molestar", alarma, conexión a auriculares, y otros iconos adicionales.

Es importante destacar que la barra superior de estado puede aparecer coloreada para informar de otras situaciones:

- Verde: existe una llamada telefónica en curso.
 - Rojo: se está grabando sonido o imágenes (o vídeo) del dispositivo.
 - Azul: se está compartiendo la conexión de datos (ver apartado "12.1.5. Personal Hotspot"), indicándose además el número de dispositivos que están conectados actualmente por este medio. Desde el punto de vista de seguridad, es importante prestar atención al número de conexiones activas por si, estando activo el servicio, se estuvieran estableciendo conexiones no deseadas.

Se recomienda monitorizar la barra superior de estado, a fin de detectar la presencia de iconos que indiquen si está teniendo lugar alguna actividad indebida.

No existe ninguna opción conocida que permita personalizar los iconos que se muestran en la barra superior de estado (a menos que el dispositivo se haya sometido a un proceso de *jailbreak*, escenario totalmente desaconsejado desde el punto de vista de seguridad).

9.2 CENTRO DE CONTROL

Recomendaciones de seguridad:

- Eliminar el "Centro de Control" de la pantalla de bloqueo desactivando el interruptor "Ajustes - Touch ID y código - [Permitir acceso al estar bloqueado] "Centro de Control"".
- No añadir al "Centro de Control" controles cuyo uso desde la pantalla de bloqueo pueda comprometer la privacidad del dispositivo.

El "Centro de Control" ("Control Center") proporciona un acceso rápido a funciones concretas mediante una serie de iconos (denominados "controles" o "temas"). Se muestra en el iPhone SE, 7, 7 Plus, 8 y 8 Plus desplazando un dedo hacia arriba desde la parte inferior de la pantalla (en iPhone X y modelos posteriores, deslizando el dedo hacia abajo desde la esquina superior derecha de la pantalla)¹⁵.

El "Centro de Control" es un elemento crítico desde el punto de vista de seguridad, pues permite activar/desactivar elementos relacionados con la conectividad del dispositivo móvil (por ejemplo, el modo avión, o los interfaces de comunicaciones Wi-Fi, Bluetooth y de red móvil o celular). Un potencial atacante con acceso al "Centro de Control" podría desactivar las capacidades de comunicación de datos (Wi-Fi y móviles 2/3/4G), impidiendo que la funcionalidad "Buscar mi iPhone" pudiese localizar el dispositivo a través de dichas capacidades (consultar el apartado "23.3. Servicios "Buscar" para localización de dispositivos"). Por tanto, ***una de las principales recomendaciones de seguridad de iOS 13 es deshabilitar el "Centro de Control" para la pantalla de bloqueo desactivando el interruptor "Ajustes - Touch ID y código - [Permitir acceso al estar bloqueado] "Centro de Control""*** (última imagen de la <Figura 22>).

El "Centro de Control" de iOS 13 está formado tanto por:

- Ajustes individuales: por ejemplo, el modo de rotación de la pantalla.
- Grupos de ajustes: un grupo se identifica por un recuadro gris oscuro que alberga un conjunto de controles, como en el caso de los ajustes de red o comunicaciones. Para obtener más detalles y desplegar los ajustes adicionales relativos a un grupo concreto, se puede pulsar prolongadamente sobre el recuadro reservado para el grupo¹⁶.
- Accesos directos a aplicaciones (por ejemplo, la Calculadora).
- Acciones rápidas (nuevo en iOS 13) que se inician al pulsar sobre un ícono (por ejemplo, la activación del modo "No molestar").

GRUPO "AJUSTES DE RED"

¹⁵ Para acceder al "Centro de Control" desde un iPad, es preciso deslizar el dedo hacia abajo desde la esquina superior derecha de la pantalla.

¹⁶ Este comportamiento está disponible solo desde iPhone 6s y modelos posteriores.

A través del uso de "haptic touch" sobre cualquier punto de la sección que engloba los iconos de comunicaciones, se desplegará un submenú desde el que se pueden controlar los elementos de conectividad del dispositivo [Ref.- 14]. Con un nuevo toque "haptic touch" sobre estos elementos, se desplegará un menú adicional asociado al elemento de comunicaciones concreto:

- Wi-Fi: se despliega la lista de redes Wi-Fi que se encuentran en el rango de alcance del dispositivo móvil. Si el dispositivo móvil está bloqueado, al pulsar sobre otra red diferente a aquella con la que existe conexión actual, se solicitará proceder al desbloqueo del dispositivo.

NOTA: Durante la elaboración de la presente guía, se constata que, si no se desbloquea el dispositivo después de seleccionar otra red diferente, en el menú de lista de redes Wi-Fi del "Centro de Control" se aparentará haber procedido a conexión con dicha red, pero, una vez se sale de la lista de redes, el ícono del "Centro de Control" volverá a mostrar la conexión Wi-Fi correcta.

- Bluetooth: con el dispositivo desbloqueado, se despliega la lista de los dispositivos Bluetooth con los que se ha establecido un emparejamiento exitoso. Si el iPhone se encuentra bloqueado, antes de proceder a presentarse esta lista se solicitará su desbloqueo.
- AirDrop: se permite habilitar/deshabilitar la recepción vía AirDrop, incluso con la pantalla bloqueada (consultar el apartado "13.1. AirDrop" para ver los distintos escenarios).

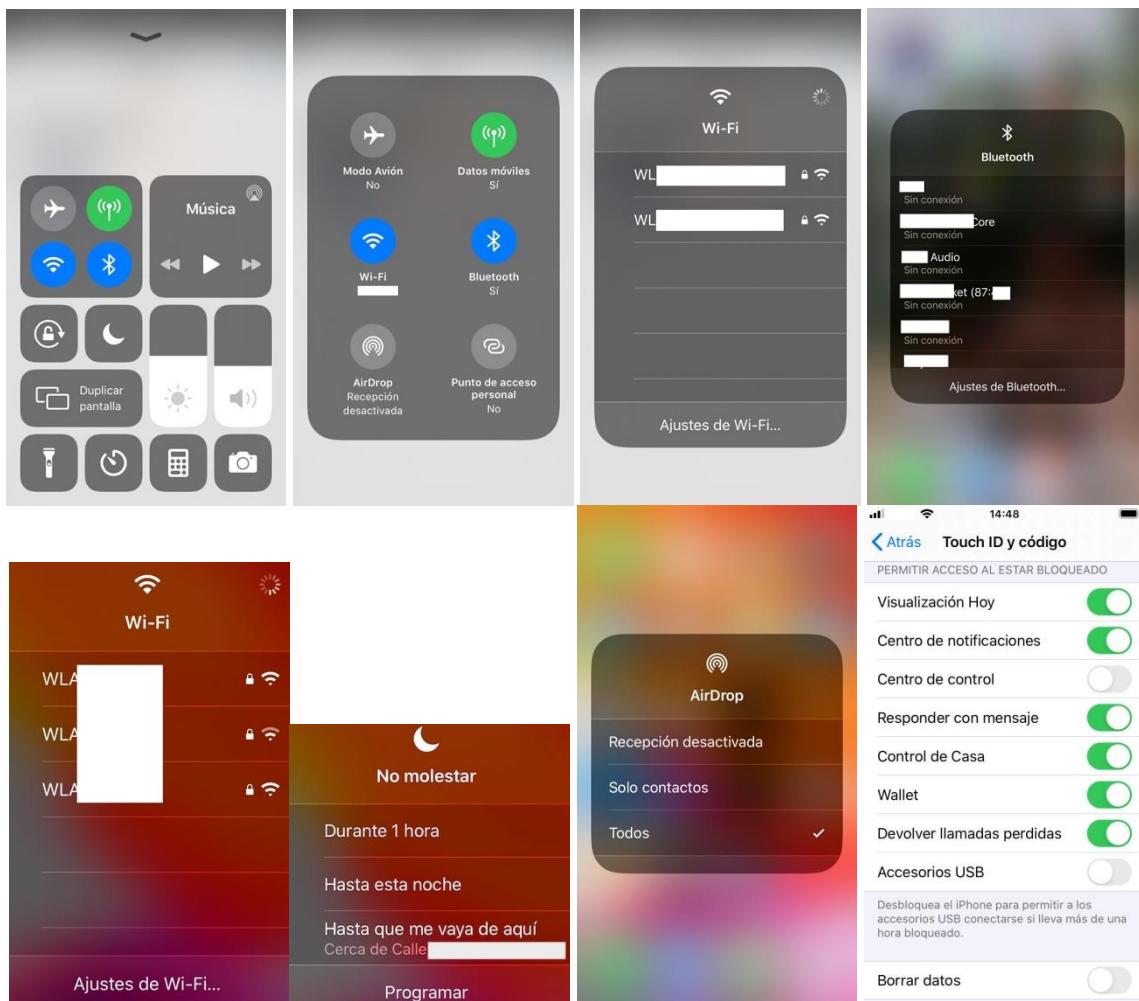


Figura 22 - "Centro de Control"

9.2.1 PERSONALIZACIÓN DEL CENTRO DE CONTROL

Los controles presentes en el "Centro de Control" se pueden personalizar desde "Ajustes - "Centro de Control" - Personalizar controles", pulsando el símbolo "+" sobre los controles que se desea añadir y el símbolo "-" sobre los que se desea eliminar. No es posible eliminar del "Centro de Control" los ajustes de red, el "modo nocturno", el control de brillo y de volumen, duplicar pantalla, reproducción de música o rotación de pantalla.



Figura 23 - Personalización de "Temas" para el "Centro de Control"

La descripción exacta de todos los controles disponibles en iOS 13 se puede consultar en la página de soporte oficial de Apple relativa al "Centro de Control" [Ref.- 5]. Aunque la mayor parte de los controles solicitarán identificación a través del método de acceso antes de realizar la acción correspondiente, existen algunos sensibles que no lo requieren:

- Notas (ícono "📝"): este control puede permitir, desde la pantalla de bloqueo, crear nuevas notas o consultar la última nota editada, según el valor definido en el ajuste "Acceder con pantalla bloqueada" (ver apartado "18.2.2. App "Notas"". **Se debe revisar cuidadosamente la configuración para impedir el acceso a Notas con el dispositivo bloqueado.**
- Accesibilidad (ícono " ⓘ"): el uso de funciones de accesibilidad en la pantalla de bloqueo (especialmente la de "VoiceOver", que enuncia en voz alta el contenido de la pantalla) ha sido desde sus inicios fuente de vulnerabilidades (se proporcionan algunos ejemplos en la [Ref.- 25]). Desde el punto de vista de seguridad, salvo que sea requisito para el uso del dispositivo, se aconseja prescindir de las funciones de accesibilidad en la pantalla de bloqueo.

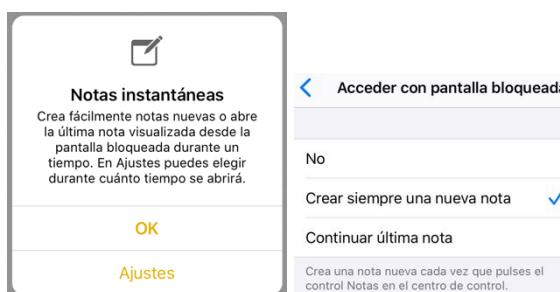


Figura 24 - Configuración de acceso a "Notas" en la pantalla de bloqueo

9.3 BÚSQUEDA MEDIANTE TEXTO Y VOZ

Recomendaciones de seguridad/privacidad:

- Desactivar "Mostrar en Buscar" y "Sugerir atajos" para las apps de contenido sensible.
- Desactivar "En la pantalla de bloqueo - Mostrar sugerencias de Siri".
- Desactivar la función "Dictado".

La búsqueda de iOS (también es conocida como "Spotlight") es un sistema de búsqueda rápida de información, tanto local como obtenida a través desde Internet, disponible en el campo superior "Buscar" de la pantalla situada a la izquierda de la pantalla de inicio. Para acceder a ella se puede deslizar el dedo de izquierda a derecha desde la pantalla de inicio (con la pantalla bloqueada o desbloqueada), lo cual da acceso además a la zona de "widgets" y a la "Vista de hoy", o también deslizar el dedo desde el centro de la pantalla de inicio hacia abajo (solo con pantalla desbloqueada).



Figura 25 - Menú "Buscar" con pantalla desbloqueada

Al pulsar dentro del campo superior "Buscar", iOS proporcionará sugerencias que se actualizan en tiempo real a medida que se introduce el texto y que concuerden con el término proporcionado según varios criterios, los cuales dependerán de si el dispositivo móvil está bloqueado o desbloqueado y de los ajustes del menú "Ajustes - Siri y Buscar - [Nombre app] Sugerencias de Siri y Buscar".

Si la pantalla está bloqueada, se mostrarán:

- Una lista de resultados de las primeras coincidencias asociadas al término de búsqueda.
- Los nombres de las apps instaladas en el dispositivo móvil coincidentes con la cadena de caracteres introducida. Este resultado puede constituir un problema desde el punto de vista de seguridad si un potencial atacante tuviese acceso temporal al dispositivo (sin conocer el código de acceso) y quisiera conocer si una determinada app, que por ejemplo tenga una vulnerabilidad explotable, se encuentra instalada en el dispositivo móvil. Antes de introducir cualquier texto, se muestran las apps más relevantes sugeridas por Siri.
- La entrada de la app "Diccionario" para ese texto.
- Las acciones "Buscar en Internet/App Store/Mapas", aunque se muestran, solicitarán el desbloqueo de la pantalla para lanzar las búsquedas correspondientes.

Adicionalmente, si la pantalla está desbloqueada (<Figura 25>), por defecto se obtendrá el resultado de:

- Los contenidos de las apps instaladas en el dispositivo, coincidentes con la cadena de caracteres introducida, incluyendo los ajustes que contienen el texto. Este resultado puede plantear problemas de seguridad si se proporciona a un tercero acceso temporal al dispositivo con objeto de mostrarle una información concreta, pues de forma rápida podría consultar contenidos específicos (mensajes, contactos, e-mails...) sin necesidad de recorrer diferentes pantallas.

NOTA: En caso de requerirse prestar temporalmente el dispositivo a un tercero, se recomienda hacer uso de la capacidad "Acceso guiado" (ver apartado "18.5. Acceso guiado").

La funcionalidad "Buscar" está estrechamente ligada a la del asistente digital personal Siri (descrito en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]), pues el comportamiento del menú "Buscar" se gestiona desde "Ajustes - Siri y Buscar" (<Figura 26>).

iOS 13 permite controlar a nivel de app la información que de ella se muestra en los resultados de la búsqueda "Spotlight" a través de los siguientes ajustes:

- "Mostrar en Buscar": con este ajuste activo (lo está por defecto para todas las apps), la función "Buscar" mostrará en sus resultados contenidos de los datos de dicha app. **Se recomienda desactivarlo para las apps de contenido sensible** (por ejemplo, la tercera imagen de la <Figura 26> ilustra esta recomendación para la app "Contactos"). Es importante destacar que, si se desactiva el ajuste "Mostrar en Buscar", si el asistente de voz Siri se encuentra activo, Siri ignorará la app correspondiente de cara a mostrar resultados asociados a ella durante las búsquedas, pero seguirá utilizando internamente los datos de dichas apps (y enviándole estadísticas y datos a Apple de forma cifrada) para seguir aprendiendo y proporcionando sugerencias personalizadas. Si se desea evitar también este comportamiento, es preciso deshabilitar adicionalmente los ajustes bajo la sección "Sugerencias de Siri": "Sugerencias de Buscar", "Sugerencias de Consultar" y "Sugerencias en pantalla bloqueada" (ver segunda imagen de la <Figura 26>). Para más información, se recomienda seleccionar el texto "Acerca de 'Consultar a Siri' y la privacidad" de esta sección.
- "Mostrar app": aparece al desactivar el ajuste "Mostrar en Buscar" (ver cuarta imagen de la <Figura 26>), que controla si el nombre de la app aparecerá en los resultados de "Buscar".
- "Sugerir atajos": controla si iOS presentará al usuario atajos basados en el uso que hace de la app (ver apartado "9.4.1. Atajos (Shortcuts): automatización en iOS 13"). Está activa por defecto, **y se recomienda desactivarlo para apps de contenido sensible**.
 - "En la pantalla de bloqueo - Mostrar sugerencias de Siri": si el ajuste "Sugerir atajos" está activo, iOS permite al usuario evitar atajos a determinadas apps con la pantalla bloqueada. **Se recomienda desactivar este ajuste para todas las apps**.



Figura 26 - Menú "Siri y Buscar" y preferencias de búsqueda para la app "Contactos"

Desde el punto de vista de privacidad, se recomienda también desactivar "Aprender de esta app" para las apps de contenido sensible, a fin de que no se envíen a Apple datos de uso.

Por tanto, desde el punto de vista de seguridad, **se recomienda al usuario valorar qué contenidos no desea que se muestren en las búsquedas** y desactive el ajuste "Mostrar en Buscar" y "Sugerir atajos", para cada app individualmente. Adicionalmente, si no se desea enviar contenidos a Apple, **se recomienda desactivar todos los ajustes de la sección "Sugerencias de Siri" dentro de "Ajustes - Siri y Buscar"**.

9.3.1 FUNCIÓN DICTADO

El campo "Buscar" permite también búsquedas por voz, funcionalidad que se invoca presionando sobre el icono de micrófono situado a la derecha de la barra de búsqueda superior; la primera vez que se pulse el micrófono, iOS solicitará el permiso para "Activar Dictado", el cual envía datos a Apple (incluyendo voz, contactos y ubicación) durante las tareas de reconocimiento de voz. Se desaconseja el uso de esta funcionalidad por cuestiones de privacidad. Sin embargo, se constata que es posible conceder el permiso de activar la función de dictado para este propósito, incluso con el dispositivo móvil bloqueado, lo que activa el ajuste disponible en "Ajustes - General - Teclado - Activar dictado" hasta que el usuario lo desactive accediendo a dicho menú. Este comportamiento resulta inconveniente si el usuario del dispositivo no desea hacer uso de la búsqueda por voz, pero un tercero consigue acceso físico momentáneo al dispositivo y concede dicho permiso:



Figura 27 - Solicitud del permiso "Activar dictado"

Una vez el usuario deshabilita intencionadamente las capacidades de dictado desde el menú de ajustes indicado previamente, no es posible habilitarlo de nuevo desde el menú superior de búsqueda (esté la pantalla bloqueada o desbloqueada).

La función de dictado permite la introducción de texto mediante voz a través del teclado, en lugar de mediante la pulsación de las teclas, incluso sin conexión a Internet para los lenguajes disponibles. Estas capacidades, junto a las de búsqueda, pueden ser ampliadas a través del asistente digital personal Siri, para disponer de capacidades de interacción por voz avanzadas con el dispositivo móvil.

NOTA: Toda la información que se registre a través de la funcionalidad "Consultar a Siri" se enviará a Apple, incluyendo datos personales (como contactos, dispositivos asociados al usuario, relaciones entre éste y sus contactos, nombres de álbumes de fotos, etc.). Para más información, se recomienda seleccionar el texto ""Consultar a Siri", Dictado y privacidad..." de esta sección.

Desde el punto de vista de privacidad, se aconseja desactivar las opciones "Activar al oír 'Oye Siri'" y "Botón de Inicio para abrir Siri" **del menú** "Ajustes - Siri y Buscar"¹⁷ y "Ajustes - General - Teclado - Activar dictado" (ver primera imagen de la <Figura 26>).

9.4 TODAY VIEW (VISTA DE HOY)

Recomendaciones de seguridad:

- Excluir de la "Vista de hoy" los widgets que incluyen contenido sensible (como "Próximamente", "Mail" o "Archivos").
- No importar "Atajos" de fuentes externas.

La "Vista de hoy" ("Today View") es una vista de la pantalla de inicio que presenta la información asociada al día en curso procedente de diferentes apps, a la que se accede deslizando el dedo de izquierda a derecha. Está formada por una serie de "widgets", que proporcionan una vista rápida a contenidos de apps, tanto con la pantalla bloqueada como desbloqueada:



¹⁷ En iPhone X y modelos posteriores, al no disponer de botón de inicio (y Touch ID), las opciones a desactivar son "Pulsar el botón lateral para abrir Siri" y "Activar al oír 'Oye Siri'".

Figura 28 - Today View

Es posible personalizar esta vista mediante el botón "Editar", que solicitará el método de acceso si se invoca con la pantalla bloqueada. Al "Editar", se abrirá el menú "Añadir widgets", que permite suprimir mediante "⊖" y añadir mediante "⊕". Para modificar el orden de presentación en la pantalla "Today", se debe pulsar mediante "haptic touch" en el símbolo de líneas horizontales y desplazarlo a la posición deseada (ver <Figura 29>).

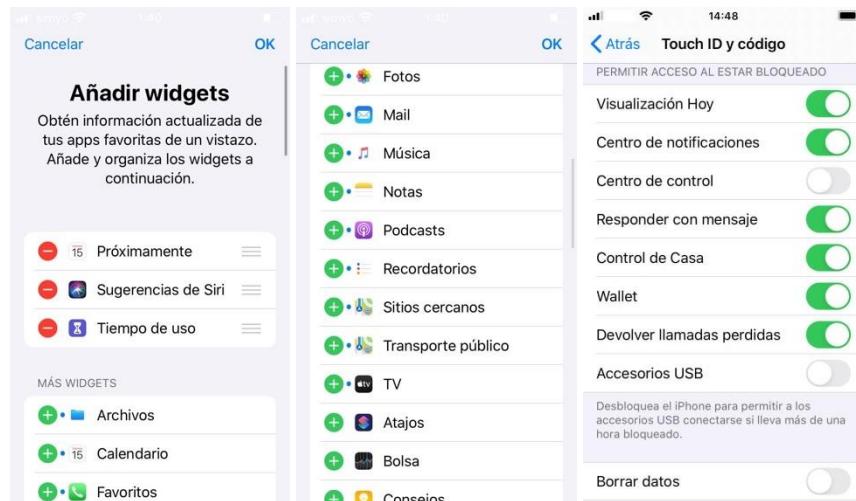


Figura 29 - Personalización de los elementos ("widgets") de la "Vista de hoy"

Desde el punto de vista de privacidad, **se recomienda no incluir** "widgets" en la "Vista de hoy" **cuyos contenidos puedan revelar información sensible del usuario** (por ejemplo, "Notas" o "Próximamente").

Para inhabilitar completamente la funcionalidad "Vista de hoy" en la pantalla de bloqueo, se debe desactivar el interruptor "Ajustes - Touch ID y código - [Permitir acceso al estar bloqueado] Visualización Hoy" (tercera imagen de la <Figura 29>).

9.4.1 ATAJOS (SHORTCUTS): AUTOMATIZACIÓN EN IOS 13

"Atajos" (anteriormente disponible como app en la App Store) es una funcionalidad de automatización que Apple ha integrado en iOS 13 a nivel de sistema. Un "atajo" está formado por un conjunto de acciones cuyo objetivo simplificar tareas rutinarias. La funcionalidad "Atajos" está estrechamente ligada a la automatización, ya que cualquier app puede actuar como disparador para iniciar una secuencia de acciones. Comprende dos tipos de automatización:

- De casa: integradas en la app "Casa", para domotización de dispositivos compatibles con HomeKit¹⁸ (fuera del alcance de la presente guía).
- Personales: destinadas a la automatización de tareas específicas del usuario y el propio dispositivo móvil.

Hay diversas formas de crear un "atajo":

- A través de las sugerencias del asistente personal Siri (si está habilitado), ya que Siri, en base a su análisis sobre el uso que se hace del dispositivo, sugiere atajos sencillos.

¹⁸ <https://developer.apple.com/homekit/>

- Mediante la app "Atajos", que, además de disponer de una galería con atajos, permite definir atajos propios. Para crear un atajo propio desde la app, se debe entrar en el menú "Automatización" (ícono "⚙") y:
 - Añadir el "activador", que actúa como disparador de la secuencia de acciones del atajo cuando se cumple su condición (una hora concreta, un cambio en algún ajuste del dispositivo, un cambio de ubicación). Aparecerá en el campo "Cuando" del atajo.
 - Añadir las "acciones" a ejecutar (aparecen en el campo "Hacer" de la automatización). En función del tipo de acción, se pueden elegir variables a las que asignar valores (segunda imagen de la <Figura 31>).
 - Decidir si la ejecución del atajo requiere confirmación por parte del usuario o si puede iniciarse automáticamente: está controlado por el interruptor "Solicitar confirmación". Si está activo, iOS enviará una notificación antes de lanzar la ejecución del atajo para que el usuario la autorice (cuarta imagen de la <Figura 31>).
 Es importante reseñar que determinadas automatizaciones personales requieren confirmación del usuario para ejecutarse (ver [Ref.- 66]). En esos casos, cuando se detecta la condición, iOS mostrará una notificación desde la que el usuario puede lanzar la acción asociada al atajo.
- El ícono "⚙" (configuración del atajo) permite seleccionar en qué escenarios estará disponible el atajo (tercera imagen de la <Figura 31>):
 - Pantalla de inicio: el atajo se mostrará como un ícono de app en la pantalla "Home".
 - Mostrar en el widget: para permitir que el atajo se presente dentro del widget asociado a la app "Atajos".
 - Mostrar al compartir: permitir que el atajo aparezca en el menú de opciones rápidas de compartición ("⚠"): ver apartado "13.3. Compartir".
 - Si se desea compartir un atajo con otros usuarios de iCloud y el atajo contiene variables con información personal o específica del usuario, se dispone de la opción "Preguntas de importación"; estas preguntas se presentarán al usuario durante la ejecución del atajo, y las respuestas que proporcione constituirán el contenido de las variables con información personal.
- Importando atajos de fuentes externas (desaconsejado desde el punto de vista de seguridad).

La <Figura 30> ilustra un atajo para lanzar la app "Mapas" con una ubicación predeterminada.

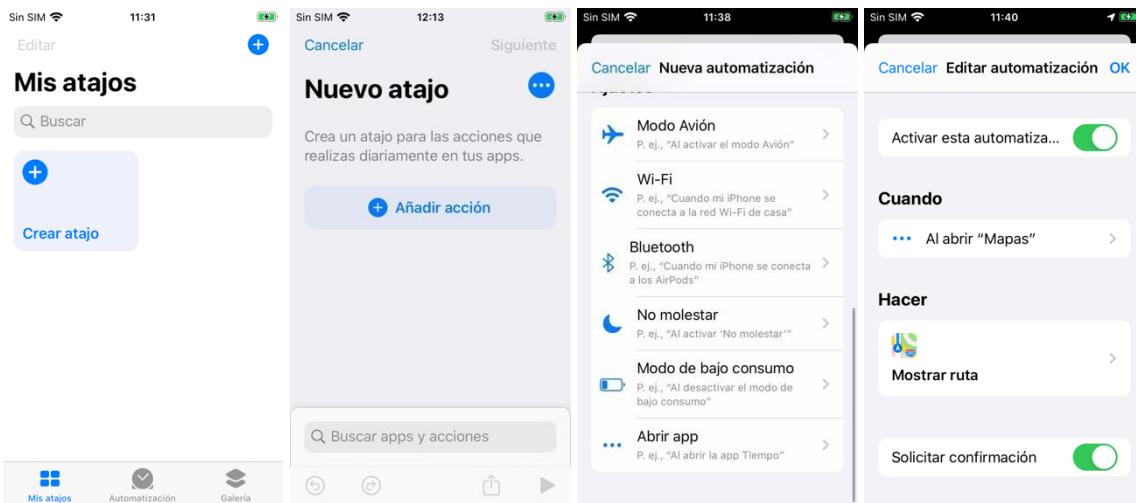


Figura 30 - Creación de "atajos"

En la pantalla "Vista de Hoy" aparece por defecto el widget asociado a la app "Atajos", desde el cual es posible iniciar la ejecución de atajos existentes y la creación de nuevos (ver segunda imagen de la <Figura 28>).



Figura 31 - Opciones de un "atajo"

Los ajustes de sistema asociados a "Atajos" están disponibles en "Ajustes - Atajos". **Se aconseja mantener desactivada la opción "Permitir atajos no fiables"**, que permitiría añadir atajos creados por terceros, a menos que se tenga certeza sobre su confiabilidad. Si se precisase importar uno de estos atajos, se deberá deshabilitar la opción una vez finalice la importación.



Figura 32 - Configuración de "Atajos"

"Atajos" soporta utilización de etiquetas NFC¹⁹ como disparador de automatizaciones, y está estrechamente relacionado con Siri, quien tiene capacidad para ejecutar el atajo como parte de su actividad como asistente personal.

Si se lanza un atajo de los disponibles en el "widget" de la "Vista de Hoy" desde la pantalla de bloqueo, puede ocurrir:

¹⁹ Para modelos iPhone XS y XR a fecha de elaboración de la presente guía: <https://appletoolbox.com/everything-you-need-to-know-about-shortcuts-automations-in-ios-13-1/>

- Que el atajo se ejecute por completo: únicamente si las acciones asociadas al atajo pueden ser invocadas con el dispositivo bloqueado, como cursar una llamada de teléfono a un contacto concreto.
- Que se solicite al usuario introducir el método de acceso: en caso de que el atajo implique ejecutar una acción no permitida con el dispositivo bloqueado, tras validarse el método de acceso se mostrará la ventana de la ejecución de la acción correspondiente al atajo (por ejemplo, el atajo disponible "Compartir ubicación", que envía un mensaje con la ubicación actual del dispositivo a un contacto, ilustrado en la <Figura 33>).



Figura 33 - Atajo "Compartir ubicación"

Los atajos de la app "Atajos" pueden sincronizarse entre los dispositivos vinculados a una misma cuenta de iCloud, y se almacenan cifrados en el almacenamiento local²⁰.

Para obtener información detallada sobre el uso de atajos, consultar la [Ref.- 32].

Desde el punto de vista de seguridad, el uso de atajos presenta:

- Ventajas:
 - Permite la ejecución de tareas predefinidas sin tener que introducir información sensible en el dispositivo, lo cual puede resultar conveniente para evitar que terceros con acceso visual al terminal puedan captar información.
 - Permite automatizar acciones útiles para casos de emergencia, como compartir ubicación.
- Desventajas:
 - Un tercero con acceso temporal al dispositivo en estado desbloqueado podría ejecutar tareas potencialmente sensibles con un simple toque.

Nota: Un ejemplo interesante de la funcionalidad "Atajos" es que permite ejecutar acciones automáticas sobre el interfaz Wi-Fi (algo que no estaba disponible en versiones anteriores de iOS): por ejemplo, activarlo/desactivarlo en función de la localización (si bien para esta acción

²⁰ Secure features in Shortcuts app. <https://support.apple.com/guide/security/secure-features-in-shortcuts-app-secec043bdae/web>

concreta es preciso que Siri se encuentre habilitado)²¹. Dado que las automatizaciones Wi-Fi requieren confirmación del usuario previa a la ejecución, estos atajos notificarán al usuario para que acepte/rechace la acción.

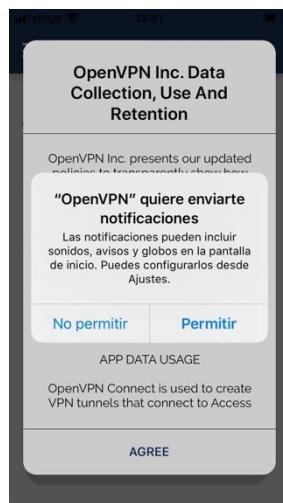
9.5 CENTRO DE NOTIFICACIONES

Recomendaciones de seguridad:

- Eliminar el "Centro de Notificaciones" de la pantalla de bloqueo desactivando el interruptor "Ajustes - Touch ID y código - [Permitir acceso al estar bloqueado] "Centro de Notificaciones"".
- Activar la opción "Ajustes - Notificaciones - Mostrar previsualizaciones - [Nunca] o [Si está desbloqueado]".
- En caso de no desearse prescindir de la funcionalidad del "Centro de Notificaciones", establecer restricciones para las notificaciones para las apps de contenido sensible.
- Revisar y limitar según sea posible la configuración de notificaciones para las apps suministradas de fábrica con iOS 13.

El denominado "Centro de Notificaciones" es un panel que se presenta al deslizar el dedo de abajo hacia arriba desde cualquier pantalla, y en el que se visualizan las notificaciones enviadas por las apps o el sistema operativo. La aparición de las notificaciones en la pantalla de bloqueo puede controlarse desde el interruptor "Ajustes - Touch ID y código - [Permitir acceso al estar bloqueado] Centro de Notificaciones" (ver última imagen de la <Figura 22>). Debido a la potencial sensibilidad de los contenidos de ciertas notificaciones, **Se aconseja desde el punto de vista de seguridad y privacidad deshabilitar esta opción, que, aunque afecte a la funcionalidad del dispositivo móvil, evita que un tercero no autorizado pueda acceder a todos los detalles de las notificaciones existentes con solo disponer de acceso temporal visual al dispositivo móvil.**

Cuando se abre por primera vez una app instalada por el usuario (las apps suministradas de fábrica con iOS 13 ya traen el permiso de notificación definido y activo por defecto), se solicitará al usuario consentimiento antes de que la app pueda enviarle notificaciones:



²¹ How to Automatically Turn Off iPhone or iPad Wi-Fi When You Leave Home: <https://www.igeeksblog.com/how-to-automatically-turn-off-iphone-ipad-wifi/>

Figura 34 - Solicitud de permiso para envío de notificaciones

Las notificaciones se ordenan cronológicamente, apareciendo las más recientes y que no se han visto aún en la parte superior de la pantalla, seguidas de las recibidas hoy que se han visto pero no se han procesado y, por último, de las recibidas en días previos.

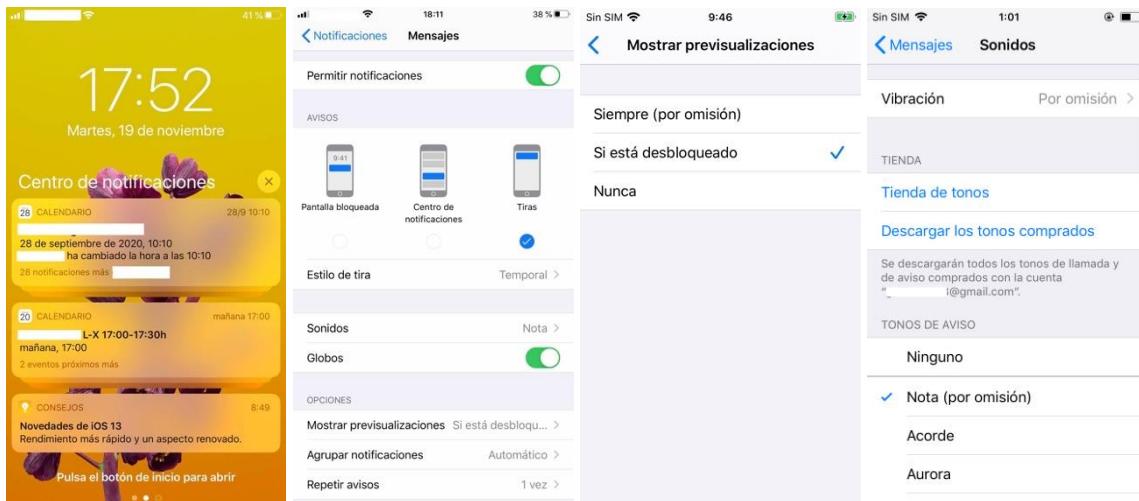


Figura 35 - Centro de Notificaciones y configuración de notificaciones a nivel de app

La sección "Ajustes - Notificaciones" permite una gestión más granular de las notificaciones:

- "Mostrar previsualizaciones": establece el comportamiento por defecto del "Centro de Notificaciones" para todas las apps. Se puede fijar a "Siempre" (desaconsejado), "Si está desbloqueado" (opción de compromiso) o "Nunca" (opción recomendada).
- Control granular por app del comportamiento de las notificaciones: seleccionando la entrada de una app concreta en la sección "Estilo de notificación" y marcando/desmarcando el "🕒" bajo "Pantalla bloqueada" (Imagen 2 de la <Figura 35>) y seleccionando "Mostrar previsualizaciones - Si está desbloqueado". Desde el punto de vista de seguridad, se recomienda aplicar esta recomendación especialmente para las apps de contenido potencialmente sensible (por ejemplo, Mensajes). Si se utilizan apps que comunican eventos de seguridad, como apps de banca, la recomendación es:
 - Habilitar "🕒" bajo "Pantalla bloqueada" para permitir detección de usos no autorizados.
 - Seleccionar "Mostrar previsualizaciones - Si está desbloqueado" para que el contenido de la notificación no permita revelar información sensible.

iOS permite agrupar las notificaciones procedentes de una misma app en una pila, con lo que pueden procesarse o eliminarse individualmente o en conjunto, a través del ajuste "Ajustes - Notificaciones - [Nombre de la app] - [Opciones] Agrupar notificaciones". Adicionalmente, las notificaciones de algunas apps pueden acompañarse de un sonido y/o una vibración, pero se permite al usuario controlar este comportamiento a través de los ajustes "Sonidos - Vibración" y "Sonidos - Tonos de aviso" (ver <Figura 35>).

Al deslizar el dedo de izquierda a derecha sobre una notificación (o una pila de notificaciones), se mostrarán tres opciones: "Gestionar", "Ver" y "Borrar". La opción "Gestionar" permite cambiar los ajustes de la notificación, por ejemplo, para que se desactive o se convierta en una notificación discreta (ver imagen derecha de la <Figura 36>). La pulsación corta sobre la notificación invoca una acción asociada a la misma, como puede ser devolver una llamada, o responder brevemente a un mensaje.



Figura 36 - Gestión de notificaciones en iOS 13

Las notificaciones se silencian si el modo "No Molestar" está activo.

Como parte de la funcionalidad "Tiempo de uso", se ofrecen estadísticas de notificaciones, que permiten al usuario analizar qué apps son las que más emiten y en qué franjas horarias (ver apartado "18.4. Tiempo de uso").

9.6 MODO "NO MOLESTAR"

Recomendaciones de seguridad:

- Activar "No molestar" ante situaciones en las que la recepción de notificaciones o llamadas inoportunas pueden comprometer la seguridad o privacidad del dispositivo o el usuario (como la recepción de un código de seguridad en presencia de terceros).
- Si se hace uso del modo "No molestar al conducir", valorar el uso de la opción "Respuesta automática a".

El modo "no molestar", configurable desde el menú "Ajustes - No molestar" tiene por objeto silenciar las llamadas y los avisos que se reciban con el dispositivo bloqueado. Las notificaciones irán directamente al "Centro de Notificaciones", sin presentarse en la pantalla de bloqueo, y no se recibirán en la pantalla de inicio cuando se salga de este modo. iOS 13 mantiene el concepto de "alerta crítica" que introdujo iOS 12, son notificaciones que solo pueden generarse por determinadas apps²² (como apps de salud o seguridad física) y que no se suprimen en el modo no molestar.

El modo "No molestar" se puede habilitar de forma rápida pulsando el icono de luna disponible en el "Centro de Control" (ver <Figura 22>), y se indica en la barra de estado mediante el símbolo . Mediante una pulsación larga sobre el símbolo "No molestar" del "Centro de Control", es posible gestionar la duración de este modo. Si la ubicación está activada, se presentará la opción "Hasta que me vaya de aquí" (que incluye una referencia a la ubicación actual). En caso contrario, las opciones disponibles son las de la última imagen de la <Figura 37>.

²² Solo las apps que obtengan certificación de Apple pueden hacer uso de alertas críticas.



Figura 37 - Configuración del modo "No molestar"

Es posible establecer comportamientos excepcionales que alteran el modo "No molestar":

- "Permitir llamadas de: Favoritos | Nadie | Contactos | Todos": para determinar si las llamadas de teléfono se permitirán o por parte de quién. Los números de teléfono que queden fuera de la categoría aquí definida recibirán la señal de "Usuario ocupado".
- "Llamadas repetidas": determina si la recepción de llamadas sucesivas por parte de un mismo interlocutor se saltarán el modo "no molestar".
- "Modo "No molestar al conducir"": para entrar en modo "No molestar" si se detecta una condición de conducción (por ejemplo, si el iPhone se conecta al Bluetooth del coche). El modo "No molestar al conducir" se puede añadir como control al "Centro de Control" (ver apartado "9.2. Centro de Control").
- "Responder con": permite establecer un mensaje (configurado en la sección) que el dispositivo móvil enviará automáticamente a los números seleccionados dentro de la opción "Respuesta automática a". Es importante reseñar que la recepción de un mensaje que contenga el texto "urgente" por parte de un favorito que haya recibido a su vez la respuesta automática invalidará el modo "No molestar" para sus llamadas posteriores.

Desde el punto de vista de seguridad y privacidad, este modo resulta útil en diversas situaciones, por ejemplo, para prevenir accidentes derivados de distracciones al atender llamadas mientras se conduce, o para evitar que un sonido asociado a una notificación se reciba en una situación inoportuna, como una reunión o una visita médica.

9.7 MENÚS CONTEXTUALES

Los menús contextuales son accesos directos que permiten el acceso a funcionalidad específica dentro de una app o de un elemento que se encuentra en primer plano sin tener que cambiar el contexto ni interferir con su interfaz [Ref.- 46]. Algunos elementos en los que dispone de menús contextuales son la pantalla de inicio, el "Centro de Control", el "Centro de Notificaciones" y dentro de las apps.

Algunas de las funciones disponibles a través de estos menús son:

- Despliegue del menú de redes Wi-Fi disponibles desde el icono "Wi-Fi" del Centro de Control.
- Despliegue de los dispositivos Bluetooth conocidos desde el icono "Bluetooth" del Centro de Control.

- Expansión de opciones disponibles para las notificaciones.
- Previsualización de mensajes de correo.
- Edición de la pantalla de inicio.
- Compartición de apps.
- Activación de la visualización de movimiento en "Live Photos".
- Y un largo etcétera.



Figura 38 - Ejemplo de acciones "Haptic Touch"

Los menús contextuales más sensibles requieren introducir el método de acceso al dispositivo si el usuario trata de abrirlos desde la pantalla de bloqueo.

Los menús contextuales de iOS 13 se apoyan en la funcionalidad "Haptic Touch" (*haptic* = táctil), un sistema de detección de la presión con el que se está pulsando sobre una determinada zona de la pantalla, a fin ofrecer acciones específicas. A diferencia de "3D Touch" (al que ha reemplazado en iOS 13), no requiere de sensores *hardware* específicos, ya que se implementa exclusivamente por *software*, por lo que está disponible para todos los dispositivos, y no solo para los que disponían del sensor.

Haptic Touch no es capaz de detectar diferentes niveles de presión (algo que sí permitía "3D Touch"), por lo que las funciones "Peek" y "Pop" dejan de estar disponibles²³.

A lo largo de la presente guía se hará referencia a "*haptic touch*" para indicar que la opción correspondiente se obtiene al realizar una pulsación sostenida sobre el elemento.

No están claras las razones por las que Apple ha decidido prescindir de "3D Touch" en los modelos de iPhone que cuentan con sensores de presión, que resultan más específicos y pueden permitir mayor variedad de acciones en función de la presión de la pulsación.

10. CONFIGURACIÓN DEL DISPOSITIVO MÓVIL: MENÚ "AJUSTES"

La configuración actual del dispositivo móvil se puede consultar y modificar desde el menú "Ajustes" (Settings) representado con un símbolo de engranaje en la pantalla de inicio, que consta de diversas secciones que se pueden recorrer deslizando el dedo hacia la parte superior de la pantalla del terminal. El símbolo ">" a la derecha de cada ajuste proporciona acceso al resto de elementos asociados a su configuración:

²³ <https://developer.apple.com/design/human-interface-guidelines/ios/user-interaction/3d-touch/>

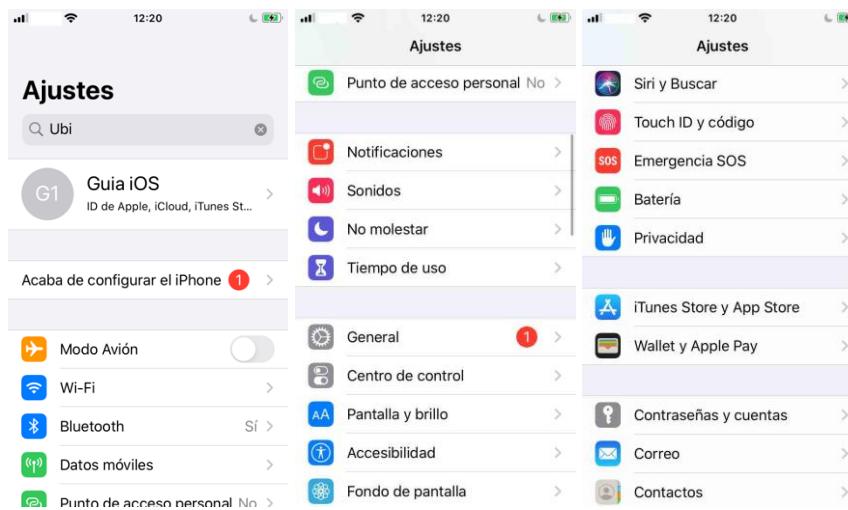


Figura 39- Menú "Ajustes" de iOS 13 (1)

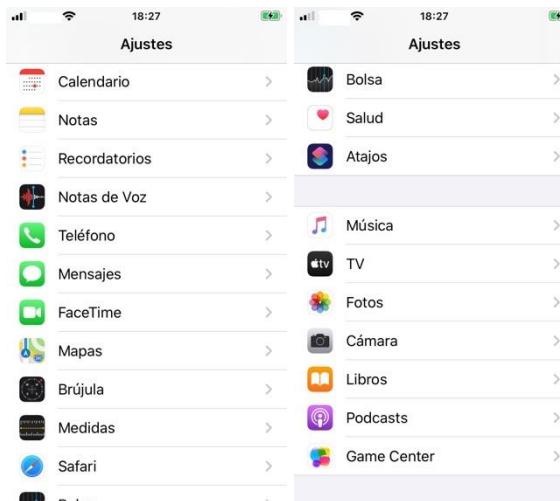


Figura 40 - Menú "Ajustes" de iOS 13 (2)

A lo largo de los sucesivos apartados se describirán los ajustes relacionados con la seguridad y privacidad, correspondientes a las distintas secciones que integran este menú.

Adicionalmente, se recomienda definir los siguientes ajustes desde el punto de vista de seguridad (no se incluyen en un apartado propio por ser muy concretos):

Sonidos

- "Clics del teclado" (activa por defecto): **se aconseja desactivar esta opción**, que ocasiona la emisión de un sonido cuando se pulsa una tecla, incluso al introducir contraseñas o el propio código de acceso. Un potencial atacante podría conocer la longitud de la contraseña contando el número de *clics*, disminuyendo así el espectro de prueba en ataques de diccionario o fuerza bruta.
- "Sonido al desbloquear" (activa por defecto): **se aconseja desactivar esta opción**, que ocasiona la emisión de un sonido cuando se desbloquea el iPhone, para evitar que un potencial atacante conozca la condición de dispositivo desbloqueado.
- "AirDrop": **se aconseja definir un sonido** (sirve la "pulsación", definida por defecto), para identificar más fácilmente los intentos de transferencia de archivos.

Batería

- "Porcentaje de la batería": estando activo, hará que la barra de estado incluya el porcentaje de batería disponible. **Se aconseja activar el interruptor** para tener mayor control cuándo se debe conectar el dispositivo a la corriente eléctrica. En caso de pérdida del dispositivo móvil, si la batería se agota, será imposible utilizar el servicio "Buscar mi iPhone" para localizarlo.
- "Modo de bajo consumo": tiene por objeto reducir el consumo de la batería, para lo cual, estando activo, minimiza la actividad de las apps en segundo plano y las actualizaciones automáticas de datos de servicios (entre otros, los correspondientes a la sección "Obtener datos" del menú "Contrasenas y cuentas" descrito en el apartado "11.4.1. Cuentas"), y fija algunos ajustes del dispositivo a valores que no se pueden modificar, por ejemplo, el bloqueo automático de pantalla (que entrará en acción transcurridos 30 segundos de inactividad).

Este modo entra en funcionamiento de forma automática cuando el nivel de batería desciende hasta el 20%, y se desactiva de forma automática cuando llega al 80%. **Se recomienda hacer uso de este interruptor para disminuir el tiempo de carga**, así como si se prevé que no se podrá recargar la batería antes de que se agote por completo, entre otras razones para no perder el acceso a la funcionalidad "Buscar mi iPhone". Es posible incluir un acceso directo a este modo en el "Centro de Control".

Cuando el modo de bajo consumo está activo, la pantalla del iPhone se bloqueará automáticamente tras.

- "Uso de la batería por apps/Mostrar actividad": permite visualizar el consumo que las apps hacen de la batería. Puede resultar útil para identificar comportamientos no usuales (por ejemplo, procesos que ejecutan en segundo plano y consumen muchos recursos, que pueden resultar potencialmente maliciosos o, simplemente, tener un fallo de funcionamiento o programación).
- "Carga optimizada": esta funcionalidad se introduce in iOS 13 con el objetivo de prolongar la vida de las baterías de litio suministradas con los iPhone. Esta funcionalidad persigue que la carga del dispositivo móvil quede al 80% en términos generales, y solo continúe cargando hasta el 100% cuando el algoritmo determine que el usuario va a necesitar llegar al máximo nivel de carga. Dado que este algoritmo aplica técnicas de aprendizaje, puede llevar semanas hasta que la funcionalidad se active en el dispositivo [Ref.- 34].



Figura 41 - Ajustes de Sonidos y Batería

Pantalla y brillo

- "Bloqueo automático": determina el periodo de inactividad tras el cual la pantalla del dispositivo móvil se suspenderá. **Se recomienda fijarlo a un valor de entre 1 y 2 minutos.** Si el modo de ahorro de batería está activo, este valor se establece automáticamente a 30 segundos, y no es posible modificarlo.
- [Aspecto]: iOS 13 introduce el "modo oscuro", en el que tanto las pantallas del sistema operativo como las de las apps que soporten este modo aparecerán en negro con texto claro. Aunque la funcionalidad persigue mejorar la visibilidad en entornos de escasa luminosidad, desde el punto de vista de seguridad puede resultar conveniente recurrir a este modo para dificultar el acceso visual de terceros. El modo oscuro se puede habilitar desde el "Centro de Control" si se añade el control "Modo oscuro" (⌚) (ver apartado "9.2. Centro de Control").

Fondo de pantalla

Se desaconseja establecer un fondo de pantalla para la pantalla de bloqueo que revele información personal del usuario, como fotografías familiares.

iOS no dispone de la funcionalidad de Android "Ajustes - Seguridad y ubicación - Ajustes pantalla de bloqueo - Mensaje en la pantalla de bloqueo", que muestra un mensaje cuando el dispositivo está bloqueado en el que se puede añadir un número de respaldo al que se puede recurrir si el dispositivo se extravía y la persona que lo encuentra desea devolverlo. Por tanto, puede ser recomendable crear una imagen que contenga esa información y fijarla como fondo de pantalla de bloqueo.

Accesibilidad

Se desaconseja el uso de funciones de accesibilidad salvo que la condición del usuario las requiera, debido a que incrementan la superficie de exposición del dispositivo ante ataques y a que han sido objeto de múltiples vulnerabilidades a lo largo de las diferentes versiones de iOS.

11. CUENTAS ASOCIADAS AL DISPOSITIVO MÓVIL

La utilización de dispositivos móviles al margen de la vinculación con uno o varios tipos de cuentas de usuario es, en la actualidad, un escenario poco común, debido a que la mayor parte de servicios demandados por los usuarios se ofrece por mediación de dichas cuentas.

Todos los detalles asociados a las cuentas vinculadas a servicios de Apple en el dispositivo móvil se detallan en el apartado "Cuentas asociadas a los servicios de Apple" de la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]. Debido a la extrema importancia de estas cuentas tanto desde el punto de vista de seguridad como de privacidad, **se aconseja aplicar las recomendaciones de seguridad descritas en dicho apartado.**

11.1 ID DE APPLE

El ID de Apple (o Apple ID) es la cuenta de usuario necesaria para acceder a los servicios de Apple, incluyendo diversas aplicaciones y productos de Apple, como la App Store, FaceTime, Buscar mi iPhone o iCloud. Consta de una dirección de correo electrónico y una contraseña. Al añadir el ID de Apple, el dispositivo podrá acceder a la configuración automática de servicios vinculados a esta cuenta.

El Apple ID actúa como un vínculo entre todos los dispositivos Apple del usuario.

El Apple ID se define normalmente durante el proceso de activación del dispositivo (ver apartado "7. Proceso de activación del dispositivo móvil"), aunque puede omitirse durante este proceso y configurarse más tarde. En este último caso, el menú "Ajustes" mostrará la primera imagen de la <Figura 42>.



Figura 42- Menú "Ajustes" sin y con sesión asociada al ID de Apple

11.1.1 INICIAR SESIÓN CON APPLE

iOS 13 introduce una nueva funcionalidad, denominada "Iniciar sesión con Apple" (*Sign in with Apple*)²⁴, que permite al usuario utilizar su ID de Apple (siempre que éste disponga de autenticación de doble factor) para iniciar sesión en los servicios de apps y sitios web que soporten este tipo de acceso en vez de tener que crear un nuevo perfil de usuario.

Según indica Apple en su página web de soporte [Ref.- 43], el principal beneficio de esta funcionalidad es proteger la privacidad del usuario, ya que evita que las apps y sitios web puedan rastrearle. Adicionalmente, para aquellos sitios/apps 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.- 44], 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.

Para más información sobre este nuevo servicio, consultar la Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413].

11.2 CUENTA DE ICLOUD

La cuenta de iCloud (únivamente ligada al ID de Apple) sirve como almacén de los datos asociados a servicios de Apple como "Fotos", "Contactos" y "Copia de seguridad en iCloud".

Desde el punto de vista de seguridad, la principal funcionalidad de la cuenta de iCloud es el servicio "Buscar", que permite realizar tareas de gestión remota de un dispositivo, como determinar su ubicación en caso de extravío o borrar sus contenidos. Los detalles de uso y configuración de la cuenta de iCloud se detallan en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413], pero en el apartado "23. Anexo A - Cuenta de iCloud" se incluyen los aspectos más relevantes del servicio "Buscar" en iOS 13.

11.3 CUENTA DE ITUNES & APP STORE

Esta cuenta se utiliza para el almacén de contenidos en iTunes (Store) y para la tienda oficial de Apple (App Store), pudiendo estar vinculada en iOS con un ID de Apple diferente del empleado

²⁴ El mecanismo "Sign in with Apple" está basado en OAuth 2.0 (https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth) y OpenID Connect (https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth)

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

En el caso habitual de que el ID de Apple esté asociado a la cuenta de iTunes, se podrá acceder al interfaz web para móviles appleid.apple.com desde el menú "Ajustes - iTunes Store y App Store - [Pinchar sobre la entrada <ID de Apple>] - Ver ID de Apple". Para poder hacer uso de los servicios de contenidos es preciso que el usuario defina una dirección y un número de teléfono en su cuenta de Apple. Si alguno de estos datos no estuviese definido, cuando se intente acceder a contenido de iTunes o App Store con un nuevo ID de Apple se informará al usuario (a fecha de elaboración de la presente guía, Apple no confirma la veracidad de estos datos personales).



Figura 43 - Gestión del ID de Apple desde el menú "iTunes Store y App Store"

Si el único método de desbloqueo del dispositivo es la contraseña, se dispone del menú "Ajustes de contraseña" (primera y segunda imagen de la <Figura 44>). Desde el punto de vista de seguridad, *se recomienda activar las opciones "Solicitar siempre" y "[Descargas gratuitas] Solicitar contraseña" para poder tener control de qué contenidos se instalan en el dispositivo*. La modificación de cualquier campo de esta sección requerirá que la sesión en la cuenta de iTunes/App Store se encuentre activa. Si está habilitado el acceso mediante biometría (por ejemplo, "Touch ID") (tercera imagen de la <Figura 44>), se requerirá validación siempre utilizando dicho método.



Figura 44 - Ajustes de la cuenta de iTunes y App Store

Se aconseja desmarcar las opciones "Reproducción automática de vídeo" y "Valoraciones dentro de la app" salvo que se requiera expresamente hacer uso de ellas.

En el apartado "0. App Store" se describen opciones de esta sección relativas a la App Store.

11.4 SECCIÓN "CONTRASEÑAS Y CUENTAS"

Recomendaciones de seguridad:

- Bloquear el acceso a la sección "Contraseñas y cuentas" estableciendo una restricción para evitar la adición/eliminación/modificación de cuentas en el dispositivo.
- Valorar la utilización de un gestor de contraseñas para almacenar credenciales.

La sección "Contraseñas y cuentas" es un elemento crítico del dispositivo móvil, ya que alberga la configuración de todas las cuentas que se hayan dado de alta en él, incluyendo la cuenta de iCloud, así como las contraseñas que el usuario haya almacenado en el gestor de contraseñas proporcionado por defecto en iOS. Por tanto, se recomienda establecer una restricción (ver apartado "18.4.2. Restricciones"), concretamente a través del ajuste "Ajustes - Tiempo de uso - Contenido y privacidad - [Permitir cambios] Cambios en la cuenta" para impedir que un tercero pueda realizar modificaciones en las cuentas. Lamentablemente, en iOS 13, no existe ninguna forma de imponer restricciones para el acceso a contenidos de contraseñas.

A continuación se describe los ajustes asociados a "Cuentas"; la información relativa a "Contraseñas" se detalla en el apartado "15. Gestión de contraseñas".



Figura 45 - Menú "Contraseñas y cuentas" de iOS 13

11.4.1 CUENTAS

La gestión de cuentas, tanto la vinculada a iCloud como a servicios de terceros, se realiza a través de la sección "Ajustes - Contraseñas y cuentas".

- "iCloud": es una forma de acceso alternativa al menú descrito en el apartado "23.1.2. Interfaz móvil" para la gestión de la cuenta de iCloud necesaria para el uso de servicios de Apple.

- "Añadir cuenta": permite la gestión de cuentas vinculadas a servicios de terceros asociados a correo electrónico, contactos y calendarios.

Es posible bloquear la adición de nuevas cuentas en el dispositivo móvil estableciendo una restricción (ver apartado "18.4.2. Restricciones"), concretamente a través del ajuste "Ajustes - Tiempo de uso - Contenido y privacidad - [Permitir cambios] Cambios en la cuenta".

Se recomienda establecer este parámetro a "No permitir" para fijar esta restricción como medida de seguridad.

El ajuste "Obtener datos" (segunda imagen de la <Figura 45>) permite configurar el mecanismo de actualización de nuevos datos de las apps asociadas a cuentas del dispositivo, siendo posible activar el modo "push" (si una cuenta soporta este modo, el servicio será notificado por parte del servidor correspondiente de los cambios acaecidos) o establecer un intervalo para que las apps que hagan uso de una cuenta consulten de forma activa al servidor sobre cambios en los datos. Si el modo "push" está inhabilitado, el valor de "Obtener" es, por defecto, "Automáticamente". Si se fija el valor a "Manualmente", los datos de una cuenta solo se actualizarán por parte de una app vinculada a ella cuando la app esté en uso. También es posible fijar valores de actualización manual para cada cuenta concreta. La configuración de "Obtener" no tiene implicaciones desde el punto de vista de seguridad, pero sí afecta al consumo de batería del dispositivo.

11.5 DISPOSITIVOS ASOCIADOS A LA CUENTA

Tras la configuración en el iPhone del ID de Apple, el dispositivo se añadirá como dispositivo de confianza a la cuenta de iCloud. Para obtener los detalles sobre el papel de los dispositivos de confianza, consultar el "23. Anexo A - Cuenta de iCloud".

12. COMUNICACIONES DEL DISPOSITIVO MÓVIL

12.1 CONEXIONES INALÁMBRICAS Y REDES

Recomendaciones de seguridad:

- Deshabilitar los interfaces inalámbricos siempre que no se requiera utilizarlos.

Las conexiones inalámbricas (Bluetooth, datos móviles y Wi-Fi) dotan al dispositivo móvil de capacidades de comunicación. Su gestión se puede realizar desde el menú "Ajustes", y también a través del "Centro de Control" (ver apartado "9.2. Centro de Control"), y el estado de cada una de ellas se puede consultar en la barra superior de estado (ver apartado "9.1. Barra superior de estado"), incluso con la pantalla bloqueada.

La opción "Restablecer ajustes de red" del menú "Ajustes - General - Restablecer" (ver <Figura 111>), permite restituir los ajustes de fábrica asociados a los interfaces de comunicaciones en el dispositivo sin afectar al resto de los datos del usuario.

12.1.1 MODO AVIÓN

El "modo avión" de iOS es un ajuste que, al activarse, deshabilita los interfaces Wi-Fi, Bluetooth y datos móviles. Se localiza en el menú principal de ">" (ver <Figura 39>) y se representa en el "Centro de Control con el icono  (en color naranja cuando el modo está activo).

En modo avión, el dispositivo móvil carece por completo de conectividad. La conectividad a redes Wi-Fi o Bluetooth puede ser habilitada a mano posteriormente y de forma independiente, pero no así la conectividad ni de telefonía móvil (voz y SMS/MMS) ni de datos móviles 2/3/4G.

Para salir del modo avión, se puede pulsar de nuevo el ícono del "Centro de Control" o desactivar el interruptor "Modo avión". iOS restaurará el estado de los interfaces de telefonía, de datos móviles, Wi-Fi y Bluetooth al estado que tuvieran antes de entrar en vigor el modo avión, sin requerirse volver a introducir el PIN de la tarjeta SIM.

Desde el punto de vista de seguridad, el modo avión implica que el dispositivo perderá toda capacidad de comunicación, por lo que la funcionalidad "Buscar mi iPhone" (ver apartado "23.3. Servicios "Buscar") no estará disponible; éste es uno de los motivos por los que se desaconseja que el "Centro de Control" esté accesible en la pantalla de bloqueo.

12.1.2 BLUETOOTH

Recomendaciones de seguridad:

- Desactivar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo.
- Desvincular los dispositivos Bluetooth de los que se haga un uso esporádico.
- Salir del menú de configuración de Bluetooth tan pronto se haya terminado de utilizar.
- No conceder el nuevo permiso "Bluetooth" a apps que no lo requieren.

El interfaz Bluetooth en iOS (en adelante, BT) tiene una importancia fundamental, ya que muchos servicios de Apple se apoyan en comunicaciones Bluetooth y Bluetooth LE (por ejemplo, "continuidad", "Handoff", "AirDrop", etc.). La desactivación del interfaz Bluetooth afecta a dichos servicios, motivo por el cual son muchos los usuarios que optan por mantenerlo activo. Sin embargo, se debe ser consciente de los riesgos inherentes a esta opción:

- 1) La pila BT, el driver BT y el propio interfaz BT han sido tradicionalmente objetivo de múltiples ataques de seguridad.
- 2) Muchos dispositivos no ofrecen mecanismos de emparejamiento seguros (por ejemplo, buena parte de los auriculares BT), y algunos son capaces de establecer emparejamientos promiscuos (con varios dispositivos simultáneamente). Ello puede provocar, por ejemplo, que un tercero se empareje al auricular BT del propietario durante un descuido de éste (empleando el PIN por defecto si el dispositivo BT se encuentra en modo emparejamiento) y pueda escuchar conversaciones telefónicas.

La dirección del interfaz BT del dispositivo está disponible a través del menú "Ajustes - General - Información" (ver <Figura 9>). El nombre del dispositivo BT (mostrado bajo el interruptor de activación mediante el texto "Ahora visible como <nombre>") corresponde al nombre del dispositivo iOS, y solo puede ser modificado cambiando el nombre del propio dispositivo. Este nombre es el que se verá desde otros equipos, como en el ejemplo de la <Figura 46>.

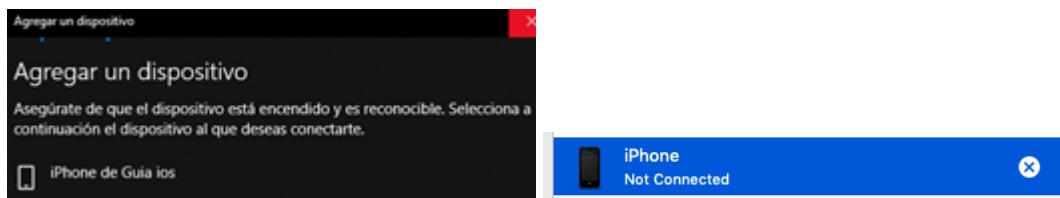


Figura 46 - Descubrimiento de un dispositivo iOS en un ordenador Windows y desde macOS

iOS 13 incorpora como nueva característica de seguridad el permiso de Bluetooth relacionado con la obtención de ubicación, con la intención de limitar el rastreo del dispositivo que muchas apps pueden realizar a través del uso de *beacons* BLE. La intención por parte de una app de acceder al interfaz BT para cualquier funcionalidad que no sea realizar *streaming* de audio se notificará al usuario, quien deberá conceder/denegar este permiso. *Se aconseja denegar el permiso BT salvo que exista un motivo claro para que la app lo solicite.*



Figura 47 - Permiso para el uso de BT concedido a las apps

Algunos ejemplos de apps que solicitan el permiso de BT son comercios, la plataforma de Google Chromecast (para su modo "invitado"), y apps de gestión de la actividad física.

12.1.2.1 Estado del interfaz Bluetooth

Por defecto, el interfaz BT queda activo:

- Tras el proceso de activación inicial del dispositivo.
- Tras aplicar la actualización de una nueva versión de iOS, independientemente de cuál era su estado antes de la actualización.

El estado el interfaz BT, además de en el menú "Ajustes - Bluetooth" (descrito posteriormente) se muestra y modifica mediante el "Centro de control" (ver apartado "9.2. Centro de Control") a través del grupo "Ajustes de red":

- El icono "Bluetooth" indica que el interfaz está activo.
- El icono "Bluetooth with a red circle" indica que el interfaz no admite conexiones pero sigue activo para ciertas conexiones: Apple Watch, Instant Hotspot, Apple Pencil y Handoff ("continuidad") [Ref.-14]. Las comunicaciones con dispositivos a los que el iPhone se haya emparejado se reanudarán al día siguiente a las 5 de la mañana, tras reiniciar el dispositivo o manualmente.
- El icono "Bluetooth with a red asterisk" indica que el interfaz está deshabilitado.

Las conexiones activas se pueden conocer desplegando el grupo (mediante *haptic touch*) sobre su espacio en el Centro de Control; desde este menú detallado, la pulsación con *haptic touch* en el icono de BT desplegará un menú contextual que incluye la lista de los dispositivos BT con los que se ha establecido un emparejamiento exitoso (si el iPhone se encuentra bloqueado, antes de proceder a presentarse este menú, se solicitará el código de acceso), y se puede proceder a conectarse/desconectarse de ellos:



Figura 48 - Comprobación del estado del interfaz Bluetooth a través del Centro de Control

En iOS 13 no existe ningún ícono de la barra superior de estado que indique el estado de activación del interfaz Bluetooth (a diferencia de lo que ocurría hasta iOS 11, en el que se disponía del ícono ".bluetooth", o iOS 12, en el que el ícono de estado de Bluetooth se mostraba cuando existe una conexión activa²⁵). Este comportamiento supone un inconveniente, ya que se pierde la posibilidad de comprobar el estado del interfaz de forma rápida. La razón que parece existir detrás de esta decisión por parte de Apple es que son muchos los servicios que se apoyan en comunicaciones Bluetooth y Bluetooth LE (por ejemplo, "continuidad", "Handoff", "AirDrop", etc.), por lo que la desactivación del interfaz Bluetooth afectaría a dichos servicios.

NOTA: El ícono "🔋" de la barra de estado representa el porcentaje de batería del dispositivo Bluetooth al que el iPhone se haya conectado. Aunque no todos los dispositivos son capaces de ofrecer este dato, la presencia del ícono puede ayudar a desvelar la existencia de una conexión Bluetooth.

iOS mantiene el estado del interfaz BT tras reiniciar el dispositivo móvil, es decir, si el interfaz BT estaba activo al apagar el terminal, al encender el dispositivo móvil, seguirá activo, y también al salir del modo avión.

Tras proceder a habilitar el modo avión, iOS permite la activación independiente del interfaz BT desde el Centro de Control y desde el menú "Ajustes". El interfaz BT también permanece activo cuando el dispositivo móvil está en espera (encendido, pero con la pantalla apagada) y/o bloqueado (suspendido).

12.1.2.2 Menú de configuración de Bluetooth

El acceso al menú "Ajustes - Bluetooth" permite:

- Habilitar/deshabilitar el interfaz Bluetooth: a través del interruptor "Bluetooth".
- Al entrar en este menú con el interfaz BT activo, iOS pondrá el interfaz en estado "visible", e iniciará de forma automática y periódica búsquedas de otros dispositivos BT que también estén en este estado; este proceso se representa mediante el ícono "Bluetooth" a la derecha de la sección "Otros Dispositivos", en la que se listarán los dispositivos descubiertos:

²⁵ "Bluetooth Icon Missing in iOS 12: What to Do?". <https://teknologya.com/bluetooth-icon-missing-in-ios-12/>

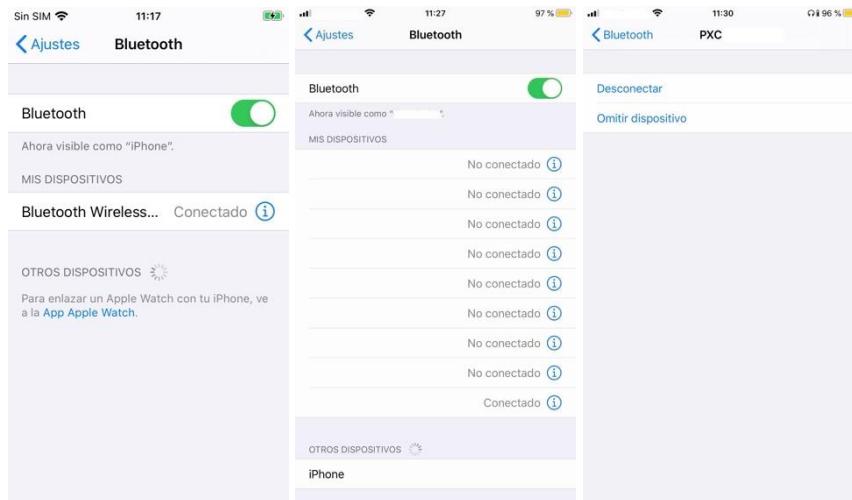


Figura 49 - Menú de configuración de Bluetooth

iOS siempre muestra los dispositivos BT que han sido emparejados previamente con el dispositivo y su estado: "No conectado" o "Conectado" (ver <Figura 49>). No se han identificado opciones en iOS para obtener la dirección BT (BD_ADDR) de cada dispositivo con el que se ha realizado el emparejamiento, lo cual impide reconocer con precisión otros dispositivos vinculados al terminal y evitar ataques de suplantación, ni tampoco para modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones deben ser autorizadas.

Se recomienda salir del menú de configuración de BT tan pronto se haya terminado de utilizar, ya que, mientras se permanezca en dicho menú (o submenús, es decir, en las pantallas de detalles de los dispositivos ya emparejados), el iPhone permanecerá en estado visible (opción desaconsejada), no existiendo ninguna opción en iOS que permita que el dispositivo quede en estado oculto²⁶. En caso de que el dispositivo iOS esté suspendido, pasará a modo oculto hasta que se desbloquee la pantalla y se acceda de nuevo a la configuración de BT.

Para desvincular un dispositivo BT se dispone de la opción "Omitir dispositivo" que se obtiene al pinchar sobre la entrada correspondiente al mismo. **Se recomienda omitir los dispositivos con los que no se mantienen conexiones asiduas**.

Se recomienda desactivar el interfaz inalámbrico Bluetooth si no se va a hacer uso de las comunicaciones o servicios asociados a él.

12.1.2.3 Perfiles BT soportados por iOS

Los dispositivos Apple soportan tanto BT clásico como BLE (Bluetooth Low Energy). En el apartado "Bluetooth security" de la [Ref.- 39] se indica qué mecanismos de seguridad se implementan en los distintos elementos de las comunicaciones BT.

La implementación BLE de iOS 13 hace uso de dos características de privacidad:

²⁶ Al encontrarse el interfaz Bluetooth del dispositivo móvil en modo oculto, todas operaciones de emparejamiento con otros dispositivos (no así las conexiones Bluetooth donde otro dispositivo conozca de antemano la dirección Bluetooth del dispositivo móvil iOS) deberán iniciarse desde el propio dispositivo móvil, siendo necesario que el otro dispositivo Bluetooth se encuentre en modo visible (opción recomendada para la protección del dispositivo iOS).

- Aleatorización de direcciones (*address randomization*): la dirección BT del dispositivo se cambia periódicamente para evitar la posibilidad de ser rastreado a través de BLE.
- Para poder reconectar con dispositivos emparejados, iOS 13 puede derivar las claves de enlace de BT clásico a partir de la clave generada con BLE.

Los perfiles BT soportados por iOS se muestran en la [Ref.- 11] e incluyen: manos libres (HFP), agenda (PBAP), audio avanzado (A2DP), control remoto de audio y vídeo (AVRCP), red de área personal (PAN), interfaz humana (HID), mensajes (MAP), WiAP (propietario de iPhone) y Braille.

iOS dispone del perfil de red de área personal (PAN, Personal Area Network) para establecer conexiones TCP/IP entre el dispositivo móvil y otros dispositivos a través de Bluetooth, y en concreto, para compartir su conexión de Internet móvil (2/3/4G) mediante lo que se denomina un "Personal Hotspot" (ver apartado "12.1.5. Personal Hotspot"). Este tipo de compartición está desaconsejada desde el punto de vista de seguridad frente a la utilización de un cable USB (si ésta es posible).

12.1.3 WI-FI

Recomendaciones de seguridad:

- Desactivar el interfaz Wi-Fi cuando se salga del rango de las redes conocidas. Si se requiere hacer uso de servicios que requieran que el interfaz esté activo (como AirDrop), activarlo puntualmente y desactivarlo después.
- Evitar conexiones a redes Wi-Fi abiertas. Si es necesario hacerlo por cualquier circunstancia:
 - Hacer uso de mecanismos de seguridad adicionales, como redes privadas virtuales (VPNs).
 - Omitir la red tan pronto cese la conexión.
 - Limitar el uso a lo imprescindible.
 - Preferir la conexión a través de datos móviles si es posible.
- Utilizar la compartición de contraseñas frente a comunicarla directamente a un tercero.

12.1.3.1 Mecanismos de seguridad y privacidad de iOS para comunicaciones Wi-Fi

A continuación se enumeran brevemente las principales características de seguridad de iOS relacionadas con las comunicaciones Wi-Fi (consultar la [Ref.- 39] para más información).

- Aleatorización de las direcciones MAC durante los escaneos, con el objetivo de evitar que el dispositivo sea rastreado mediante su tráfico Wi-Fi, que se realizan para:
 - Encontrar redes Wi-Fi conocidas (a excepción de los escaneos asociados al proceso de conexión a las redes Wi-Fi "preferidas").
 - ePNO (*enhanced Preferred Network Offload*) como mecanismo de los servicios de localización para las apps que usan "*geofencing*" (perímetros virtuales que delimitan un área geográfica real), como los recordatorios basados en la ubicación o al fijar una posición en Mapas.
- Aleatorización de los números de secuencia de las tramas Wi-Fi durante los escaneos (para los iPhone 7 y posteriores).

- Aleatorización de las direcciones MAC en las conexiones Wi-Fi punto a punto utilizadas en AirDrop, AirPlay y Personal Hotspot.
- Detección automática de redes ocultas (desde iPhone 6S) a fin de:
 - Evitar que el dispositivo anuncie los nombres de las redes ocultas a las que se conectó previamente: para ello, iOS solo envía las *probe requests* que incluyen el SSID cuando detecta la existencia de una red oculta.
 - Por tanto, no envía las *probe requests* con el SSID incluido si todas las redes en rango son visibles, para evitar que se revelen los nombres de redes conocidas no ocultas.
- Soporte para cifrado WPA3 en comunicaciones Wi-Fi, concretamente para WPA3 Personal mediante SAE y WPA3 Empresarial, pero no para WPA3 OWE.

12.1.3.2 Estado del interfaz Wi-Fi

Durante el proceso de configuración inicial del dispositivo móvil (que se inicia automáticamente la primera vez que se enciende el terminal), iOS ofrece al usuario la posibilidad de activar el interfaz Wi-Fi y conectarse a una red Wi-Fi (usando el proceso de configuración de una red Wi-Fi estándar de iOS), para completar el proceso de activación. Tras completar el proceso inicial de configuración, se recomienda deshabilitar el interfaz Wi-Fi del dispositivo móvil con el objetivo de aplicar las recomendaciones de seguridad descritas a lo largo de la presente guía antes de establecer conexiones Wi-Fi adicionales.

iOS proporciona información sobre la existencia de una conexión Wi-Fi en la parte izquierda de la barra superior de estado a través del ícono " ⓘ" (el número de barras refleja la intensidad de la señal Wi-Fi), pero la no aparición de este ícono en la barra no significa que el interfaz esté desactivado.

Para conocer el estado del interfaz, además de mediante el interruptor "Ajustes - Wi-Fi - Wi-Fi", se puede utilizar el grupo "Ajustes de red" del "Centro de Control" (ver apartado "9.2. Centro de Control") y observar el ícono:

- " ⓘ" indica que el interfaz está activo y que existe una conexión a una red Wi-Fi. El nombre de la red se indica bajo este ícono si se despliega el grupo (ver <Figura 48>).
 - " ⓘ" indica que el interfaz está activo, pero sin conexión actual a una red Wi-Fi. La conexión a redes Wi-Fi conocidas por el iPhone se reanudará cuando se verifique alguna de las condiciones descritas en la [Ref.- 14] (por ejemplo, desplazarse a una ubicación diferente, o al reiniciar el dispositivo), y se notificará al usuario de ello (con una ventana de diálogo la primera vez que se usa este acceso y con un mensaje en la parte superior de la pantalla en veces sucesivas).
- En este estado, el interfaz todavía permite comunicaciones vía AirDrop, Instant Hotspot y de mejora de la precisión de la ubicación.
- " ⓘ" indica que el interfaz está deshabilitado.

iOS mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil y tras salir del modo avión, aun cuando el terminal esté bloqueado. Adicionalmente, aun con el modo avión activo, iOS permite la activación independiente del interfaz Wi-Fi.

La conexión a una red Wi-Fi puede realizarse desde el "Centro de Control" si el dispositivo está desbloqueado. Para ello, al pulsar sobre el ícono " ⓘ" mediante "haptic touch", se desplegará el menú contextual de la quinta imagen de la <Figura 22>, desde el cual se puede seleccionar la red o acceder al menú de los ajustes "Wi-Fi".

El mecanismo empleado por iOS para decidir a qué red Wi-Fi se conecta automáticamente cuando se dispone de varias redes Wi-Fi conocidas en rango está detallado oficialmente por Apple en la [Ref.- 65], dando prioridad a las redes "preferidas" (y entre estas premiando el nivel de seguridad y a igualdad de condiciones, la intensidad de la señal), la última red privada a la que el dispositivo había estado conectado anteriormente, redes privadas (domésticas, empresariales y *hotspots* de iOS) y públicas. iOS introduce el concepto de redes "preferidas" asignándoles dinámicamente, en base a las acciones del usuario, una puntuación para incrementar o reducir su importancia.

12.1.3.3 Configuración del interfaz Wi-Fi

El interfaz inalámbrico Wi-Fi se configura en iOS a través del menú "Ajustes - Wi-Fi". El estado del interruptor "Wi-Fi" determina el del interfaz:

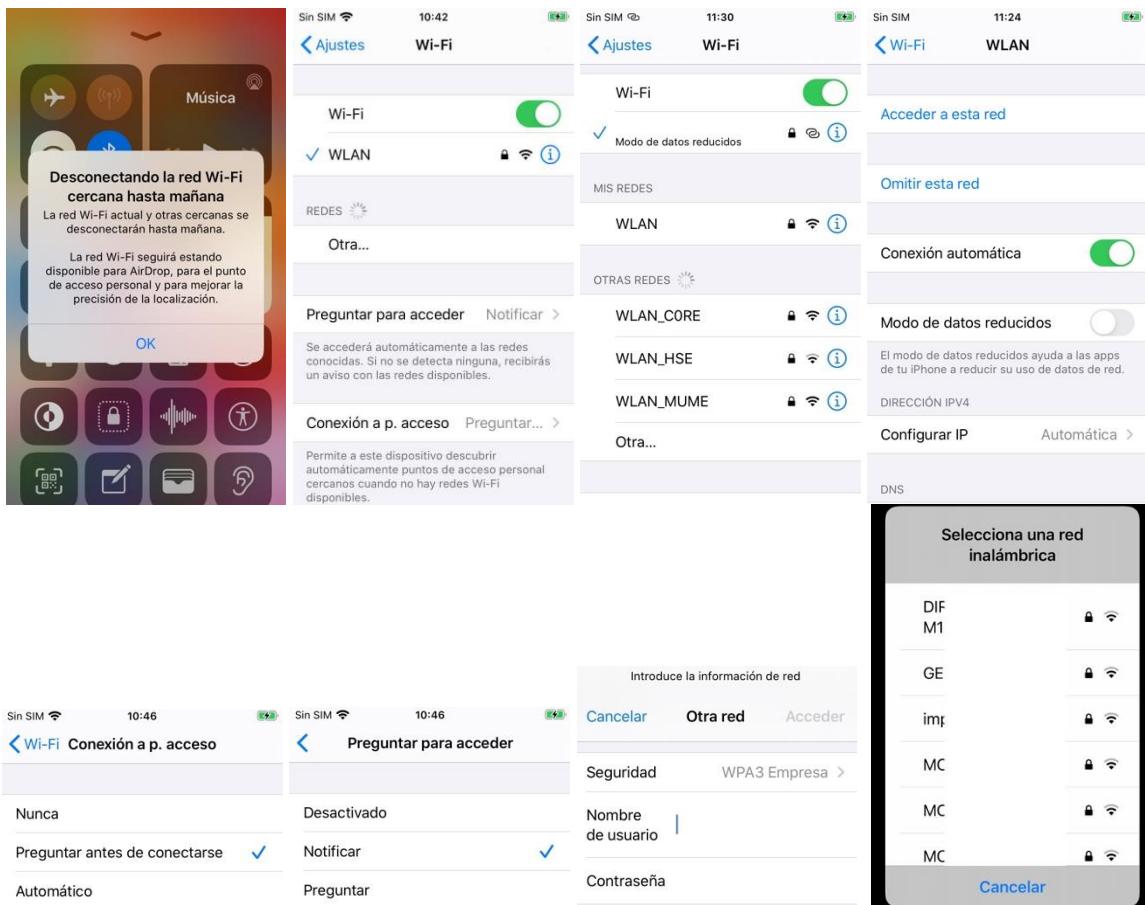


Figura 50 - Configuración de comunicaciones Wi-Fi

La dirección MAC del interfaz Wi-Fi del dispositivo está disponible a través del menú "Ajustes - General - Información" (ver <Figura 9>).

Las opciones disponibles en el menú "Wi-Fi" son:

- Lista de redes en rango: se muestra ordenada alfabéticamente, y se actualiza de forma automática.
 - El símbolo "✓" a la izquierda identifica la red a la que está conectado el interfaz Wi-Fi.
 - El símbolo "🔒" a la derecha del nombre de la red indica que se trata de una red protegida con contraseña (no se informa de los mecanismos de seguridad concretos).

empleados por cada una de las redes: WEP, WPA, WPA2, WPA3, etc.). La ausencia del candado implica que la red es una red no protegida o abierta.

- El símbolo " ⓘ " representa una red Wi-Fi de tipo "Hotspot" (ver apartado "12.1.5. Personal Hotspot").
- El símbolo " ⓘ " indica que la red es oculta.
- "Otra...": opción necesaria para la conexión a redes ocultas. Esta última opción es la única que permite seleccionar todas las opciones de configuración de conexión de una nueva red Wi-Fi, incluyendo el nombre de red (o SSID), el mecanismo de seguridad a emplear (ninguna o redes abiertas, WEP, WPA Personal, WPA2 o WPA2/WPA3 Personal, WPA/WPA2/WPA3 Empresa²⁷) y la contraseña (si la red la requiere).

Para poder añadir una nueva red de forma manual, es preciso que ésta se encuentre en la zona de cobertura y poder establecer la conexión a través del botón "Acceder". Sin embargo, **se desaconseja añadir redes Wi-Fi manualmente en iOS ya que éstas serán consideradas como redes ocultas (aunque no lo sean) y desveladas por el dispositivo.**

No.	Time	Source	Destination	Protocol	Length	Info
65	13.438642147	be:35:42:7b:64:c3	Broadcast	802.11	152	Probe Request, SN=1162, FN=0, Flags=....., SSID=CCN-CERT
68	13.444125168	be:35:42:7b:64:c3	Broadcast	802.11	152	Probe Request, SN=1164, FN=0, Flags=....., SSID=CCN-CERT
104	23.327317568	32:6e:37:2e:7b:94	Broadcast	802.11	152	Probe Request, SN=1259, FN=0, Flags=....., SSID=CCN-CERT
105	23.328702639	32:6e:37:2e:7b:94	Broadcast	802.11	152	Probe Request, SN=1260, FN=0, Flags=....., SSID=CCN-CERT
156	40.189267999	aa:d2:3f:e4:c6:ef	Broadcast	802.11	152	Probe Request, SN=1351, FN=0, Flags=....., SSID=CCN-CERT
157	40.202444817	aa:d2:3f:e4:c6:ef	Broadcast	802.11	152	Probe Request, SN=1352, FN=0, Flags=....., SSID=CCN-CERT
158	40.546960304	aa:d2:3f:e4:c6:ef	Broadcast	802.11	152	Probe Request, SN=1366, FN=0, Flags=....., SSID=CCN-CERT
159	40.548301385	aa:d2:3f:e4:c6:ef	Broadcast	802.11	152	Probe Request, SN=1367, FN=0, Flags=....., SSID=CCN-CERT

Figura 51 - Trazo de red mostrando cómo iOS 13 desvela el SSID de una red oculta

- "Preguntar para acceder": por defecto, iOS se conecta de forma automática a las redes conocidas si están en rango. Si no se detecta ninguna de estas redes, este menú permite:
 - "Desactivado": el usuario tendrá que seleccionar manual y activamente una de las redes disponibles cuando desee establecer una conexión Wi-Fi. **Esta opción es la recomendada desde el punto de vista de seguridad.** Las otras dos opciones permiten que iOS notifique o pregunte activamente al usuario si desea conectarse a alguna de las redes disponibles.
 - "Notificar": el usuario recibirá una notificación cuando haya nuevas redes disponibles.
 - "Preguntar": en caso de que se requiera una conexión Wi-Fi y no se disponga de ella (por ejemplo, si una aplicación genera tráfico), se ofrecerá al usuario la posibilidad de conectarse a alguna de las redes Wi-Fi disponibles en la ubicación, incluidas las redes Wi-Fi abiertas.
- "Conexión a puntos de acceso": controla si el iPhone debe buscar o no puntos de acceso de tipo "Hotspot" cuando no existan redes Wi-Fi disponibles. Para evitar conexiones no deseadas, **se recomienda fijar este valor a "Nunca" o "Preguntar antes de conectarse", pero en ningún caso que se establezca la conexión de manera automática.**
- Ajustes para una red concreta (disponibles al seleccionar el nombre de dicha red):
 - "Conexión automática": por defecto, iOS se conecta de forma automática a las redes conocidas. Este comportamiento se deshabilita para una red concreta mediante este interruptor.
 - "Omitir esta red": iOS almacena en su lista de redes conocidas o PNL (*Preferred Network List*) los datos de las redes Wi-Fi a las que se ha conectado previamente, a fin de encontrarlas cuando estén en rango y mostrarlas como redes disponibles. Cuando se realiza una conexión a una red de forma puntual (por ejemplo, en una oficina o domicilio

²⁷ Las opciones de seguridad Wi-Fi de iOS 13 disponibles dependen del modelo de dispositivo móvil, por ejemplo, no estando disponibles las opciones "WPA2/WPA3" o "WPA3" (Personal) en el iPhone SE.

ajeno, un hotel, una cafetería, etc.), **se aconseja eliminar la red de la PNL mediante esta opción mientras todavía se encuentra el dispositivo en el área de cobertura de la misma**. Esto es especialmente importante para las redes públicas y aún más para las redes abiertas y las ocultas.

iOS dispone de la posibilidad de compartir la conexión de Internet móvil (2/3/4G) mediante Wi-Fi (ver apartado "12.1.5. Personal Hotspot"). En caso de hacer uso de esta funcionalidad, el dispositivo móvil utilizará la conexión Wi-Fi en exclusiva para el *hotspot*, no pudiendo mantener además su propia conexión a una red Wi-Fi.

En resumen, desde el punto de vista de seguridad de iOS como cliente Wi-Fi, **se recomienda hacer uso de redes inalámbricas no ocultas, basadas en WPA2 o WPA3 con cifrado AES (CCMP), y autenticación de tipo Personal, con una contraseña de acceso (PSK, Pre-Shared Key) suficientemente robusta (más de 20 caracteres), o de tipo Empresa, basada en mecanismos de autenticación 802.1X/EAP, y preferiblemente basada en EAP-TLS, con todos los ajustes de certificados y del servidor RADIUS minuciosamente configurados a través de un perfil de configuración.**

NOTIFICACIÓN DE REDES ABIERTAS EN RANGO

iOS 13 introduce como una de sus novedades la notificación al usuario sobre disponibilidad de redes Wi-Fi abiertas cuando no existe ninguna red conocida en rango, que puede acompañarse del botón "Join". Esta funcionalidad filtra las redes en rango y selecciona para la notificación aquella a la que existe más probabilidad de que se desee conexión, al considerarse redes populares a las que están conectados otros usuarios.

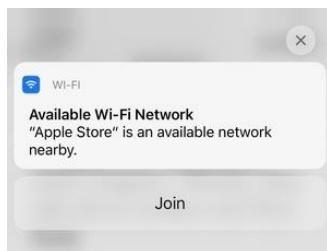


Figura 52 - Notificación sobre red Wi-Fi cercana disponible²⁸

No se dispone de ninguna documentación oficial sobre los mecanismos que iOS utiliza para implementar esta funcionalidad. Desde un punto de vista técnico, lo más probable es que el dispositivo monitorice y analice el tráfico Wi-Fi (potencialmente en modo monitor) para identificar el número de clientes conectados a una red concreta y determine cuál es la red más popular en rango.

CONEXIÓN A REDES EMPRESARIALES

En caso de emplear WPA2 o WPA3 en sus versiones empresariales, la pantalla de ajustes de iOS no permite especificar los parámetros de configuración asociados al modo o tipo de mecanismo EAP a emplear, gestionándolo automáticamente o, preferiblemente, debiendo ser gestionados estos ajustes a través de un perfil de configuración:

²⁸ Imagen obtenida de <https://www.macworld.com/article/3482122/what-the-new-ios-13-wi-fi-message-means-about-nearby-available-networks.html>.



Figura 53 - Configuración manual de una red Wi-Fi basada en WPA3 Empresa

El modo automático de iOS requiere proporcionar las credenciales del usuario ("Nombre de usuario" y "Contraseña", y, opcionalmente, el dominio Windows "DOMINIO\usuario") (ver <Figura 53>). Para poder fijar otros tipos EAP, así como opciones de configuración más avanzadas, es necesario hacer uso de los perfiles de configuración de iOS (por ejemplo, a través de Apple Configurator²⁹). El perfil de configuración debe incluir el certificado digital de la autoridad certificadora (CA) - raíz o intermedia - empleada para generar los certificados digitales asociados al servidor de autentificación de la red Wi-Fi (servidor RADIUS), salvo que se usen certificados emitidos por una de las CAs ya existentes por defecto en iOS.

En el momento de establecer la primera conexión con una red Wi-Fi WPA2 o WPA3 Empresa, iOS solicitará al usuario verificar la identidad del servidor de autentificación (RADIUS) al que se está conectando a través de su certificado digital. Se recomienda aceptar el certificado digital del servidor tras verificar exhaustivamente sus detalles y confirmar que pertenece al servidor RADIUS al que pretendemos conectarnos, ya que, en caso contrario, las credenciales de acceso (usuario y contraseña) serían enviadas a otro servidor potencialmente controlado por un atacante. Debe tenerse en cuenta que las credenciales empleadas por el dispositivo móvil para conectarse a la red Wi-Fi empresarial normalmente no solo se emplean para la conexión a la red Wi-Fi, sino que también constituyen las credenciales del usuario en el dominio de la organización, permitiendo igualmente el acceso a la cuenta de correo, a los entornos Windows, a servidores web internos o a los concentradores VPN de la organización.

En el caso de emplear EAP-TLS, es necesario importar en el iPhone un certificado digital personal (en formato PKCS #12). Para instalar el certificado personal, se debe transferir el fichero del certificado (.pfx ó .p12) al dispositivo móvil (ver apartado "17.2. Certificados cliente").

12.1.3.4 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 primaria a la que está conectado a otro dispositivo iOS [2] sin revelar directamente al otro usuario las credenciales de la red³⁰ (sección "Wi-Fi password sharing" de la [Ref.- 39]).

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 de [2].

²⁹ La descripción de Apple Configurator queda fuera del ámbito de la presente guía, pero se puede consultar en la [Ref.- 22].

³⁰ Este procedimiento no es de aplicación en redes Wi-Fi que emplean filtros por dirección MAC.

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

- [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 la contraseña de la red.
- Los dispositivos Apple cercanos que conocen la contraseña de la red, 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 "13.1. AirDrop").
- Si [1] valida la identidad proporcionada por [2], solicitará al usuario, mediante la ventana de diálogo de la <Figura 54> autorización para compartir la contraseña con [2].
- Si el usuario del dispositivo [1] acepta:
 - [1] enviará a [2] la contraseña de la red cifrada con AES 256³¹.
 - [2] almacenará esta contraseña en su *keychain* de [2] empleando un hash, por lo que la contraseña en claro no podrá conocerse por el usuario de [2].

La principal ventaja de este mecanismo es que evita tener que proporcionar 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.

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



Figura 54 - Compartición de contraseñas de redes Wi-Fi

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

12.1.4 VOZ Y DATOS MÓVILES

El interfaz de telefonía móvil se habilita por defecto en iOS tan pronto se introduce una tarjeta SIM que proporciona servicio, activándose adicionalmente el interfaz de datos móviles si la tarjeta SIM los incluye. En la barra superior de estado aparecerá el símbolo "■■■" (el número de barras representa la intensidad de la señal), junto al nombre del operador de telefonía móvil y, opcionalmente, el tipo de conexión (GPRS, E, 3G, 4G, LTE). iOS 13 no soporta 5G, si bien para algunos proveedores como AT&T puede mostrar ■■■5GE para indicar 4G LTE. El soporte de 5G está previsto para los modelos de iPhone que Apple liberará en 2020.

³¹ El cifrado mediante AES 256 se introdujo en iOS 11. Hasta entonces, este procedimiento utilizaba un cifrado inseguro.

iOS determina cuál es la mejor conexión de datos disponible, sin interrogar al usuario, y proporciona la conectividad necesaria a las aplicaciones que ejecutan en el dispositivo móvil. En el "Centro de Control", se dispone del ícono  (ver <Figura 22>), que informa del estado del interfaz de datos móviles y permite su activación y desactivación. El "modo avión" es incompatible con el uso del interfaz de telefonía y datos móviles.

Si el dispositivo tiene conexión de datos a través de una red Wi-Fi, todo el tráfico se cursará a través de dicho interfaz. Así, los datos móviles solo se emplean si no se dispone de acceso a Internet vía Wi-Fi. El único caso en que ambas conexiones estarán activas simultáneamente es cuando el dispositivo móvil se configura para actuar como punto de acceso Wi-Fi y compartir su conexión de datos (ver apartado "12.1.5. Personal Hotspot"), y cuando está activa la opción "Asistencia para Wi-Fi" y la señal de la red Wi-Fi es débil. Desde el punto de vista de seguridad, se considera más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil (cuando estén disponibles, según la cobertura existente) en lugar de a través de redes Wi-Fi abiertas, siempre que la conexión de datos de telefonía móvil emplee tecnologías 3G/4G frente a 2G.

iOS mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil e introducir el PIN de la tarjeta SIM. El único modo de desactivar las capacidades de telefonía de voz y SMS/MMS es activar el modo avión.

12.1.4.1 Ajustes del módulo de datos móviles

Están disponibles en el menú "Ajustes - Datos móviles". El interruptor "Datos móviles" activa y desactiva las capacidades de transmisión de datos a través de las redes de telefonía móvil, pero aún deshabilitado, sigue siendo posible emplear las capacidades de voz y SMS/MMS. La vinculación con un operador fijará en el dispositivo móvil una serie de ajustes, tanto para los servicios de telefonía de voz como de datos móviles, algunos de los cuales no son modificables.

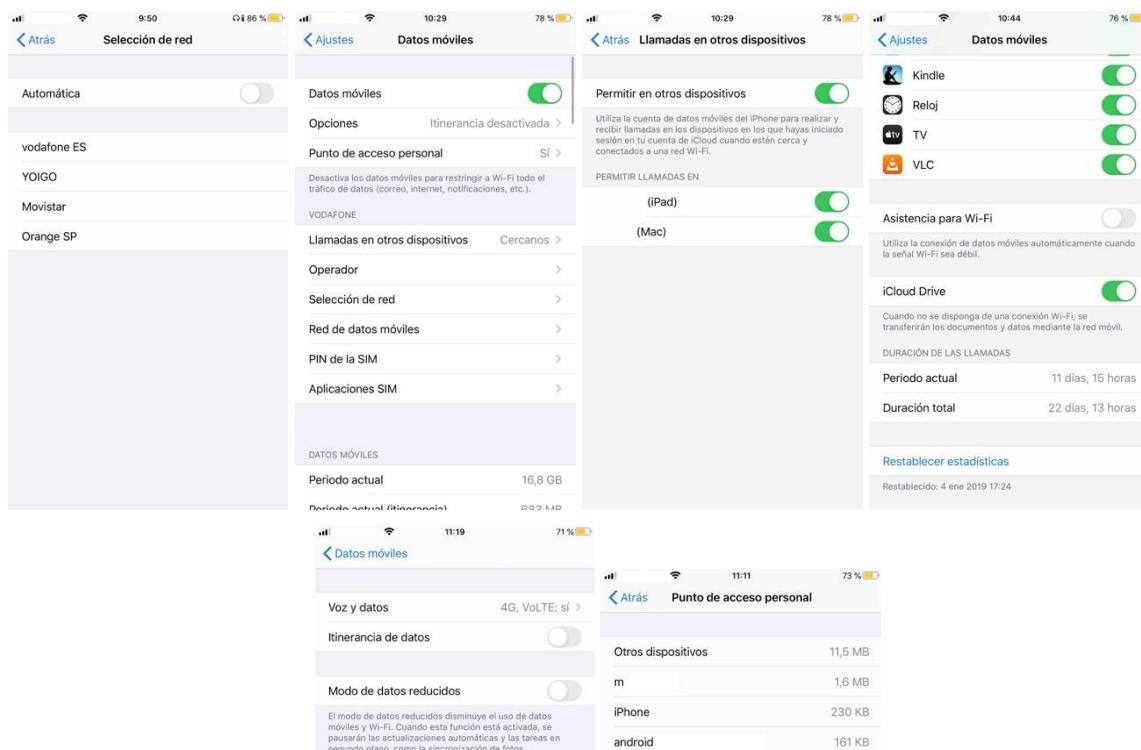


Figura 55 - Ajustes de telefonía y datos móviles

- "Selección de red": en modo manual, permite seleccionar el operador de telecomunicaciones de la lista ofrecida. Esta opción tiene sentido cuando se hace uso del dispositivo en el extranjero a través de *roaming*; de lo contrario, el valor debe ser "Automático".
- "Opciones":
 - "Voz y datos": se recomienda seleccionar "4G, VoLTE: si" y solo cambiar a 3G si no existe cobertura 4G en la zona.
 - "Itinerancia de datos": **se recomienda deshabilitarla** para bloquear el uso automático de las capacidades de datos de telefonía móvil cuando se viaja al extranjero y el terminal se encuentra en una red de otro operador al asociado por defecto a su tarjeta SIM³². Únicamente se procederá a habilitarlo cuando se requiera.
- "Modo de datos reducido": se recomienda activarlo si el usuario tiene limitaciones en el consumo de datos móviles, de forma que se pausen trasferencias de datos desde las apps y el sistema de actualizaciones automáticas.
- "PIN de la SIM": **se recomienda disponer de un PIN para la tarjeta SIM**, según lo descrito en el apartado "8.1.1. Código de acceso a la tarjeta SIM".
- "Sección DATOS MÓVILES": permite establecer limitaciones para el uso de datos de forma individual. De este modo, si el contrato asociado a la SIM tiene limitaciones en el consumo de datos, podrá activarse solo el interruptor para las apps cuyas trasferencias de datos se requieran, bien permanente o puntualmente.

Desde el punto de vista de seguridad, **se recomienda vigilar el consumo de datos móviles de las apps**, a fin de detectar consumos inusuales que podrían desvelar que la app está cursando tráfico no deseado.

 - La información sobre el consumo de datos asociado a los procesos del sistema operativo se muestra en la lista de apps como "Servicios del sistema", no siendo posible deshabilitar los mismos, pero sí recomendándose vigilar este valor.
 - La entrada "Punto de acceso personal" permite conocer el uso que otros dispositivos han hecho de los datos móviles del iPhone por conexión a su *hotspot*. Se recomienda vigilar esta entrada para identificar consumos irregulares o dispositivos a los que no se ha autorizado el uso del *hotspot*.
- "Llamadas en otros dispositivos": se corresponde con el ajuste del mismo nombre del apartado "12.1.4.2. Ajustes del módulo de telefonía".
- "Restablecer estadísticas": permite restaurar las estadísticas de consumo de datos móviles recopiladas actualmente.

³² Muchas aplicaciones iOS generan tráfico de red sin necesidad de interacción directa con el usuario. Al viajar al extranjero, tener la opción de itinerancia de datos activa puede suponer un elevado gasto (en función del contrato de telefonía móvil de que se disponga).

12.1.4.2 Ajustes del módulo de telefonía

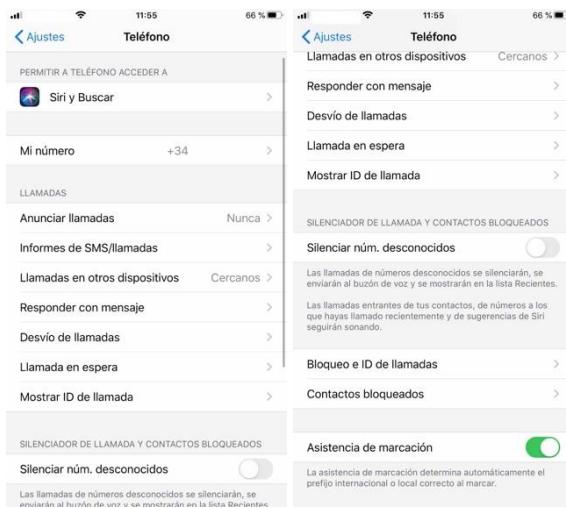


Figura 56 - Ajustes del módulo de telefonía

Para proteger la privacidad del usuario, se dispone de ciertos ajustes en el menú "Ajustes - Teléfono", que se recomienda revisar.

Desde el punto de vista de seguridad y privacidad, se recomienda la configuración:

- "Permitir a teléfono acceder a Siri y Buscar": dado que el uso de Siri implica que datos sensibles de usuario se envíen a Apple, **se desaconseja el uso de esta opción**.
- "Anunciar llamadas": **Nunca**. Este ajuste controla si el aviso de llamada tradicional se sustituirá por la voz de Siri informando de quién realiza la llamada, lo que podría ser inadecuado en presencia de terceros.
- "Informes de SMS/llamadas": **se desaconseja habilitar este servicio**, que hace uso de extensiones que pueden enviar a desarrolladores de apps contenidos de los mensajes enviados e información sobre las llamadas.
- "Bloqueo e ID de llamadas": incluir los contactos no deseados.
- "Llamadas en otros dispositivos": esta opción permite utilizar la conexión de telefonía del iPhone para realizar y recibir llamadas en otros dispositivos Apple vinculados a la misma cuenta de iCloud que el dispositivo; deben estar cercanos, conectados por Wi-Fi y haber iniciado sesión en FaceTime con dicha cuenta (ver < Figura 55>)³³. Desde el punto de vista de seguridad, **se recomienda deshabilitar esta opción, para proteger la conexión de telefonía del dispositivo móvil en caso de compromiso de algún otro equipo que comparta la cuenta de iCloud o de la propia cuenta de iCloud**.
- "Responder con mensaje": permite configurar una serie de mensajes por defecto que se mostrarán en la pantalla de llamada, de forma que el usuario pueda elegir con un solo toque cuál remitir si no puede atender la llamada. Estos mensajes predefinidos estarán disponibles si se recibe una llamada con el dispositivo bloqueado.
- "Desvío de llamadas": permite redirigir la llamada a un número distinto cuando la opción está activa.
- "Mostrar ID de llamada": permite al usuario definir si se enviará la información de identificación de la llamada. No dispone de opciones para actuar en función del llamante.

³³ <https://support.apple.com/es-es/guide/iphone/iphf90f372f0/ios>

- "Silenciar núm. desconocidos": este ajuste, nuevo en iOS 13 [Ref.- 29], hace uso de los servicios de Siri para enviar directamente al buzón de voz los números llamantes que no estén en los contactos del usuario que se pueden obtener de las apps Contactos, Mail o Mensajes.
- "Contactos bloqueados": permite establecer una lista de exclusión de elementos pertenecientes a Contactos, de forma que no se recibirá ninguna comunicación de ellos.

En la [Ref.- 29] se indica que iOS 13 marcará en la lista de llamadas recientes aquellas cuyo número ha sido verificado por el operador (según el país, y cumpliendo con las normas STIR/SHAKEN).

12.1.5 PERSONAL HOTSPOT

iOS permite compartir su conexión de Internet de datos móviles (actuando como punto de acceso Wi-Fi para otros equipos) con otros dispositivos (*tethering*) mediante lo que Apple denomina "Personal Hotspot" [Ref.- 48]. La compartición de datos puede llevarse a cabo a través del interfaz Bluetooth, Wi-Fi, y mediante un cable USB. El servicio se configura a través de "Ajustes - Punto de acceso personal"³⁴.

Uno de los principales cambios de iOS 13 es la forma en la que se gestiona el punto de acceso personal:

- Uso persistente: el punto de acceso personal se mantiene disponible para los dispositivos conectados al iPhone, aunque éste esté suspendido.
- Conexión automática: podrán conectarse al punto de acceso del dispositivo iOS sin necesidad de aprobación activa por parte del usuario, los dispositivos:
 - Vinculados a la misma cuenta de iCloud.
 - Asociados al grupo "Familia" de iCloud, si se habilita la opción "En familia"³⁵ en el menú "Punto de acceso personal".

Estos dispositivos no necesitan introducir la contraseña para conectarse al *hotspot* del iPhone, ya que el establecimiento de la conexión se realiza a través de los servicios de "Continuidad" (que se detallan en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]).

La conexión automática para dispositivos vinculados a la propia cuenta de iCloud tiene como consecuencia que el interruptor de versiones anteriores de iOS para habilitar/deshabilitar el punto de acceso ha desaparecido en iOS 13, es decir, no existe ningún mecanismo conocido para deshabilitar completamente las conexiones a través del punto de acceso personal.

- La opción "Permitir a otros conectarse" controla si dispositivos ajenos a la cuenta de iCloud pueden compartir la conexión al punto de acceso del iPhone.

NOTA: 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 a la misma cuenta de iCloud que el iPhone se conecta al *hotspot*, y no se deshabilita cuando cesa la conexión con éste. Si durante el intervalo en que dura la conexión se recibe una

³⁴ en versiones anteriores de iOS, este servicio estaba disponible en "Ajustes - Compartir Internet"

³⁵ La configuración de "Familia" queda fuera del ámbito de la presente guía. Consultar la documentación oficial de Apple "Configurar En familia" para más información <https://support.apple.com/es-es/HT201088>.

solicitud de conexión por parte de otro dispositivo que conoce la contraseña, se permitirá su conexión sin informar al usuario.

El interruptor "Permitir a otros conectarse" no se deshabilita cuando finaliza la conexión del dispositivo vinculado a la cuenta de iCloud, por lo que otras conexiones al *hotspot* por parte de dispositivos que conozcan la contraseña serán cursadas desde ese momento.

- Compartición automática de la contraseña del punto de acceso: cuando se reciba por primera vez un intento de conexión al *hotspot* por parte de un dispositivo que figure en los contactos del usuario, se mostrará la ventana de la imagen central de la <Figura 55>; si se pulsa "Compartir punto de acceso", la contraseña se enviará cifrada al otro dispositivo, que podrá conectarse a partir de ese momento mientras no se modifique la contraseña. Este proceso es similar al descrito en el apartado "12.1.3.4. Compartición de contraseñas de redes Wi-Fi".

Por defecto, iOS proporciona una contraseña de 13 caracteres alfanuméricos. Desde el punto de vista de seguridad, se recomienda seleccionar una contraseña propia y personalizada de más de 20 caracteres frente a la generada automáticamente.

La contraseña debe modificarse de forma regular, y, especialmente, siempre que haya sido preciso compartir la conexión con un dispositivo ajeno.

La compartición de un punto de acceso personal con un dispositivo propio se considera más segura que recurrir a redes Wi-Fi abiertas.

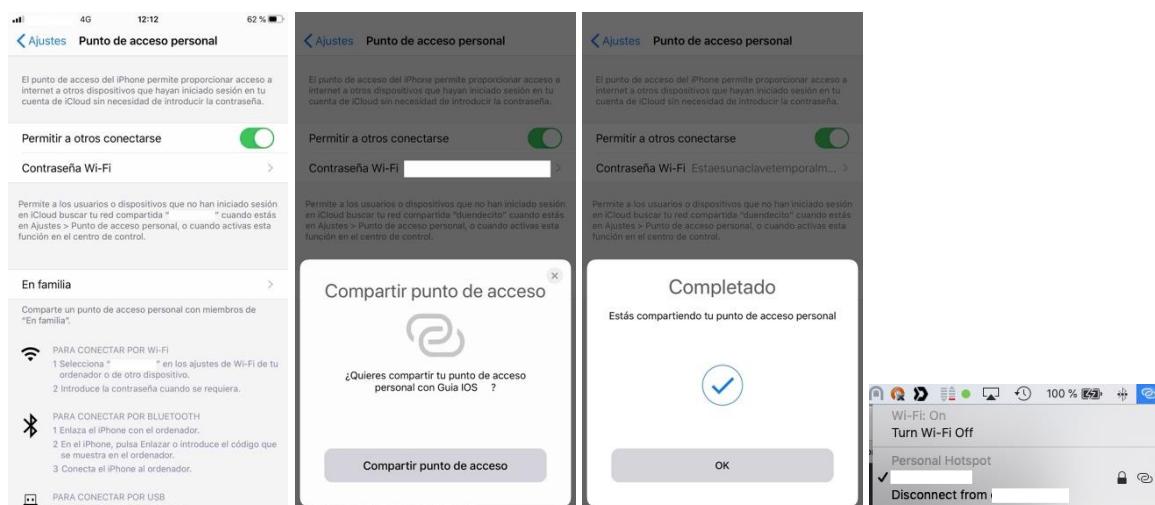


Figura 57 - Configuración de un punto de acceso personal (*hotspot*)

Cuando se establezca una conexión desde otro dispositivo, iOS 13 mostrará brevemente el mensaje de la primera imagen de la <Figura 58> en la parte superior de la pantalla. Sin embargo, transcurridos unos instantes, desaparecerá, y únicamente quedará referencia a la existencia de la conexión por el color azul de la barra superior de estado:



Figura 58 - Identificación de conexión a punto de acceso en la barra superior de estado

Se recomienda prestar atención a la barra de estado para detectar conexiones al punto de acceso, ya que el hotspot se comporta como una red Wi-Fi más, visible para otros dispositivos, y a la que dichos dispositivos pueden elegir conectarse automáticamente.

Desde el punto de vista de seguridad, en caso de ser factible, la compartición más segura es la de tipo USB, seguida de Wi-Fi. La <Figura 57> muestra un ejemplo de compartición de Internet con un ordenador macOS vinculado a la misma cuenta de iCloud que el usuario.

12.2 COMUNICACIONES TCP/IP

iOS dispone de soporte de TCP multi-ruta, que permite realizar conexiones a través de varias interfaces como LTE (4G), Wi-Fi y Bluetooth simultáneamente. En la práctica, esta funcionalidad implica que las transmisiones de datos no se interrumpen si, habiéndose iniciado sobre una conexión Wi-Fi, se sale de su alcance, ya que se cursarían a través de la red 2/3/4G disponible.

Los adaptadores de red disponibles en el dispositivo móvil para las diferentes tecnologías de comunicaciones (principalmente, Wi-Fi y 2/3/4G) se acceden desde el menú correspondiente: "Ajustes - Wi-Fi" (apartado "12.1.3. Wi-Fi") o "Ajustes - Datos móviles" (apartado "12.1.4. Voz y datos móviles").

En el caso del interfaz Wi-Fi, los ajustes avanzados (direcciónamiento IP, máscara de subred, router, servidores DNS primario y secundario, etc.) se obtienen pulsando sobre el ícono " ⓘ" situado a la derecha del nombre de la red.

La configuración de direcciónamiento IP del interfaz Wi-Fi es independiente para cada una de las redes Wi-Fi configuradas.

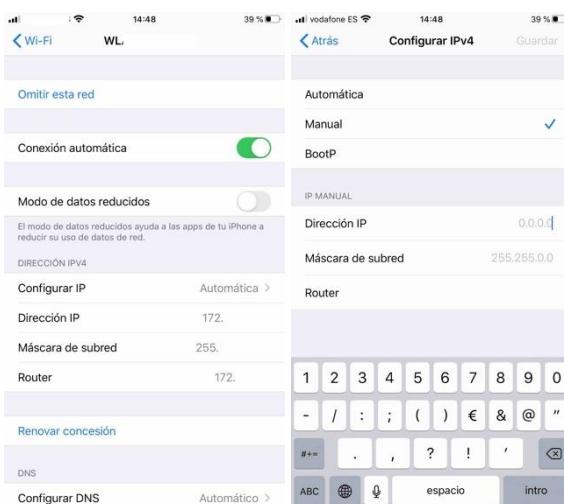


Figura 59 - Configuración de los parámetros TCP/IP del interfaz Wi-Fi

Para el interfaz móvil 2/3/4G, iOS no proporciona a nivel de interfaz de usuario estándar opciones de configuración para TCP/IP, ni siquiera para consultar la dirección IP asignada de forma dinámica por el operador de telefonía móvil al utilizar las redes de datos 2/3/4G. Desde iOS 11 esta información no es mostrada tampoco a través del denominado "modo de prueba" (*Field Test*), disponible en iOS al marcar el código *3001#12345#, y pulsar la tecla de llamada:

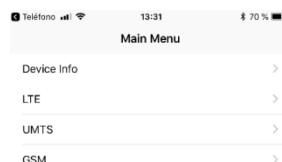


Figura 60 - Información del interfaz de telefonía y datos móviles a través del "Field Test"

El "Field Test" proporciona detalles relacionados con las redes de telefonía móvil y el interfaz de radio del dispositivo móvil, como la intensidad de diferentes parámetros de la señal y frecuencias empleadas, y la celda de servicio actual y las celdas vecinas, para LTE, UMTS y GSM.

12.3 COMUNICACIONES USB

Recomendaciones de seguridad:

- Mantener siempre desactivada la opción "Accesorios USB".
- No autorizar emparejamientos USB entre el dispositivo móvil y equipos de terceros.

La conexión USB del dispositivo a un ordenador proporciona cinco funcionalidades:

- Suministro de corriente para cargar el dispositivo móvil: recientemente se ha extendido el uso de cargadores USB en lugares públicos, como cafeterías o aeropuertos. Desde el punto de vista de seguridad, en caso de requerirse conectar el dispositivo móvil a uno de estos cargadores, **se recomienda hacer uso de un adaptador USB especial que bloquee la transferencia de datos**.
- Acceso limitado al almacenamiento interno que ofrece la descarga de imágenes y vídeos.
- Un servicio de compartición de ficheros disponible a través de Finder (desde macOS 10.15 Catalina) o iTunes (desde macOS 10.14 Mojave o anterior) para escribir contenido que consumirán las apps que ofrecen "*File sharing*" (por ejemplo, un certificado digital, una configuración concreta o ficheros multimedia) y descargar al ordenador los contenidos que la app permita. Para que esta conexión se produzca, es necesario establecer una relación de confianza entre el ordenador y el dispositivo móvil, que se establece al aceptar el mensaje "*¿Confiar en este ordenador?*" que se mostrará en la pantalla del dispositivo móvil.
- Operaciones de copia de seguridad y restauración (mediante iTunes hasta macOS 10.14 inclusive) y de Finder en macOS Catalina (ver apartado "20. Copias de seguridad y restauración"). Para que esta conexión se produzca, es también necesario establecer la relación de confianza entre el ordenador y el dispositivo móvil (ver <Figura 61>).
- Compartición de la conexión de datos de telefonía móvil (2/3/4G), *tethering* (no así la de Wi-Fi), del dispositivo móvil con el ordenador.

Para que el dispositivo iOS acepte conexiones a través de USB con otro equipo, es preciso que se establezca previamente una relación de confianza (ver apartado "12.3.1. Proceso de emparejamiento"). Se debe tener en cuenta que el acceso a ciertos datos (con clases de protección más estrictas) a través de la conexión USB, mediante la relación de confianza ya establecida, puede requerir que el dispositivo móvil haya sido desbloqueado por el usuario mediante el código de acceso al menos una vez desde que fue arrancado, o que incluso se encuentre desbloqueado en el momento de comenzar la sincronización de datos.

La compartición de la conexión de datos a través de USB con un ordenador propio **se considera más segura que la basada en Bluetooth o Wi-Fi** (ver apartado "12.1.5. Personal Hotspot").

12.3.1 PROCESO DE EMPAREJAMIENTO

El proceso de emparejamiento permite establecer una relación de confianza entre dos equipos.

De acuerdo con la [Ref.- 39], el proceso de emparejamiento USB con un ordenador exige que el dispositivo iOS esté desbloqueado, acepte la petición proveniente del equipo externo y que

el usuario introduzca el código de acceso del dispositivo iOS (desde iOS 9). Si el proceso se completa, se intercambiarán entre ambos dispositivos un par de claves públicas RSA de 2.048 bits, que se utilizarán para iniciar una sesión TLS (Apple indica SSL) necesaria para que el iPhone envíe cualquier tipo de datos al ordenador. El ordenador recibirá la clave de 256 bits necesaria para desbloquear la "escrow keybag" (bolsa de custodia de claves).

Los registros o relaciones de emparejamiento exirán a los 30 días desde iOS 11 en adelante.

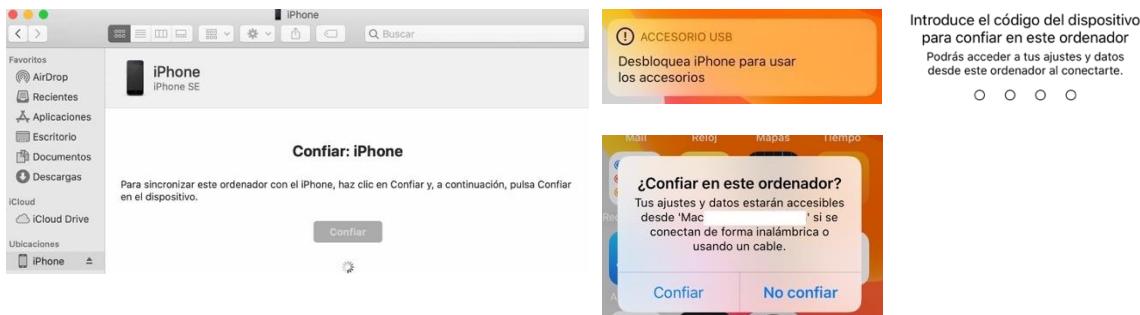


Figura 61 - Establecimiento de la relación de confianza por USB entre iOS 13 y macOS Catalina

Lamentablemente, iOS no dispone de ningún menú para consultar las relaciones de confianza que se han establecido previamente con otros equipos, ni tampoco ninguna opción para eliminarlas sin afectar a ningún otro ajuste. La única acción que permite eliminarlas es devolver los ajustes de privacidad al estado de fábrica (evitando así conexiones automáticas futuras desde los equipos en los que se había confiado anteriormente, pero que también elimina muchos otros ajustes), a través del menú "Ajustes - General - Restablecer - Restablecer localización y privacidad".

Desde el punto de vista de seguridad, se desaconseja conectar el dispositivo móvil a ordenadores de terceros vía USB. En caso de que tal conexión sea requerida, y se autorice el establecimiento de una relación de confianza, se aconseja restablecer las conexiones de confianza existentes a través del menú "Ajustes - General - Restablecer - Restablecer localización y privacidad".

12.3.2 MODO RESTRINGIDO USB

Con la versión 11.4.1 de iOS, Apple introdujo el denominado "modo restringido USB" (USB Restricted Mode) [Ref.- 40], consistente en impedir que se establezcan conexiones de datos por parte de dispositivos USB con el iPhone si ha transcurrido más de una hora desde la última vez que se estableció la conexión USB. Para que este modo esté vigente, la opción "Ajustes - Touch ID & código - Accesos USB" ha de estar desmarcada (ver tercera imagen de la <Figura 12>). Como protección adicional para evitar la manipulación de esta opción, se recomienda establecer una restricción sobre el acceso al menú "Touch ID & código", tal como se recomienda en el correspondiente apartado.

Para obtener información detallada sobre el modo restringido USB, su evolución a través de iOS 12, y las mejoras introducidas en iOS 13, consultar la [Ref.- 50]. Entre las novedades introducidas en iOS 13 destaca que adicionalmente al establecimiento de emparejamientos o relaciones de confianza entre un dispositivo móvil iOS y un ordenador, Apple ha introducido el concepto de emparejamientos con dispositivos USB.

Para emparejar un dispositivo USB con iOS 13, a diferencia de un ordenador, no es necesario introducir el código de acceso y no existe ningún intercambio de claves criptográficas (tal como

se ha descrito anteriormente), pero el dispositivo móvil debe de estar desbloqueado, o debe ser desbloqueado en ese momento. Como resultado, se almacenará información sobre el dispositivo USB en iOS, y éste pasará a ser un dispositivo de confianza. Durante el periodo de una hora en el que se permiten conexiones USB, la conexión de un dispositivo USB en iOS 13 es gestionada de manera diferente si se trata de un dispositivo de confianza previamente parejado, o de un dispositivo nuevo: en el primer caso se permitirá la conexión de datos, mientras que en el segundo caso, las capacidades de datos del puerto USB serán restringidas, incluso dentro del periodo de una hora. Es decir, la conexión de cualquier nuevo dispositivo USB en iOS 13 requiere desbloquear el dispositivo móvil.

12.4 VPN

Recomendaciones de seguridad:

- Hacer uso de soluciones de VPN, especialmente si se requiere conexión a través de redes Wi-Fi abiertas (lo cual está desaconsejado).

iOS proporciona soporte para las siguientes tecnologías VPN:

- IPSec (*Cisco IP Security*).
- IKEv2.
- L2TP (*Layer Two Tunneling Protocol*; 1701/udp) en combinación con *Internet Protocol Security* (L2TP/IPSec; 500/udp).
- Redes VPN SSL: no de forma nativa, sino a través de aplicaciones cliente propietarias.

La opción recomendada desde el punto de vista de seguridad pasa por emplear IPSec o L2TP/IPSec. Para ello, existen en el mercado diversas soluciones VPN, incluso gratuitas.

iOS proporciona capacidades VPN en modo *split tunneling* para separar el tráfico entre/desde redes públicas y privadas, en función de cómo se defina la política de seguridad asociada.

Adicionalmente, iOS dispone de capacidades VPN personalizables (*VPN On Demand*) para dispositivos gestionados a través de una solución MDM (*Mobile Device Management*), que permiten establecer automáticamente la VPN al acceder a ciertos dominios o direcciones IP pre-configuradas.

El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi o VPN se detalla en el apartado "17. Certificados digitales".

La configuración de redes VPN en iOS puede realizarse a través de perfiles de configuración (cuya descripción excede el ámbito de la presente guía) o de forma manual. Para ello, se accederá a "Ajustes - General - VPN - Añadir configuración VPN...":

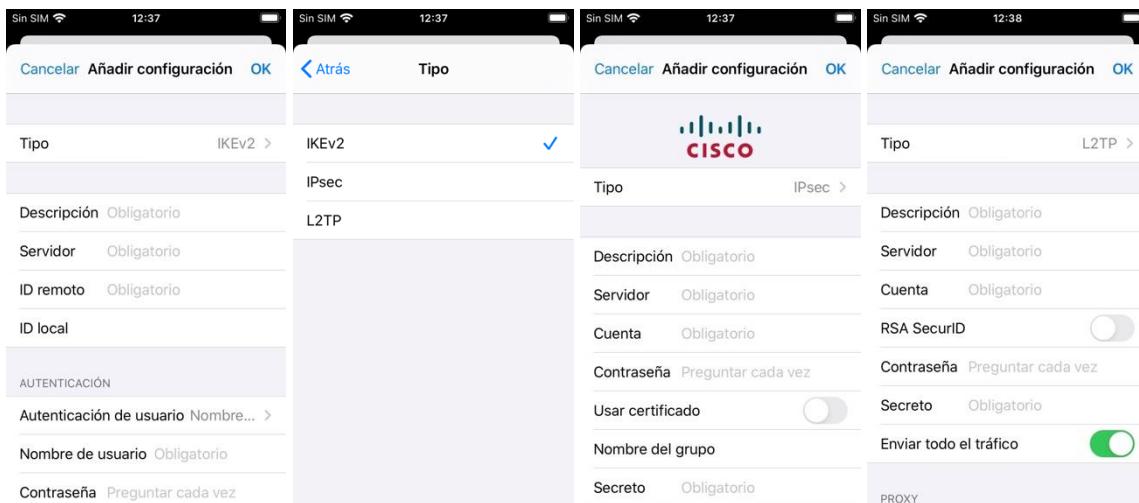


Figura 62 - Menú de configuración de VPN

En el caso de redes L2TP/IPSec (reflejadas como "L2TP"), iOS obliga a configurar el secreto L2TP (o clave pre-compartida para el acceso a la red), opción que permite autenticar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (ver imagen derecha de la <Figura 62>). Como se puede ver en dicha imagen, la configuración para L2TP/IPSec permite especificar si se hará uso de autenticación mediante contraseña o a través de dos factores, (opción RSA SecurID, deshabilitado por defecto), así como definir si se enviará todo el tráfico a través de la red VPN (en lugar de hacer uso de *split tunneling*), mediante la opción "Enviar todo el tráfico" (habilitada por defecto), y **recomendada desde el punto de vista de seguridad**.

Una vez establecida la conexión con la red VPN, el usuario (junto al servidor de VPN) es quien puede restringir las comunicaciones, de forma que todo el tráfico sea cursado a través de la VPN hasta que ésta sea desconectada, es decir, no usando *split tunneling* u *horizon* (conexiones simultáneas directas hacia Internet y a través de la VPN).

En el caso de redes Cisco IPSec, iOS permite establecer el secreto o clave pre-compartida para el acceso a la red, el nombre de grupo IPSec, y si se hará uso de un certificado digital para la autenticación del dispositivo móvil. En caso de emplear un certificado digital, las opciones de "Nombre grupo" y "Secreto" serán reemplazadas por la opción "Certificado", que permite seleccionar el certificado digital cliente de la lista de certificados disponibles (ver apartado "17. Certificados digitales"), tanto los importados previamente por el usuario a través de los perfiles de configuración como los que iOS proporciona por defecto. El certificado digital necesario para Cisco IPSec es de tipo personal, y permitirá autenticar al dispositivo móvil y a su usuario. Adicionalmente es necesario instalar un certificado raíz (perteneciente a la CA), asociado a la generación del certificado digital empleado por el servidor o concentrador de VPN.

Una vez configurada, el uso de una red VPN puede activarse desde "Ajustes - VPN". iOS reflejará la duración de la conexión actual e informará sobre el direccionamiento IP, y mostrará el ícono "VPN" en la barra superior de estado.



Figura 63 - Conexión VPN establecida

Las contraseñas de las redes VPN pueden:

- Quedar almacenadas por defecto en los ajustes de configuración de red, no siendo necesario por parte del usuario introducir las credenciales de acceso a la VPN (nombre de usuario y contraseña) para establecer la conexión con la red VPN seleccionada. En este caso, si un potencial atacante dispusiera de acceso no autorizado al dispositivo móvil, podría establecer conexiones con la red VPN automáticamente, salvo que la red VPN haga uso de autentificación de dos factores, en el cual sería necesario adicionalmente disponer del *token* de generación de contraseñas de un solo uso asociado.
- Omitirse de la configuración de la VPN dejando en blanco el campo "Contraseña", con lo que el campo quedará marcado como "Preguntar cada vez" (en color gris).

Los dispositivos móviles iOS no disponen de un mecanismo por defecto (sí a nivel empresarial) para limitar la conectividad únicamente a través de redes VPN, estando en manos del usuario o de las capacidades *On Demand* (solo para ciertas direcciones o dominios) el establecimiento de la conexión VPN, además de las posibles desconexiones de la VPN cuando el dispositivo móvil es suspendido por falta de actividad.

13. SERVICIOS PROPIETARIOS DE APPLE

iOS hace uso de diversos servicios propietarios destinados a simplificar la comunicación y/o la compartición de datos entre dispositivos Apple. Estos servicios pueden estar vinculados a que exista una sesión activa en la cuenta de iCloud del iPhone (como iMessages, Handoff e Instant Hotspot, que se describen en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.-413]) o no, como los descritos en este apartado.

13.1 AIRDROP

Recomendaciones de seguridad:

- Mantener AirDrop desactivado.
- En caso de requerirse el uso de AirDrop, deshabilitarlo tan pronto finalice la necesidad.
- Evitar habilitar el modo "Todos", especialmente en lugares concurridos, y hacer únicamente uso del modo "Solo Contactos" al hacerse uso de AirDrop.
- 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 para compartición de contenido entre dispositivos Apple que se encuentran en un rango de alcance de Bluetooth. El intercambio requiere que ambos

dispositivos estén desbloqueados³⁶ (si bien para la detección de dispositivos receptores es suficiente con que la pantalla no esté suspendida).

13.1.1 MECANISMO DE FUNCIONAMIENTO DE AIRDROP

Este apartado describe a nivel técnico las características asociadas a AirDrop [Ref.- 39]. AirDrop está basado en:

- El protocolo AWDL (Apple Wireless Direct Link)³⁷, que integra:
 - Bluetooth Low Energy (BLE) para el descubrimiento de dispositivos que soporten el servicio.
 - Una conexión Wi-Fi extremo a extremo (es decir, 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.
- Un mecanismo de autentificación basado en una identidad RSA de 2.048 bits que se almacena en el dispositivo cuando el usuario inicia sesión en iCloud.
- Un conjunto de *hashes* cortos (a partir de los hashes SHA256) que se utilizan como identidad 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.

MECANISMO DE FUNCIONAMIENTO

- El dispositivo emisor desea realizar un envío mediante AirDrop, y emite un anuncio BLE que incluye su identidad 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 identidad 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.
- La respuesta se envía a través de una conexión Wi-Fi punto a punto, y contiene la identidad AirDrop del potencial receptor (mediante un *hash* corto), que el emisor 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 66>):
 - "Personas": si la identidad AirDrop del receptor encontró coincidencia en los contactos del emisor, éste envía a través de una conexión Wi-Fi punto a punto su identidad larga.

³⁶ Existe una excepción a este comportamiento: si emisor y receptor comparten cuenta de iCloud, la transferencia puede efectuarse aunque el receptor esté bloqueado. Dependiendo de la app receptora del contenido, podrá hacerse completamente efectiva o no.

³⁷ <https://owlink.org/wiki/#what-is-apple-wireless-direct-link-awdl>

- Si el receptor valida la identidad larga del emisor en su app Contactos, 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 vinculados a la misma cuenta de iCloud que el emisor.
- "Otras personas": si la identidad AirDrop del receptor no encuentra coincidencia en los contactos del emisor, el emisor mostrará en el panel un ícono 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 AWDL³⁸: 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.

MitM: Mitigation



Figura 64 - Panel de compartición de AirDrop

- Cuando el usuario emisor realiza su selección en el panel, el dispositivo emisor inicia una conexión TLS con el receptor, en la que se intercambian sus certificados de identidad 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.

13.1.2 USO DE AIRDROP

Las capacidades de comunicación de AirDrop en iOS 13 se pueden activar y desactivar desde 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 comunicaciones y

³⁸ <https://www.youtube.com/watch?v=5T7Qatoh0Vo>

seleccionando el ícono "AirDrop" (ver <Figura 22>). Por defecto, se encuentra habilitado solo para los contactos.

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 ícono "↑"³⁹ y:

- Seleccionar el ícono genérico de AirDrop "↑" del menú de compartición (parte inferior de la cuarta imagen de la <Figura 66>): ésta es la opción recomendada desde el punto de vista de seguridad, porque facilita la identificación de ataques de suplantación (ver apartado "13.1.1. Mecanismo de funcionamiento de AirDrop").
- Seleccionar un acceso directo a un contacto mediante su ícono concreto (parte superior de la cuarta imagen de la <Figura 66>). Desde el punto de vista de seguridad, **se debe prestar especial atención a los íconos mostrados por el interfaz gráfico de usuario de iOS** de cara a confirmar si un usuario ha sido autenticado 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). Sin embargo, si se muestra el ícono 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.

NOTA: Durante las pruebas realizadas durante la elaboración de la presente guía, se ha observado que, si el dispositivo está dentro del menú de configuración del punto de acceso personal, las comunicaciones a través de AirDrop no pueden cursarse, incluso aunque no exista ningún dispositivo conectado al *hotspot*.



Figura 65 - Error de AirDrop durante el uso de un punto de acceso personal

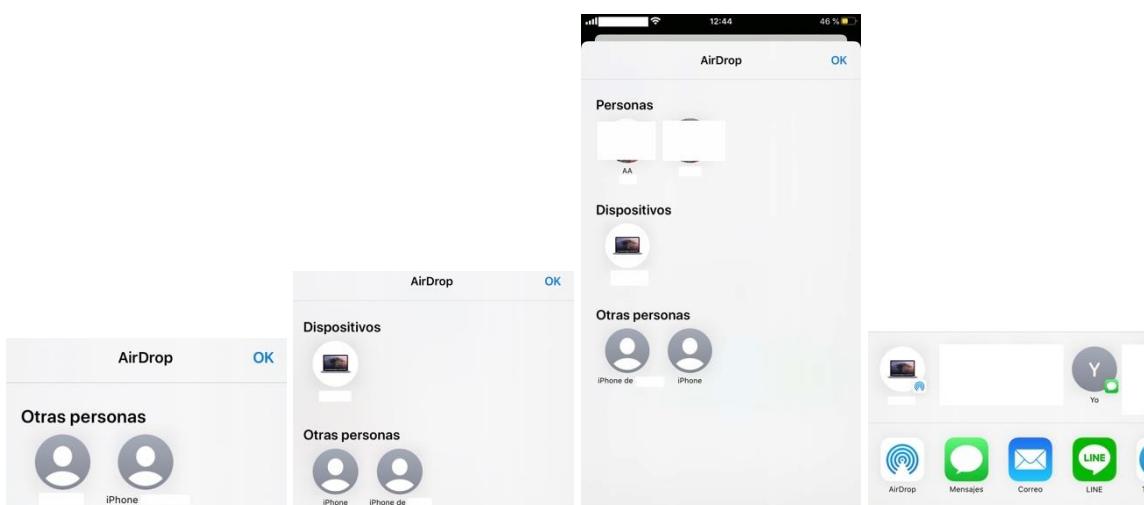


Figura 66 - Compartición de contenidos vía AirDrop

³⁹ Algunas apps disponen del menú "Pulsa para compartir con AirDrop".

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 comienza a divulgar su identidad de AirDrop incluso con la pantalla bloqueada.

El dispositivo receptor mostrará un mensaje solicitando confirmación. Si la emisión proviene de un contacto conocido, iOS mostrará una previsualización del contenido a enviar (primera y segunda imagen de la <Figura 67>). En caso contrario, solo se mostrará una notificación (tercera imagen). Si el dispositivo receptor está bloqueado, se informará al usuario a través de una notificación que, si se despliega, solicitará el método de desbloqueo (cuarta imagen)⁴⁰:

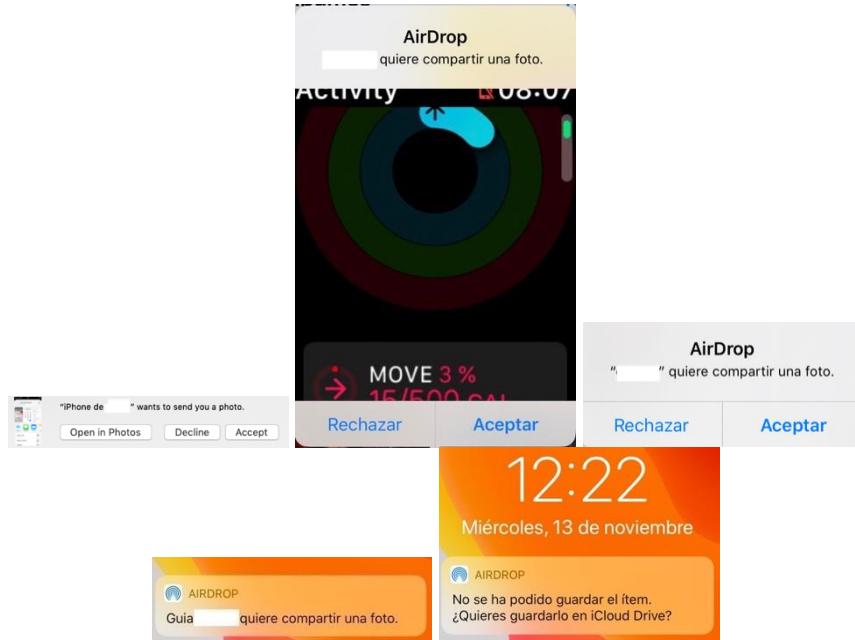


Figura 67 - Solicitud de aceptación de recepción de contenido vía AirDrop

Desde el punto de vista de seguridad, **se recomienda mantener deshabilitado el servicio AirDrop, para lo cual se debe fijar el parámetro "Recepción desactivada" en el "Centro de Control", 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.- 26] para más información).

Es posible establecer una restricción sobre AirDrop (ver apartado "18.4.2. Restricciones") de forma que se impida el envío de datos desde el iPhone mediante este mecanismo.

⁴⁰ 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, podrá hacerse completamente efectiva (por ejemplo, para la app "Notas") o no (por ejemplo, "Fotos" - quinta imagen de la <Figura 69>).

13.2 AIRPLAY

AirPlay es un servicio que permite reproducir contenido audiovisual de dispositivos iOS en un Apple TV utilizando una conexión Wi-Fi punto a punto cifrada con AES 128 bits en la que las direcciones MAC se aleatorizan.

AirPlay utiliza una autenticación IC (*integrated circuit*) que asegura que el extremo receptor ha sido certificado por Apple (ver sección "Verifying accessories" de la [Ref.- 39]).

El uso de este servicio queda fuera del ámbito de la presente guía. Para obtener detalles de uso, consultar la [Ref.- 51].

13.3 COMPARTIR

La función "Compartir" (*Sharing*) permite la transferencia de contenidos desde el contexto actual con otras apps y servicios, tanto dentro del propio dispositivo como con dispositivos externos.

Está basada en el uso de las denominadas "extensiones", que son capacidades dentro de una app cuyo propósito es ofrecer funcionalidad a otros componentes a través de APIs, imponiendo políticas para una determinada área del sistema. El sistema operativo comprueba las extensiones disponibles según las reglas que sean de aplicación para un entorno concreto y lanza los procesos correspondientes. En el caso de la función "Compartir", sus extensiones asociadas (denominadas "*share extensions*") solo pueden estar disponibles en el panel de compartición, que se inicia pulsando sobre el ícono "✉" dentro de una app que lo soporte.

El mecanismo detallado de funcionamiento de las extensiones queda fuera del ámbito de la presente guía, pudiéndose obtener más información en la [Ref.- 52].

13.3.1 PANEL DE COMPARTICIÓN

El panel de compartición de iOS 13 se organiza en cuatro secciones, ordenadas de arriba a abajo:

- Contenido que se va a compartir.
- Accesos directos: opciones de compartición asociadas a un contacto concreto a través de una app predeterminada que iOS ofrece según el historial de actividad del usuario. La app destino se indica mediante un pequeño ícono bajo el avatar del contacto.
- Barra de compartición de apps ("*share extensions*"): muestra las apps con las que se puede compartir el contenido, incluyendo el servicio AirDrop en primer lugar (si está habilitado). Para compartir con otra app o contacto que no se muestre en los menús anteriores, se dispone de la opción "Más" a la derecha de esta barra, que despliega el menú "Apps" con la sección "Sugerencias" desde el que se puede elegir otra app, tras lo cual se mostrará un nuevo menú "Compartir con" particular de dicha app.
- Acciones ("*action extensions*"): lista de todas las acciones compatibles con el contexto. A su vez se divide en:
 - Favoritos: son acciones añadidas manualmente para que estén disponibles como acción.
 - Acciones específicas de la app que proporciona los datos o contenidos.
 - Otras acciones: asociadas a otras apps distintas de la que comparte.

Es posible añadir atajos (ver apartado "9.4.1. Atajos (Shortcuts): automatización en iOS 13"), a la lista de acciones disponibles, pero siempre observando las recomendaciones de seguridad descritas en dicho apartado.

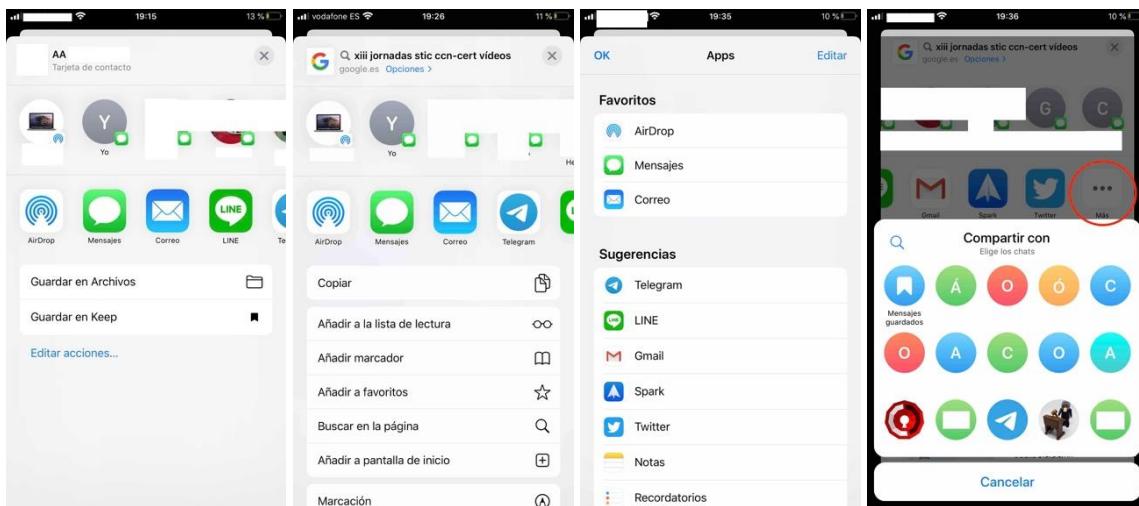


Figura 68 - Panel de compartición

13.3.1.1 Personalización del panel de compartición

Las opciones del panel de compartición se pueden personalizar parcialmente. Por ejemplo, no hay ninguna opción para evitar que la compartición vía AirDrop sea eliminada de este panel.

Desde el punto de vista de privacidad, se aconseja eliminar aquellos elementos (apps o acciones específicas) con los que no se desea poder compartir contenido (por ejemplo, apps de mensajería instantánea) que pueden provocar que una pulsación accidental envíe contenido no deseado.

CONTACTOS DE ACCESO RÁPIDO

No existe ningún procedimiento conocido para modificar (añadir, suprimir, reordenar, etc.) los contactos que se muestran como accesos directos del panel de compartición. Es posible optar por un "todo o nada" eliminando la app de la barra de compartición de apps (según se describe posteriormente) o, para algunas apps (como "Mensajes") eliminando la conversación con un contacto concreto (cosa que puede no resultar deseable).

Este comportamiento es controvertido, ya que puede exponer los contactos y sus avatares a cualquier tercero con acceso visual a la pantalla, y propiciar comparticiones accidentales.

BARRA DE COMPARTICIÓN DE APPS

A través de la función "Más" y el botón "Editar" de "Apps" (tercera imagen de la <Figura 68>) es posible eliminar elementos de la barra "Favoritos" (a través del icono "⊖"), añadirlos (icono "⊕") y ordenar los elementos de la barra (mediante *haptic touch* sobre el botón "≡" y desplazando el elemento a la posición deseada). El interruptor a la izquierda de cada app "⊖" permite deshabilitar/habilitar la presentación de dicha app en los menús de compartición (ver <Figura 69 >).

ACCIONES

Para elegir qué acciones específicas de la app estarán disponibles en el panel, hay que abrir la app y elegir un elemento, datos o contenido, para compartir. Al final del menú de acciones específicas, aparece la opción "Editar acciones", que permite añadir, eliminar y ordenar estas acciones.

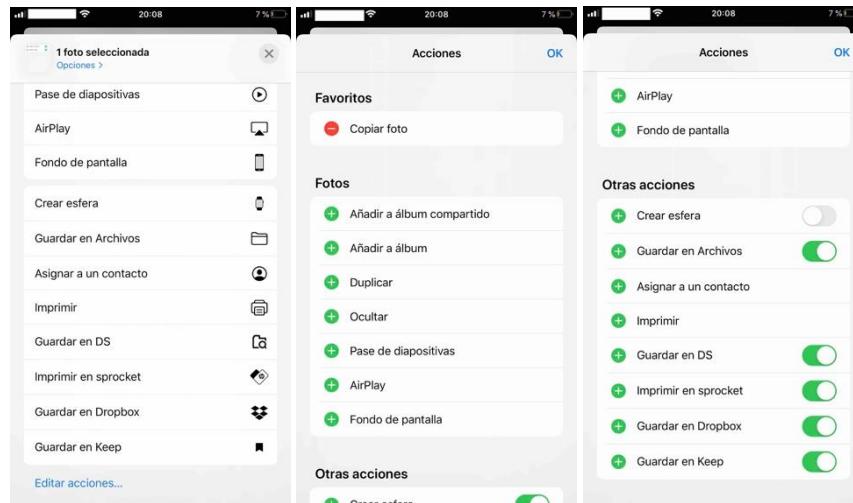


Figura 69 - Personalización de las acciones específicas de compartición de una app

14. SERVICIOS DE LOCALIZACIÓN

Recomendaciones de seguridad:

- Evitar conceder permisos de localización permanentes a apps para las cuales no se desea recibir información de contexto de ubicación salvo cuando se use la app.
- No conceder ningún permiso de localización a las apps cuyo propósito no lo requiera.
- Revisar los privilegios de ubicación de la sección "Servicios del sistema", y limitarlos en lo posible.
- No conceder a "Fotos" el permiso de localización, especialmente si se comparten fotografías a través de cualquier medio.
- No conceder el permiso de localización a apps que ofrecen servicios de redes sociales.

El servicio de localización de iOS permite a las apps y a los servicios del sistema conocer la ubicación del dispositivo móvil, no solo a través del módulo GPS sino también a través de las redes Wi-Fi y las torres de telefonía móvil cercanas. Cuando la ubicación está activa, Apple recibirá del dispositivo datos de localización de antenas de telefonía y redes Wi-Fi cercanas.

Una de las principales características relativas a la privacidad introducidas por iOS 13 son los cambios en los permisos de localización de las apps (sección "Privacidad" de la [Ref.- 29]). Sin embargo, pese a los anuncios de Apple relacionados con la importancia de la privacidad de la localización, hay que resaltar que iOS 13 activa por defecto multitud de ajustes que van en contra de este argumento, por lo que se recomienda conocer y adaptar las opciones de configuración de ubicación para salvaguardar la privacidad del usuario. Tampoco se ha encontrado ningún documento de Apple en el que se describa de forma clara todos los casos de uso de la localización, ni por parte de sus servicios ni de otras apps.

Para deshabilitar por completo el servicio de localización, se puede desactivar el interruptor "Ajustes - Privacidad - Localización". A fecha de elaboración de la presente guía, aunque la localización esté desactivada, el servicio "Buscar" puede localizar el dispositivo si se inicia el "modo perdido" (ver apartado "23.3. Servicios "Buscar").

El ícono "↗" informa, según el código de colores mostrado al final de este menú, qué uso puede hacer o ha hecho de la ubicación un determinado componente.

Dada la importancia de la manipulación de los ajustes de localización, **se aconseja establecer los valores deseados y, una vez completado el proceso, habilitar una restricción para la localización que impida modificarlos por parte de terceros** (ver apartado "18.4.2. Restricciones").

Para restablecer los ajustes de localización y que el usuario vuelva a ser preguntado acerca de los permisos de localización de todas las apps, se dispone de la opción "Ajustes - General - Restablecer - Restablecer localización y privacidad" (ver <Figura 111>).

14.1 PERMISOS DE LOCALIZACIÓN DE LAS APPS

Los permisos de ubicación de una app están disponibles "Privacidad - Localización - [App]" [Ref.-53]. Además de las apps de navegación (como "Mapas"), muchas otras aplicaciones y servicios hacen uso de la localización, entre ellas App Store, Cámara, Safari, Twitter, Brújula, Tiempo o Buscar. Adicionalmente, durante su uso, Siri enviará la localización del dispositivo a Apple. Por este motivo, es importante controlar qué apps tienen concedido el permiso de localización, y adaptarlo según los condicionantes del usuario.

Una de las novedades de iOS 13 es la modificación en el modo que las apps tienen para obtener el permiso de localización. En versiones anteriores, era posible conceder el permiso "Siempre" desde la primera invocación de la app. En iOS 13, se ha comprobado que tiene lugar este flujo:

- 1) La primera vez que se lanza una app, se dispondrá de las opciones de la primera imagen de la <Figura 70>. El permiso que obtendrá la app dependerá de la respuesta del usuario:
 - a. "No permitir": la app "Nunca" podrá acceder a la ubicación del usuario, ni se volverá a interrogar a éste en invocaciones sucesivas.
 - b. "Permitir una vez": la app podrá acceder a la ubicación durante la ejecución en curso, y su permiso de localización quedará fijado en "Preguntar la próxima vez", por lo que, en la siguiente invocación, el usuario recibirá de nuevo la solicitud de permiso.
 - c. "Permitir al usarse la app": la app dispondrá de acceso a la ubicación siempre que lo solicite estando en ejecución. En su sección de permisos aparecerá el texto que la app mostró en la petición de acceso a la ubicación, que, supuestamente, debe informar al usuario del propósito por el que lo solicita.

Algunas apps que solicitan este privilegio y a las que el usuario se lo ha concedido, incluirán la opción "Siempre" entre las opciones de ajustes del permiso de localización, por lo que el usuario puede habilitarlo de forma manual. Adicionalmente, en determinados momentos durante la ejecución de la app, ésta podrá solicitar al usuario el permiso permanente, mediante el cuadro de diálogo de la cuarta imagen de la <Figura 70>. Curiosamente, este menú no permite revocar el permiso de la app.

- 2) En sucesivas invocaciones, las apps que disponen del permiso:
 - a. "Permitir al usarse la app": podrán solicitar periódicamente la concesión de permiso permanente de la cuarta imagen de la <Figura 70>.

En las pruebas realizadas durante la elaboración de la presente guía, transcurridas dos veces de haber solicitado el permiso permanente, la nueva solicitud irá acompañada de un mapa en

el que se mostrará un mapa con ubicaciones que la app ha recopilado en ejecuciones anteriores.

- b. "Permitir siempre": cada cierto tiempo, se volverá a presentar al usuario el menú de la cuarta imagen de la <Figura 70>, junto a un mapa que mostrará actualizaciones de ubicación que la app recogió sin estar en ejecución.

Complementariamente, según se describió en el apartado "12.1.2. Bluetooth", iOS 13 ha introducido una mejora para evitar el rastreo basado en Wi-Fi y BT por parte de apps.



Figura 70 - Permisos de localización de apps en iOS 13

14.2 PERMISOS DE LOCALIZACIÓN PARA SERVICIOS DEL SISTEMA

La primera vez que se activa el interruptor "Localización", por defecto iOS habilitará el permiso de ubicación para los componentes de la sección "Servicios del sistema", que recopilan periódicamente datos de ubicación, y que pueden proporcionar sugerencias basados en ellos (se recomienda leer la [Ref.- 54] para obtener los detalles). Aunque Apple insiste en que estos datos están cifrados, y que no puede obtenerlos, el usuario debe valorar cuidadosamente si desea que esta información sensible esté en poder de un tercero. Desde el punto de vista de la privacidad, *se aconseja suprimir todos los permisos a excepción de "Buscar mi iPhone", "Compartir mi ubicación" (cuando se desee hacer uso de este servicio) y "Llamadas de emergencia y SOS"*.

A modo de ejemplo, en la <Figura 71> se ilustra la información recopilada por el servicio "Lugares importantes". Aunque la consulta de estos datos requiere la autentificación del usuario mediante su método de acceso, el acceso no autorizado a estos datos por parte de un tercero supondría un riesgo importante para su privacidad. Especialmente, el elemento "Casa", que no se define por el usuario, sino que se infiere por parte de Apple basándose en heurísticas sobre el análisis de los datos de ubicación, corresponde al lugar de residencia del propietario del dispositivo, e indica (al igual que para el resto de lugares) los horarios de llegada y permanencia, con total exactitud, y el medio de transporte utilizado.

Con estos datos, es posible que el usuario reciba, aun sin que "Mapas" esté en ejecución y disponiendo de permiso "Al usarse", mensajes como el de la quinta imagen de la <Figura 71>.

NOTA: Este tipo de notificación de mapas contiene información sobre el lugar al que referencia, incluso cuando se recibe estando la pantalla bloqueada, y pese a que el ajuste "Mostrar previsualizaciones" esté a "Si está desbloqueado" (ver apartado "9.5. Centro de notificaciones").

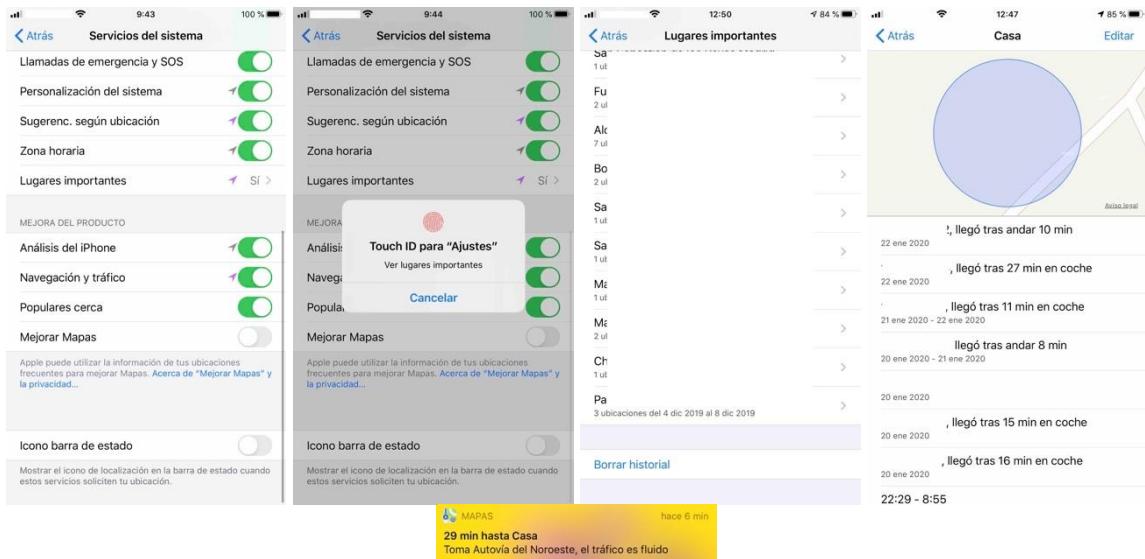


Figura 71 - Uso de la localización por parte de "Servicios del sistema"

El ajuste "Servicios del sistema - Icôno de barra de estado" permite que la barra superior de estado del dispositivo informe cuando un servicio del sistema esté haciendo uso del servicio de localización.

14.2.1 SERVICIO "COMPARTIR MI UBICACIÓN"

iOS proporciona el servicio "Compartir mi ubicación", cuya activación/desactivación puede conseguirse desde:

- Desde el propio menú "Buscar".
- Desde el menú "Ajustes - Privacidad - Localización": para ello, el interruptor "Compartir mi ubicación" de la sección "Servicios del sistema" debe estar habilitado.

Cuando este servicio está activo, a través del cual se permite compartir la ubicación del dispositivo a través de la app "Mensajes" y del servicio "Buscar a mis amigos" (el cual queda fuera del ámbito de la presente guía, pero del cual se puede obtener información en la [Ref.-12]). Este servicio puede resultar interesante como medida de control parental sobre dispositivos de menores, especialmente para los miembros de una familia en iCloud. Desde el punto de vista del usuario adulto, la activación del ajuste debería ser solo puntual, y eliminarse tan pronto finalice la necesidad de usarlo. Ambas acciones requieren que el dispositivo móvil disponga de conexión a Internet.

14.2.2 PERMISO DE LOCALIZACIÓN EN FOTOGRAFÍAS

iOS permite añadir información de la localización geográfica (conocida como geoetiquetas o *geotags*) a las fotografías obtenidas con la cámara del dispositivo móvil si la app "Cámara" tiene concedido el permiso de localización. En caso afirmativo, se añadirá a la cabecera EXIF de la imagen las coordenadas GPS.

La concesión de permisos de ubicación a "Fotos" debe sopesarse cuidadosamente, en especial para su publicación o distribución en Internet, o si se acostumbra a compartir fotografías mediante redes sociales, debido a que las geoetiquetas se incluyen en el fichero que contiene la imagen, permitiendo a cualquier tercero con acceso a ella determinar dónde fue tomada.



Figura 72 - Información de localización en las fotografías

La información de geolocalización de una fotografía no está disponible a través de la app "Fotos", pero sí si se copia a la app "Archivos" y, desde el menú contextual asociado al fichero de la foto, se selecciona "Información - Mostrar más".

Como medida de preservación de la privacidad del usuario, la opción de compartición de la app "Fotos", a través del menú "Opciones" de la parte superior, muestra si la ubicación está incluida en la fotografía y permite, mediante el interruptor "Incluir - Ubicación", suprimirla.

15. GESTIÓN DE CONTRASEÑAS

Recomendaciones de seguridad:

- No acceder al contenido del menú "Contraseñas de webs y apps" si el entorno puede permitir, aunque sea mínimamente, el acceso visual a la pantalla por parte de terceros.
- Hacer uso de la función de autorrelleno frente a teclear el código manualmente en presencia de terceros.
- Si se opta por el uso de gestores de contraseña, elegir uno que requiera autentificación previa.

Desde el punto de vista de seguridad, la principal recomendación que todo usuario debe seguir es la **no reutilización de contraseñas entre servicios y/o apps diferentes**, así como la **selección de contraseñas robustas no vinculadas con información que podría inferirse conociendo al usuario** (como fechas importantes, nombres de familiares, etc.). Dado el elevado número de servicios digitales que actualmente se requiere emplear, para poder seguir esta recomendación de forma factible, es preciso hacer uso de un gestor de contraseñas seguro.

15.1 LLAVEROS - KEYCHAIN

Las credenciales en iOS se almacenan en elementos denominados "llaveros" (*keychains*⁴¹), que son repositorios para la custodia segura de pequeñas cantidades de información sensible: certificados digitales, credenciales asociadas a redes VPN y redes Wi-Fi, contraseñas asociadas a apps y sitios web (para este último caso, solo si el usuario lo autoriza), tarjetas de crédito y otros secretos (por ejemplo, notas seguras). El llavero está a su vez protegido por mecanismos de cifrado.

Apple permite a las apps almacenar contraseñas en el llavero, manteniéndolas fuera de sus respectivos *sandboxes*. Las consultas sobre el llavero se restringen en función del grupo de acceso de la app (las apps de sistema utilizan el grupo de acceso "apple").

La copia de seguridad de un dispositivo almacena también una copia del llavero, la cual puede restaurarse en otro dispositivo (salvo para las apps que establezcan restricciones explícitas).

No todos los elementos del llavero están accesibles para el usuario (tal es el caso de las contraseñas de VPN o Wi-Fi). Únicamente lo están los albergados en la sección "Contraseñas de webs y apps" (ver apartado "15.2. Gestión de los elementos del llavero").

Desde el punto de vista del contenedor, se distingue:

- Llavero local: las credenciales se almacenan cifradas en el propio dispositivo, de forma centralizada, en una base de datos SQL Lite gestionada por iOS para que únicamente cada app pueda acceder a sus propias entradas en el llavero.

El principal riesgo del llavero local es el de sustracción del dispositivo si existe conocimiento del código de acceso por parte de un tercero, lo que permitiría hacer uso del sistema y las apps y de las credenciales almacenadas en el llavero, o que se consiguiese hacer *jailbreak* del dispositivo, lo que posibilitaría la extracción de los contenidos del llavero.

- Llavero de iCloud: las credenciales se almacenan en la nube de Apple asociada a la cuenta de iCloud del dispositivo, de forma que todos los dispositivos vinculados a esta cuenta pueden compartir las credenciales.

El principal riesgo de este llavero está asociado a un potencial compromiso de la cuenta de iCloud desde cualquiera de los dispositivos vinculados a ella.

Complementariamente, el usuario puede optar por el uso de un gestor de credenciales de terceros. En este caso, se debe hacer uso de un gestor que requiera autentificación activa lo más robusta posible por parte del usuario (y, preferiblemente, independiente de la del método de desbloqueo del dispositivo), antes de proporcionar acceso a sus contenidos⁴².

El llavero es un complemento a la solución de cifrado del dispositivo, que iOS proporciona a través de otros mecanismos específicos (ver apartado "19. Cifrado del dispositivo móvil").

15.2 GESTIÓN DE LOS ELEMENTOS DEL LLAVERO

Desde el punto de vista del usuario, los elementos almacenados por él en un llavero se pueden gestionar desde la sección "Contraseñas y cuentas - Contraseñas de webs y apps".

⁴¹ https://developer.apple.com/documentation/security/keychain_services

⁴² Queda fuera del ámbito de la presente guía la evaluación de gestores de contraseñas, siendo tarea del usuario la selección del que mejor responda a sus necesidades.

De esta forma cuando inicie sesión en uno de esos sitios o apps, iOS podrá llenar automáticamente, si el usuario así lo autoriza, las credenciales de acceso.

Para poder manipular los elementos disponibles en el llavero, se solicitará al usuario introducir un método válido de desbloqueo del dispositivo (por ejemplo, *Touch ID* o código de acceso). Los elementos se muestran en el menú "Contraseñas" con entradas que incluyen la app o el sitio web y el login que se ha definido para él. Si se utiliza la misma contraseña para sitios web del mismo dominio, solo se mostrará una entrada que indicará uno de los sitios y el número de sitios adicionales que comparten las credenciales (segunda y tercera imágenes de la <Figura 73>).

Las acciones disponibles sobre estos elementos son:

- Añadir nuevos (menú "+").
- Modificarlos: seleccionando el elemento y, seguidamente, la opción "Editar".
- Eliminarlos: de forma individual (posicionando el dedo sobre él y desplazándolo hacia la izquierda de la pantalla), o colectiva (a través de "Editar" seguido de la selección de los elementos a suprimir y la confirmación mediante el botón "Eliminar").
- Copiar el nombre de usuario o la contraseña: mediante "*haptic touch*" sobre el elemento y eligiendo el componente a copiar.
- Compartirlos entre dispositivos vinculados a una misma cuenta de iCloud: accediendo a los contenidos de un elemento y mediante "*haptic touch*" sobre los campos "Nombre de usuario" o "Contraseña" hasta que aparezca el menú que incluye "AirDrop" (segunda imagen de la <Figura 74>). El elemento será transferido al dispositivo que se seleccione, y añadido a su sección "Contraseñas y cuentas" (esta opción no es de aplicación si el usuario hace uso del Llavero de iCloud en ambos dispositivos, porque, en dicho caso, los servicios de Apple mantendrán los elementos sincronizados en la nube de iCloud, accesible por todos los dispositivos vinculados a la cuenta).

Para ayudar al usuario en las buenas prácticas en el uso de contraseñas, iOS marcará con el símbolo "⚠" las entradas para las cuales se haya detectado alguna anomalía. Por ejemplo:

- Reutilización de contraseñas para sitios no pertenecientes al mismo dominio.
- Uso de contraseñas débiles.

En ambos casos, accediendo al elemento, se indicará cuál es la anomalía y se ofrecerá el menú "Cambiar la contraseña en el sitio web", que conectará con el sitio.

IMPORTANTE: en iOS 13, si toma una captura de pantalla desde el menú "Contraseñas" para un elemento concreto, en la captura no se mostrará el campo "Contraseña", lo cual es un elemento de seguridad notable para evitar fuga de credenciales mediante el método de captura de pantalla y envío a través de la función de compartición (ver apartado "13.3. Compartir").

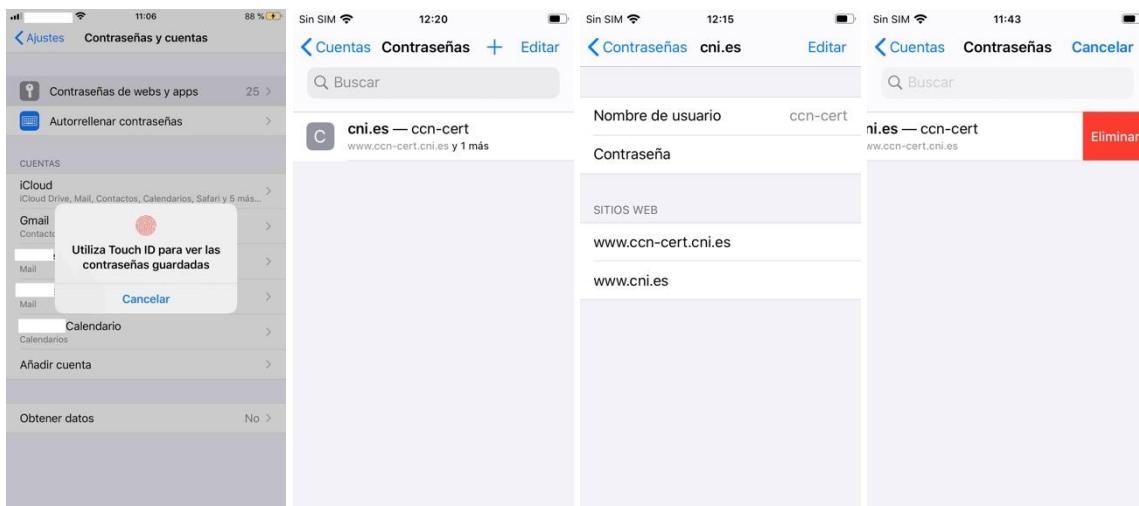


Figura 73 - Menú "Contraseñas de webs y apps" de iOS 13



Figura 74 - Copia de campos y elementos y alertas de seguridad de credenciales

Otra medida adicional de seguridad en iOS 13 es que, si el usuario deja en segundo plano la pantalla de configuración de "Contraseñas de webs y apps" mientras está consultando o accediendo a sus elementos, la próxima vez que el menú vuelva a primer plano no la hará en esta pantalla, sino en su pantalla madre "Contraseñas y cuentas", por lo que se requerirá de nuevo autenticación para acceder a este contenido sensible.

El contenido del llavero puede ser consultado de forma activa por parte del usuario cuando requiera introducir las credenciales en un sitio web o una app, y también puede ser empleado por parte de la función "Autorrellenar contraseñas" si está activa (ver apartado "15.4. Autorrellenar contraseñas").

15.3 LLAVERO DE ICLOUD

Apple proporciona capacidades centralizadas de almacenamiento de credenciales, similares a las de otros gestores de contraseñas, en un repositorio (*keychain*) residente en iCloud (de lo cual surge el apelativo de "Llavero de iCloud" o *iCloud Keychain*), que permite compartición de elementos entre los diferentes dispositivos Apple asociados a una misma cuenta de iCloud.

La funcionalidad del llavero de iCloud se habilita/deshabilita a través de "Ajustes - [Cuenta de usuario] - iCloud - Llavero" (ver tercera imagen de la <Figura 113>). Si se desea desactivar el uso del llavero de iCloud, se podrá optar por mantener las credenciales almacenadas en el llavero local o eliminarlas del dispositivo móvil (ver imagen derecha de la <Figura 114>). En la [Ref.-56] se pueden obtener los detalles de uso y configuración del llavero de iCloud.

El llavero de iCloud solo sincroniza aquellos elementos del *keychain* del usuario que han sido identificados con el atributo que permite su sincronización entre dispositivos, es decir, que son exportables (o no son únicos) para cada dispositivo. Por ejemplo, las identidades de redes VPN no son sincronizadas y 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.

Tanto la versión de Mobile Safari disponible en iOS como la 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). Esta funcionalidad de Safari se complementa con capacidades para autocompletar formularios web.

Desde el punto de vista de seguridad, *se debe valorar si se confía plenamente en Apple para la custodia en la nube de las contraseñas, así como tener en cuenta que, al estar disponibles en todos los dispositivos de un usuario (se empleen o no todas las credenciales en todos los dispositivos), basta con que uno de ellos sea comprometido para que todas las contraseñas puedan quedar expuestas.*

15.3.1 GENERACIÓN AUTOMÁTICA DE CONTRASEÑAS

Si el llavero de iCloud está habilitado, iOS podrá detectar cuándo el usuario está creando una nueva credencial para un sitio web o una app compatible y sugerirá una contraseña única y segura para el usuario, cuya parte inicial se mostrará. El usuario podrá optar por "Usar contraseña segura" (para crear la credencial en base a dicha contraseña) o "Seleccionar yo la contraseña" (para crear la credencial en base a una contraseña propia).



Figura 75 - Generación automática de contraseña

15.4 AUTORRELLENAR CONTRASEÑAS

Esta funcionalidad iOS permite al usuario llenar los campos de un formulario de credenciales sin tener que teclearlos manualmente [Ref.- 37]. Cuando el autorrelleno está activo, iOS hace uso de heurísticas para que, al tratar de ingresar en una app o sitio web, se presente al usuario la denominada barra "QuickType".

- Si no existe ningún gestor de contraseñas instalado por el usuario en el dispositivo, la funcionalidad hará uso del llavero local de iOS, que solo requiere la activación del interruptor "Contraseñas y cuentas - Autorrellenar contras." (primera imagen de la <Figura 76>).

- Si existe algún gestor instalado que implemente una extensión de proveedor de credenciales, asociada al *framework "AuthenticationServices"*⁴³ [Ref.- 36], aparecerá el menú "Autorrellenar contraseñas" (primera imagen de la <Figura 73>), que da acceso al interruptor de activación y al de selección de los gestores disponibles para utilizar para el autorrelleno, incluyendo el llavero de iOS. Es posible seleccionar uno o varios gestores de los mostrados en la sección "Permitir autorrelleno automático desde".

Con la función de autorrelleno activa, cuando se acceda a un sitio web o app que solicite introducción de credenciales, iOS presentará al usuario un menú con las opciones resultantes de la aplicación de sus heurísticas, entre las que se pueden incluir:

- En caso de que un gestor incluya elementos para el sitio web en concreto, iOS mostrará el campo correspondiente al nombre de usuario en primer lugar.
- Si el usuario ha autorizado el autorrelleno para más de un gestor (primera imagen de la <Figura 77>), y varios incluyen entradas para el sitio, el usuario podrá elegir de qué gestor se deben tomar las credenciales. Adicionalmente, se incluirá un acceso genérico al gestor por si se desea utilizar una credencial diferente, aunque no esté asociada al sitio concreto.
- Si el usuario solo dispone del llavero de iOS, se presentará el menú "Contraseñas" (cuarta imagen de la <Figura 77>).
- Si ningún gestor incluye elementos para el sitio web concreto, se ofrecerá al usuario acceso a todos los gestores autorizados para el autorrelleno, de modo que pueda seleccionar, si lo desea, alguna otra credencial.

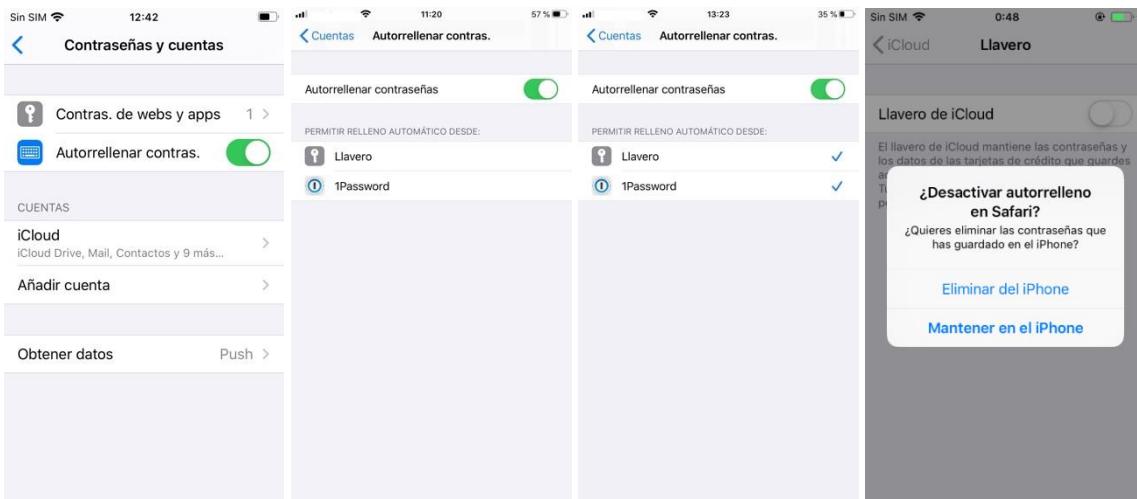


Figura 76 - Configuración de la funcionalidad de autorrelleno de contraseñas

⁴³ Por ejemplo, Last Pass (<https://www.lastpass.com/es>), Dashlane (<https://www.dashlane.com/es/>) y 1Password (<https://1password.com/es/>).

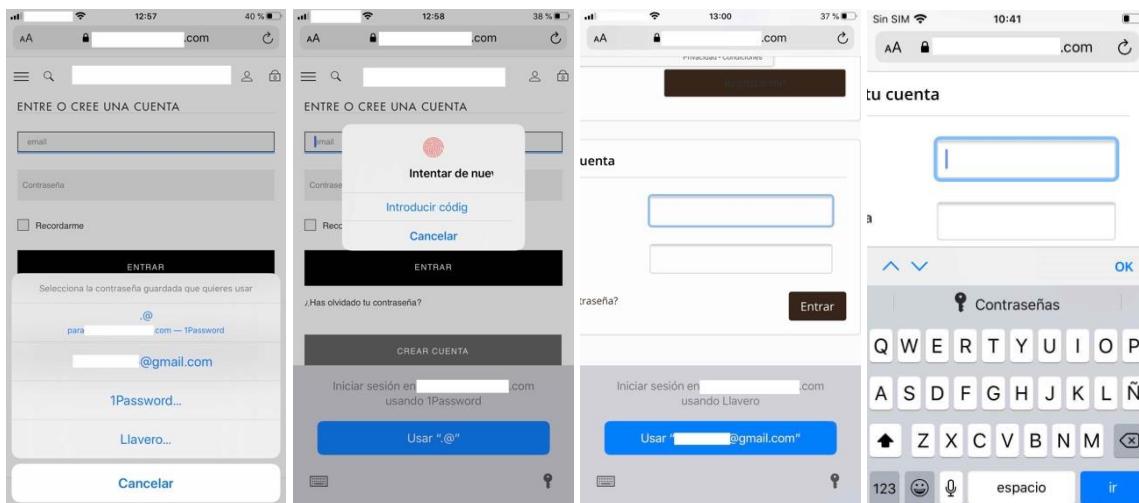


Figura 77 - Autorrelleno de contraseñas en Safari

15.4.1 RELLENO AUTOMÁTICO DE CÓDIGOS DE SEGURIDAD RECIBIDOS POR SMS

La activación del autorrelleno de contraseñas conlleva desde iOS 12 el denominado "relleno automático de códigos de seguridad" (*security code autofill*), que captura los mensajes SMS asociados a contraseñas o códigos de un solo uso (OTP - *One Time Password*) y muestra la opción de autorrellenar automáticamente el código recibido en la app destinataria a través de la barra "QuickType" (disponible en la parte superior del teclado). El usuario podrá pulsar sobre el código, que se insertará automáticamente en el campo correspondiente. Esta función pretende simplificar de cara al usuario la introducción de credenciales asociadas a un segundo factor de autentificación (2FA). Para detectar cuándo un SMS puede corresponder a un código, se utilizan elementos heurísticos como inclusión en el texto de las palabras "código" o "contraseña".



Figura 78 - Función de autorrelleno códigos de un solo uso recibidas por SMS

16. NAVEGADOR WEB MOBILE SAFARI

Mobile Safari es el navegador web incluido por defecto en iOS, cuyos ajustes se acceden a través de "Ajustes - Safari", y que presenta bastantes novedades en iOS 13:

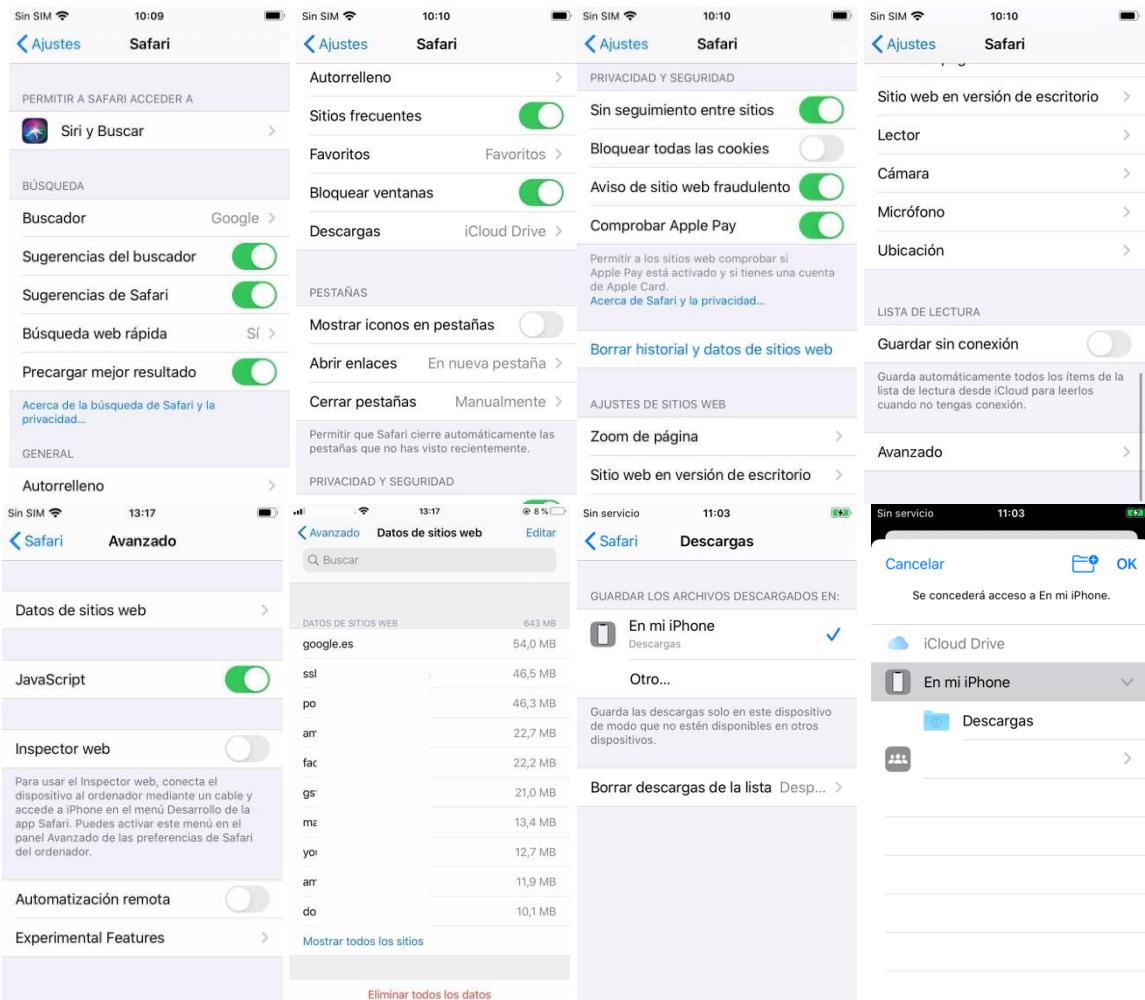


Figura 79 - Ajustes del navegador web Mobile Safari

Safari puede almacenar sus datos de navegación bien en el propio iPhone, bien en iCloud, de forma que puedan ser compartidos con y desde otros dispositivos vinculados a la cuenta (si la opción "iCloud - Safari" está activa, que es la situación por defecto). Aunque con iOS 13 Apple ha añadido cifrado punto a punto para el historial de Safari y las pestañas abiertas que están sincronizadas con iCloud, desde el punto de vista de privacidad se aconseja mantener los datos de Safari en el almacenamiento local.

16.1 NUEVAS FUNCIONALIDADES DE IOS 13 PARA SAFARI

Entre las características que se incorporan a Safari en iOS 13 se encuentran [Ref.- 64]:

- Se añade compatibilidad con llaves de seguridad FIDO2, tanto con interfaz USB y *Lighting* como NFC.
- Detección de contraseñas débiles en sitios web, que permite acceder a la URL para reemplazarla por una nueva.

- Soporte para la funcionalidad "*Sign in with Apple*", descrita en el apartado "11.1.1. Iniciar sesión con Apple".
- Mejoras en la prevención de seguimiento por parte de sitios web a través de la cabecera "*referrer*" y de técnicas de "*link decoration*"⁴⁴ (que utilizan URLs únicas con contenido extra añadido para obtener información del usuario).
- Mejoras en el *sandbox* de Webkit, el motor de navegación que utiliza Safari.
- Medidas de prevención para que los *iframes* de terceros no puedan navegar en la página.
- Incorpora opciones para activar bloqueadores de contenido, tanto a nivel general como granular (para cada sitio web), si se dispone de extensiones específicas para ello⁴⁵.

A continuación se describen las nuevas funcionalidades accesibles para el usuario.

16.1.1 INTERFAZ DE USUARIO DE SAFARI

A nivel de interfaz gráfico, la versión de Safari suministrada con iOS 13 se muestran diversas categorías adaptadas a la navegación del usuario, que incluyen sus sitios favoritos, los sitios visitados con más frecuencia y sugerencias de Siri (si están habilitadas), entre las que se incluyen los sitios abiertos en instancias de Safari de otros dispositivos vinculados a la misma cuenta de iCloud (esta funcionalidad está asociada a los denominados "servicios de Continuidad", descritos en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]). *Se recomienda desactivar la presentación de sugerencias de Safari para proteger la privacidad*, para lo cual se dispone del ajuste "Safari - Sugerencias de Safari" (ver <Figura 79>).

Safari incorpora un menú contextual accesible mediante *haptic touch*, desde el que se accede a la previsualización del sitio web y a diferentes opciones (ver <Figura 80>), que son dependientes del elemento que se haya seleccionado (por ejemplo, un botón que proporciona funcionalidad en la web, una imagen, etc.) y del contexto desde el que se haya seleccionado (por ejemplo, si se ha seleccionado desde la sección de sugerencias del interfaz de Safari, se puede elegir que no se vuelva a incluir esa página como sugerencia, lo que resulta interesante desde el punto de vista de privacidad).

La gestión de los marcadores y favoritos, así como otras propias de la función de navegación se proporcionan a través del menú "Compartir" "✉", desde el que es posible, mediante el menú "Opciones", elegir el formato que se utilizará para enviar el contenido del sitio.

El menú "AA" de la barra de navegación, además de permitir adaptar el tamaño de la fuente, da acceso a los ajustes específicos del sitio web.

Safari 13 mejora la gestión de pestañas, disponiendo de la opción "[Pestañas] Cerrar pestañas" para cerrar automáticamente las pestañas abiertas, y facilitando su incorporación al menú "Marcadores" mediante el menú contextual que se despliega desde el icono "☰".

La gestión de certificados digitales no ha cambiado con la versión de Safari de iOS 13, por lo que el navegador sigue presentando las carencias descritas en el apartado "17.4. Gestión de certificados en Mobile Safari").

⁴⁴ Intelligent Tracking Prevention 2.3. Webkit. <https://webkit.org/blog/9521/intelligent-tracking-prevention-2-3/>

⁴⁵ How to Enable Content Blockers in Safari for iOS. MacRumors. <https://www.macrumors.com/how-to/enable-content-blockers-safari/>

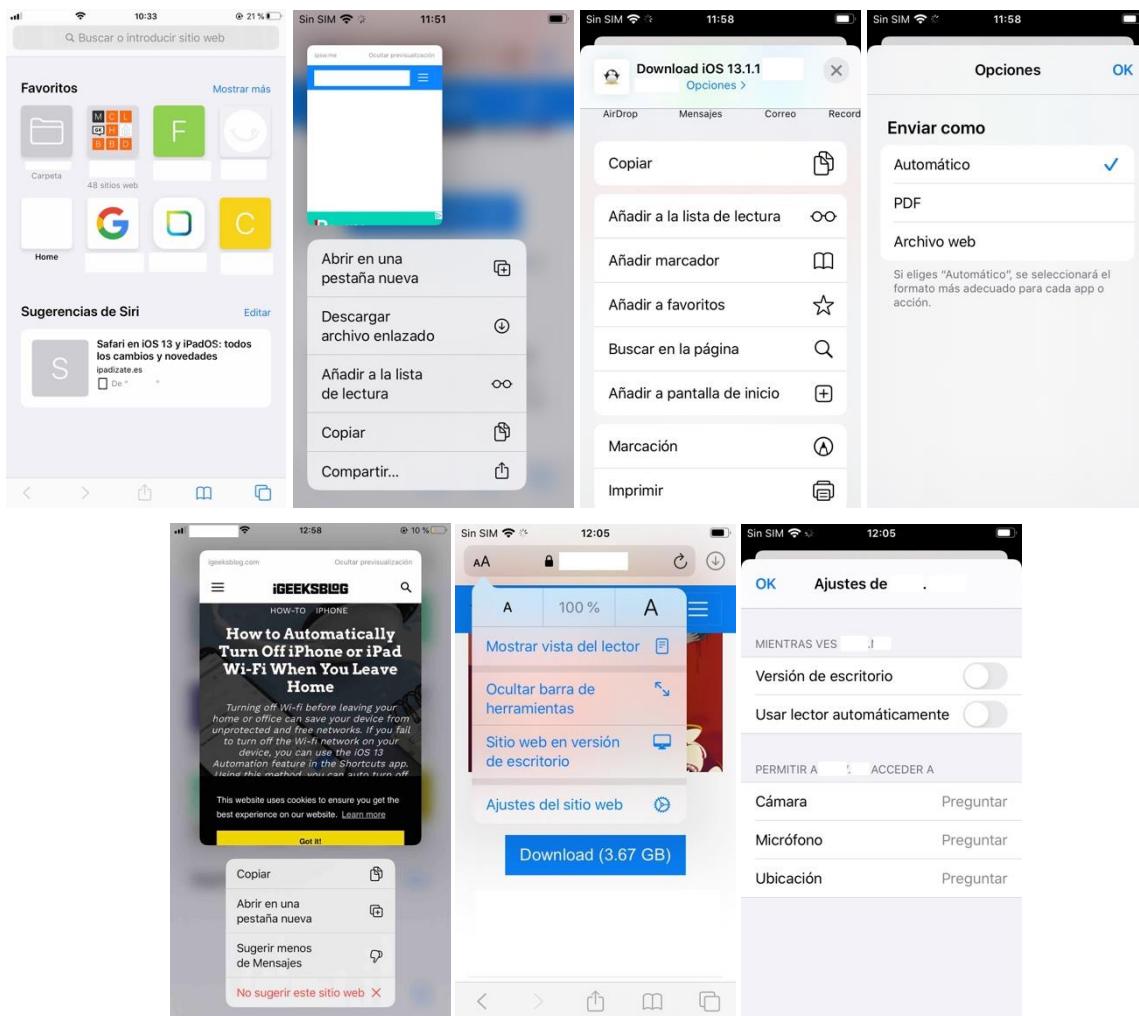


Figura 80 - Interfaz de usuario de Safari, menú contextual y opciones de compartir

16.1.2 AJUSTES DE PRIVACIDAD SELECTIVOS

Safari incorpora ajustes selectivos a nivel de sitio web para controlar el uso de la cámara, el micrófono y la localización (ver <Figura 80>). Estos ajustes se acceden desde el menú "AA" que se encuentra a la izquierda de la barra de navegación.

Desde el punto de vista de seguridad/privacidad, *se aconseja evitar la concesión de estos permisos a los sitios web*. Si se hiciese uso de un servicio que los requiera, por ejemplo, servicios de videoconferencia, *se aconseja suprimirlo tan pronto cese la necesidad de uso*.

16.1.3 GESTOR DE DESCARGAS

Safari incorpora en iOS 13 un nuevo gestor de descargas para almacenar los ficheros que se obtienen de Internet a través suyo, y que, por defecto, son ubicados en "iCloud Drive" si existe una cuenta de iCloud activa en el dispositivo. Esta ubicación se puede cambiar desde el ajuste "Safari - Descargas" (ver <Figura 79>).

Cuando el usuario inicia una descarga, el gestor aparecerá en la barra superior de Safari con el símbolo "🕒", desde el que se puede controlar la descarga: ver el progreso, pausarla,

reanudarla, y acceder a sus detalles mediante el icono "🔍", que abre el interfaz de la app "Archivos", con acceso a toda su funcionalidad.

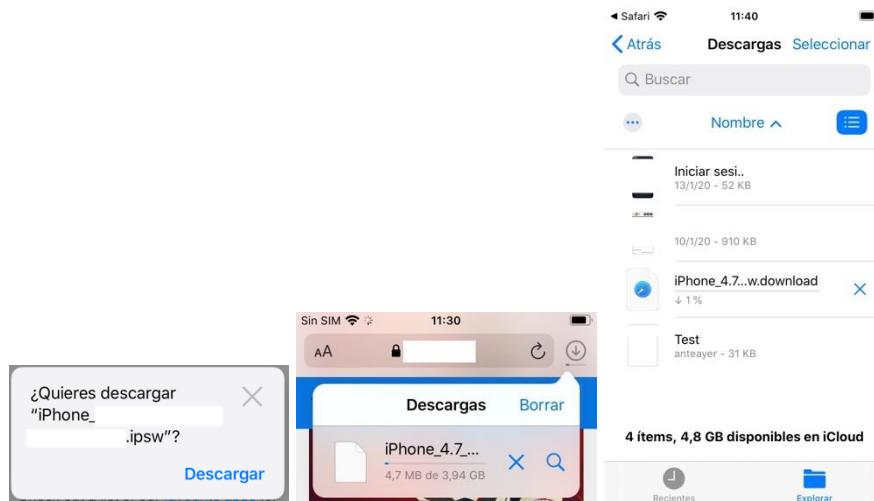


Figura 81 - Gestor de descargas de Safari y menú contextual

16.2 AJUSTES DE SAFARI

Desde el punto de vista de seguridad, **se recomienda**:

- "Precargar mejor resultado": **desactivar**, evitando que se acceda a páginas sin control por parte del usuario.
- "Bloquear ventanas": **activar** para evitar las ventanas emergentes (*pop-ups*) que los sitios web pueden tratar de abrir sin que el usuario lo solicite expresamente.
- "Sin seguimiento entre los sitios": **activar** para evitar que los sitios web realicen seguimiento de las actividades de navegación y búsquedas con objetivos de publicidad.
- "Aviso de sitio web fraudulento": **activar**.
- "Cámara", "Micrófono", "Ubicación": **activar**.
- "Comprobar Apple Pay": **desactivar**.
- "Avanzado - Automatización remota": **desactivar**.
- "Avanzado - JavaScript": dependerá de las preferencias del usuario.
- "Autorrelleno": esta sección permite configurar si el navegador web puede completar automáticamente en los formularios de páginas web los datos de contacto del usuario a partir de la entrada definida en el campo "Mis datos" (que permite seleccionar un contacto concreto de la agenda de contactos), así como tarjetas de crédito. Desde el punto de vista de privacidad/seguridad, no resulta conveniente que Safari disponga de esta información, ya que una potencial vulnerabilidad del navegador podría exponerla en sitios web fraudulentos, además de posibilitar que el usuario acepte introducirla de forma accidental e involuntaria por lo sencillo de su acceso. Únicamente estaría recomendado el uso de autorrelleno si el usuario debe introducir frecuentemente esta información sensible en presencia de terceros, ya que, en este caso, puede resultar más comprometido el acceso visual no deseado.

Si el autorrelleno está activo, Safari mostrará en la barra "QuickType" situada sobre el teclado la opción correspondiente (por ejemplo, "Autorrelleno de contacto" - segunda imagen de la <Figura 82>).

Complementariamente, Safari puede autorrellenar credenciales de sitios web (ver apartado "15.4. Autorrellenar contraseñas"). Con esta función activa, si se introducen unas credenciales para un sitio web para el cual no se tienen almacenadas, Safari solicitará confirmación para añadirlas al llavero.

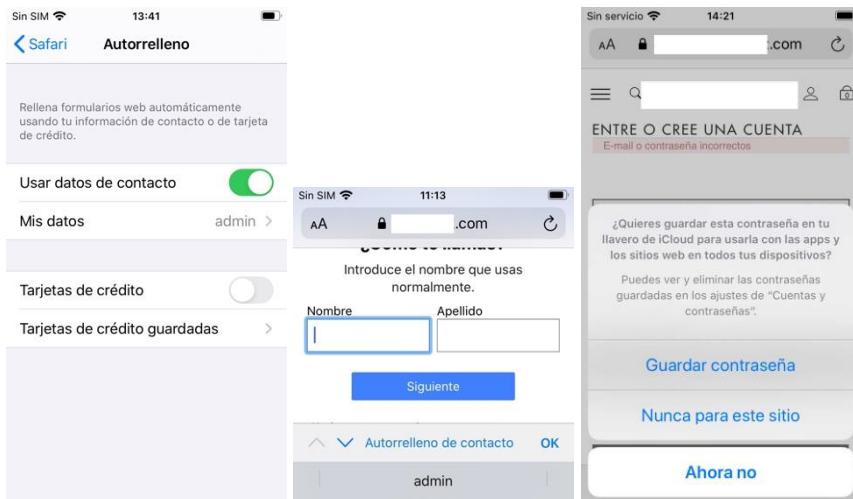


Figura 82 - Uso de las capacidades de autorrelleno en Safari

Los ajustes permiten además "Borrar historial y datos de sitios web", tanto global (aplicará a los datos de navegación y cookies de todos los sitios web) como individualmente, a través de "Avanzado - Datos de sitios web - Editar". **Se recomienda limpiar el historial periódicamente para proteger la privacidad del usuario.**

Se recomienda hacer uso de las capacidades de navegación privada (Private Browsing) de Mobile Safari, que evitan que se almacene en el dispositivo el histórico de navegación o las cookies, o que se sincronicen otros datos de navegación con otros dispositivos, para salvaguardar la privacidad del usuario. Para ello se dispone de la opción "Nav. privada" existente en la esquina inferior izquierda del menú que se despliega al abrir una nueva pestaña vacía.

17. CERTIFICADOS DIGITALES

Recomendaciones de seguridad:

- No instalar ningún certificado digital cuya confianza no esté convenientemente verificada.
- Procurar descargar los certificados a través de medios fiables.
- No aceptar conexiones con sitios web cuyo certificado no sea válido.

Los certificados digitales en iOS se almacenan en el *keychain* (ver apartado "15.1. Llaveros - Keychain").

iOS admite la importación de certificados digitales X.509 en formato PKCS#12 que contengan solo una identidad, tanto ficheros con extensión .p12 y .pfx, como .cer, .crt y .der.

Los certificados digitales cliente pueden emplearse para el acceso y autentificación a través de Microsoft Exchange ActiveSync, redes Wi-Fi o conexiones VPN, y para la firma y cifrado de correos electrónicos con S/MIME; los certificados digitales servidor son empleados para la

protección de las comunicaciones, incluyendo las anteriores y, para el acceso a páginas web mediante HTTPS desde Safari (incluyendo soporte para OCSP).

17.1 CERTIFICADOS RAÍZ

Los certificados de autoridades certificadoras, conocidas como CAs (*Certificate Authorities*), necesarios para establecer cadenas de confianza, y que en iOS se denominan "perfiles" pueden ser instalados:

- Automáticamente (opción recomendada desde el punto de vista de seguridad), mediante el uso de perfiles MDM (*Mobile Device Management*) o a través de Apple Configurator.
- Manualmente: transfiriéndolos al dispositivo móvil a través de:
 - Una conexión a un ordenador desde iTunes (hasta macOS 10.14 Mojave) o Finder (desde macOS 10.15 Catalina).
 - A través de un fichero adjunto a un correo electrónico: en ese caso, se recomienda hacer uso de mecanismos de cifrado y firma, para permitir la verificación de su autenticidad.
 - A través de AirDrop: dados los problemas de seguridad inherentes a este servicio, se desaconseja la descarga de certificados por este medio (ver apartado "17.3. Instalación de certificados transferidos vía AirDrop").
 - Descargándolos directamente desde una página web mediante Safari. En caso de emplear un servidor web interno a la organización, éste debe hacer uso de mecanismos de autenticación y de cifrado para proteger sus comunicaciones.

Las implicaciones del uso de certificados digitales en funciones de seguridad críticas requieren que el usuario del dispositivo móvil sea muy cuidadoso a la hora de añadir nuevos certificados digitales al dispositivo móvil, y especialmente, al almacén de certificados raíz o autoridades certificadoras reconocidas.

Respecto al conjunto de certificados digitales raíz preinstalados por defecto en el dispositivo móvil, conocido como "almacén de confianza" (*Trust Store*), iOS no proporciona ningún menú o interfaz gráfico del dispositivo móvil que permita consultarlos, ni tampoco se dispone de ninguna opción en el interfaz de usuario que permita modificar la lista de autoridades certificadoras raíz proporcionada por defecto. Sí es posible acceder a los certificados digitales raíz instalados por el usuario a través del menú "Ajustes - General - Perfiles", desde donde pueden eliminarse de forma individual.

Los certificados de confianza se clasifican según tres políticas de confianza:

- De confianza (*trusted*): corresponden a los certificados de confianza de autoridades certificadoras (CAs) raíz o intermedias.
- Preguntar siempre (*always ask*): corresponden a certificados que no son de confianza; al ser utilizados, se interrogará al usuario para que decida si confía en él y lo acepta o no.
- Bloqueados (*blocked*): corresponden a certificados que han sido comprometidos y nunca serán aceptados como de confianza.

En la [Ref.- 21] se puede consultar la versión de la *Trust Store* correspondiente a iOS 13. Para conocer la versión de la *Trust Store* instalada en el dispositivo iOS, se dispone del ajuste "General - Información - Ajustes de cert. de confianza". En esta sección también se pueden gestionar los certificados raíz instalados mediante un perfil (última imagen de la <Figura 86>).

La instalación manual de un certificado (como parte de un perfil) no implica que se confíe en él para las comunicaciones que usan TLS, sino que se requiere que el usuario del dispositivo

móvil active la confianza en él a través del interruptor "Ajustes de cert. de confianza - [Confiar en los certificados raíz] [entrada del certificado]":



Figura 83 - Certificados raíz disponibles en el dispositivo

17.2 CERTIFICADOS CLIENTE

Al instalar un certificado digital cliente, denominado certificado de identidad (*Identity Certificate*) y también conocido como certificado "hoja", protegido por una contraseña, iOS solicitará al usuario tanto el código de acceso al dispositivo móvil como la contraseña del certificado antes de proceder a su instalación (al introducir esta última, los caracteres se mostrarán brevemente tras cada pulsación, por lo que debe realizarse esta operación fuera del alcance visual de terceros), confirmándose finalmente si el perfil ha sido o no instalado:

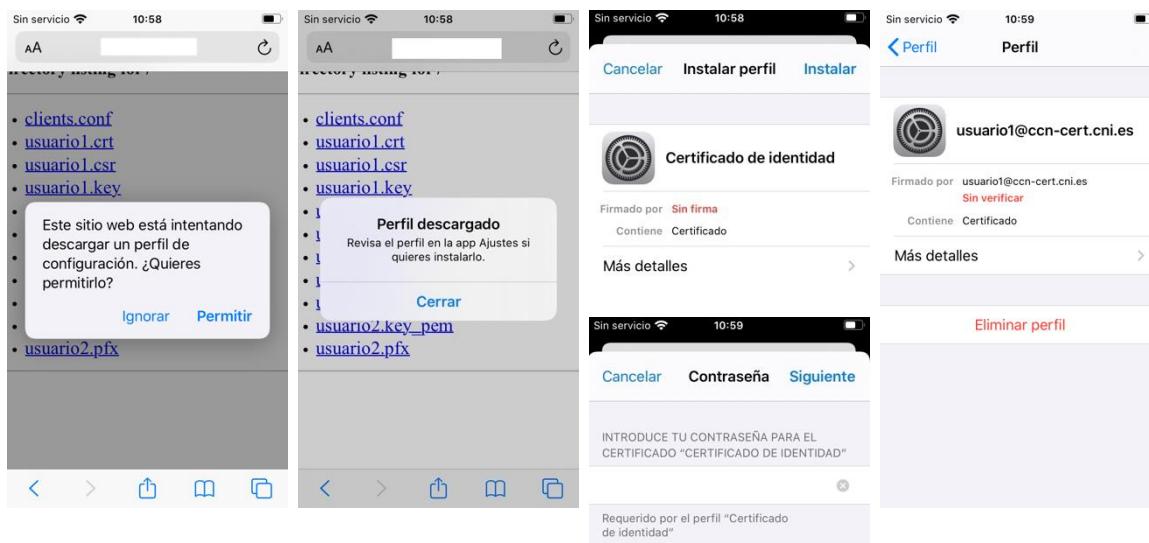


Figura 84 - Instalación de un certificado cliente o de usuario

NOTA: Los requisitos que debe cumplir un certificado digital de servidor para ser aceptado en iOS 13 se detallan en la [Ref.- 57]. Por ejemplo, no se admiten certificados firmados empleando hashes SHA-1, ni certificados cuyas claves RSA sean de tamaño inferior a 2.048 bits.

La confianza reflejada en el certificado ("Sin verificar", cuarta imagen de la <Figura 84>) depende de si iOS dispone de la cadena de confianza completa para dicho certificado, es decir, si también confía en la CA que lo ha emitido, así como de si el certificado cumple los requisitos establecidos por Apple para iOS 13 (ver nota previa). En iOS, si un certificado hoja ha sido emitido por una CA que aún no se ha dado de alta en el almacén de certificados del dispositivo móvil, el certificado hoja aparecerá como "Sin verificar".

Al igual que para los certificados de CA, es posible acceder a los certificados hoja instalados previamente a través del menú "Ajustes - General - Perfiles", y eliminarlos de forma individual.



Figura 85 - Información sobre los perfiles

17.3 INSTALACIÓN DE CERTIFICADOS TRANSFERIDOS VÍA AIRDROP

iOS 13 permite la transferencia de certificados en formato soportado desde cualquier dispositivo Apple al iPhone a través de AirDrop. Como ilustra la <Figura 86>, iOS cataloga los certificados recibidos como perfiles, y los añade a la sección "Ajustes - Perfil descargado", desde donde el usuario puede examinarlos e instalarlos.

La instalación del certificado requiere introducir el código de acceso, tras lo cual será añadido a la sección "Ajustes - General - Perfil" con la condición "Verificado". No obstante, no podrá hacerse uso del certificado hasta que se active su interruptor en la sección "Ajustes de certif. de confianza" (última imagen de la <Figura 86>).





Figura 86 - Instalación de un certificado descargado vía AirDrop

17.4 GESTIÓN DE CERTIFICADOS EN MOBILE SAFARI

La descarga de certificados a través de Safari provocará que se muestre al usuario una ventana de diálogo informando de la intención del sitio web de instalar un perfil de configuración (primera imagen de la <Figura 84>); si el usuario acepta mediante el botón "Permitir", el perfil se descargará y podrá instalarse accediendo a "Ajustes - Perfil descargado". El resto del proceso es idéntico al descrito en los apartados previos.

iOS dispone de una implementación propia de los protocolos TLS (*Transport Layer Security*), utilizando TLS 1.2 por defecto para conexiones HTTPS y la negociación Wi-Fi EAP-TLS (este comportamiento se puede cambiar mediante un perfil de configuración).

Aplicaciones cliente como Safari, Calendario o Mail hacen uso de estos protocolos si el acceso al servidor correspondiente solicita su utilización. Al acceder a un sitio web mediante HTTPS (y, por tanto, HTTP sobre TLS) utilizando Safari, el dispositivo móvil verificará el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (*CA, Certificate Authority*) reconocida correspondiente.

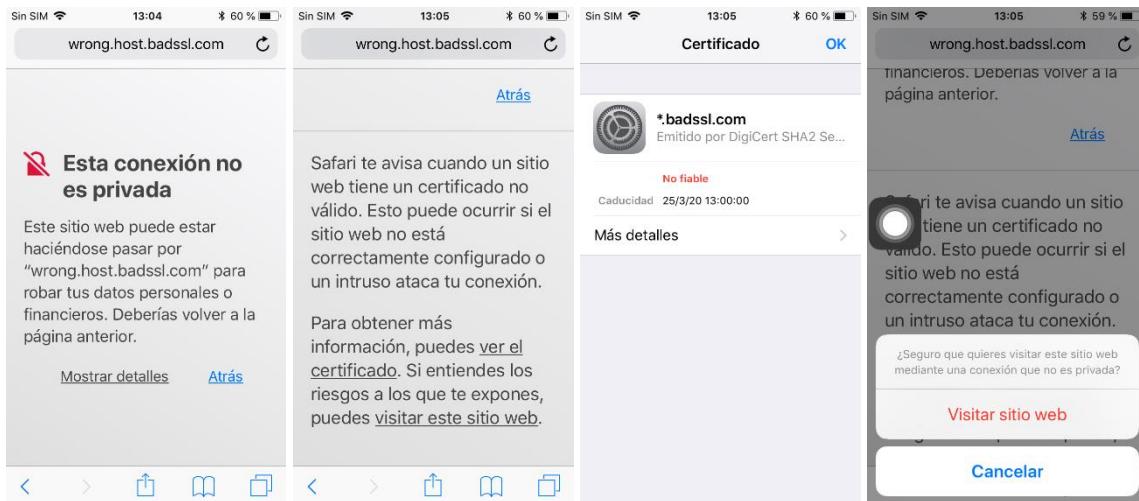


Figura 87 - Manejo de certificados inválidos en Safari

En caso de que no sea posible verificar la validez de un certificado, el navegador web de iOS generará un mensaje de advertencia, indicando el motivo del error y permitiendo al usuario ver y analizar algunos detalles del certificado digital obtenido (mediante el botón "Mostrar detalles"). Si, pese a ello, se opta por aceptar el certificado, se volverá a pedir al usuario confirmación sobre la intención de visitar el sitio web (ver imagen previa).

El navegador web Safari presenta diversas y notables deficiencias, tanto en la gestión de certificados digitales como en la notificación al usuario sobre la existencia de diferentes escenarios relacionados con HTTPS, que limitan significativamente la validación de sitios web:

- iOS presenta una vulnerabilidad desde sus versiones iniciales: la aceptación de un certificado digital lo convierte en válido de forma permanente. ***Es extremadamente importante evitar la aceptación de un certificado que no sea de confianza y no haya podido ser validado, ya que el certificado no podrá eliminarse:***

- Ni cerrando la instancia actual del navegador Safari.
- Ni reiniciando el dispositivo.
- Ni mediante la eliminación de los datos del sitio web accedido a través del menú "Ajustes - Safari - Avanzado - Datos de sitios web".
- Ni mediante el borrado del historial y de todas las cookies y datos de Safari (a través del menú "Ajustes - Safari" y los botones "Borrar historial" y "Borrar cookies y datos").

La acción de aceptar un certificado no verificado tiene el riesgo de que el certificado digital aceptado (y desconocido) pertenezca a un potencial atacante realizando un ataque de interceptación, **MitM (Man-in-the-Middle)**, sobre el protocolo TLS y las comunicaciones (supuestamente) cifradas del usuario.

- Una vez se ha establecido una conexión de confianza mediante HTTPS con un sitio web, no se dispone de ninguna opción en el interfaz de usuario de Safari o iOS para poder ver el certificado digital asociado, lo que facilita la realización de ataques de suplantación sobre los certificados TLS e imposibilita que el usuario realice ninguna verificación.
- La verificación de certificados digitales con validación extendida solo se identifica a través del color de las letras y el candado asociado al título de la página web, que será de color verde si se trata de un certificado con validación extendida y negro o gris si no lo es (<Figura 88>).



Figura 88 - Visualización del uso de un certificado en la barra de Safari

En el caso de páginas web que combinan tráfico HTTPS cifrado con tráfico HTTP no cifrado, el usuario podrá ver la indicación de "https://" en la barra de dirección de Safari, pero el candado asociado al uso de HTTPS no aparecerá en el título de la página, indicando que cierto tráfico es intercambiado de forma no cifrada (no siendo notificado el usuario mediante ningún otro mensaje de aviso).



Figura 89 - Ausencia del candado en una página web con contenido mixto en la barra de Safari

NOTA: Los perfiles de configuración de iOS (fuera del ámbito de la presente guía) disponen del ajuste ("Allow user to accept untrusted certificates"), que permite configurar el dispositivo móvil para impedir al usuario aceptar certificados digitales que no son de confianza. Se recomienda hacer uso de este ajuste para limitar los riesgos asociados al establecimiento de

comunicaciones con servicios remotos que emplean certificados digitales que no son de confianza.

18. GESTIÓN DE LAS APPS

Apple indica que iOS 13 introduce (aunque condicionado a múltiples factores) mejoras en el tiempo de arranque de las apps, que, complementariamente, se comprimirán en la App Store para reducir su tamaño y el de sus actualizaciones⁴⁶.

APP STORE

La "App Store" es el mercado oficial de software de Apple, desde el que es posible instalar y actualizar aplicaciones, así como la versión de iOS. El uso de los servicios de la App Store requiere la existencia de una cuenta vinculada a ella, definida en el menú "Ajustes - iTunes Store y App Store - ID de Apple" (ver apartado "11.3. Cuenta de iTunes & App Store"), y que puede o no coincidir con la cuenta vinculada al ID de Apple del dispositivo (empleada para el acceso a los servicios de iCloud según se describe en el capítulo "23. Anexo A - Cuenta de iCloud"). **Se recomienda independizar el Apple ID utilizado para la App Store del utilizado para los servicios de iCloud**, de forma que no sea fácil inferir uno a partir del otro, y que se independicen los servicios de iCloud del acceso y las compras de apps y contenidos en la App Store.

Para instalar una nueva app en iOS 13, es preciso abrir la app "App Store" (ícono "A") (la primera vez solicitará el permiso de ubicación, que se aconseja denegar) y buscar la app por nombre a través del menú "Buscar" (Q). En función del método de desbloqueo del dispositivo y de los ajustes "iTunes Store y App Store - Ajustes de contraseña" (esto último solo si no está activo ningún método de desbloqueo basado en biometría), será o no preciso introducir la contraseña vinculada a la cuenta de "App Store".

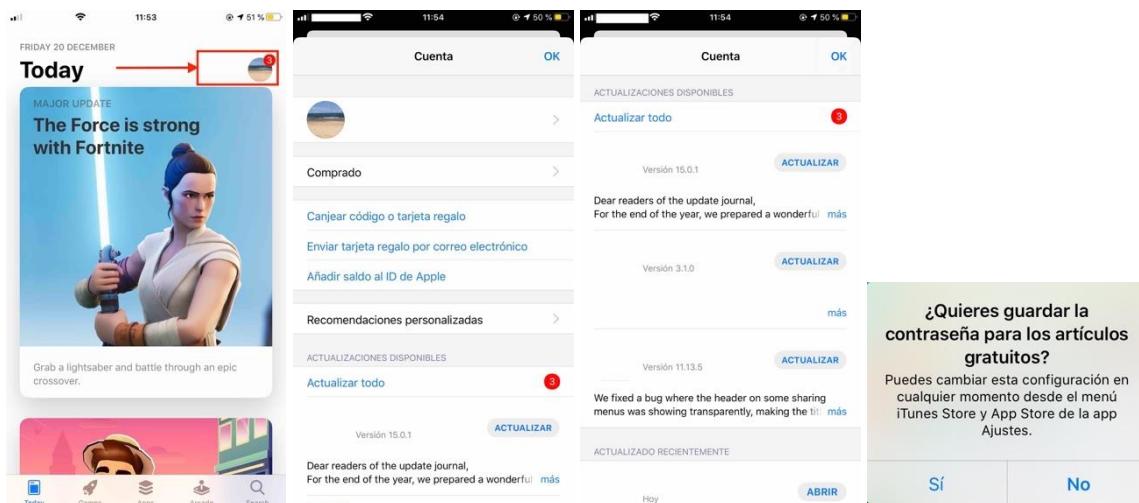


Figura 90 - App "App Store"

Se aconseja no fijar el ajuste "Descargas de apps" a "Permitir siempre" para evitar consumo de datos inesperado, especialmente si se está accediendo a través de una conexión de roaming.

Se aconseja no guardar la contraseña para evitar instalación accidental de apps.

⁴⁶ <https://www.apple.com/es/ios/ios-13/features/#footnote-8>

18.1 ACTUALIZACIÓN Y ELIMINACIÓN DE APPS

Recomendaciones:

- Mantener las apps actualizadas para evitar vulnerabilidades ya resueltas en versiones recientes, pero realizar actualizaciones manuales para controlar qué funcionalidades añade o suprime la nueva versión, incluyendo las modificaciones a los términos y condiciones de uso.
- Desinstalar las apps cuyo uso ya no es necesario.

Una vez instalada una app, es posible:

- Actualizarla: **se recomienda mantener actualizadas las apps para evitar problemas de seguridad resueltos en versiones más recientes**, bien:
 - Manualmente (**opción recomendada**), tras haber comprobado la estabilidad de la nueva versión y que no introduce ningún cambio indeseado (para ello, consultar siempre la descripción de la actualización (botón "Más" <Figura 90>). Para que iOS no proceda a la actualización automática de apps, la opción "Ajustes - iTunes Store y App Store - Actualizaciones de apps" (tercera imagen de la <Figura 44>) debe estar desmarcada. La disponibilidad de una nueva versión se reconoce porque el ícono de la "App Store" presentará una bola roja con un número en la parte superior que identifica el número de apps pendientes de actualizar (""). En iOS 13, para actualizar una app, se requiere abrir la "App Store", pulsar en el ícono asociado al perfil de la cuenta (en la parte superior izquierda) y seleccionar el botón "Actualizar" (<Figura 90>). **Se recomienda realizar una copia de seguridad antes de proceder a la actualización.**
 - Automáticamente (opción por defecto): si la opción "Ajustes - iTunes Store y App Store - Actualizaciones de apps" (tercera imagen de la <Figura 44>) está activa.
- Desinstalarla:
 - Manualmente (opción recomendada):
 - Eliminando sus binarios, pero manteniendo sus datos y configuración, de forma que estén disponibles si se reinstala: para ello, se debe desinstalar la app a través de "Ajustes - General - Almacenamiento del iPhone - [Nombre de la App] - Desinstalar app" (tercera imagen de la <Figura 91>).
 - Eliminando todos los ficheros (datos y binarios) de la app, de dos formas posibles:
 - "Ajustes - General - Almacenamiento del iPhone - [Nombre de la App] - Eliminar app" (tercera imagen de la <Figura 91>).
 - Pulsando sobre su ícono en la pantalla de inicio mediante "*haptic touch*" y seleccionando "Eliminar app" (primera y segunda imagen de la <Figura 91>).
 - Manteniendo pulsado el ícono de cualquier app en la pantalla de inicio mediante "*haptic touch*" y, una vez se obtiene el primer menú contextual, mantener la presión sobre el ícono hasta que aparezcan en pantalla los iconos de todas las apps en movimiento con el símbolo "" sobre ellos.
 - iOS permite eliminar algunas de las apps que vienen suministradas de fábrica, incluyendo Mail, Notas, Recordatorios, Atajos, FaceTime y Mapas. Las que no pueden eliminarse son aquellas cuyo ícono no presenta la "" cuando se efectúa la pulsación para eliminar apps (por ejemplo, Teléfono, Cámara, Fotos o Salud).
 - Automáticamente: iOS 13 dispone de la opción "Ajustes - iTunes Store y App Store - Desinstalar apps no utilizadas" (cuarta imagen de la <Figura 44>). Las apps desinstaladas a

causa de esta opción aparecerán en la pantalla Home con el símbolo "⟳", y, para reinstalarlas, no será necesario abrir la App Store, sino únicamente pulsar sobre ese icono.

- Permitir/denegar que pueda actualizar sus datos en segundo plano (es decir, sin que el usuario interactúe directamente con ella). Para ello, se dispone de la opción "Ajustes - General - Actualización en segundo plano" (cuarta imagen de la <Figura 91>), que permite desactivarse globalmente (seleccionando "No") y activarse globalmente o por aplicación (mediante "Wi-Fi" o "Wi-Fi y datos móviles"). **Se aconseja permitir actualizaciones automáticas solo de aquellas apps que lo requieran** (por ejemplo, apps de mensajería) y denegarlo para aquellas cuyo estado solo importa durante el tiempo en que se interactúa con ellas (por ejemplo, procesadores de texto).



Figura 91 - Gestión de apps en el dispositivo móvil

18.2 APPS RELEVANTES DESDE EL PUNTO DE VISTA DE SEGURIDAD

El presente apartado profundiza en las apps suministradas con iOS 13 que tienen impacto desde el punto de vista de seguridad.

18.2.1 APP "ARCHIVOS"

Recomendaciones de seguridad:

- Restringir el tipo de acceso a los ficheros de la app "Archivos" al compartirlos.
- Comprobar los metadatos de los ficheros obtenidos de fuentes externas.

La app "Archivos", que proporciona acceso a determinados contenidos del almacenamiento del dispositivo móvil, ha sido mejorada en iOS 13, incluyendo nuevas funcionalidades:

- Proporciona información de metadatos de los ficheros, de forma que es posible conocer su tipo, tamaño, y fecha de creación y modificación (<Figura 94>). **Se recomienda consultar estos metadatos, especialmente para la comprobación de ficheros descargados de Internet.**

- Permite crear carpetas en el almacenamiento local, y acceder a sus contenidos de forma similar a cualquier otro tipo de disco externo (hasta iOS 12 solo permitía gestión de iCloud Drive). Esto permite, por ejemplo, conectar otros dispositivos de almacenamiento, como cámaras de fotos o tarjetas de memoria, y transferir sus contenidos al iPhone sin necesidad de utilizar la app "Fotos".
- Soporta acceso a dispositivos USB, incluso discos externos.
- Incorpora la carpeta "Descargas" para albergar los ficheros descargados por el gestor de descargas de Mobile Safari y los adjuntos de la app Mail.
- Soporta compresión y descompresión de ficheros a través de menús contextuales.
- Incorpora accesos directos (disponibles si se utiliza un teclado externo).
- Permite acceder a ficheros de almacenamiento externo, tanto para visualizarlos como para copiarlos.
- Soporta SMB para conectarse a un servidor de ficheros en red de forma remota (a través del menú "... de la sección "Explorar").
- Soporta compartición de carpetas de iCloud Drive a través de enlaces [Ref.- 58]. Desde el punto de vista de seguridad, **se recomienda restringir el acceso al archivo** utilizando el menú contextual que aparece aplicando "haptic touch" sobre la carpeta y seleccionando la opción "Compartir - Opciones para compartir" con las opciones más restrictivas posibles (<Figura 93>).
- Incorpora opciones de búsqueda para localizar contenidos de forma rápida, y sugerencias de búsqueda que se muestran bajo la barra horizontal del menú "Buscar".
- Incorpora un escáner para digitalizar documentos y almacenarlos tanto en local como en iCloud Drive (a través del menú "...").



Figura 92 - Acceso a un servidor de ficheros remotos a través de SMB



Figura 93 - Compartición de carpetas de iCloud Drive en iOS13

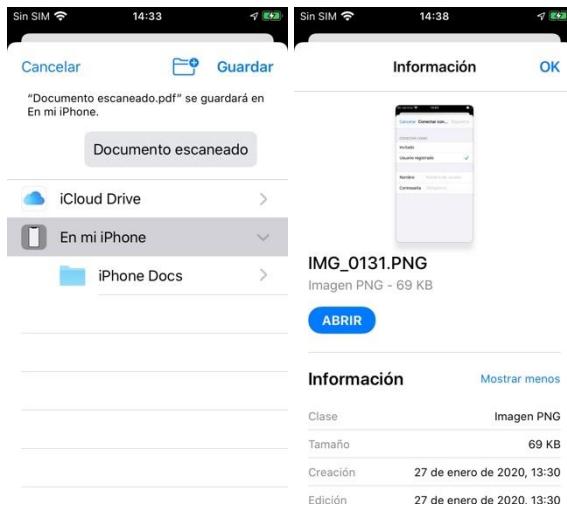


Figura 94 - Funcionalidad de escaneo de documentos y visualización de metadatos de la app "Archivos"

18.2.2 APP "NOTAS"

Recomendaciones de seguridad:

- Bloquear con contraseña las notas de contenido sensible.
- Utilizar contraseñas diferentes para las notas bloqueadas almacenadas en iCloud y para las notas almacenadas en el iPhone.
- No permitir el acceso a "Notas" con la pantalla bloqueada.

En iOS 13, la app "Notas" cuenta con ajustes y funcionalidades estrechamente relacionados con la seguridad y/o la privacidad. La app "Notas" puede almacenar sus contenidos en:

- La cuenta de iCloud vinculada al dispositivo móvil (valor por omisión).
- El almacenamiento local del dispositivo móvil. Para ello, debe habilitarse el interruptor "Ajustes - Notas - Cuenta de iPhone" (ver primera imagen de la <Figura 95>).

Cuando se habilita el ajuste "Cuenta de iPhone", se creará una nueva carpeta raíz en la app "Notas" asociada a "iPhone". Desde ese momento, cuando se cree una nueva carpeta de notas

en el nivel raíz, iOS interrogará al usuario sobre el destino de almacenamiento de dicha carpeta.

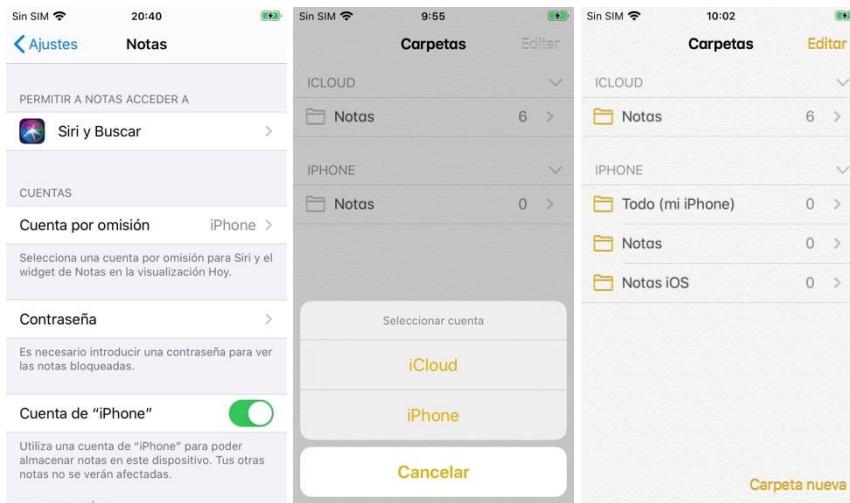


Figura 95 - Almacenamiento de la app "Notas"

El ajuste "Cuenta por omisión" afecta únicamente a cuál será el almacenamiento que se consultará para el *widget* "Notas" en la "Vista de hoy" (ver apartado "9.4. Today View") y por parte del asistente Siri.

18.2.2.1 Notas bloqueadas

Una de las funcionalidades más importantes es el establecimiento de un código de acceso para poder visualizar las denominadas "Notas bloqueadas", de forma que sea imposible acceder a ellas si no se conoce este código.

La contraseña que protege el acceso a la nota se configura desde el menú "Ajustes - Notas - Contraseña" (ver primera imagen de la <Figura 95>), y es posible (*y recomendable*) establecer contraseñas distintas para las notas almacenadas en iCloud y las almacenadas en el iPhone.

Para bloquear una nota, una vez creada, se debe realizar una pulsación prolongada sobre ella hasta que aparezca el menú de la cuarta imagen de la <Figura 96>. Si no se ha definido aún una contraseña de acceso, esta acción abrirá el menú "Contraseña" del ajuste "Notas" (tercera imagen de la <Figura 96>). La nota permanecerá desbloqueada hasta que se reinicie la app "Notas" o pulsando sobre el menú "Bloquear ahora" que aparece en la parte inferior de la pantalla. Las notas bloqueadas presentan el símbolo "🔒" a su izquierda, y únicamente se mostrará en claro la primera línea de dicha nota, por lo que se recomienda que dicha línea no incluya contenido sensible.

El intento de acceso a una nota bloqueada mostrará un mensaje indicativo de la condición de bloqueo, seguido del menú para introducir la contraseña si el usuario pulsa en "Ver nota".

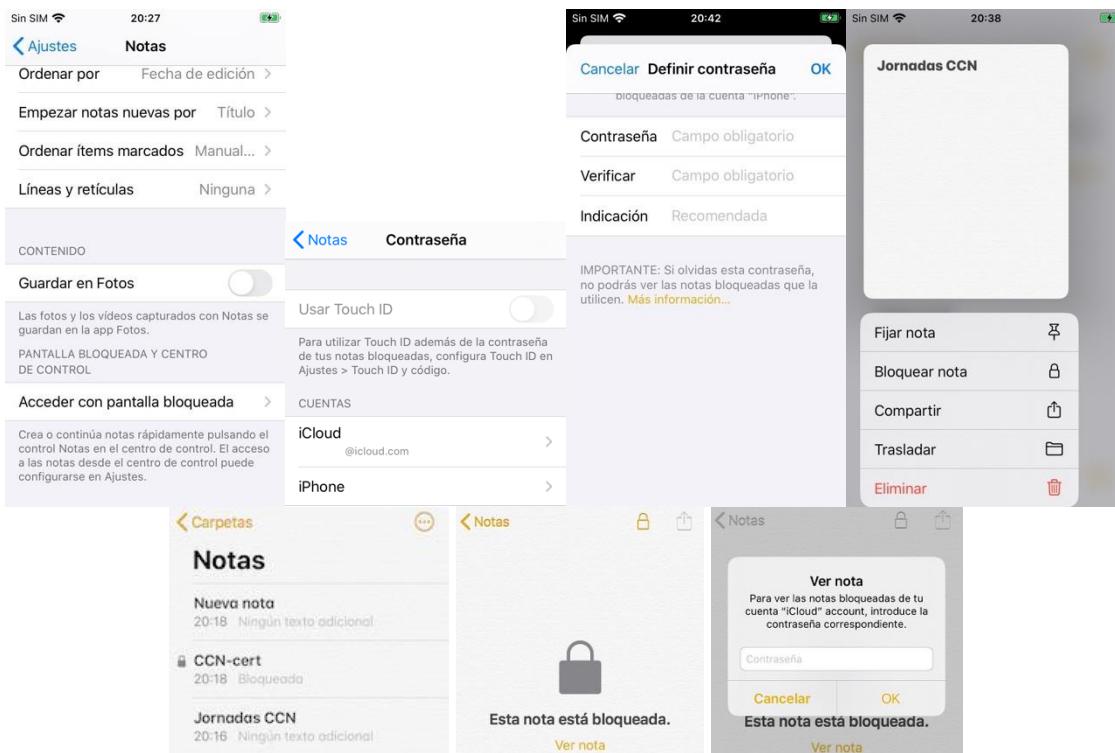


Figura 96 - Configuración de la app "Notas"

18.2.2.2 Control "Notas" en el "Centro de Control"

iOS 13 introduce un nuevo control para la app "Notas" para crear nuevas notas o acceder a la última nota creada. Si el "Centro de Control" está habilitado desde la pantalla de bloqueo (*opción desaconsejada desde el punto de vista de seguridad*), será posible añadir nuevas notas (incluso incluyendo contenido de fotografías tomadas desde la nota) que se almacenarán en la cuenta designada en el ajuste "Cuenta por omisión". Para controlar este comportamiento, se dispone del ajuste "Acceder con pantalla bloqueada" (ver primera imagen de la <Figura 96>), que puede tomar estos valores:

- "No": impide que el control "Notas" funcione con la pantalla bloqueada. **Se recomienda establecer este valor.**
- "Crear siempre una nueva nota": éste es el valor por defecto, pero, debido a las implicaciones que puede tener que un tercero con acceso temporal al dispositivo pueda crear notas cuyo contenido resulte engañoso o comprometido, **se desaconseja su uso.**
- "Continuar última nota": la app "Notas" se abrirá desde el control proporcionando capacidades de edición sobre la última nota modificada por el usuario definida en la sección "Continuar última nota" (ver <Figura 97>). Este valor podría exponer información confidencial desde la pantalla de bloqueo, por lo que, salvo requisitos específicos, **se desaconseja su uso.** Si, pese a la recomendación, se requiere hacer uso de esta funcionalidad, se debe evitar poner el valor "Vista en la app Notas" y se debe establecer el mínimo tiempo posible (5 minutos en el caso de iOS 13) para minimizar el riesgo de exposición de contenido sensible.

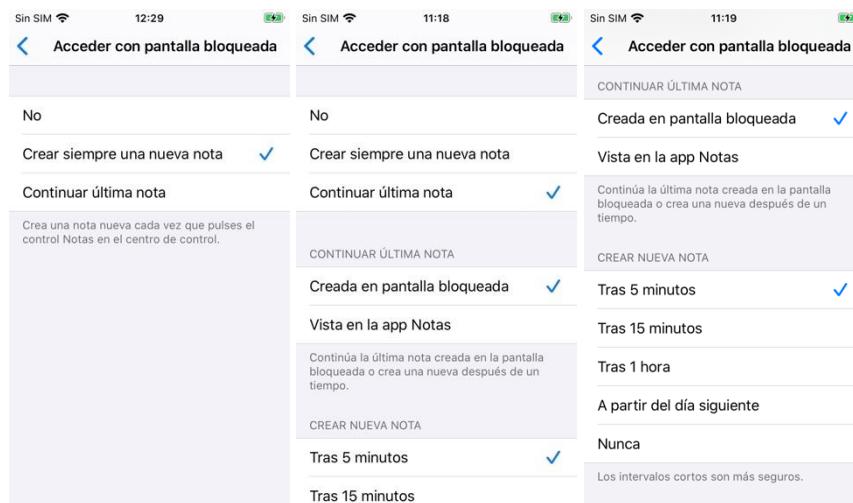


Figura 97 - Creación de notas por parte del control "Notas" en la pantalla de bloqueo

APP "MAIL"

La app de correo electrónico "Mail" incorpora algunas funcionalidades relevantes desde el punto de vista de seguridad/privacidad:

- Permite bloquear a un remitente particular y hacer extensivo el bloqueo a todos los dispositivos vinculados a la misma cuenta de iCloud: para ello, al seleccionar la información del remitente, se dispone de la opción "Bloquear este contacto". Al intentar abrir un mensaje de un contacto bloqueado, se mostrará una indicación en la parte superior del mensaje. Para ver la lista de contactos bloqueados, se dispone del ajuste "Correo - Bloqueados". Por su parte, el menú "Correo - Opciones del remitente bloqueado" permite determinar si los mensajes correspondientes a los contactos bloqueados se trasladarán a la papelera o se mantendrán en la bandeja de entrada.
- Permite salvar los adjuntos al almacenamiento interno del iPhone (carpeta "Descargas" de la app "Archivos" - ver apartado "18.2.1. App "Archivos"").
- Permite silenciar un hilo deslizando el dedo de izquierda a derecha sobre el mensaje y accediendo al menú "Más ... - Silenciar", lo cual interrumpirá las notificaciones de Mail asociadas a dicho hilo.

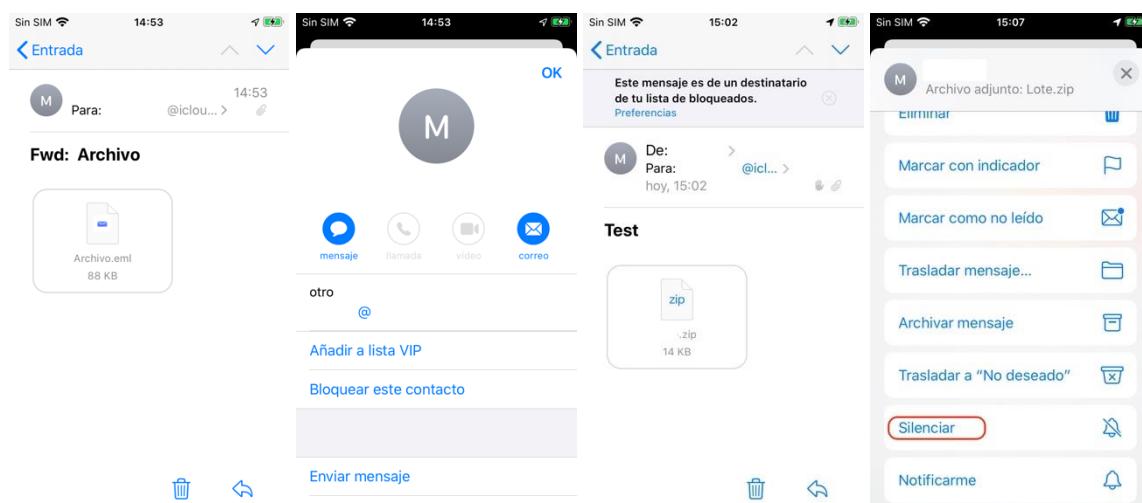


Figura 98 - Funcionalidades nuevas de la app Mail en iOS 13

Por defecto, iOS añade una firma a los correos salientes, que se configura en el menú "Correo - Firma". Se aconseja sustituir el texto por defecto "Enviado desde mi iPhone" por uno que no revele el tipo de dispositivo origen.

18.3 AJUSTES DE PRIVACIDAD: PERMISOS DE LAS APPS

Recomendaciones de seguridad:

- Analizar cuidadosamente el acceso a los permisos de que dispone cada app y suprimir los que no sean necesarios para su propósito.
- Intentar conceder el mínimo permiso para el correcto funcionamiento de la app.
- Para las apps de uso no cotidiano, habilitar los permisos a recursos sensibles solo cuando se vaya a usar la app y suprimirlos después.

iOS ofrece un modelo de control de acceso a las apps basado en permisos o privilegios que se conceden en tiempo de ejecución, y que imponen restricciones a los recursos y componentes del sistema a los que un proceso puede acceder. La primera vez que una app solicite acceso a un recurso, iOS presentará un menú de diálogo al usuario, el cual deberá .

Se distinguen varios tipos de permiso:

- "Localización": ver apartado "14. Servicios de localización".
- "Notificaciones": ver apartado "9.5. Centro de notificaciones".
- Los englobados en el menú "Ajustes - Privacidad": bajo cada permiso se puede ver qué apps lo tienen concedido y, si el permiso admite distintas opciones, qué valor se ha autorizado (por ejemplo, lectura/escritura, nunca/siempre/al usarse, etc.):



Figura 99 - Menú de diálogo solicitando el permiso de ubicación

Los permisos considerados más delicados desde el punto de vista de seguridad/privacidad son:

- Cámara: ya que permite a una app tomar fotografías y vídeos.
- Micrófono: permite a la app grabar conversaciones.
- Salud: por el carácter sensible de esta información.
- Contactos (personales y/o profesionales).
- Localización: permite a la app conocer la ubicación del dispositivo (ver apartado "14. Servicios de localización").
- Archivos y carpetas: ya que proporciona acceso al almacenamiento interno del iPhone.

Adicionalmente, se incluyen las secciones "Análisis" (que remite a Apple datos sobre el uso del dispositivo) y "Publicidad" (para la recepción de anuncios personalizados, que también es enviada a Apple). Se recomienda **limitar el acceso a estos servicios, marcando la opción "Publicidad - Limitar seguimiento" y desmarcar todas las opciones bajo "Análisis"**.

Se puede restablecer los valores que iOS ofrece por defecto para los permisos concedidos a las apps a través de la opción "Ajustes - General - Restablecer - Restablecer localización y privacidad" (ver <Figura 111>). Al ejecutar esta opción, iOS volverá a consultar al usuario sobre los permisos que cada app solicite cuando la app se ejecute de nuevo.

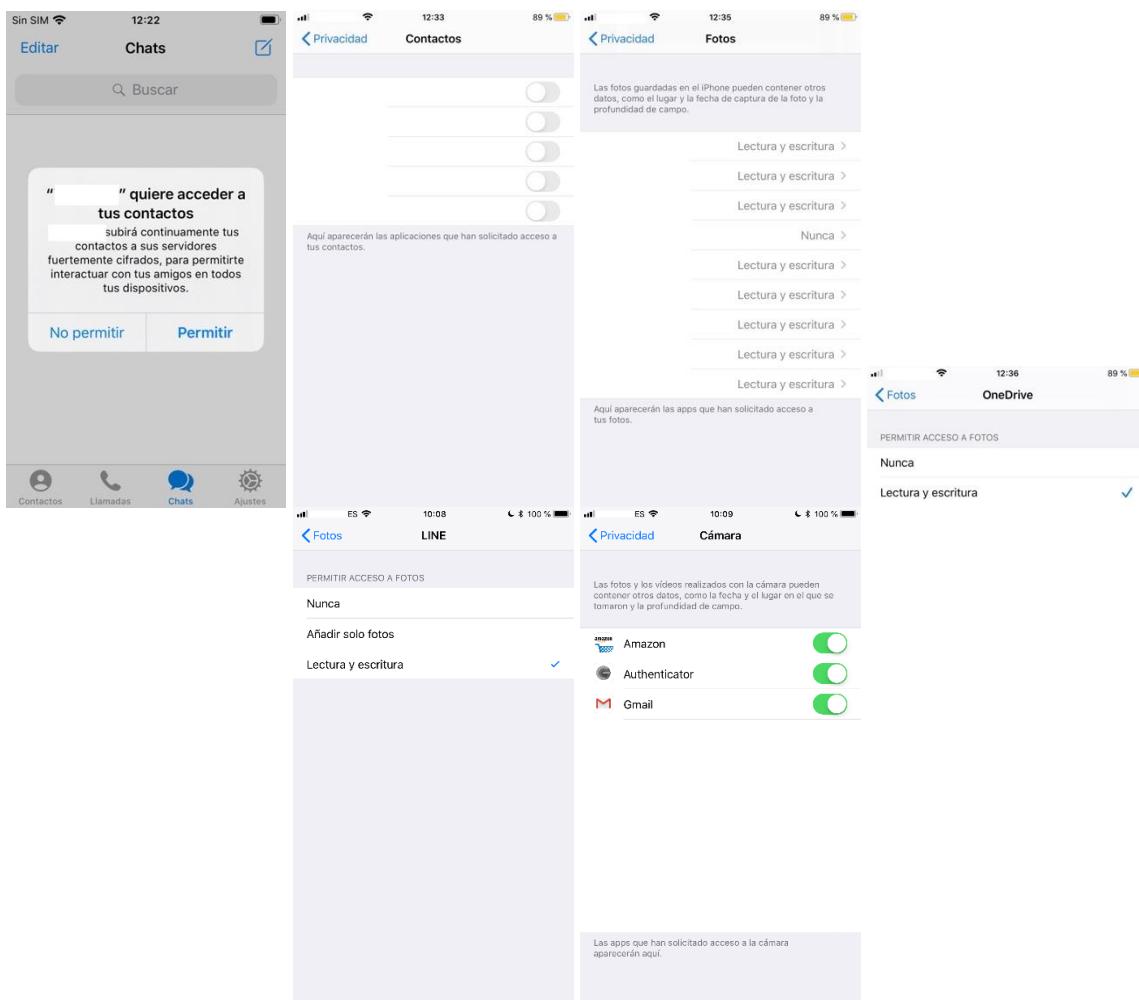


Figura 100 - Permisos de acceso a algunos recursos específicos

18.4 TIEMPO DE USO

La funcionalidad "Tiempo de uso" está formada por un conjunto de herramientas y ajustes destinados a proporcionar al usuario información sobre el tiempo que dedica a interactuar con los dispositivos móviles asociados a una misma cuenta de iCloud, con las distintas apps en él instaladas, las visitas a sitios web, y el número de notificaciones recibidas (ver <Figura 102>).

La configuración del tiempo de uso (descrita en la [Ref.- 60]) permite establecer:

- "Tiempo de inactividad": período durante el cual únicamente podrá accederse a las llamadas telefónicas y a las apps que se definan como excepción en la sección "Siempre permitido".

- "Límite de uso de las apps": las apps se clasifican en una serie de categorías, pudiéndose establecer un plazo máximo de utilización tanto a nivel de categoría como de app individual.
- "Límites de comunicación": esta característica se introduce en iOS 13 para permitir establecer límites para el uso de apps de comunicación basándose en la información del contacto. Como indica el menú, las comunicaciones con números de emergencias siempre se cursarán.
- "Siempre permitido": actúa como lista de excepciones (a nivel de contactos y de apps) a las limitaciones que se hayan establecido en las funcionalidades anteriores.
- "Restricciones": esta sección es muy relevante desde el punto de vista de seguridad y privacidad, por lo que se describe en detalle en el apartado "18.5.1. Restricciones".

Al pulsar sobre la sección "Ver toda la actividad", se obtendrá las estadísticas de interacción con las diferentes apps, tanto por nombre como por categoría, y, al final de la pantalla, se presentarán estadísticas sobre la actividad asociada a las notificaciones, desde donde se puede abrir el interfaz de gestión de notificaciones para cambiar los ajustes de cada una de las apps que han emitido notificaciones en el intervalo de tiempo consultado.

Las apps para las que se cumple alguna de las limitaciones establecidas se mostrarán con su ícono en gris en la pantalla "Home", y, si se intenta abrir las, se mostrará un menú que indica que se ha alcanzado el límite de tiempo, desde el cual es posible activar una excepción ("Ignorar el límite") que permita abrir la app.



Figura 101 - Tiempo de uso

Dado el carácter de control parental que tiene "Tiempo de uso", se incluye una sección "Configurar el tiempo de uso para la familia", desde el que se puede definir limitaciones para las cuentas de niño definidas en la sección "Ajustes - ID de Apple - Configurar "En familia"".

18.4.1 CÓDIGO DE ACCESO PARA "TIEMPO DE USO"

IMPORTANTE: antes de proceder a la configuración de restricciones, se recomienda realizar una copia de seguridad del dispositivo móvil, ya que, si se olvidase la contraseña de "Tiempo de uso", no sería posible realizar ninguna modificación adicional (ni tan siquiera desactivar la funcionalidad), siendo preciso restablecer a fábrica los ajustes del dispositivo móvil. Tampoco

la opción "Restablecer ajustes" puede ejecutarse sin conocer el código de "Tiempo de uso", que se solicita si está vigente antes de proceder al restablecimiento.

En iOS 13, al activar el código para "Tiempo de uso" se permitirá también restablecerlo mediante la cuenta de iCloud.

iOS permite establecer un código de acceso específico para "Tiempo de uso", que será requerido si está vigente y se intenta hacer cualquier modificación en alguno de las secciones que integran la funcionalidad (no para su consulta).

El código está compuesto por 4 dígitos, y **se recomienda que no guarde ninguna relación con el código de acceso al dispositivo**. El código se configura en "Ajustes - Tiempo de uso - Usar código para "Tiempo de uso"" (Imagen izquierda de la <Figura 102>).

NOTA: En la versión de iOS utilizada en la elaboración de la presente guía, se constata que, una vez configurado, el código para "Tiempo de uso" se mantiene en el dispositivo, de forma que, si se desactiva "Tiempo de uso" y posteriormente se vuelve a activar, se mantendrá el código que estaba vigente antes de la desactivación. La única forma de suprimir el código vigente es utilizar la opción "Cambiar código para "Tiempo de uso" - Desactivar código de "Tiempo de uso"".

El código para desbloquear la configuración de las restricciones presenta el mismo comportamiento que el código de acceso al dispositivo móvil (descrito en el apartado "8.1.2. Método de bloqueo del dispositivo móvil"), incrementando progresivamente el tiempo necesario para un nuevo reintento tras 5 intentos fallidos.



Figura 102 - Configuración del código de acceso para "Tiempo de uso"

18.4.2 RESTRICCIONES

La funcionalidad "restricciones" permite limitar el uso de apps, determinada funcionalidad dentro de dichas apps, y funcionalidades específicas del dispositivo móvil, protegiendo parcialmente elementos importantes y sensibles. Aunque el propósito principal de este servicio es el control parental sobre el dispositivo, cumple una función de protección complementaria, limitando las acciones que un tercero puede realizar aun disponiendo de acceso temporal a él con la pantalla desbloqueada.

Para el óptimo aprovechamiento de la funcionalidad "restricciones", se debe:

- Activar la funcionalidad "Tiempo de uso" a través de "Ajustes - Tiempo de uso - Activar "Tiempo de uso"").
- Fijar un código de acceso específico para "Tiempo de uso", de forma que no sea posible deshabilitar las restricciones sin introducir este código (ver apartado "18.4.1. Código de acceso para "Tiempo de uso"").



Figura 103 - Configuración de "Restricciones"

Los ajustes de seguridad recomendados en esta sección son:

- "Compras en iTunes y App Store": **establecer "Solicitar contraseña - Requerir siempre"**.
- "Compras y descargas repetidas en tiendas": **fijar todos los parámetros a "No permitir"**, salvo cuando puntualmente se vaya a hacer uso de estos servicios.
- "Restricciones de contenido - [Game Center)": establecer "No permitir" para la "Grabación de pantalla".
- "Restricciones de contenido - [Siri] Contenido de búsquedas web": su propósito es permitir/bloquear las búsquedas web cuando se invoca a Siri.
- "Privacidad": en esta sección es posible definir restricciones de permisos para las apps que se instalen en el dispositivo con posterioridad al establecimiento del ajuste correspondiente, y no se aplicará a las apps que lo obtuvieron previamente. **Se recomienda valorar cada uno de estos recursos, y fijar a "No permitir" aquellos sobre los que se desea tomar más control**. De forma particular, se aconseja desactivar el permiso a "Localización", "Contactos", "Compartir Bluetooth", "Micrófono" y "Compartir mi ubicación".
- "Permitir cambios": todos los ajustes que se fijen a "No permitir" provocarán que el menú correspondiente de la sección principal de "Ajustes" no se muestren, impidiendo así que se puedan modificar. Por ejemplo, si se establece "Cambios del código - No permitir", el menú "Touch ID y código" desaparecerá de la pantalla de "Ajustes", impidiendo la modificación del código de acceso al dispositivo mientras esté vigente la restricción. **Se recomienda fijar a "No permitir" "Cambios en la cuenta" y "Cambios del código", teniendo presente que habrá que retornar el valor "Permitir" cuando voluntariamente se desee llevar a cabo alguna de estas acciones.**

- "Apps permitidas": este ajuste resulta muy interesante desde el punto de vista de seguridad, ya que permite suprimir de la pantalla "Home" los accesos correspondientes a las apps cuyo interruptor esté desactivado. Esto permite ocultar (y, por tanto, impedir) el uso de apps de forma selectiva. Si se desactiva el interruptor "AirDrop" se eliminará la capacidad tanto de emisión como de recepción a través de este servicio.

Para más información sobre la configuración de restricciones en iOS 13, se aconseja la lectura de la [Ref.- 28].

18.5 ACCESO GUIADO

Recomendaciones de seguridad:

- Hacer uso de la funcionalidad "Acceso guiado" si, por circunstancias determinadas, es preciso prestar el dispositivo a un tercero.
- Definir un código para "Acceso guiado" que no guarde relación con el general del iPhone.
- Excluir del acceso guiado el área de la app que no se desea pueda manipularse.
- Inhabilitar los recursos que estarán disponibles en este modo.

iOS 13 introduce esta nueva funcionalidad para emular un modo quiosco en el iPhone, que permite restringir el uso del dispositivo al de una única app mientras esté vigente⁴⁷.

Aunque se engloba dentro de las funciones de accesibilidad, resulta especialmente útil desde el punto de vista de seguridad en aquellos casos en los que, por circunstancias excepcionales, deba prestarse el móvil a un tercero. Este modo permite:

- Definir un área de la pantalla que no responderá a la interacción táctil, con lo cual se amplía el margen de seguridad al inhabilitar el acceso a parte de su funcionalidad (se puede, por ejemplo, inhabilitar la zona de opciones de configuración de la app fijada).
- Habilitar/deshabilitar elementos del dispositivo, mediante el menú "Opciones" que se muestra en el margen inferior de la pantalla al iniciar el modo de acceso guiado. Entre los recursos que se pueden limitar está el teclado (lo que impediría que el tercero pudiera introducir datos), la función táctil y los botones físicos del iPhone. La opción "Límite de tiempo" permite definir el tiempo máximo de uso del dispositivo en este modo (entre 1 minuto y 23 horas 59 minutos).

Para habilitar el acceso guiado, se dispone de la opción "Ajustes - Accesibilidad - Acceso guiado" (ver [Ref.- 61]). Una vez activo el interruptor, para iniciar el uso de este modo se debe pulsar tres veces sobre el botón lateral (para los modelos desde el iPhone X en adelante) o de inicio (modelos iPhone 8 y anteriores).

⁴⁷ El "acceso guiado" es equivalente a la funcionalidad "Fijar pantalla" de la plataforma Android.

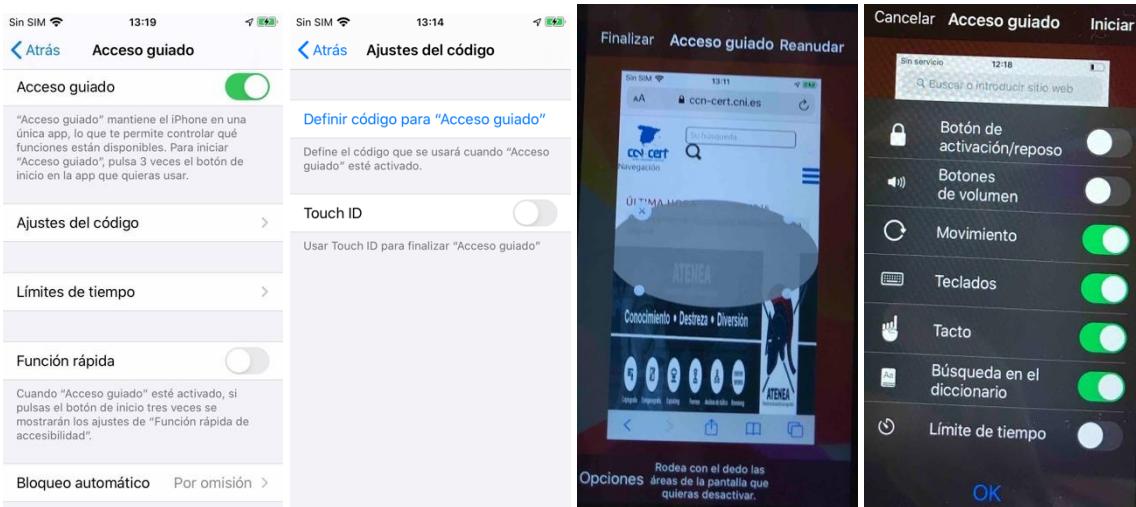


Figura 104 - Modo quiosco en iOS 13: acceso guiado

Es importante configurar un código de desbloqueo para "acceso guiado" a través del menú "Ajustes del código", que se solicitará si el usuario trata de salir de la aplicación fijada, o si el dispositivo ha entrado en bloqueo automático (configurable según muestra la cuarta imagen de la <Figura 104>). Este código será de 4 dígitos si el código de bloqueo general del dispositivo tiene esa longitud, y de 6 dígitos en otro caso. *Se recomienda que el código de acceso específico para acceso guiado no guarde relación con el código de acceso general del dispositivo, y que nunca se comunique al tercero al que se va a prestar el iPhone.* Si no se define un código a través del menú, se solicitará que se configure al iniciar el acceso guiado. Complementariamente, se puede habilitar el interruptor "Touch ID" o "Face ID" para que la biometría vigente en el iPhone sirva también para salir del modo guiado.

19. CIFRADO DEL DISPOSITIVO MÓVIL

Apple implementa la tecnología conocida como "*data protection*", basada en capacidades de cifrado mediante un chip criptográfico, para proteger el acceso a la memoria *flash* del dispositivo móvil (en la que residen los datos de usuario), con objeto de proteger los datos incluso aunque otros elementos hayan sido comprometidos.

"*Data protection*" emplea una jerarquía de claves criptográficas AES 256 ligadas a cada fichero (según su clase), y al sistema de ficheros en su conjunto, que se crea en la partición de datos de usuario. Cada clase ofrece una categoría de protección, según el estado del dispositivo: dispositivo desbloqueado, dispositivo bloqueado, tras el primer desbloqueo, o siempre (ver sección "*Keychain data protection and data classes*" de la [Ref.- 39]).

El acceso a los datos se encuentra protegido por cuatro claves:

- La clave única del dispositivo móvil (disponible en el módulo *hardware* criptográfico de los dispositivos móviles iOS).
- La clave del sistema de ficheros.
- Las claves individuales de cada fichero.
- Las claves para las diferentes categorías de protección disponibles en el sistema, junto al código de acceso del usuario.

Adicionalmente, iOS implementa cuatro repositorios de claves o *keybags* diferentes para almacenar las claves de las diferentes clases:

- Usuario (*user*), utilizado internamente para proporcionar acceso a los datos del sistema de ficheros y a los secretos del *keychain*.
- Dispositivo (*device*), empleado para operaciones asociadas a datos específicos del dispositivo.
- Copias de seguridad (*backup*), que ofrece la funcionalidad de copias de seguridad cifradas.

Custodia (*escrow*), empleado para permitir a un ordenador con iTunes emparejado o asociado con el dispositivo móvil acceder a su sistema de ficheros cuando el dispositivo está bloqueado.

Se dispone de información más detallada sobre el propósito e implementación de cada clase de protección de los ficheros y las entradas en la *keychain*, así como del uso de las *keybags*, y los mecanismos de cifrado en el documento oficial de seguridad de iOS [Ref.- 39] (y documentos como el citado en la [Ref.- 15]).

20. COPIAS DE SEGURIDAD Y RESTAURACIÓN

Apple proporciona dos alternativas para realizar una copia de seguridad de la mayoría de los datos almacenados en los dispositivos móviles basados en iOS: copia en otro dispositivo propiedad del usuario y copia en iCloud (ésta última se describe en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413]).

Se recomienda realizar copias de seguridad de forma regular, y siempre que se vaya a realizar una actualización de sistema operativo y/o una configuración en el dispositivo que pueda ser preciso revertir (o que, por lo delicado de su proceso, pueda ocasionar pérdidas de datos o de ajustes en el dispositivo móvil).

Desde el punto de vista de seguridad, ***se recomienda realizar el backup del dispositivo móvil a través de un equipo de total confianza, frente a la opción de que los datos del usuario sean almacenados por Apple en iCloud.***

En caso de llevar a cabo una restauración de los datos del dispositivo móvil iOS desde una copia de seguridad realizada previamente, el código de acceso no estará fijado inicialmente. El dispositivo móvil notificará al usuario la primera vez que acceda al mismo tras la restauración, ofreciéndole la posibilidad de definir un código en ese instante.

20.1 COPIA DE SEGURIDAD EN UN ORDENADOR

La copia de seguridad mediante conexión a un ordenador de confianza requiere de un proceso de emparejamiento por USB previo (apartado "12.3.1. Proceso de emparejamiento"). Una vez establecido, el dispositivo móvil será visible en el ordenador. La sesión cifrada que se establece podrá utilizarse para cualquier comunicación, incluida la que se realiza vía Wi-Fi, si bien es necesario habilitar las capacidades Wi-Fi al menos una vez a través de una conexión USB, establecer la relación de confianza mediante USB, y tener en cuenta que los registros de emparejamiento expiran a los 30 días desde la última conexión (desde iOS 11).

Hasta macOS 10.14 Mojave, la copia de seguridad de un iPhone se realizaba a través de iTunes. Desde macOS 10.15 Catalina, la conexión USB se gestiona a través de la app Finder (salvo en Windows, para el que sigue existiendo la aplicación iTunes), que incorpora un interfaz específico para conexión con dispositivos iOS:



Figura 105 - Conexión vía "Finder" con un dispositivo iOS 13 en macOS 10.15 Catalina

La copia de seguridad no incluye ni el código de acceso ni los ajustes relacionados con el acceso al dispositivo móvil por biometría. Por su parte, para salvaguardar los datos de salud y los asociados al llavero de iCloud, se requiere que la **copia sea cifrada** (opción que, aunque está desactivada por defecto, es la **recomendada desde el punto de vista de seguridad**)⁴⁸.

Para cifrar la copia de seguridad, se debe marcar la casilla "Cifrar copia de seguridad local", seleccionando una contraseña robusta. Es importante recordar esta contraseña, porque, en caso contrario, no será posible restaurar la copia de seguridad en el dispositivo móvil. Esta contraseña se almacena en el llavero del ordenador con macOS, y no será necesario volver a introducirla para hacer copias sucesivas. La contraseña también se solicita para dejar de cifrar las copias del dispositivo (opción no recomendada desde el punto de vista de seguridad).

A diferencia de en versiones previas de iOS, desde iOS 11 es posible eliminar los requisitos de contraseña de las copias de seguridad de iTunes/Finder, mediante "Ajustes - General - Restablecer - Restablecer ajustes", pudiendo realizar nuevos *backups* no cifrados o con una nueva contraseña en iTunes/Finder.

20.2 RESTAURACIÓN DEL DISPOSITIVO DESDE UNA COPIA DE SEGURIDAD

La restauración de una copia de seguridad requiere que el dispositivo móvil se conecte (preferiblemente a través de USB) al ordenador en el que reside esta copia. Una vez realizada esta conexión, el proceso de restauración dependerá de la versión de iOS actualmente instalada en el dispositivo móvil y la que residía en él en el momento de la copia de seguridad:

- Si ambas coinciden o la versión de iOS es más reciente que la de la copia, bastará con pulsar "Restaurar copia" y elegir la copia óptima.
- Si la versión de iOS actualmente instalada en el dispositivo es más antigua, se deberán seguir los pasos descritos en la [Ref.- 23].

⁴⁸ Para ver los datos que se almacenan en la copia realizada en un ordenador, consultar la [Ref.- 63].

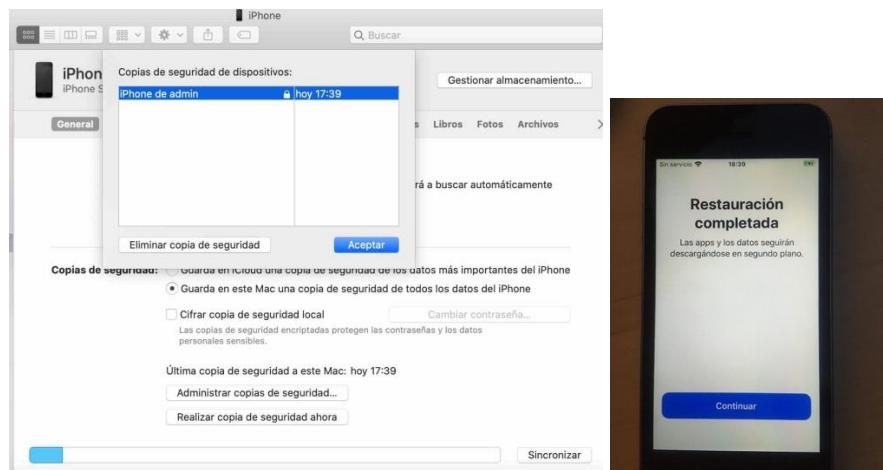


Figura 106 - Restauración de una copia de seguridad en iOS

Tras completarse la restauración, el dispositivo solicitará una nueva configuración de biometría y un nuevo código de acceso.

Actualización del sistema operativo iOS

Desde el punto de vista de seguridad, *se recomienda mantener actualizada la versión de iOS*, pues en cada revisión se incluyen los parches que resuelven problemas de seguridad. No obstante, antes de proceder a instalar una nueva versión, *se recomienda esperar un periodo prudencial de varios días para evitar las consecuencias de los fallos no detectados en las fases beta*, a menos que la migración a la nueva versión solucione problemas de seguridad que afecten significativamente al dispositivo móvil.

IMPORTANTE: no existe ningún mecanismo soportado para cargar en un iPhone una versión de iOS anterior a la existente en el dispositivo. Por tanto, una vez completada una actualización, no es posible volver a la versión anterior, ni tan siquiera restaurando una copia de seguridad realizada para dicha versión.

La información sobre las diferentes actualizaciones de iOS 13 está disponible en la [Ref.- 17]. La información específica de las actualizaciones de seguridad de cada subversión puede consultarse en la [Ref.- 4].

IMPORTANTE: Antes de proceder a la instalación de una nueva actualización, se recomienda realizar una copia de seguridad del dispositivo móvil que posibilite la vuelta atrás (*rollover*) en caso de fallo o si surge algún problema con la versión de iOS más moderna (ver apartado "20. Copias de seguridad y restauración").

Antes de proceder a la instalación de una nueva actualización, se solicitará al usuario confirmación del código de acceso del dispositivo móvil, no siendo válida la confirmación mediante biometría (aunque esté configurado Touch ID o Face ID).

Los dos métodos disponibles para proceder a la actualización de la versión de iOS son la descarga a través de la red Wi-Fi desde el propio dispositivo móvil o la actualización a través de iTunes; ambos se describen a continuación.

20.3 ACTUALIZACIÓN VÍA WI-FI

Durante el proceso de activación de iOS 13 el usuario debe decidir si desea que el dispositivo móvil se actualice automática o manualmente (imagen central de la <Figura 6>). La opción

seleccionada dará valor al ajuste "General - Actualización de software - Actualizaciones automáticas". En caso de haber elegido la opción "Continuar", se activará este ajuste y el dispositivo móvil procederá a descargar y actualizar la versión de iOS tan pronto detecte que existe una nueva versión. **Se recomienda deshabilitar esta opción para disponer de mayor control sobre las actualizaciones de sistema operativo.**



Figura 107 - Menú de activación de actualizaciones automáticas



Figura 108 - Detección de actualización y cancelación de la misma

La inhabilitación de actualizaciones automáticas no impide que el dispositivo chequee periódicamente la disponibilidad de una nueva versión de iOS, presentando al usuario una notificación que solo permite proceder a la instalación en ese momento ("Instalar ahora") o posponerla hasta la madrugada ("Más tarde") (si el dispositivo está encendido y conectado a la corriente, la actualización se llevará a cabo). Para impedir que la actualización tenga lugar aunque se den ambas circunstancias, se puede entrar en el menú "Ajustes - General - Actualización de software" y seleccionar "Cancelar instalación automática".

20.4 ACTUALIZACIÓN MEDIANTE CONEXIÓN A UN ORDENADOR

La actualización de iOS requiere de la conexión a través de USB⁴⁹ del dispositivo móvil a un ordenador con el cual se haya establecido una relación de confianza (ver apartado "12.3. Comunicaciones USB"), que debe disponer de una versión de iTunes lo más reciente posible (plataformas Windows o macOS hasta 10.14 inclusive), o Finder (desde macOS 10.15 inclusive).

La búsqueda de actualizaciones se realiza de forma semanal por parte del *software* del ordenador, pero también se puede iniciar la búsqueda manualmente desde Finder o iTunes, según corresponda.

Cuando se detecta una nueva versión disponible para el dispositivo, la ventana principal del interfaz del ordenador mostrará información sobre dicha versión, y ofrecerá la posibilidad de actualizar a ella, solicitándose en el dispositivo móvil la introducción del código de acceso. Una vez validado el código, comenzará la descarga de la nueva versión y su posterior instalación. El interfaz de iTunes/Finder irá informando de las diferentes etapas asociadas a la actualización.

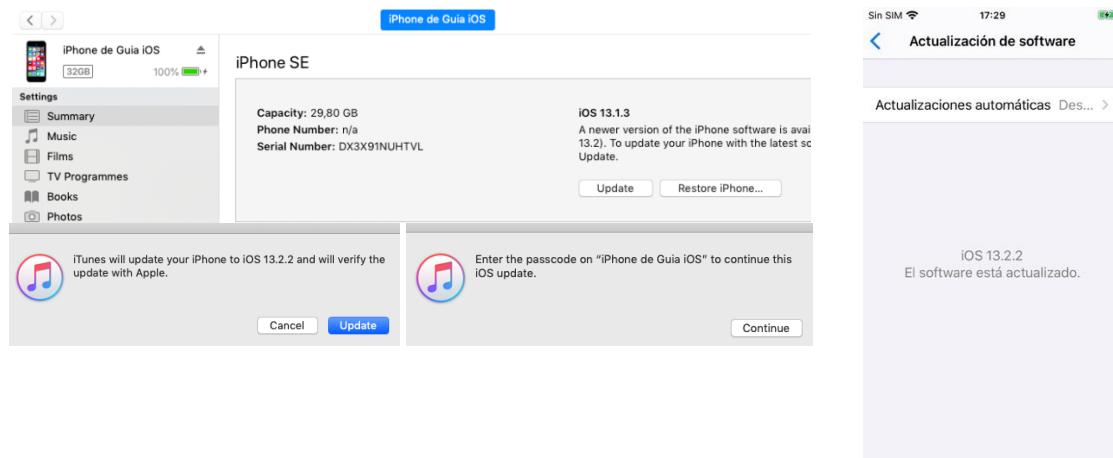


Figura 109 - Actualización de iOS a través de iTunes

21. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

iOS proporciona capacidades locales para el restablecimiento de los datos almacenados en el dispositivo móvil a través del menú "Ajustes - General - Restablecer". Este menú alberga distintas opciones con diferente alcance del borrado de datos, y todos sus submenús requieren confirmación de la operación mediante introducción del código de desbloqueo (a excepción de "Restablecer pantalla de inicio").

⁴⁹ No es posible emplear las capacidades de comunicación con iTunes a través de la red Wi-Fi para las actualizaciones de iOS.

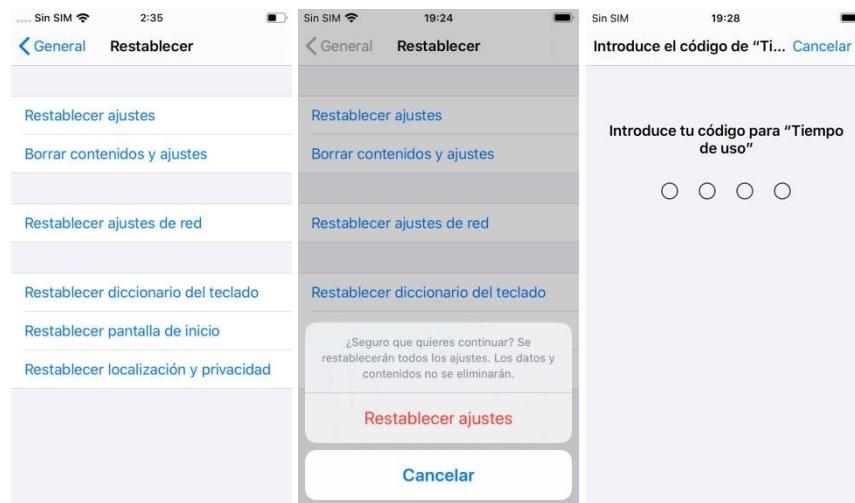


Figura 110 - Menú "Restablecer" para eliminación de datos

21.1 ELIMINACIÓN DE DATOS DE USUARIO MANTENIENDO LA VERSIÓN DE IOS

Para eliminar todos los datos de usuario del dispositivo, incluyendo:

- Cuentas de iCloud, iTunes y App Store.
- Configuraciones realizadas por el usuario.
- Datos de aplicaciones y del sistema.
- Aplicaciones previamente instaladas.

pero manteniendo la versión existente del sistema operativo y las actualizaciones de sistema ya aplicadas⁵⁰, se dispone de la opción "Borrar contenidos y ajustes". Este mecanismo es el recomendado en caso ir a deshacerse del dispositivo móvil [Ref.- 31]. Además del código de desbloqueo del iPhone, puede ser necesario introducir la contraseña asociada al ID de Apple. Si el dispositivo tiene vigente un código para "Tiempo de uso" (ver apartado "18.4.1. Código de acceso para "Tiempo de uso""), este código también se solicitará.

Este proceso, una vez completado, llevará al menú de configuración inicial del dispositivo móvil (descrito en el apartado "7. Proceso de activación del dispositivo móvil").

La operación de borrado de datos local puede ser activada tras un número determinado de intentos de desbloqueo de pantalla fallidos, ya sea de forma manual o a través de las políticas de seguridad de los mecanismos de gestión empresariales de dispositivos móviles iOS (la cual queda fuera del alcance de la presente guía). El número máximo de intentos fallidos de acceso por defecto en iOS es de 10. Este valor también puede ser definido mediante las políticas de seguridad a través de los perfiles de configuración o las soluciones de gestión empresariales (MDM). Puede verificarse si esta funcionalidad ha sido activada a través del menú "Ajustes - Touch ID y Código - Borrar datos" (ver apartado "8.1.2.1. Código de acceso").

⁵⁰ Si se hubiese descargado una nueva actualización pero ésta no se hubiera instalado, la descarga se perdería, siendo necesario descargarla de nuevo tras completar el proceso de restablecimiento.

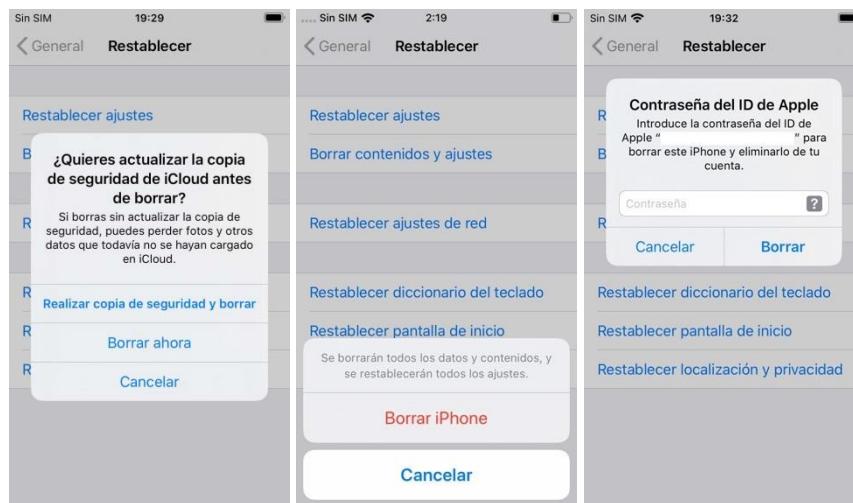


Figura 111 - Borrado de datos del dispositivo móvil

Adicionalmente, en caso de pérdida del dispositivo móvil, también es posible invocar la operación de borrado a través del servicio "Buscar" (ver apartado "23.3. Servicios "Buscar").

21.2 RESTABLECIMIENTO DE LOS AJUSTES DEL DISPOSITIVO A LOS AJUSTES DE FÁBRICA

La opción "Restablecer ajustes" permite restaurar los ajustes del dispositivo móvil a la configuración de fábrica, incluyendo los ajustes de red, los de localización, los de privacidad y los asociados a la pantalla "Home". No se eliminan los datos ni los contenidos de usuario.

El tiempo requerido para este proceso puede variar según el tipo de dispositivo móvil y la versión de iOS; no se solicitará el código de acceso, pero sí el de "Tiempo de uso" (si está vigente).

21.3 PROCEDIMIENTO PARA ELIMINAR LOS DATOS DE UN DISPOSITIVO DEL QUE YA NO SE DISPONE

Si el usuario perdió el acceso a su iPhone antes de haber podido llevar a cabo la eliminación completa de datos según lo descrito en el apartado "21.1. Eliminación de datos de usuario manteniendo la versión de iOS", se recomienda seguir el procedimiento de la [Ref.- 31].

22. RESUMEN DE RECOMENDACIONES DE SEGURIDAD DE IOS 13

Decálogo de seguridad de dispositivos móviles iOS 13

- 1 El dispositivo móvil no debe dejarse desatendido, menos aún con la pantalla desbloqueada, y debe evitarse su préstamo a terceros, incluso temporalmente.
El acceso al dispositivo móvil debe estar protegido mediante un código, preferiblemente una contraseña alfanumérica, de al menos 8 caracteres, que no esté directamente relacionado con información del usuario.
El código de acceso debe solicitarse inmediatamente tras apagarse la pantalla, de forma automática, a la mayor brevedad posible si el usuario deja de interactuar con el dispositivo.
- 2 Mantener el dispositivo actualizado (sistema operativo y apps), de forma manual, y realizando previamente una copia de seguridad antes de proceder a la actualización. La copia de seguridad debe estar cifrada, y, preferiblemente, realizarse en un ordenador de confianza (frente al uso de iCloud).
- 3 El acceso al "Centro de Control" (y el uso de Siri) deben estar deshabilitado en la pantalla de bloqueo⁵¹. No añadir al "Centro de Control" controles cuyo uso desde la pantalla de bloqueo pueda comprometer la privacidad/seguridad del dispositivo.
- 4 Evitar presentar el contenido de las notificaciones en la pantalla de bloqueo, sobre todo para las apps más sensibles⁵¹.
- 5 Evitar la conexión a redes Wi-Fi abiertas y ocultas, dando preferencia a conexiones de datos a través de un *hotspot* de uso personal.
Desconectar los interfaces Wi-Fi y Bluetooth cuando no se estén utilizando, pero mantener habilitada la conexión de datos móviles para permitir la localización del dispositivo a través del servicio "Buscar" (y el "Modo perdido").
- 6 Mantener desactivado el servicio AirDrop, y, en caso de tener que utilizarlo, configurarlo solo para los contactos.
- 7 Mantener una política de "mínimo privilegio" en la concesión de permisos a las apps, y deshabilitar el permiso global de localización cuando no se requiera.
- 8 Evitar conexiones USB con dispositivos de terceros, y prestar atención a los mensajes de solicitud de relaciones de confianza si, eventualmente, se requiere conectar el dispositivo a una toma USB de datos ajena.
- 9 Configurar en el dispositivo restricciones para limitar el acceso a ajustes críticos, apps sensibles, funcionalidad dentro de dichas apps, y ciertos servicios del dispositivo móvil, protegiéndolas mediante un código específico para "Tiempo de uso".
- 10 Hacer uso de la funcionalidad "Acceso guiado" en caso de tener que prestar el dispositivo móvil a un tercero de forma temporal.

⁵¹ La utilización de mecanismos biométricos mejora la usabilidad frente a las restricciones impuestas por esta recomendación.

23. ANEXO A - CUENTA DE ICLOUD

iCloud es un servicio multiplataforma de Apple en la nube [Ref.- 6] destinado 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 únicamente ligada al ID de Apple.

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 "23.3. Servicios "Buscar" para localización de dispositivos").

Respecto al resto de servicios, 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.

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

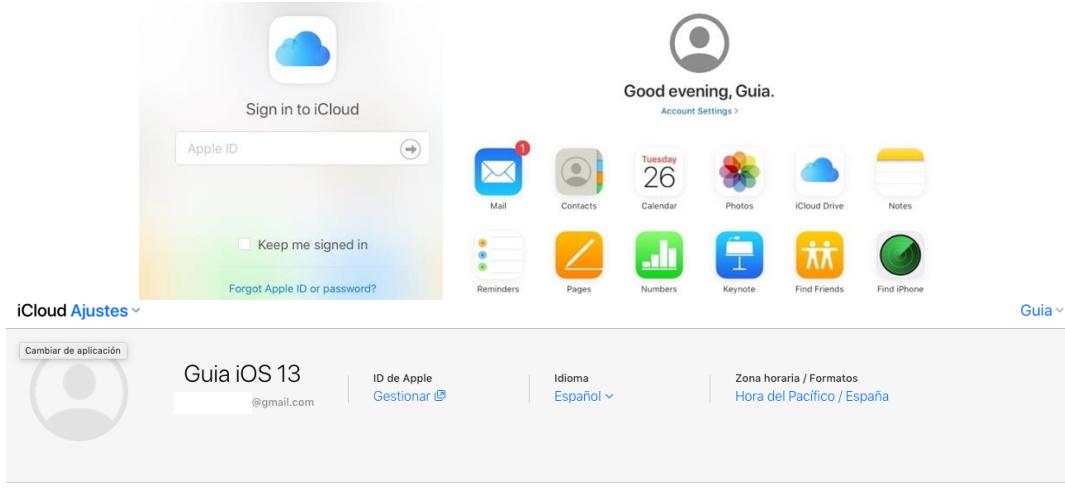
23.1 GESTIÓN DE LA CUENTA DE ICLOUD

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

23.1.1 INTERFAZ WEB

El inicio de sesión en el sitio web "icloud.com" con las credenciales del ID de Apple proporciona acceso al interfaz de administración de la cuenta, desde el cual es posible:

- Acceder a los contenidos almacenados por las diferentes apps que almacenan sus datos en iCloud, pinchando sobre los correspondientes iconos de la <Figura 112>.
- Gestionar los dispositivos vinculados a la cuenta (los denominados "de confianza").
- Restaurar copias de seguridad de determinados datos (si las apps correspondientes sincronizan sus contenidos en iCloud), como contactos y marcadores.
- Cerrar la sesión de todos los navegadores que la tengan activa.
- Definir qué apps pueden buscar a un determinado usuario mediante su ID de Apple.



Almacenamiento
Tienes 5 GB de almacenamiento de iCloud.
4,92 GB disponibles

Mis dispositivos
Has iniciado sesión y tienes instalado iOS 8, macOS Yosemite, watchOS 1 o una versión posterior en estos dispositivos.

Avanzado

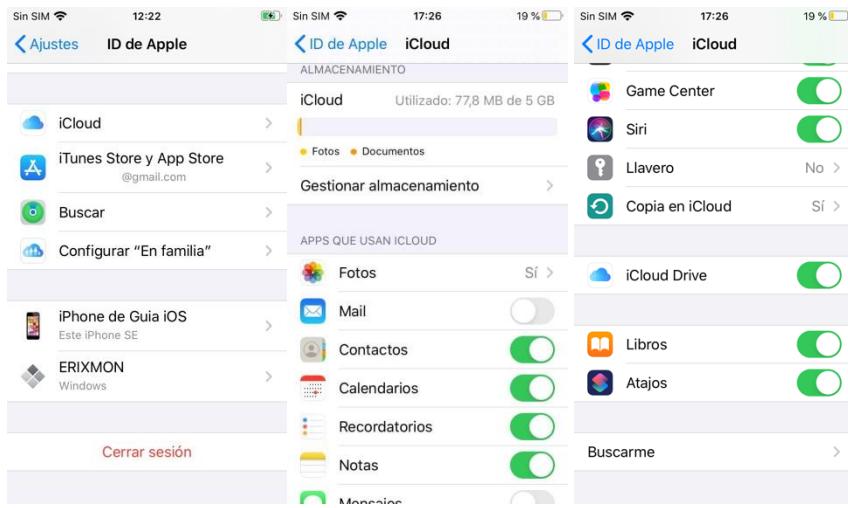
Restaurar archivos	Cerrar la sesión en todos los navegadores	Gestionar las aplicaciones que pueden buscarme
Restaurar contactos	Cierra inmediatamente la sesión de iCloud.com en todos los navegadores donde la hayas iniciado.	Permite que las personas puedan buscarme por tu ID de Apple en las aplicaciones que utilizas. Las personas que te busquen podrán ver tu nombre y tus apellidos.
Restaurar tus calendarios y recordatorios		
Restaurar tus marcadores		

En familia: Comparte música, películas, apps, fotos y mucho más con los miembros de tu familia. [Más información >](#)

Figura 112 - Gestión de la cuenta de iCloud vía web

23.1.2 INTERFAZ MÓVIL

Una vez se da de alta la cuenta del ID de Apple en un iPhone, se iniciará sesión en iCloud, y, por defecto, se habilitará la sincronización en iCloud para buena parte de las apps proporcionadas de serie con iOS.



Ajustes ID de Apple

ID de Apple iCloud

ALMACENAMIENTO

- iCloud Utilizado: 77,8 MB de 5 GB
- Fotos Documentos
- Gestionar almacenamiento

APPS QUE USAN ICLOUD

- Fotos Sí
- Mail
- Contactos
- Calendarios
- Recordatorios
- Notas
- Monedero
- Game Center
- Siri
- Llavero
- Copia en iCloud
- iCloud Drive
- Libros
- Atajos
- Buscarme

Figura 113 - Ajustes de iCloud

Para dejar de sincronizar con iCloud el contenido de una app concreta, se desactivará el interruptor de dicha app. En ese escenario, 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 que sigan teniendo la sincronización activa.



Figura 114 - Desactivación de la sincronización en iCloud para las apps "Fotos", "Notas" y "Safari"

Si se desea dejar de hacer uso de los servicios de iCloud, es posible cerrar la sesión a través del menú "Ajustes - [ID de Apple] Cerrar sesión" (ver primera imagen de la <Figura 111>). Se recomienda mantener la sesión de iCloud abierta permanentemente en el dispositivo a fin de poder disponer del servicio "Buscar". Si 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.

23.2 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. 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" [Ref.- 27].

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.

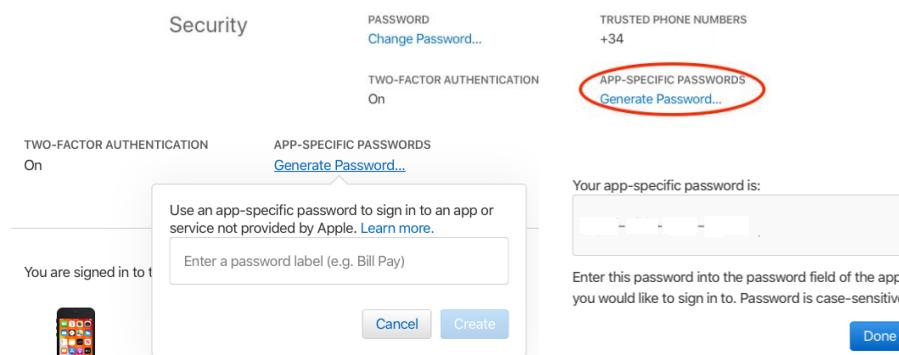


Figura 115 - Uso de una contraseña específica para acceder a iCloud

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

23.3 SERVICIOS "BUSCAR" PARA LOCALIZACIÓN DE DISPOSITIVOS

El servicio "Buscar" nació con el objetivo de localizar un dispositivo extraviado, y, eventualmente, permitir su borrado remoto en caso de no ser posible su recuperación. Desde iOS 13 y macOS Catalina, Apple ha integrado este servicio dentro de la app "Buscar", que ofrece, además del servicio de localización del dispositivo, otras funcionalidades adicionales (descritas a continuación)⁵². Puede obtenerse información adicional sobre la funcionalidad "Buscar" en la [Ref.- 35].

Ante la más mínima sospecha de que el dispositivo puede estar en manos de terceros, se recomienda proceder a su borrado.

El correcto funcionamiento de los servicios de búsqueda del dispositivo requiere:

- Que esté abierta la sesión de iCloud en el dispositivo a gestionar.
- Que el ajuste "[ID de Apple] - iCloud - Buscar mi iPhone" esté activo.
- Disponer de conexión de datos (a través de red Wi-Fi o de datos móviles).

Como demuestra la tercera imagen de la <Figura 117>, no es necesario que los servicios de localización a nivel de sistema ("Ajustes - Privacidad - Localización") estén activos para poder realizar tareas de gestión remota en el dispositivo. De hecho, si se invoca la opción "Modo perdido" y el dispositivo dispone de conexión de datos, Apple será capaz de activar temporalmente la localización mientras el dispositivo permanezca bloqueado, y la desactivará cuando salga del "Modo perdido" mediante introducción del código de acceso correcto en el iPhone.

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 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 a continuación). Los dispositivos cuya ubicación se conoce se marcarán con el símbolo "●", y con el símbolo "●" si la ubicación es desconocida.

Si el dispositivo no dispone de conexión de datos (red o móvil), las peticiones de gestión remota se encolarán, y se procesarán una vez que se recupere esta conectividad (<Figura 117>). Si se opta por realizar una operación "borrar" sobre un dispositivo de confianza (ver apartado "11.5. Dispositivos asociados a la cuenta"), dejará de serlo.

En el 2019 Apple introdujo la opción "Encontrar sin conexión" dentro de los servicios asociados a "Buscar", que permite la localización de un dispositivo que no dispone de conexión de red. Este servicio se describe en la "Guía Práctica de Seguridad de Servicios de Apple" [Ref.- 413].

Es posible dar de baja de la cuenta un dispositivo extraviado seleccionando la opción "☒" (ver tercera imagen de la <Figura 117>). Si se habían invocado operaciones de gestión remota de

⁵² <https://support.apple.com/es-es/guide/icloud/mmfc0f2442/icloud>

https://support.apple.com/kb/PH19300?locale=en_US&viewlocale=es_ES

este dispositivo mediante la funcionalidad "Buscar" descrita en el apartado "23.3. Servicios "Buscar" para localización de dispositivos", 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 116 - Desactivación de la función "Buscar" en iOS 13

23.3.1 TAREAS DE GESTIÓN REMOTA EN IOS

Las tareas de gestión remota asociadas al servicio "Buscar" sobre iOS son:

- "Bloquear": hará que se envíe una solicitud de bloqueo al dispositivo, pudiéndose introducir un número de teléfono del usuario y un mensaje personalizado, que se mostrarán en la pantalla del dispositivo. **Se recomienda realizar esta acción como primera medida para asegurar que el dispositivo quede bloqueado.** El modo perdido se puede desactivar tanto desde el interfaz de iCloud como introduciendo el código de acceso en el propio dispositivo. Cuando se invoca este modo, el servicio Apple Pay quedará deshabilitado en el dispositivo⁵³.
- "Reproducir sonido": genera una señal sonora en el dispositivo 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 el teléfono puede estar en un lugar con acceso público. En todo caso, antes de iniciar esta acción, **se recomienda activar el "modo perdido"** para que, si el sonido es oido por un tercero, el terminal se encuentre bloqueado.
- "Borrar iPhone": 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.



⁵³ <https://ios.gadgethacks.com/how-to/setting-makes-easier-locate-your-iphone-when-its-dead-offline-0157562/>

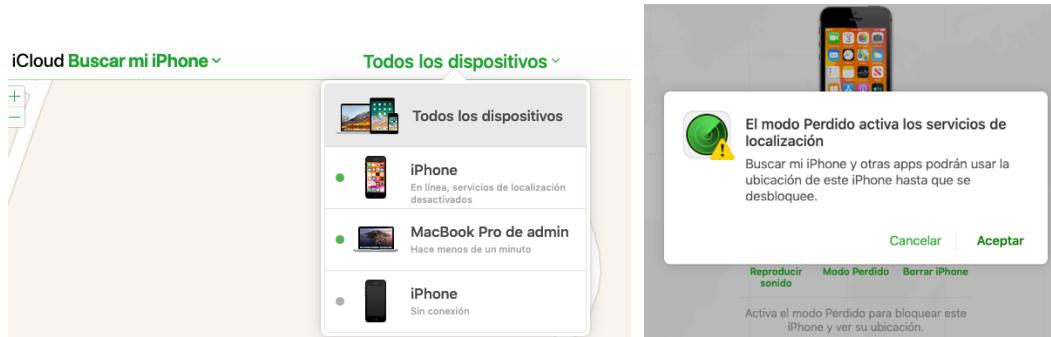


Figura 117 - Interfaz web del servicio "Buscar"

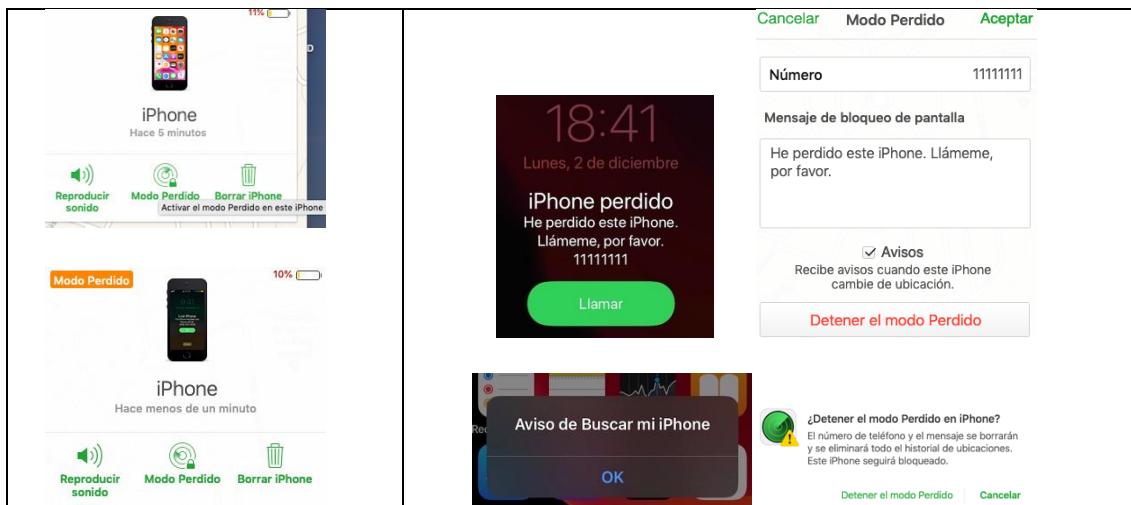


Figura 118 - iPhone en "Modo Perdido" y gestión del modo desde la web de iCloud

AJUSTES VINCULADOS A "BUSCAR"

Desde iOS 13, el antiguamente denominado servicio "Buscar mi iPhone" se integra con la app "Buscar", y sus ajustes se encuentran bajo "Ajustes - [Cuenta Apple] - Buscar":



Figura 119 - 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 ante la pérdida o sustracción de un dispositivo.

- "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.
 - "Enviar última ubicación": provoca que el dispositivo envíe a Apple su ubicación cuando el nivel de batería sea crítico. Apple almacenará esta ubicación durante 24 horas⁵⁴.
 - "Encontrar sin conexión": permite a un usuario localizar un dispositivo (iPhone, Mac, iPad o Apple Watch) extraviado que no dispone de conectividad hacia Internet, pero sí tiene activo el interfaz Bluetooth y habilitada la opción "Encontrar sin conexión" bajo "Ajustes - [ID de Apple] Buscar - Buscar mi iPhone" (iOS) / "Ajustes - [ID de Apple] Buscar mi Mac" (macOS). Es preciso, disponer de un segundo dispositivo vinculado al mismo ID de Apple. 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 de cifrado que se apoya en el siguiente mecanismo⁵⁵:
 - Cuando se habilita el ajuste "Encontrar sin conexión", el dispositivo (1) genera una clave privada que se compartirá entre todos los dispositivos vinculados al mismo ID de Apple mediante comunicaciones cifradas.
 - Adicionalmente, el dispositivo (1) genera una clave pública, que rota periódicamente, y que emitirá mediante mensajes *broadcast* de Bluetooth (de forma similar a un *beacon*), siendo recibida por otros dispositivos Apple ajenos que se encuentren en rango. Este dispositivo ajeno obtendrá la ubicación, la cifrará con la clave pública obtenida, y enviará a Apple este dato de ubicación cifrado y un *hash* de la clave pública.
 - Cuando el propietario del dispositivo extraviado (1) intenta localizarlo mediante la app "Buscar" en 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. Apple buscará entre todos los *hashes* almacenados hasta dar con el coincidente que recibió por parte del dispositivo ajeno para el dispositivo (1).
 - Cuando localice el *hash* coincidente, enviará al dispositivo (2) los datos de localización que se recibieron junto a ese *hash*, y que corresponderán a la ubicación de (1). Como (2) posee la misma clave privada que (1), podrá descifrar los datos de ubicación.

Apple afirma que solo se almacena una ubicación para cada dispositivo marcado como extraviado.

⁵⁴ <https://support.apple.com/es-es/guide/icloud/mmfc0f2442/icloud>

⁵⁵ <https://www.wired.com/story/apple-find-my-cryptography-bluetooth/#>

24. 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. URL: https://www.apple.com/ios/ios-13/
[Ref.- 2]	iPhone. Apple. URL: https://www.apple.com/iphone/
[Ref.- 3]	Iconos y símbolos de estado en el iPhone. Apple. URL: https://support.apple.com/es-es/guide/iphone/iphef7bb57dc/ios
[Ref.- 4]	"Acerca del contenido de seguridad de iOS 13.2 y iPadOS 13.2". Apple. URL: https://support.apple.com/es-es/HT210721
[Ref.- 5]	"Utilizar y personalizar el "Centro de Control" del iPhone, el iPad y el iPod touch". Apple. URL: https://support.apple.com/es-es/HT202769
[Ref.- 6]	"ID de Apple". Apple. URL: https://support.apple.com/es-es/HT203993
[Ref.- 7]	"iCloud". Apple. URL: https://www.apple.com/es/icloud/ "Si has olvidado el código del iPhone, iPad o iPod touch o si el dispositivo está desactivado". Apple. URL: https://support.apple.com/es-es/HT204306
[Ref.- 8]	"Utilizar Touch ID en el iPhone y el iPad". Apple. URL: https://support.apple.com/es-es/HT201371
[Ref.- 9]	"Usar Face ID en el iPhone X o posterior". Apple. URL: https://support.apple.com/es-es/HT208109
[Ref.- 10]	"Chaos Computer Club breaks Apple Touch ID". CCC. September 2013. URL: https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid URL: https://vimeo.com/75324765
[Ref.- 11]	"Perfiles de Bluetooth compatibles con iOS". Apple. URL: https://support.apple.com/es-es/HT204387
[Ref.- 12]	"Configurar y usar Buscar a mis amigos". Apple. URL: https://support.apple.com/es-es/HT201493
[Ref.- 13]	"Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions". Bkav. November 2017. URL: https://www.bkav.com/en/top-news/-/view-content/65202/bkav-s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions
[Ref.- 14]	"Utilizar Bluetooth y Wi-Fi en el Centro de control". Apple. URL: https://support.apple.com/es-es/HT208086
[Ref.- 15]	"iOS Hardening Configuration Guide for iPod Touch, iPhone and iPad devices running iOS 9.3 or higher". Australian Cyber Security Center. August 2016. URL: https://www.cyber.gov.au/sites/default/files/2019-03/iOS9_Hardening_Guide.pdf
[Ref.- 16]	"iPhone security model & vulnerabilities". Cédric Halbronn, Jean Sigwald. Sogeti / ESEC. HITB SecConf 2010. 2010. URL: http://esec-lab.sogeti.com/static/publications/10-hitbkl-iphone.pdf
[Ref.- 17]	"Acerca de las actualizaciones de iOS 13". Apple. URL: https://support.apple.com/es-es/HT210393
[Ref.- 18]	"iOS Forensic Analysis for iPhone, iPad, and iPod touch". Sean Morrissey. APress. URL: http://www.apress.com/9781430233428
[Ref.- 19]	"CCN-CERT IA-04/19: Informe Anual 2018 - Dispositivos y comunicaciones móviles". CCN-CERT. Enero 2019. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html
[Ref.- 20]	"Configurar tus datos médicos en la app Salud de tu iPhone". Apple. URL: https://support.apple.com/es-es/HT207021

Referencia	Título, autor y ubicación
[Ref.- 21]	"List of available trusted root certificates in iOS 13, macOS 10.15, watchOS 6, and tvOS 13". Apple. URL: https://support.apple.com/es-es/HT210770
[Ref.- 22]	"Apple Configurator". Apple. URL: https://support.apple.com/apple-configuration
[Ref.- 23]	"Restaurar una copia de seguridad del iPhone, iPad o iPod touch desde iCloud o un ordenador que requiere una versión posterior de iOS o iPadOS". Apple. URL: https://support.apple.com/es-es/HT203434
[Ref.- 24]	"Acerca de la tecnología avanzada Face ID". Apple. URL: https://support.apple.com/es-es/HT208108
[Ref.- 25]	"Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html
"Acerca del contenido de seguridad de iOS 12.0.1". Apple. URL: https://support.apple.com/es-es/HT209162	
"Canal de YouTube "videosdebarraquito". José Rodríguez. URL: https://www.youtube.com/watch?v=pWOTTnBCA04	
URL: https://www.youtube.com/watch?v=X2yQS1VzmZ0	
[Ref.- 26]	"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.
URL: https://www.usenix.org/conference/usenixsecurity19/presentation/stute	
URL: https://news.northeastern.edu/2019/08/19/airdrop-is-making-your-iphone-vulnerable-to-attackers/	
[Ref.- 27]	"Usar contraseñas específicas para apps". Apple. URL: https://support.apple.com/es-es/HT204397
"Ajustes de servidor de correo para clientes de correo electrónico de iCloud". Apple. URL: https://support.apple.com/es-es/HT202304	
[Ref.- 28]	"Utilizar los controles parentales del iPhone, iPad y iPod touch de tu hijo/a". Apple. URL: https://support.apple.com/es-es/HT201304
[Ref.- 29]	"Las nuevas prestaciones de iOS 13". Apple. URL: https://www.apple.com/es/ios/ios-13/features/
[Ref.- 30]	"Actualizaciones de seguridad de Apple". Apple. URL: https://support.apple.com/es-es/HT201222
[Ref.- 31]	"Qué debes hacer antes de vender, regalar o renovar tu iPhone, iPad o iPod touch". Apple. URL: https://support.apple.com/es-es/HT201351
[Ref.- 32]	"Manual del usuario de Atajos". Apple. URL: https://support.apple.com/es-es/guide/shortcuts/welcome/ios
"Descubrir los atajos de la galería". Apple. URL: https://support.apple.com/es-es/guide/shortcuts/apdd018638ca/3.2/ios/13.2	
[Ref.- 33]	"Shortcuts Library". Matthew Cassinelli. URL: https://airtable.com/shrhYQ0UVa0UBavpU/tblsM2nRGxtYcxKF1?backgroundColor=blue&view=Controls=on&blocks=hide
[Ref.- 34]	"iOS 13 iPhone features: What is Optimized Battery Charging?". 9to5Mac. URL: https://9to5mac.com/2019/10/01/ios-13-iphone-optimized-battery-charging/
[Ref.- 35]	"Configurar Buscar mi iPhone". Apple. URL: https://support.apple.com/es-es/guide/icloud/mmfc0f0c67/1.0/icloud/1.0
[Ref.- 36]	"AuthenticationServices Framework". Apple Developers. URL: https://developer.apple.com/documentation/authenticationservices
[Ref.- 37]	"Create website and app passwords on iPhone". iPhone user Guide - Apple. URL: https://support.apple.com/guide/iphone/create-website-and-app-passwords-iphf9219d8c9/ios
[Ref.- 38]	"Usar un PIN con la tarjeta SIM del iPhone o el iPad". Apple. URL: https://support.apple.com/es-es/HT201529

Referencia	Título, autor y ubicación
[Ref.- 39]	"Apple Platform Security". Otoño 2019. Apple. URL: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
[Ref.- 40]	"Uso de accesorios USB con iOS 11.4.1 y versiones posteriores". Apple.
[Ref.- 41]	URL: https://support.apple.com/es-es/HT208857
[Ref.- 42]	"Utilizar Emergencia SOS en el iPhone". Apple. URL: https://support.apple.com/es-es/HT208076
[Ref.- 43]	"App Salud". Apple. URL: https://www.apple.com/es/ios/health/ "Gestionar datos de Salud en el iPhone, el iPod touch o el Apple Watch". Apple.
[Ref.- 44]	URL: https://support.apple.com/es-es/HT204351
[Ref.- 45]	"Cómo se utiliza Iniciar sesión con Apple". Apple. URL: https://support.apple.com/es-es/HT210318
[Ref.- 46]	"Ocultar mi Correo Electrónico en Iniciar sesión con Apple". Apple. URL: https://support.apple.com/es-es/HT210425
[Ref.- 47]	"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.- 48]	"Context Menus". Apple. URL: https://developer.apple.com/design/human-interface-guidelines/ios/controls/context-menus/
[Ref.- 49]	"Cómo compartir la contraseña de tu Wi-Fi desde el iPhone, iPad o iPod touch". Apple. URL: https://support.apple.com/es-es/HT209368
[Ref.- 50]	"Compartir la conexión a internet del iPhone". Apple. URL: https://support.apple.com/es-es/guide/iphone/iph45447ca6/ios
[Ref.- 51]	"Acerca de la alerta "Confiar en este ordenador" en el iPhone, iPad o iPod touch". Apple. URL: https://support.apple.com/es-es/HT202778
[Ref.- 52]	"USB Restricted Mode in iOS 13: Apple vs. GrayKey, Round Two". Vladimir Katalov. Septiembre 2019. URL: https://blog.elcomsoft.com/2019/09/usb-restricted-mode-in-ios-13-apple-vs-graykey-round-two/ URL: https://blog.elcomsoft.com/tag/usb-restricted-mode/
[Ref.- 53]	"Transmitir contenido mediante AirPlay con el Apple TV". Apple. URL: https://support.apple.com/es-es/guide/tv/atvbf2be9ef7/tvos
[Ref.- 54]	"Share". App extension programming guide". Apple developers. URL: https://developer.apple.com/library/archive/documentation/General/Conceptual/ExtensibilityPG/Share.html
[Ref.- 55]	"Definir qué apps pueden acceder a tu ubicación en el iPhone". Apple. URL: https://support.apple.com/es-es/guide/iphone/iph3dd5f9be/ios
[Ref.- 56]	"Localización y la privacidad". Apple. URL: https://support.apple.com/es-es/HT207056
[Ref.- 57]	"Compartir tu ubicación con amigos en iCloud.com". Apple.
[Ref.- 58]	URL: https://support.apple.com/es-es/guide/icloud/mmee1c40b139/icloud
[Ref.- 59]	"Obtener ayuda para usar el llavero de iCloud". Apple. URL: https://support.apple.com/es-es/HT203783
[Ref.- 60]	"Requisitos de certificados de confianza en iOS 13 y macOS 10.15". Apple. URL: https://support.apple.com/es-es/HT210176
[Ref.- 61]	"Compartir archivos en iCloud Drive en el iPhone". Apple. URL: https://support.apple.com/es-es/guide/iphone/iph17f9f92a6/ios

Referencia	Título, autor y ubicación
[Ref.- 62]	"Cómo hacer una copia de seguridad del iPhone, iPad y iPod touch". Apple. URL: https://support.apple.com/es-es/HT203977
[Ref.- 63]	"Acerca de las copias de seguridad para el iPhone, el iPad y el iPod touch". Apple. URL: https://support.apple.com/es-es/HT204136
[Ref.- 64]	"Safari 13 Release Notes". Apple. URL: https://developer.apple.com/documentation/safari_release_notes/safari_13_release_notes
[Ref.- 65]	"Cómo decide iOS a qué red inalámbrica se conecta automáticamente". Apple. URL: https://support.apple.com/es-es/HT202831
[Ref.- 66]	"Activar o desactivar una automatización personal". Apple. URL: https://support.apple.com/es-es/guide/shortcuts/apd602971e63/3.2/ios/13.2

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]	"Buenas Prácticas. CCN-CERT BP-03/16. 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 (iOS 7.x)". 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
[Ref.- 407]	"Guía CCN-STIC-455: Seguridad en iPhone (iOS 7.x)". 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

Referencia	Título, autor y ubicación
[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-dispositivos-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-dispositivos-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-dispositivos-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-459: Guía práctica de seguridad de servicios de Apple". CCN-CERT. Publicación prevista para febrero/marzo de 2020.