



Seguridad de las plataformas de Apple

Mayo de 2022



Contenido

Seguridad de las plataformas de Apple	5
Introducción a la seguridad de las plataformas de Apple	5
Seguridad del hardware y la biometría	8
Descripción general de la seguridad del hardware	8
Seguridad de los SoC de Apple	10
Secure Enclave	11
Face ID y Touch ID	21
Desconexión del micrófono de hardware	31
Tarjetas exprés con reserva de energía	32
Seguridad del sistema	33
Descripción general de la seguridad del sistema	33
Arranque seguro	34
Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS	61
Actualizaciones seguras de software	63
Integridad del sistema operativo	65
Funciones de seguridad del sistema de macOS adicionales	68
Seguridad del sistema de watchOS	81
Generación de números aleatorios	86
Dispositivo de investigación de seguridad de Apple	87
Encriptación y Protección de datos	89
Descripción general de la encriptación y Protección de datos	89
Códigos y contraseñas	90
Protección de datos	93
FileVault	109
Cómo protege Apple los datos personales de los usuarios	113
Encriptación y firma digital	116

Seguridad de las apps	118
Descripción general de la seguridad de las apps	118
Seguridad de las apps en iOS y iPadOS	120
Seguridad de las apps en macOS	126
Funciones de seguridad en la app Notas	131
Funciones de seguridad en la app Atajos	132
Seguridad de los servicios	133
Descripción general de la seguridad de los servicios	133
ID de Apple e ID de Apple gestionado	134
iCloud	137
Gestión del código y de la contraseña	148
Apple Pay	160
Usar la app Cartera	175
iMessage	187
Seguridad de Apple Messages for Business	191
Seguridad de FaceTime	192
Buscar	193
Continuidad	197
Seguridad de la red	201
Descripción general de la seguridad de la red	201
Seguridad de TLS	201
Seguridad de IPv6	203
Seguridad de la red privada virtual (VPN)	204
Seguridad de la red wifi	205
Seguridad del Bluetooth	209
Seguridad de la banda ultraancho en iOS	211
Seguridad del inicio de sesión único	211
Seguridad de AirDrop	213
Seguridad de las contraseñas wifi compartidas en el iPhone y el iPad	215
Seguridad del firewall en macOS	215
Seguridad del kit de desarrollo	216
Descripción general de la seguridad del kit de desarrollo	216
Seguridad de HomeKit	216
Seguridad de SiriKit en iOS, iPadOS y watchOS	223
Seguridad de DriverKit para macOS	224
Seguridad de ReplayKit en iOS y iPadOS	225
Seguridad de ARKit en iOS y iPadOS	227

Gestión segura de dispositivos	228
Descripción general de la gestión segura de dispositivos	228
Seguridad del modelo de enlace en el iPhone y el iPad	229
Gestión de dispositivos móviles	230
Seguridad de Apple Configurator	238
Seguridad de "Tiempo de uso"	239
Glosario	241
Historial de actualizaciones del documento	247
Historial de actualizaciones del documento	247
Copyright	254

Seguridad de las plataformas de Apple

Introducción a la seguridad de las plataformas de Apple

Apple diseña sus plataformas en torno a la seguridad. Aprovechando la experiencia de crear el sistema operativo móvil más avanzado del mundo, Apple ha creado arquitecturas de seguridad que abordan los requisitos únicos de los móviles, relojes, sistemas de escritorio y entornos domésticos.

Todos los dispositivos Apple combinan *hardware*, *software* y *servicios* que se han diseñado para funcionar conjuntamente con el fin de proporcionar la máxima seguridad y una experiencia de usuario transparente con el objetivo último de garantizar la seguridad de la información personal. Por ejemplo, el hardware de seguridad y el chip diseñados por Apple potencian las funciones de seguridad críticas. Además, las protecciones de software funcionan para mantener la seguridad del sistema operativo y de las apps de terceros. Por último, los servicios proporcionan un mecanismo para disponer de actualizaciones de software seguras y oportunas, respaldar un ecosistema de apps protegido y facilitar comunicaciones y pagos seguros. En consecuencia, los dispositivos Apple protegen el dispositivo y los datos que contiene, así como el ecosistema en su totalidad, incluidas todas las acciones que los usuarios realizan de forma local, en redes y con servicios clave de internet.

Al igual que diseñamos nuestros productos para que resulten sencillos, intuitivos y compatibles, también los diseñamos para que sean seguros. Las funciones de seguridad clave, como la encriptación de los dispositivos basada en hardware, no se pueden desactivar por error. Otras funciones, como Face ID y Touch ID, mejoran la experiencia del usuario al facilitar la protección del dispositivo y hacerla más intuitiva. Y puesto que muchas de estas funciones están activadas por defecto, los usuarios o los departamentos de TI no tienen que llevar a cabo demasiadas configuraciones.

En esta documentación se proporciona información detallada sobre la implementación de la tecnología y las funciones de seguridad en las plataformas de Apple. También será de ayuda a las organizaciones que quieran combinar la tecnología y las funciones de seguridad de las plataformas de Apple con sus propias políticas y procedimientos a fin de satisfacer sus necesidades de seguridad específicas.

El contenido se divide en los siguientes temas:

- **Seguridad del hardware y la biometría:** El hardware y el chip constituyen la base de la seguridad de los dispositivos Apple, que incluye el chip de Apple, Secure Enclave, motores de encriptación, Face ID y Touch ID.
- **Seguridad del sistema:** Las funciones de hardware y software integradas que hacen que el proceso de arranque, las actualizaciones de software y el funcionamiento continuo de los sistemas operativos de Apple puedan llevarse a cabo de forma segura.
- **Encriptación y Protección de datos:** La arquitectura y el diseño que se encargan de proteger los datos del usuario en caso de pérdida o robo del dispositivo, o si una persona o un proceso no autorizados intentan utilizarlo o modificarlo.
- **Seguridad de las apps:** El software y los servicios que proporcionan un ecosistema seguro para las apps y que permiten la ejecución segura de las apps, sin poner en peligro la integridad de la plataforma.
- **Seguridad de los servicios:** Los servicios de Apple para la identificación, la gestión de contraseñas, los pagos, las comunicaciones y la búsqueda de dispositivos perdidos.
- **Seguridad de la red:** Los protocolos de red estándar del sector que proporcionan la autenticación segura y la encriptación de los datos durante la transmisión.
- **Seguridad del kit de desarrollo:** "Kits" de estructuras para la gestión segura y privada de la casa y de la salud, así como una extensión del dispositivo Apple y de las prestaciones de servicio para las apps de terceros.
- **Gestión segura de dispositivos:** Los métodos que permiten gestionar dispositivos Apple, ayudar a impedir su uso no autorizado y activar el borrado remoto si se pierde un dispositivo o si lo roban.

Compromiso con la seguridad

Apple se compromete a proteger a los clientes mediante tecnologías líderes en privacidad y seguridad (diseñadas para salvaguardar la información personal) y mediante métodos integrales que ofrecen protección a los datos corporativos en entornos empresariales. Apple recompensa a los investigadores por el trabajo que hacen para descubrir vulnerabilidades ofreciendo la recompensa de seguridad de Apple. Los detalles del programa y las categorías de recompensas pueden consultarse en <https://developer.apple.com/security-bounty/>.

Disponemos de un experto equipo de seguridad con el fin de ofrecer soporte a todos los productos Apple. Este equipo realiza auditorías y pruebas de seguridad de los productos, tanto en proceso de desarrollo como de los que ya se han lanzado al mercado. Además, el equipo de Apple proporciona herramientas de seguridad y formación, y supervisa activamente si hay amenazas e informa de los nuevos riesgos de seguridad. Apple es miembro del [Forum of Incident Response and Security Teams](#) (FIRST, Foro de equipos de seguridad y respuesta a incidentes).

Apple sigue ampliando los límites de lo posible en cuanto a seguridad y privacidad. Usa chips personalizados en toda la gama de productos (desde el Apple Watch, iPhone y iPad hasta el chip de seguridad T2 y el chip de Apple en el Mac) a fin de optimizar tanto la computación como la seguridad. Por ejemplo, los chips de Apple son la base del arranque seguro, Face ID y Touch ID, y la protección de datos. Además, las funciones de seguridad de los dispositivos equipados con chip de Apple (como la protección de la integridad del kernel, los códigos de autenticación de puntero y las restricciones de permisos rápidas) ayudan a frustrar tipos comunes de ciberataques. Por lo tanto, incluso en el caso de que el código del atacante logre ejecutarse, los daños se verán drásticamente reducidos.

Para aprovechar al máximo las amplias funciones de seguridad integradas en nuestras plataformas, animamos a las organizaciones a que revisen sus políticas de TI y de seguridad para asegurarse de que se están beneficiando totalmente de las capas de tecnología de seguridad que ofrecen estas plataformas.

Si quieres obtener más información sobre cómo informar de incidencias a Apple y sobre la suscripción a las notificaciones de seguridad, consulta [Notificar una vulnerabilidad de seguridad o privacidad](#).

Para Apple la privacidad es un derecho humano fundamental y por eso ha incorporado en sus productos numerosos controles y opciones que permiten a los usuarios decidir cómo y cuándo las apps usan su información y qué información utilizan. Para obtener más información acerca de cómo entiende Apple la privacidad, qué controles de privacidad hay en los dispositivos Apple y cuál es la política de privacidad de Apple, consulta <https://www.apple.com/es/privacy>.

Nota: A menos que se especifique lo contrario, esta documentación es aplicable a las siguientes versiones de los sistemas operativos: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 y watchOS 8.5.

Seguridad del hardware y la biometría

Descripción general de la seguridad del hardware

Para que el software sea seguro, debe residir en un hardware con seguridad integrada. Por eso, los dispositivos Apple (con iOS, iPadOS, macOS, tvOS o watchOS) tienen funciones de seguridad diseñadas en el propio procesador. Entre ellas, se incluye una CPU que potencia las funciones de seguridad del sistema y una parte del chip dedicada a las funciones de seguridad. El hardware centrado en la seguridad sigue el principio de respaldar de forma limitada y discreta funciones definidas a fin de minimizar la superficie de ataque. Entre estos componentes se incluye una ROM de arranque, que forma una raíz de confianza de hardware para el arranque seguro, motores AES dedicados para una encriptación y desencriptación eficientes y seguras, y Secure Enclave. *Secure Enclave* es un sistema en un chip (SoC) incluido en todos los modelos recientes de iPhone, iPad, Apple Watch, Apple TV y HomePod, así como en los ordenadores Mac con chip de Apple y en aquellos con el chip de seguridad T2 de Apple. Secure Enclave sigue el mismo principio de diseño que el sistema en un chip, ya que contiene su propia ROM de arranque discreta y su motor AES. Secure Enclave también proporciona la base para la generación y el almacenamiento seguros de las claves necesarias para encriptar datos en reposo, y protege y evalúa los datos biométricos para Face ID y Touch ID.

La encriptación del almacenamiento debe ser rápida y eficaz. Al mismo tiempo, no puede exponer los datos (ni el *material de claves*) que utiliza para establecer relaciones de claves criptográficas. El motor de hardware AES resuelve este problema al realizar una encriptación y desencriptación en línea rápidas *al escribir o leer archivos*. Un canal especial de Secure Enclave proporciona el material de claves necesario al motor AES sin exponer esta información al procesador de aplicaciones (o CPU) o al sistema operativo general. Esto ayuda a garantizar que las tecnologías de Protección de datos y FileVault de Apple protejan los archivos de los usuarios sin revelar las claves de encriptación de larga duración.

El arranque seguro de Apple está diseñado para garantizar que los niveles más bajos del software no se manipulen y que únicamente se permita cargar software de confianza del sistema operativo de Apple durante el arranque. El arranque seguro empieza en un código inmutable llamado ROM de arranque, que se establece durante la fabricación del SoC de Apple y se conoce como raíz de confianza de hardware. En los ordenadores Mac con un chip T2, la confianza del arranque seguro de macOS comienza con el propio chip T2 (tanto el chip T2 como Secure Enclave también ejecutan sus propios procesos de arranque seguro mediante sus ROM de arranque independientes, exactamente igual a como la familia de chips M1 y de la serie A realizan su arranque seguro).

Secure Enclave también procesa datos faciales y de huella digital desde los sensores de Face ID y Touch ID de los dispositivos Apple. Esto proporciona autenticación segura al tiempo que garantiza la privacidad y seguridad de los datos biométricos del usuario. Esto también permite a los usuarios aprovechar la seguridad de códigos y contraseñas más largos y complejos que, en muchas situaciones, ofrecen la comodidad de una autenticación rápida para acceder a servicios o realizar compras.

Seguridad de los SoC de Apple

El chip diseñado por Apple conforma una arquitectura común en todos los productos de Apple con la que funcionan tanto los Mac como los iPhone, iPad, Apple TV y Apple Watch. Durante más de una década, el equipo de diseño de chips avanzados de Apple ha estado creando y perfeccionando los sistemas en chips de Apple (SoC). El resultado es una arquitectura escalable diseñada para todos los dispositivos que está a la cabeza del sector en prestaciones de seguridad. Esta base común para sus funciones de seguridad solo es posible de una empresa que diseña su propio chip para que funcione con su software.

El chip de Apple se ha diseñado y fabricado para permitir usar las funciones de seguridad del sistema descritas a continuación.

Función	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Familia M1
Protección de la integridad del kernel	✓	✓	✓	✓	✓	✓
Restricciones rápidas de permisos		✓	✓	✓	✓	✓
Protección de la integridad del coprocesador del sistema			✓	✓	✓	✓
Códigos de autenticación de puntero			✓	✓	✓	✓
Capa de protección de la página		✓	✓	✓	✓	Consulta la nota a continuación.

Nota: La capa de protección de la página (PPL) requiere que la plataforma *solo* ejecute código firmado y de confianza; este es un modelo de seguridad que no es aplicable para macOS.

Los procesadores diseñados por Apple también activan específicamente las funciones de Protección de datos que se describen a continuación.

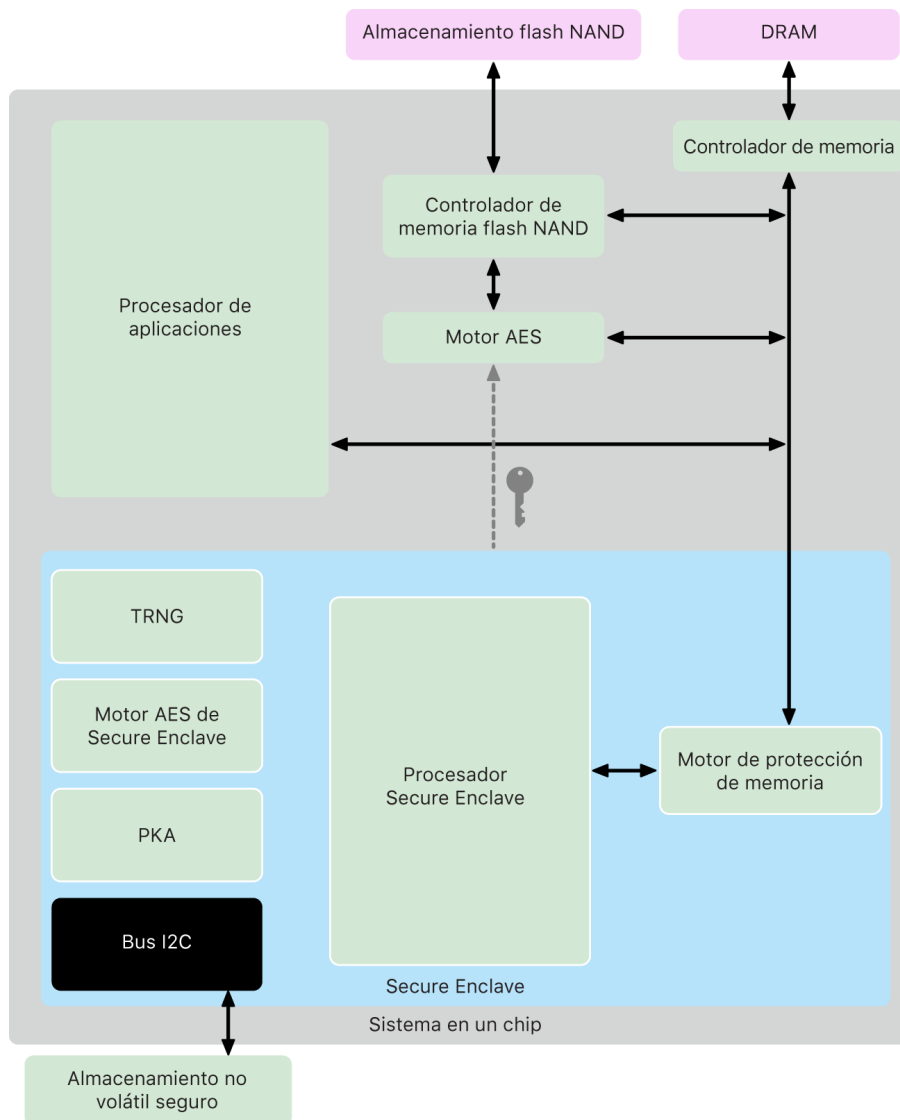
Función	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Protección de clave sellada (SKP)	✓	✓	✓	✓	✓
Sistema operativo de recuperación todas las clases de Protección de datos	✓	✓	✓	✓	✓
Arranques alternativos de DFU, diagnóstico y actualización: protección de datos de clase A, B y C			✓	✓	✓

Secure Enclave

Secure Enclave es un subsistema seguro dedicado presente en las versiones más recientes de iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch y HomePod.

Descripción general

Secure Enclave es un subsistema de seguridad dedicado que se integra en los [sistemas en chips \(SoC\)](#) de Apple. Secure Enclave está aislado del procesador principal para ofrecer una capa adicional de seguridad y está diseñado para mantener la seguridad de los datos sensibles del usuario aunque el kernel del procesador de aplicaciones se vea comprometido. Sigue los mismos principios de diseño que el SoC: una ROM de arranque para establecer una raíz de confianza de hardware, un motor AES para operaciones criptográficas eficientes y seguras y memoria protegida. Aunque Secure Enclave no incluye almacenamiento, tiene un mecanismo para almacenar información de forma segura en un almacenamiento adjunto independiente del almacenamiento flash NAND que usa el procesador de aplicaciones y el sistema operativo.



Secure Enclave es una característica de hardware de la mayoría de las versiones de iPhone, iPad, Mac, Apple TV, Apple Watch y HomePod; concretamente:

- iPhone 5s o posterior
- iPad Air o posterior
- Ordenadores MacBook Pro con Touch Bar (2016 y 2017) con el chip T1 de Apple
- Ordenadores Mac basados en Intel con el chip de seguridad T2 de Apple
- Ordenadores Mac con chip de Apple
- Apple TV HD o posterior
- Apple Watch Series 1 o posterior
- HomePod y HomePod mini

Procesador Secure Enclave

El procesador Secure Enclave proporciona la potencia de computación principal para Secure Enclave. Para ofrecer el máximo aislamiento, el procesador Secure Enclave se dedica exclusivamente a los usos de Secure Enclave. Esto ayuda a evitar ataques de canal lateral que dependen de que el software malintencionado comparta el mismo núcleo de ejecución que el software que es objeto del ataque.

El procesador Secure Enclave se ejecuta como una versión personalizada por Apple del microkernel L4. Está diseñado para funcionar de forma eficiente a una velocidad de reloj más baja, lo que contribuye a protegerlo contra ataques de reloj y de energía. El procesador Secure Enclave, a partir de los SoC A11 y S4, incluye un motor de memoria protegida y una memoria encriptada con funciones antirreproducción, arranque seguro, un generador de números aleatorios dedicado y su propio motor AES.

Motor de protección de memoria

Secure Enclave funciona desde una zona dedicada de la memoria DRAM del dispositivo. Varias capas de protección aíslan la memoria protegida de Secure Enclave del procesador de aplicaciones.

Cuando se inicia el dispositivo, la ROM de arranque de Secure Enclave genera una clave de protección de memoria efímera y aleatoria para el motor de protección de memoria. Cada vez que Secure Enclave escribe en la zona de memoria que tiene dedicada, el motor de protección de memoria encripta el bloque de memoria mediante AES en el modo xor-encrypt-xor (XEX) del Mac y calcula una etiqueta de autenticación con código de autenticación de mensajes basado en cifrado (CMAC) para la memoria. El motor de protección de memoria almacena la etiqueta de autenticación junto con la memoria encriptada. Cuando Secure Enclave lee la memoria, el motor de protección de memoria verifica la etiqueta de autenticación. Si coincide, el motor de protección de memoria descrypta el bloque de memoria. Si no coincide, el motor de protección de memoria indica que hay un error a Secure Enclave. Después de un error de autenticación de memoria, Secure Enclave deja de aceptar solicitudes hasta que se reinicie el sistema.

A partir de los SoC A11 y S4 de Apple, el motor de protección de memoria añade protección de reproducción para la memoria de Secure Enclave. Para ayudar a evitar la reproducción de datos cruciales en términos de seguridad, el motor de protección de memoria almacena un número único, llamado *nonce*, para el bloque de memoria junto con la etiqueta de autenticación. El nonce se utiliza como un ajuste adicional para la etiqueta de autenticación CMAC. Los nonces de todos los bloques de memoria están protegidos mediante un árbol de integridad radicado en la SRAM dedicada dentro de Secure Enclave. Para las escrituras, el motor de protección de memoria *actualiza* el nonce y cada nivel del árbol de integridad hasta la SRAM. Para las lecturas, el motor de protección de memoria *verifica* el nonce y cada nivel del árbol de integridad hasta la SRAM. Las divergencias del nonce se manejan de forma similar a las divergencias de las etiquetas de autenticación.

En el SoC A14, A15, en la familia M1 de Apple y modelos posteriores, el motor de protección de memoria admite dos claves de protección de memoria efímeras. La primera se usa para los datos privados para Secure Enclave, mientras que la segunda se utiliza para los datos compartidos con el motor Neural Engine seguro.

El motor de protección de memoria funciona en línea y de forma transparente para Secure Enclave. Secure Enclave lee y escribe en la memoria como si fuera una DRAM normal sin encriptar, mientras que un observador ajeno a Secure Enclave solo ve la versión encriptada y autenticada de la memoria. El resultado es una sólida protección para la memoria sin compensaciones de rendimiento o complejidad del software.

ROM de arranque de Secure Enclave

Secure Enclave incluye una ROM de arranque de Secure Enclave dedicada. Al igual que la ROM de arranque del procesador de aplicaciones, la ROM de arranque de Secure Enclave es un código inmutable que establece la raíz de confianza de hardware para Secure Enclave.

Al arrancar el sistema, iBoot asigna una zona de la memoria dedicada a Secure Enclave. Antes de usar la memoria, la ROM de arranque de Secure Enclave inicializa el motor de protección de memoria para proporcionar protección criptográfica de la memoria protegida de Secure Enclave.

A continuación, el procesador de aplicaciones envía la imagen del [sepOS](#) a la ROM de arranque de Secure Enclave. Después de copiar la imagen del sepOS en la memoria protegida de Secure Enclave, la ROM de arranque de Secure Enclave comprueba el hash criptográfico y la firma de la imagen para verificar que el sepOS tiene permiso para ejecutarse en el dispositivo. Si la imagen del sepOS está firmada correctamente para poder ejecutarse en el dispositivo, la ROM de arranque de Secure Enclave transfiere el control al sepOS. En cambio, si la firma no es válida, la ROM de arranque de Secure Enclave está diseñada para impedir que se pueda usar Secure Enclave de cualquier manera hasta que se restablezca el chip.

En los SoC A10 de Apple y en modelos posteriores, la ROM de arranque de Secure Enclave bloquea un hash del sepOS en un registro específico para este fin. El acelerador de claves públicas usa este hash para las claves vinculadas al sistema operativo.

Monitor de arranque de Secure Enclave

En el SoC A13 de Apple y en modelos posteriores, Secure Enclave incorpora un monitor de arranque diseñado para garantizar una mayor integridad en el hash del sepOS arrancado.

Al arrancar el sistema, la configuración de la [protección de la integridad del coprocesador del sistema \(SCIP\)](#) del procesador Secure Enclave ayuda a impedir que el propio procesador Secure Enclave ejecute cualquier código que no sea la ROM de arranque de Secure Enclave. Asimismo, el monitor de arranque contribuye a impedir que Secure Enclave modifique la configuración de la SCIP directamente. Para que el sepOS cargado se pueda ejecutar, la ROM de arranque de Secure Enclave envía al monitor de arranque una solicitud con la dirección y el tamaño del sepOS cargado. Al recibir la solicitud, el monitor de arranque restablece el procesador Secure Enclave, aplica un hash al sepOS cargado, actualiza los ajustes de la SCIP para permitir la ejecución del sepOS cargado e inicia la ejecución dentro del código recién cargado. Mientras el sistema sigue arrancando, se usa este mismo proceso siempre que hay nuevo código por ejecutar. Cada vez, el monitor de arranque actualiza un hash en ejecución del proceso de arranque. El monitor de arranque también incluye parámetros de seguridad cruciales en el hash en ejecución.

Cuando se completa el arranque, el monitor de arranque termina el hash en ejecución y lo envía al acelerador de claves públicas para usarlo en las claves vinculadas al sistema operativo. Este proceso está diseñado para que la vinculación de claves del sistema operativo no se pueda omitir aunque haya una vulnerabilidad en la ROM de arranque de Secure Enclave.

Generador de números aleatorios verdaderos

El generador de números aleatorios verdaderos sirve para generar datos aleatorios seguros. Secure Enclave utiliza el generador de números aleatorios verdaderos siempre que genera una clave criptográfica aleatoria, una semilla aleatoria u otra entropía. El generador de números aleatorios verdaderos se basa en varios osciladores en anillo posprocesados con CTR_DRBG (un algoritmo basado en cifrados por bloques en modo de contador).

Claves criptográficas raíz

Secure Enclave incluye una clave criptográfica raíz de identificador único (UID). El UID es único para cada dispositivo individual y no está relacionado con ningún otro identificador del dispositivo.

Un UID generado aleatoriamente se asigna al SoC durante la fabricación. A partir del SoC A9, el generador de números aleatorios verdaderos genera durante la fabricación el UID, que se escribe en la configuración mediante un proceso de software que se ejecuta completamente en Secure Enclave. Este proceso protege el UID para que nunca pueda verse fuera del dispositivo durante la fabricación y, por lo tanto, ni Apple ni ninguno de sus proveedores podrá acceder a él ni almacenarlo.

El sepOS utiliza el UID para proteger los secretos específicos del dispositivo. El UID permite vincular los datos a un dispositivo determinado mediante la encriptación. Por ejemplo, la jerarquía de claves que protege el sistema de archivos incluye el UID, de modo que si la unidad de almacenamiento SSD interno se traslada físicamente de un dispositivo a otro, no será posible acceder a los archivos. Entre otros secretos protegidos específicos del dispositivo, se incluyen los datos de Face ID o Touch ID. En un Mac, solo el almacenamiento completamente interno vinculado al motor AES recibe el nivel de encriptación. Por ejemplo, ninguno de los dispositivos de almacenamiento externo conectados por USB ni las unidades de almacenamiento PCIe añadidas al Mac Pro de 2019 están encriptados de esta manera.

Secure Enclave también tiene un identificador de grupo de dispositivos (GID), que es común a todos los dispositivos que utilizan un determinado SoC (por ejemplo, todos los dispositivos que utilizan el SoC A15 de Apple comparten el mismo GID).

El UID y el GID no están disponibles a través del [grupo de acción de pruebas conjuntas \(JTAG\)](#) u otras interfaces de depuración.

Motor AES de Secure Enclave

El motor AES de Secure Enclave es un bloque de hardware que sirve para realizar criptografía simétrica basada en el cifrado AES. El motor AES está diseñado para resistir la filtración de información mediante la temporización y el análisis de tensión estática. A partir del SoC A9, el motor AES también incluye contramedidas de análisis de tensión dinámica.

El motor AES es compatible con el uso de claves de hardware y software. Las claves de hardware se derivan del UID o GID de Secure Enclave. Estas claves permanecen dentro del motor AES y no se hacen visibles ni siquiera para el software del sepOS. Aunque el software puede solicitar operaciones de encriptación y desencriptación con claves de hardware, no es capaz de extraerlas.

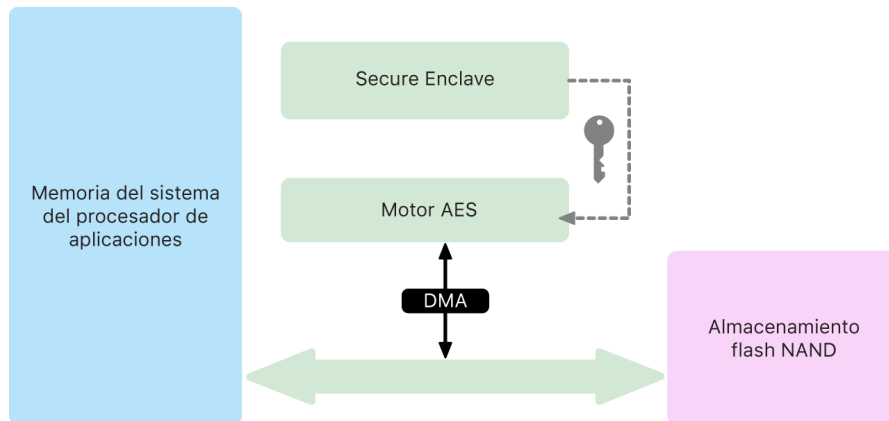
En el SoC A10 de Apple y en modelos más recientes, el motor AES incluye bits semilla bloqueables que diversifican las claves derivadas del UID o GID. Esto permite que el acceso a los datos esté condicionado por el modo de funcionamiento del dispositivo. Los bits semilla bloqueables se usan, por ejemplo, para denegar el acceso a los datos protegidos por contraseña al arrancar en el modo de actualización del firmware del dispositivo (DFU). Para obtener más información, consulta [Códigos y contraseñas](#).

Motor AES

Todos los dispositivos Apple con Secure Enclave tienen también un motor de encriptación AES256 (el "motor AES") integrado en la ruta de acceso directo a memoria (DMA), entre el almacenamiento flash NAND (no volátil) y la memoria del sistema principal. Esto permite conseguir una encriptación de archivos muy eficiente. En los procesadores A9 o posteriores de la serie A, el subsistema de almacenamiento flash se encuentra en un bus aislado que solo tiene acceso a la memoria que contiene datos del usuario mediante el motor de encriptación de DMA.

En el momento del arranque, el sepOS genera una clave de encapsulación efímera mediante el generador de números aleatorios verdaderos. Secure Enclave transmite esta clave al motor AES mediante cables dedicados para impedir que cualquier software fuera de Secure Enclave acceda a él. A continuación, sepOS puede usar la clave de encapsulación efímera para encapsular claves de archivo para que el controlador del sistema de archivos del procesador de aplicaciones las utilice. Cuando el controlador del sistema de archivos lee o escribe un archivo, envía la clave encapsulada al motor AES, que la desencapsula. El motor AES nunca expone la clave desencapsulada al software.

Nota: El motor AES es un componente independiente tanto de Secure Enclave como del motor AES de Secure Enclave, pero su funcionamiento está estrechamente vinculado con Secure Enclave, como se describe a continuación.



Acceptor de claves públicas

El acelerador de claves públicas (PKA) es un bloque de hardware que sirve para realizar operaciones de criptografía asimétrica. El acelerador de claves públicas admite algoritmos de firma y encriptación RSA y ECC (criptografía de curva elíptica). El acelerador de claves públicas está diseñado para resistir la filtración de información a través de ataques de canal lateral y temporización, como el análisis de tensión estática y dinámica.

El acelerador de claves públicas es compatible con el uso de claves de software y hardware. Las claves de hardware se derivan del UID o GID de Secure Enclave. Estas claves permanecen dentro del acelerador de claves públicas y no se hacen visibles ni siquiera para el software del sepOS.

A partir de los SoC A13, se ha demostrado que las implementaciones de encriptación del acelerador de claves públicas son matemáticamente correctas mediante técnicas de verificación formal.

En el SoC A10 de Apple y en modelos posteriores, el acelerador de claves públicas (PKA) admite claves vinculadas al sistema operativo, lo que también se conoce como **Protección de clave sellada (SKP)**. Estas claves se generan mediante una combinación del UID del dispositivo y el hash del sepOS que se ejecuta en el propio dispositivo. El hash procede de la ROM de arranque de Secure Enclave o del monitor de arranque de Secure Enclave en los SoC A13 de Apple y modelos posteriores. Estas claves también sirven para verificar la versión de sepOS al realizar solicitudes a ciertos servicios de Apple y se usan asimismo para mejorar la seguridad de los datos protegidos por código al ayudar a impedir el acceso al material de claves si se realizan cambios críticos en el sistema sin la autorización del usuario.

Almacenamiento seguro no volátil

Secure Enclave está equipado con un dispositivo de almacenamiento seguro no volátil dedicado. El almacenamiento seguro no volátil se conecta a Secure Enclave mediante un bus I2C específico para este fin, por lo que solo Secure Enclave tiene acceso. Todas las claves de encriptación de datos de usuario se basan en la entropía guardada en el almacenamiento no volátil de Secure Enclave.

En dispositivos con el SoC A12, el SoC S4 y modelos posteriores, Secure Enclave se asocia con un componente de almacenamiento seguro para el almacenamiento de la entropía. El propio componente de almacenamiento seguro está diseñado con código de ROM inmutable, un generador de números aleatorios de hardware, una clave criptográfica única por dispositivo, motores criptográficos y detección de manipulaciones físicas. Secure Enclave y el componente de almacenamiento seguro se comunican mediante un protocolo encriptado y autenticado que proporciona el acceso exclusivo a la entropía.

Los dispositivos que salieron al mercado a partir de otoño de 2020 están equipados con un componente de almacenamiento seguro de 2.ª generación. El componente de almacenamiento seguro de 2.ª generación incorpora cajas de seguridad de contadores. Cada caja de seguridad almacena una sal criptográfica de 128 bits, un verificador de 128 bits, un contador de 8 bits y un valor máximo de 8 bits. El acceso a las cajas de seguridad de contadores se realiza mediante un protocolo encriptado y autenticado.

Las cajas de seguridad albergan la entropía necesaria para desbloquear los datos de usuario protegidos por código. Para el acceso a los datos de usuario, el procesador Secure Enclave enlazado debe obtener el valor de entropía de código correcto del código del usuario y el UID de Secure Enclave. El código del usuario no puede obtenerse con intentos de desbloqueo enviados desde un origen distinto al Secure Enclave enlazado. Si se supera el límite de intentos del código (por ejemplo, 10 intentos en el iPhone), el componente de almacenamiento seguro borra por completo los datos protegidos por el código.

Para crear una caja de seguridad de contadores, Secure Enclave envía al componente de almacenamiento seguro el valor de entropía del código y el valor máximo de intentos. El componente de almacenamiento seguro genera el valor de la sal mediante su generador de números aleatorios. A continuación, obtiene un valor de verificador del código y un valor de entropía de la caja de seguridad a partir de la entropía del código proporcionada, la clave criptográfica única del componente de almacenamiento seguro y el valor de la sal. El componente de almacenamiento seguro inicializa la caja de seguridad de contadores con un recuento de 0, el valor máximo de intentos proporcionado, el valor de verificador del código derivado y el valor de la sal. El componente de almacenamiento seguro devuelve el valor de entropía de la caja de seguridad generado a Secure Enclave.

Para recuperar posteriormente el valor de entropía de la caja de seguridad de una caja de seguridad de contadores, Secure Enclave envía la entropía del código al componente de almacenamiento seguro. El componente de almacenamiento seguro primero incrementa el contador de la caja de seguridad. Si el contador incrementado supera el valor máximo de intentos, el componente de almacenamiento seguro borra la caja de seguridad de contadores. Si el máximo de intentos no se ha alcanzado, el componente de almacenamiento seguro intenta obtener el valor de verificador del código y el valor de entropía de la caja de seguridad con el mismo algoritmo usado para crear la caja de seguridad de contadores. Si el valor de verificador del código obtenido coincide con el valor de verificador del código almacenado, el componente de almacenamiento seguro devuelve el valor de entropía de la caja de seguridad a Secure Enclave y restablece el contador a 0.

Las claves utilizadas para acceder a los datos protegidos con contraseña se radican en la entropía almacenada en las cajas de seguridad de contadores. Para obtener más información, consulta [Descripción general de Protección de datos](#).

El almacenamiento seguro no volátil se usa para todos los servicios antirreproducción de Secure Enclave. Los servicios antirreproducción de Secure Enclave se usan para la revocación de datos debido a eventos que marcan los límites antirreproducción, entre los que se incluyen los siguientes:

- Cambio del código
- Activación o desactivación de Face ID o Touch ID
- Adición o eliminación de la cara para Face ID o la huella digital para Touch ID
- Restablecimiento de Face ID o Touch ID
- Adición o eliminación de una tarjeta Apple Pay
- Borrar contenidos y ajustes

En arquitecturas que no incluyen un componente de almacenamiento seguro, se utiliza la memoria de solo lectura programable y borrable eléctricamente (EEPROM) para proporcionar servicios de almacenamiento seguro para Secure Enclave. Al igual que los componentes de almacenamiento seguro, la EEPROM se conecta y es accesible solo desde Secure Enclave, pero no contiene funciones de seguridad de hardware dedicadas ni garantiza acceso exclusivo a la entropía (aparte de sus características de conexión física) ni a la funcionalidad de cajas de seguridad de contadores.

Neural Engine seguro

En dispositivos con Face ID, el motor Neural Engine seguro convierte imágenes 2D y mapas de profundidad en una representación matemática del rostro de un usuario.

En los SoC A11 a A13, el motor Neural Engine seguro está integrado en Secure Enclave. El motor Neural Engine seguro utiliza el acceso directo a memoria (DMA) para garantizar un alto rendimiento. Una unidad de gestión de memoria de entrada/salida (IOMMU) bajo el control del kernel del seOS limita este acceso directo a las regiones autorizadas de la memoria.

A partir del SoC A14 y la familia M1, el motor Neural Engine seguro viene implementado como modo seguro en el motor Neural Engine del procesador de aplicaciones. Un controlador de seguridad del hardware dedicado cambia entre las tareas del procesador de aplicaciones y de Secure Enclave, restableciendo el estado de Neural Engine en cada transición para preservar la seguridad de los datos de Face ID. Un motor dedicado aplica encriptación de memoria, autenticación y control de acceso. Al mismo tiempo, utiliza una clave criptográfica independiente y un intervalo de memoria para limitar el motor Neural Engine a regiones autorizadas de la memoria.

Monitores de reloj y energía

Todos los componentes electrónicos están diseñados para funcionar dentro de una envolvente de frecuencia y tensión limitada. Al funcionar fuera de esta envolvente, la electrónica puede fallar, de modo que podrían omitirse los controles de seguridad. Para ayudar a garantizar que la tensión y la frecuencia permanecen en un rango seguro, Secure Enclave integra en su diseño circuitos de supervisión. Estos circuitos de supervisión están diseñados para tener una envolvente operativa mucho mayor que la del resto de Secure Enclave. Si los monitores detectan un punto de funcionamiento ilegal, el reloj de Secure Enclave se detiene automáticamente y no se reinicia hasta que se vuelva a restablecer el SoC.

Resumen de características de Secure Enclave

Nota: Los productos A12, A13, S4 y S5 que salieron al mercado en otoño de 2020 incorporan un componente de almacenamiento seguro de segunda generación, mientras que los modelos anteriores basados en estos SoC tienen un componente de primera generación.

SoC	Motor de protección de memoria	Almacenamiento seguro	Motor AES	PKA
A8	Encriptación y autenticación	EEPROM	Sí	No
A9	Encriptación y autenticación	EEPROM	Protección DPA	Sí
A10	Encriptación y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A11	Encriptación, autenticación y prevención de reproducción	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A12 (dispositivos Apple que han salido antes de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 1.ª generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A12 (dispositivos Apple que han salido después de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2.ª generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
A13 (dispositivos Apple que han salido antes de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 1.ª generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque
A13 (dispositivos Apple que han salido después de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2.ª generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque

SoC	Motor de protección de memoria	Almacenamiento seguro	Motor AES	PKA
A14, A15	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque
S3	Encriptación y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Sí
S4	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 1. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S5 (dispositivos Apple que han salido antes de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 1. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S5 (dispositivos Apple que han salido después de otoño de 2020)	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
S6, S7	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
T2	Encriptación y autenticación	EEPROM	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo
Familia M1	Encriptación, autenticación y prevención de reproducción	Componente de almacenamiento seguro de 2. ^a generación	Protección DPA y bits semilla bloqueables	Claves vinculadas al sistema operativo y monitor de arranque

Face ID y Touch ID

Seguridad de Face ID y Touch ID

Los códigos y contraseñas son fundamentales para la seguridad de los dispositivos Apple. Al mismo tiempo, los usuarios necesitan poder acceder cómodamente a sus dispositivos, a menudo más de cien veces al día. La autenticación biométrica ofrece la posibilidad de preservar la seguridad de un código seguro (o incluso reforzar la seguridad del código o la contraseña, puesto que no es necesario introducirlo manualmente) y proporciona al mismo tiempo la comodidad de desbloquear el dispositivo rápidamente simplemente pulsando con un dedo o con la mirada. Face ID y Touch ID no sustituyen al código ni a la contraseña, pero en la mayoría de los casos permiten un acceso más rápido y sencillo.

La arquitectura de seguridad biométrica de Apple se basa en una estricta separación de las responsabilidades entre el sensor biométrico y Secure Enclave, y en una conexión segura entre ambos. El sensor captura la imagen biométrica y la transmite con seguridad a Secure Enclave. Durante la inscripción, Secure Enclave procesa, encripta y almacena los datos de plantilla de Face ID y Touch ID correspondientes. Durante la comparación, Secure Enclave compara los datos entrantes del sensor biométrico con las plantillas almacenadas para determinar si desbloquear el dispositivo o responder si hay una correspondencia válida (para Apple Pay, dentro de una app y otros usos de Face ID y Touch ID). La arquitectura admite dispositivos que incluyen tanto el sensor como Secure Enclave (como el iPhone, el iPad y muchos sistemas Mac) y permite separar físicamente el sensor en un periférico que se enlaza con seguridad al procesador Secure Enclave en un Mac con chip de Apple.

Seguridad de Face ID

Con una simple mirada, Face ID desbloquea de forma segura los dispositivos Apple compatibles. Ofrece una autenticación intuitiva y segura gracias al sistema de cámara TrueDepth, cuya tecnología avanzada permite registrar con precisión la geometría del rostro de un usuario. Face ID usa redes neuronales para determinar la atención y la coincidencia, y proteger frente a la suplantación de identidad, para que un usuario pueda desbloquear su teléfono con una mirada, incluso con la mascarilla puesta cuando se usan dispositivos compatibles. Face ID se adapta automáticamente a los cambios en la apariencia y protege cuidadosamente la privacidad y seguridad de los datos biométricos de un usuario.

Face ID se ha diseñado para confirmar la atención del usuario, ofrecer una autenticación robusta con una tasa baja de reconocimientos erróneos y reducir la suplantación de identidad, tanto digital como física.

La cámara TrueDepth busca el rostro del usuario automáticamente al activar un dispositivo Apple con Face ID cuando el usuario lo levanta o cuando pulsa la pantalla, así como cuando el dispositivo intenta autenticar al usuario para mostrar una notificación entrante o cuando una app compatible solicita una autenticación mediante Face ID. Cuando se detecta un rostro, Face ID confirma el estado de atención del usuario y su intención de desbloquear el dispositivo al detectar que tiene los ojos abiertos y que dirige su atención al dispositivo. Por razones de accesibilidad, la comprobación de atención de Face ID se desactiva al activar VoiceOver y, si es necesario, se puede desactivar por separado. Al usar "Face ID con mascarilla", siempre es necesario que se detecte si estás mirando.

Una vez que la cámara TrueDepth confirma la presencia de un rostro atento, proyecta y analiza miles de puntos infrarrojos que crean un mapa de profundidad del rostro, del que se obtiene también una imagen infrarroja 2D. Estos datos se utilizan para crear una secuencia de imágenes 2D y mapas de profundidad que llevan una firma digital y se envían a Secure Enclave. Para frenar la suplantación de identidad tanto digital como física, la cámara TrueDepth ordena de forma aleatoria la secuencia de imágenes 2D y el mapa de profundidad que captura, y proyecta un patrón aleatorio específico del dispositivo. Una parte del motor Neural Engine, protegida en Secure Enclave, transforma estos datos en una representación matemática y la compara con la representación de los datos faciales registrados correspondientes. Estos datos faciales registrados son, en sí mismos, una representación matemática del rostro del usuario capturado en diversas poses.

Seguridad de Touch ID

Touch ID es el sistema de detección de huellas digitales que hace posible un acceso seguro, más rápido y sencillo a los dispositivos Apple compatibles. Esta tecnología lee los datos de huella digital desde cualquier ángulo y almacena continuamente más información sobre la huella del usuario, ya que el sensor amplía el mapa de huella digital en cada uso al identificar nuevos nodos superpuestos.

Los dispositivos Apple con un sensor Touch ID se pueden desbloquear con una huella digital. Touch ID no sustituye la necesidad de tener un código del dispositivo o una contraseña de usuario, que todavía se requiere después de encender el dispositivo o de cerrar sesión (en un Mac). En algunas apps, Touch ID también se puede usar en lugar del código de un dispositivo o de la contraseña del usuario, por ejemplo, para desbloquear notas protegidas por contraseña en la app Notas, para desbloquear sitios web protegidos por el llavero y para desbloquear contraseñas compatibles con la app. Sin embargo, en algunos casos siempre se requiere un código de dispositivo o una contraseña de usuario (por ejemplo, para cambiar el código del dispositivo o la contraseña del usuario existentes, o para eliminar las huellas digitales existentes registradas o crear unas nuevas).

Cuando el sensor de huellas digitales detecta el tacto de un dedo, activa la matriz de imágenes avanzada que escanea el dedo y envía la imagen obtenida a Secure Enclave. El canal empleado para proteger esta conexión varía dependiendo de si el sensor de Touch ID está integrado en el dispositivo con Secure Enclave o se encuentra en un periférico separado.

Mientras el escaneo de la huella digital se vectoriza para su análisis, la imagen escaneada se almacena temporalmente en la memoria encriptada de Secure Enclave y, después, se descarta. El análisis utiliza la [correspondencia de ángulos del patrón de arrugas](#) subdérmico; este proceso con pérdidas de información descarta los datos detallados que serían necesarios para reconstruir la huella real del usuario. Durante la inscripción, el mapa de nodos resultante se almacena en un formato encriptado que solo puede leer Secure Enclave como una plantilla de comparación para determinar futuras correspondencias, pero sin información de identidad. Estos datos nunca salen del dispositivo. No se envían a Apple ni se incluyen en las copias de seguridad del dispositivo.

Seguridad del canal de Touch ID integrado

La comunicación entre Secure Enclave y el sensor de Touch ID integrado tiene lugar a través de un bus de interfaz de periféricos serie. El procesador envía los datos a Secure Enclave, pero no puede leerlos, puesto que están encriptados y se autentican mediante una clave de sesión que se negocia con una clave compartida proporcionada de fábrica para cada sensor Touch ID y el correspondiente Secure Enclave. Para cada sensor de Touch ID, la clave compartida es segura, aleatoria y distinta. En el intercambio de claves de sesión, se utiliza la [encapsulación de claves AES](#) y ambas partes proporcionan una clave aleatoria que establece la clave de sesión y que utiliza la encriptación de transporte que proporciona autenticación y confidencialidad (mediante AES-CCM).

Magic Keyboard con Touch ID

El teclado Magic Keyboard con Touch ID (y el teclado Magic Keyboard con Touch ID y teclado numérico) proporciona un sensor de Touch ID en un teclado externo que puede usarse con cualquier Mac con chip de Apple. El teclado Magic Keyboard con Touch ID hace la función de sensor biométrico; no almacena plantillas biométricas, realiza comparaciones biométricas ni aplica políticas de seguridad (por ejemplo, exigir que se introduzca la contraseña después de 48 horas sin desbloquear). El sensor de Touch ID del teclado Magic Keyboard con Touch ID debe enlazarse de forma segura con Secure Enclave en el Mac antes de poder usarse. A continuación, Secure Enclave realizará las operaciones de inscripción y comparación y aplicará políticas de seguridad del mismo modo que con un sensor de Touch ID integrado. Apple realiza el proceso de enlace en la fábrica para un teclado Magic Keyboard con Touch ID incluido con un Mac. El usuario también puede realizar el enlace si es necesario. Un teclado Magic Keyboard con Touch ID solo puede estar enlazado de forma segura con un único Mac, pero un Mac puede mantener enlaces seguros con hasta cinco teclados Magic Keyboard con Touch ID distintos.

El teclado Magic Keyboard con Touch ID y los sensores de Touch ID integrados son compatibles. Si se utiliza un dedo registrado en un sensor de Touch ID integrado de un Mac en un teclado Magic Keyboard con Touch ID, el procesador Secure Enclave del Mac procesa correctamente la correspondencia, y viceversa.

Para posibilitar el enlace seguro y, por tanto, la comunicación entre el procesador Secure Enclave del Mac y el teclado Magic Keyboard con Touch ID, el teclado está equipado con un bloque acelerador de claves públicas (PKA) de hardware, para proporcionar acreditación, y con claves basadas en hardware, para realizar los procesos criptográficos necesarios.

Enlace seguro

Antes de poder usar un teclado Magic Keyboard con Touch ID para las operaciones de Touch ID, debe enlazarse con el Mac de forma segura. Para realizar el enlace, el procesador Secure Enclave del Mac y el bloque PKA del teclado Magic Keyboard con Touch ID intercambian claves públicas, radicadas en la autoridad de certificación de Apple de confianza, y utilizan claves de acreditación del hardware y protocolos ECDH efímeros para acreditar la identidad con seguridad. En el Mac, Secure Enclave protege estos datos, mientras que en el teclado Magic Keyboard con Touch ID, los protege el bloque PKA. Después de realizar el enlace seguro, todos los datos de Touch ID comunicados entre el Mac y el teclado Magic Keyboard con Touch ID se encriptan mediante AES-GCM con una longitud de clave de 256 bits, y con claves ECDH efímeras que usan la curva P-256 del NIST basadas en las identidades almacenadas. (Las pulsaciones normales de teclas se intercambian usando la seguridad del Bluetooth de la misma manera que lo hace cualquier teclado Bluetooth).

Intención segura para enlazar

Para realizar por primera vez algunas operaciones de Touch ID, como inscribir una nueva huella digital, el usuario debe confirmar físicamente su intención para usar un teclado Magic Keyboard con Touch ID con el Mac. La intención física se confirma pulsando dos veces el botón de encendido del Mac cuando lo indique la interfaz de usuario, o bien utilizando una huella digital que se haya inscrito anteriormente con el Mac que coincida correctamente. Para obtener más información, consulta [Intención segura y conexiones a Secure Enclave](#).

Las transacciones de Apple Pay pueden autorizarse con una coincidencia de Touch ID o al introducir la contraseña del usuario de macOS y pulsar dos veces el botón de Touch ID del teclado Magic Keyboard con Touch ID. Este último método permite al usuario confirmar la intención física incluso sin una coincidencia de Touch ID.

Canal de seguridad del teclado Magic Keyboard con Touch ID

Para ayudar a garantizar un canal de comunicación seguro entre el sensor de Touch ID del teclado Magic Keyboard con Touch ID y Secure Enclave en el Mac enlazado, se requiere lo siguiente:

- Un enlace seguro entre el bloque PKA del teclado Magic Keyboard con Touch ID y Secure Enclave, tal y como se ha descrito anteriormente.
- Un canal seguro entre el sensor del teclado Magic Keyboard con Touch ID y su bloque PKA.

El canal seguro entre el sensor del teclado Magic Keyboard con Touch ID y su bloque PKA se establece de fábrica mediante una clave única compartida entre los dos (esta es la misma técnica que se emplea para crear el canal seguro entre el procesador Secure Enclave del Mac y su sensor integrado, en ordenadores Mac con Touch ID integrado).

Face ID, Touch ID, códigos y contraseñas

Para usar Face ID o Touch ID, el usuario debe configurar su dispositivo de modo que se requiera un código o contraseña para desbloquearlo. Cuando Face ID o Touch ID detectan una coincidencia, el dispositivo del usuario se desbloquea sin solicitar el código del dispositivo o la contraseña. Gracias a esto, no hay que introducir el código o la contraseña muy a menudo, por lo que el usuario puede utilizar contraseñas o códigos más largos y complejos. Face ID y Touch ID no sustituyen el código o contraseña del usuario; en lugar de eso, ofrecen un acceso sencillo al dispositivo dentro de unos límites y un tiempo razonables. Esto es importante, puesto que un código o contraseña seguros son la base de la protección criptográfica de los datos del iPhone, iPad, Mac o Apple Watch del usuario.

Cuándo se requiere un código del dispositivo o contraseña

Los usuarios pueden usar sus códigos o contraseñas en cualquier momento en lugar de Face ID o Touch ID, pero hay determinadas situaciones en las que no se puede usar la autenticación biométrica. Las siguientes operaciones, que exigen un alto nivel de seguridad, siempre requieren la introducción de un código o contraseña:

- Actualizar el software.
- Borrar el dispositivo.
- Ver o cambiar los ajustes del código.
- Instalar perfiles de configuración.
- Desbloquear el panel "Seguridad y privacidad" en Preferencias del Sistema en el Mac.
- Desbloquear el panel "Usuarios y grupos" en Preferencias del Sistema en el Mac (si FileVault está activado).

También se requiere un código o contraseña si el dispositivo se encuentra en cualquiera de los siguientes estados:

- Cuando el dispositivo se acaba de encender o reiniciar.
- Cuando el usuario ha cerrado la sesión de su cuenta del Mac (o todavía no ha iniciado sesión).
- Cuando el usuario no ha desbloqueado su dispositivo en las últimas 48 horas.
- Cuando el usuario no ha usado su código o contraseña para desbloquear el dispositivo en las últimas 156 horas (seis días y medio) ni ha usado la autenticación biométrica para desbloquear el dispositivo en las últimas 4 horas.
- Cuando el dispositivo ha recibido un comando de bloqueo remoto.
- Cuando el usuario ha salido del apagado del dispositivo o llamada de emergencia manteniendo pulsados simultáneamente cualquiera de los botones de volumen y el botón de activación/reposo durante 2 segundos y, a continuación, pulsando Cancelar.
- Después de cinco intentos erróneos de reconocimiento biométrico (aunque, para mejorar la usabilidad, es posible que el dispositivo ofrezca introducir el código o la contraseña en lugar de usar la autenticación biométrica después de un número menor de errores).

Si "Face ID con mascarilla" está activado en un iPhone, está disponible durante las siguientes 6,5 horas después de una de las siguientes acciones del usuario:

- Intento correcto de reconocimiento con Face ID (con o sin mascarilla)
- Validación del código del dispositivo
- Desbloqueo del dispositivo con el Apple Watch

Cuando se lleva a cabo cualquiera de estas acciones, prolonga el periodo 6,5 horas más.

Si Face ID o Touch ID está activado en un iPhone o iPad, el dispositivo se bloquea de inmediato al pulsar el botón de activación/reposo. Además, el dispositivo se bloquea cada vez que entra en reposo. Face ID y Touch ID siempre requieren una coincidencia satisfactoria (o, de forma opcional, el uso del código) para activarlo.

La probabilidad de que una persona cualquiera pueda desbloquear el iPhone o el iPad de un usuario es inferior a 1 entre 1.000.000 con Face ID (incluso si "Face ID con mascarilla" está activado). Para los modelos de iPhone, iPad o Mac con Touch ID de un usuario y aquellos enlazados con un Magic Keyboard es inferior a 1 entre 50.000. Esta probabilidad aumenta si se registran varias huellas digitales (hasta 1 entre 10.000 con cinco huellas digitales) o aspectos (hasta 1 entre 500.000 con dos aspectos). Para una mayor protección, tanto Face ID como Touch ID solo permiten cinco intentos erróneos de reconocimiento; después será necesario introducir el código o la contraseña para obtener acceso al dispositivo o la cuenta del usuario. Con Face ID la probabilidad de un reconocimiento erróneo es mayor para:

- gemelos y hermanos que se parecen al usuario,
- niños menores de 13 años, ya que sus rasgos faciales distintivos pueden no estar totalmente desarrollados.

La probabilidad aumenta aún más en estos dos casos si se usa "Face ID con mascarilla". Si a un usuario le preocupa esta posibilidad, Apple recomienda utilizar un código para la autenticación.

Seguridad del reconocimiento facial

El reconocimiento facial se lleva a cabo en Secure Enclave, que utiliza redes neuronales entrenadas específicamente para ese propósito. Apple ha desarrollado las redes neuronales de reconocimiento facial utilizando más de mil millones de imágenes, entre las que se incluyen imágenes infrarrojas y de profundidad recopiladas en estudios realizados con el consentimiento informado de los participantes. Apple ha trabajado a continuación con participantes de todo el mundo para incluir un grupo representativo de personas con el que tener en cuenta factores como el género, la edad y el origen étnico, entre otros. Estos estudios se reforzaron según las necesidades para ofrecer un alto grado de precisión para una gran diversidad de usuarios. Face ID se ha diseñado para que funcione con sombreros, bufandas, gafas, lentillas y muchos tipos de gafas de sol. Face ID también admite el desbloqueo con una mascarilla puesta en los dispositivos iPhone a partir del iPhone 12 y de iOS 15.4 o posterior. Además, funciona en interiores, en exteriores e incluso en la oscuridad total. Una red neuronal adicional, entrenada para detectar y rechazar la suplantación de identidad, evita los intentos de desbloquear el dispositivo con fotos o máscaras. Secure Enclave encripta los datos de Face ID, incluidas las representaciones matemáticas de tu rostro, y tiene acceso exclusivo a ellos. Estos datos nunca salen del dispositivo. No se envían a Apple ni se incluyen en las copias de seguridad del dispositivo. Durante el funcionamiento normal, se guardan los siguientes datos de Face ID, que Secure Enclave encripta para su uso exclusivo:

- Las representaciones matemáticas del rostro de un usuario calculadas durante el registro.
- Las representaciones matemáticas del rostro de un usuario calculadas durante algunos intentos de desbloqueo si Face ID las considera útiles para mejorar el reconocimiento en el futuro.

Las imágenes faciales capturadas durante el funcionamiento normal no se guardan, sino que se descartan inmediatamente después de haber calculado la representación matemática para el registro o para la comparación con los datos de Face ID registrados.

Mejorar los reconocimientos de Face ID

Para mejorar el rendimiento del reconocimiento y seguir el ritmo de los cambios naturales de un rostro y su aspecto, Face ID aumenta con el tiempo las representaciones matemáticas almacenadas. Una vez reconocido, Face ID puede utilizar la representación matemática que acaba de calcular (si su calidad es suficiente) para realizar un número limitado de reconocimientos adicionales antes de descartar esos datos. En cambio, si Face ID no reconoce un rostro, pero la calidad del reconocimiento es superior a cierto umbral y el usuario introduce su código inmediatamente después del intento erróneo, Face ID hace otra captura y aumenta los datos de Face ID registrados con la representación matemática que acaba de calcular. Estos datos nuevos de Face ID se descartan si dejan de producirse coincidencias de reconocimiento o después de un número limitado de reconocimientos; los nuevos datos también se descartan cuando se selecciona la opción para restablecer Face ID. Estos procesos incrementales permiten que Face ID se adapte a los cambios significativos del vello facial o al uso de maquillaje de un usuario, además de reducir al mínimo los falsos positivos.

Usos de Face ID y Touch ID

Desbloquear un dispositivo o una cuenta de usuario

Si Face ID o Touch ID está desactivado, cuando el dispositivo o la cuenta se bloquea, se descartan las claves de las clases más altas de [Protección de datos](#) (almacenadas en Secure Enclave). No se podrá acceder a los archivos e ítems del [llavero](#) de dicha clase hasta que el usuario desbloquee el dispositivo o la cuenta introduciendo su código o contraseña.

Si Face ID o Touch ID está activado, cuando se bloquea el dispositivo o la cuenta, no se descartan las claves sino que se encapsulan con una clave que se proporciona al subsistema de Face ID o Touch ID en Secure Enclave. Cuando un usuario intenta desbloquear el dispositivo o la cuenta (si el dispositivo detecta una coincidencia), proporciona la clave para desencapsular las claves de Protección de datos y el dispositivo o la cuenta se desbloquea. Este proceso ofrece protección adicional, ya que requiere la cooperación entre los subsistemas de Protección de datos y de Face ID o Touch ID para desbloquear el dispositivo.

Al reiniciar el dispositivo, se pierden las claves necesarias para que Face ID o Touch ID puedan desbloquear el dispositivo o la cuenta; Secure Enclave las descarta si se cumple cualquier condición que requiera la introducción del código o de la contraseña.

Asegurar las compras con Apple Pay

El usuario también puede utilizar Face ID y Touch ID con Apple Pay para realizar compras de forma sencilla y segura en tiendas, apps e internet:

- *Con Face ID en tiendas:* Para autorizar un pago en la tienda con Face ID, el usuario debe confirmar primero su intención de pagar pulsando dos veces el botón lateral. Esta doble pulsación indica la intención del usuario mediante un gesto físico que está directamente vinculado a Secure Enclave y que evita cualquier tipo de falsificación maliciosa. Luego el usuario debe autenticarse con Face ID antes de colocar el dispositivo cerca del lector de pagos sin contacto. Para seleccionar un método de pago diferente a Apple Pay después de la autenticación con Face ID, el usuario tiene que autenticarse de nuevo, pero no será necesario volver a pulsar dos veces el botón lateral.
- *Con Face ID en apps e internet:* Para realizar un pago desde las apps y en internet, el usuario debe confirmar su intención de pagar pulsando dos veces el botón lateral y, a continuación, autenticarse con Face ID para autorizar el pago. Si la transacción de Apple Pay no se completa a los 60 segundos de haber pulsado dos veces el botón lateral, el usuario tendrá que confirmar de nuevo su intención de pagar volviéndolo a pulsar dos veces.
- *Con Touch ID:* En el caso de Touch ID, la intención de pagar se confirma mediante el gesto de activación del sensor de Touch ID combinado con la detección correcta de la huella dactilar del usuario.

Uso de API proporcionadas por el sistema

Las apps de terceros pueden usar las API proporcionadas por el sistema para solicitar al usuario que se autentique con Face ID, Touch ID, un código o una contraseña. Además, las apps compatibles con Touch ID pasarán a ser compatibles con Face ID de forma automática sin tener que realizar ningún cambio. Al usar Face ID o Touch ID, solo se informa a la app de si la autenticación se ha realizado correctamente o no, pero no se le proporciona acceso a Face ID, a Touch ID ni a los datos asociados con el usuario registrado.

Proteger los ítems del llavero

Los ítems del llavero también se pueden proteger con Face ID o Touch ID, de modo que Secure Enclave solo los desbloquee con un reconocimiento correcto o con el código del dispositivo o la contraseña de la cuenta. Los desarrolladores de apps disponen de varias API para verificar si el usuario ha establecido un código o una contraseña antes de requerir Face ID, Touch ID, un código o una contraseña para desbloquear ítems del [llavero](#). Los desarrolladores de apps pueden realizar cualquiera de las siguientes acciones:

- Solicitar que las operaciones API de autenticación no recurran a la contraseña de una app o al código de un dispositivo. Pueden consultar si un usuario está registrado, lo que permite utilizar Face ID o Touch ID como un segundo factor en apps en las que la seguridad es importante.
- Generar y utilizar claves de criptografía de curva elíptica (ECC) en el procesador Secure Enclave. Estas claves pueden estar protegidas mediante Face ID o Touch ID. Las operaciones con estas claves siempre se llevan a cabo en Secure Enclave después de que este autorice su uso.

Realizar y aprobar compras

Los usuarios también pueden configurar Face ID o Touch ID para aprobar las compras en iTunes Store, App Store y Apple Books, por ejemplo, de modo que no tengan que introducir la contraseña de su ID de Apple. Al realizar compras, el procesador Secure Enclave verifica que se ha producido una verificación biométrica y, a continuación, libera las claves ECC usadas para firmar la solicitud de la tienda.

Intención segura y conexiones a Secure Enclave

La intención segura ofrece una manera de confirmar la intención del usuario sin interacción con el sistema operativo o el procesador de aplicaciones. La conexión es un enlace físico (desde un botón físico al procesador Secure Enclave) que está disponible en los siguientes dispositivos:

- iPhone X o posterior
- Apple Watch Series 1 o posterior
- iPad Pro (todos los modelos)
- iPad Air (2020)
- Ordenadores Mac con chip de Apple

Con este enlace, los usuarios pueden confirmar su intención de completar una operación de una forma tal que incluso un software que se ejecute con privilegios raíz o en el kernel no pueda suplantar identidades.

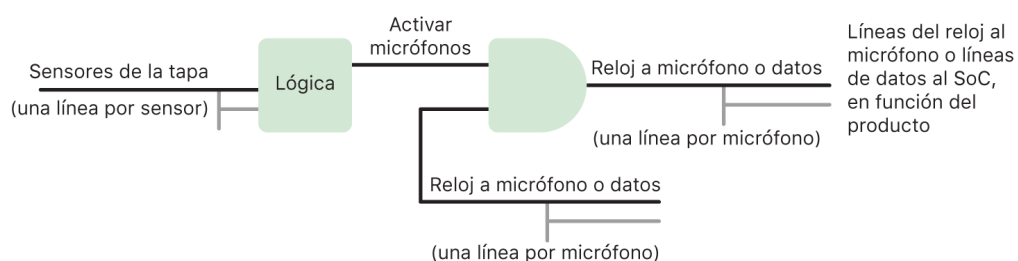
Esta función se usa para confirmar la intención del usuario durante las transacciones de Apple Pay y al finalizar el enlace del teclado Magic Keyboard con Touch ID con un Mac con chip de Apple. Al pulsar dos veces el botón correspondiente (para Face ID) o al realizar un escaneo de la huella digital (para Touch ID) cuando lo solicite la interfaz de usuario, se indica la confirmación de la intención del usuario. Para obtener más información, consulta [Asegurar las compras con Apple Pay](#). Un mecanismo similar (basado en Secure Enclave y el firmware T2) se admite en modelos de MacBook con el chip de seguridad T2 de Apple y sin Touch Bar.

Desconexión del micrófono de hardware

Todos los portátiles Mac con chip de Apple y los basados en Intel con el chip de seguridad T2 de Apple cuentan con una desconexión a nivel de hardware que desactiva el micrófono cada vez que se cierra la tapa. En todos los MacBook Air y MacBook Pro de 13 pulgadas con el chip T2, todos los portátiles MacBook con un chip T2 de 2019 o posteriores y todos los portátiles Mac con chip de Apple, esta desconexión se implanta solo a nivel de hardware. La desconexión está diseñada para evitar que cualquier software (incluso con privilegios de raíz de kernel en macOS, e incluso el software del chip T2 u otro firmware) pueda activar el micrófono cuando la tapa está cerrada (la cámara no se desconecta en el hardware porque su campo de visión queda totalmente obstruido con la tapa cerrada).

Los modelos de iPad de principios de 2020 también incorporan la función de desconexión del micrófono a nivel de hardware. Cuando una funda MFi (incluidas las vendidas por Apple) se coloca en el iPad y se cierra, el micrófono se desconecta en el hardware. Esto está diseñado para impedir que los datos de audio del micrófono estén disponibles para cualquier software, incluido el software con privilegios de kernel o raíz en iPadOS, o cualquier firmware del dispositivo.

Las protecciones de esta sección se implementan directamente con la lógica del hardware, de acuerdo con el siguiente diagrama de circuito:



En cada producto con un límite para el micrófono de hardware, uno o varios sensores de tapa detectan el cierre físico de la tapa o la carcasa mediante alguna propiedad física (por ejemplo, un sensor de efecto Hall o uno de ángulo de bisagra) de la interacción. Para los sensores en los que es necesaria la calibración, los parámetros se establecen durante la producción del dispositivo y el proceso de calibración incluye el bloqueo de hardware no reversible de cualquier cambio posterior en los parámetros sensibles del sensor. Estos sensores emiten una señal de hardware directa que atraviesa un conjunto simple de lógica de hardware no reprogramable. Esta lógica proporciona antirrebote, histéresis y un retardo de hasta 500 ms antes de desactivar el micrófono. Dependiendo del producto, esta señal se puede implementar desactivando las líneas que transportan datos entre el micrófono y el sistema en chip (SoC) o desactivando una de las líneas de entrada al módulo del micrófono que permite que esté activo, por ejemplo, la línea de reloj o un control efectivo similar.

Tarjetas exprés con reserva de energía

Si el sistema iOS no se está ejecutando porque el iPhone tiene que cargarse, es posible que aún haya energía suficiente en la batería para admitir transacciones con tarjetas exprés. Los dispositivos iPhone compatibles admiten automáticamente esta función con:

- Una tarjeta de pago o de transporte designada como tarjeta exprés.
- Carnés de estudiante con el modo exprés activado.
- Llaves de coche con el modo exprés activado.
- Llaves de casa con el modo exprés activado.
- Tarjetas de acceso empresariales o de hostelería con el modo exprés activado.

Al pulsar el botón lateral (o el botón de inicio en el iPhone SE de 2.ª generación), se muestra el icono de batería baja junto con un mensaje que indica que es posible utilizar tarjetas exprés. El controlador NFC realiza transacciones de tarjetas exprés en las mismas condiciones que cuando iOS se está ejecutando, salvo que las transacciones solo se notifican con una vibración (no se muestra ninguna notificación visible). En el iPhone SE de 2.ª generación, es posible que las transacciones finalizadas tarden unos segundos en aparecer en pantalla. Esta función no está disponible cuando se realiza un apagado iniciado por un usuario estándar.

Seguridad del sistema

Descripción general de la seguridad del sistema

Aprovechando las capacidades únicas del hardware de Apple, la seguridad del sistema es responsable de controlar el acceso a los recursos del sistema en los dispositivos Apple sin que afecte a la utilización del dispositivo. La seguridad del sistema abarca el proceso de arranque, actualizaciones de software y la protección de los recursos del sistema informático, como la CPU, la memoria, el disco, los programas de software y los datos almacenados.

Las versiones más recientes de los sistemas operativos de Apple son las más seguras. Una parte importante de la seguridad de Apple es el *arranque seguro*, que protege el sistema de posibles infecciones por software malicioso al arrancar. Un arranque seguro comienza en el hardware y crea una cadena de seguridad mediante software, por la que cada paso está diseñado para garantizar que el siguiente funciona correctamente antes de ceder el control. Este modelo de seguridad no solo respalda el arranque por defecto de los dispositivos Apple, sino también sus diversos modos de recuperación y las actualizaciones oportunas. Los subcomponentes, como el chip T2 y Secure Enclave, también realizan su propio arranque seguro para ayudar a garantizar que solo ejecutan código de confianza de Apple. El sistema de actualización está diseñado para evitar los ataques que intentan restablecer versiones anteriores, para que no se puedan utilizar esas versiones anteriores del sistema operativo (cuya seguridad un atacante sabe poner en riesgo) como método para robar los datos del usuario.

Los dispositivos Apple también incluyen protecciones durante el arranque y la ejecución para mantener su integridad durante el funcionamiento continuo. Los iPhone, iPad, Apple Watch, Apple TV y HomePod con procesadores diseñados por Apple y los ordenadores Mac con chips de Apple proporcionan una arquitectura común para proteger la integridad del sistema operativo. macOS también incluye un conjunto ampliado y configurable de funciones de protección que respaldan su exclusivo modelo informático, así como funciones compatibles en todas las plataformas de hardware de Mac.

Arranque seguro

Proceso de arranque para dispositivos iOS y iPadOS

Todos los pasos del proceso de arranque contienen componentes firmados criptográficamente por Apple para permitir la comprobación de integridad de forma que el arranque continúe únicamente después de haber verificado la cadena de confianza. Entre estos componentes se incluyen los cargadores de arranque, el kernel, las extensiones del kernel y el firmware de banda base móvil. Esta cadena de arranque segura está diseñada para verificar que los niveles más bajos del software no se han manipulado.

Cuando se enciende un dispositivo iOS o iPadOS, el procesador de aplicaciones ejecuta inmediatamente código de la memoria de solo lectura (que se conoce como [ROM de arranque](#)). Este código inmutable, que también se conoce como *raíz de confianza de hardware*, se establece durante la fabricación del chip y se confía en él implícitamente. El código de la ROM de arranque contiene la clave pública de la autoridad de certificación raíz de Apple, que se utiliza para verificar que el cargador de arranque [iBoot](#) tiene la firma de Apple antes de permitir que se cargue. Este es el primer paso de la cadena de confianza, en la que cada paso comprueba que el siguiente está firmado por Apple. Cuando iBoot termina de realizar las tareas que tiene asignadas, verifica y ejecuta el kernel de iOS o iPadOS. En el caso de los dispositivos con un procesador A9 o anterior de la serie A, la ROM de arranque carga y verifica otra fase del [cargador de arranque de bajo nivel \(LLB\)](#) que, a su vez, carga y verifica iBoot.

Los fallos a la hora de cargar o de verificar las siguientes fases se gestionan de manera diferente en función del tipo de hardware:

- *Boot ROM no puede cargar el LLB (dispositivos más antiguos):* [Modo de actualización del firmware del dispositivo \(DFU\)](#).
- *LLB o iBoot:* [Modo de recuperación](#).

En cualquier caso, el dispositivo debe estar conectado al Finder (macOS 10.15 o posterior) o a iTunes (macOS 10.14 o anterior) mediante USB y se deben restaurar los ajustes originales de fábrica.

Para limitar el acceso a los datos del usuario en distintos modos, Secure Enclave utiliza el [registro de progreso de arranque \(BPR\)](#), que se actualiza antes de entrar en los siguientes modos:

- *Modo DFU:* Establecido por la ROM de arranque en dispositivos con un sistema en un chip (SoC) de Apple A12 o posteriores.
- *Modo de recuperación:* Establecido por iBoot en dispositivos con un SoC de Apple A10, S2 o posteriores.

En los dispositivos que disponen de acceso a datos móviles, un subsistema de banda base móvil realiza un arranque seguro adicional con software firmado y claves verificadas por el procesador de banda base.

Secure Enclave también realiza un arranque seguro que garantiza que su software (sepOS) está verificado y firmado por Apple.

Implementación segura de iBoot en la memoria

En iOS 14 y iPadOS 14, Apple ha modificado la cadena de herramientas del compilador de C usada para compilar el cargador de arranque iBoot para mejorar su seguridad. La cadena de herramientas modificada implementa código diseñado para evitar problemas de memoria y seguridad de tipos que suelen encontrarse en programas de C. Por ejemplo, ayuda a prevenir la mayoría de las vulnerabilidades en las siguientes clases:

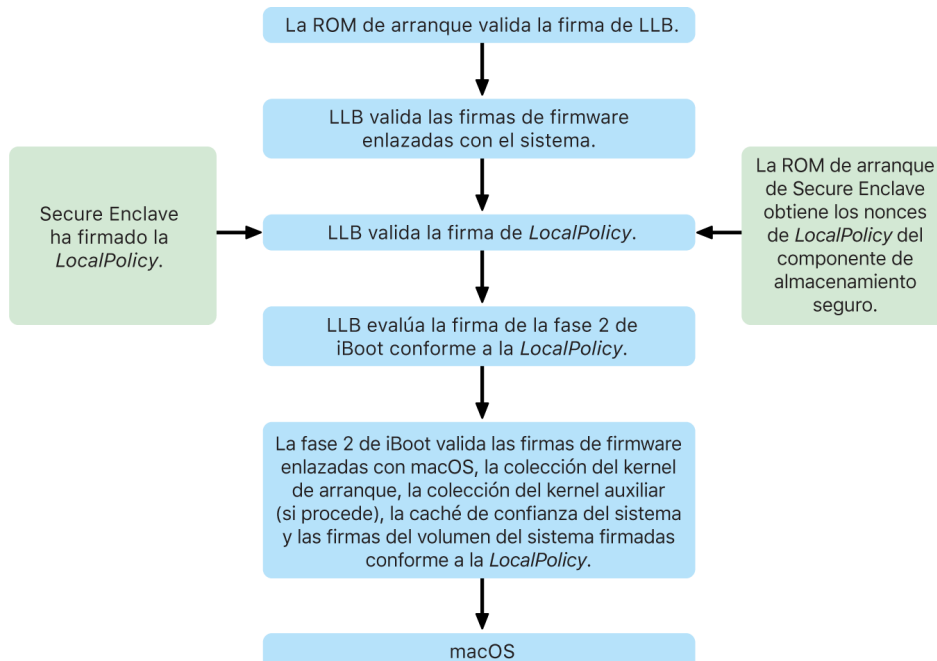
- Desbordamientos de búfer, al garantizar que todos los punteros contengan información de límites que se verifica al acceder a la memoria.
- Vulnerabilidad del montículo, al separar datos del montículo de sus metadatos y detectar con precisión condiciones de error, como los errores de doble liberación.
- Confusión de tipos, al garantizar que todos los punteros contienen información de tipo de tiempo de ejecución que se verifica durante las operaciones de casting de punteros.
- Confusión de tipos provocada por errores de utilización después de liberación, al segregar todas las asignaciones de memoria dinámica por tipo estático.

Esta tecnología está disponible en los iPhone con el chip A13 Bionic de Apple o modelos posteriores, así como en los iPad con el chip A14 Bionic.

Ordenadores Mac con chip de Apple

Proceso de arranque para un Mac con chip de Apple

Cuando se enciende un Mac con chip de Apple, realiza un proceso de arranque muy similar al del iPhone y el iPad.



El chip ejecuta código de la [ROM de arranque](#) en el primer paso de la cadena de confianza. El arranque seguro de macOS en un Mac con chip de Apple no solo verifica el propio código del sistema operativo, sino también las políticas de seguridad e incluso las kexts (admitidas, aunque no recomendadas) configuradas por usuarios autorizados.

Cuando se inicia el cargador de arranque de bajo nivel (LLB), verifica las firmas y carga firmware enlazado por el sistema para núcleos intraSoC, como los controladores de almacenamiento, pantalla, gestión del sistema y Thunderbolt. El LLB también es responsable de cargar el archivo LocalPolicy, que es un archivo firmado por el procesador Secure Enclave. Este archivo describe la configuración que el usuario ha seleccionado para las políticas de arranque del sistema y de seguridad en tiempo de ejecución. El archivo LocalPolicy tiene el mismo formato de estructura de datos que todos los demás objetos de arranque, pero está firmado localmente por una clave privada que solo está disponible en el componente Secure Enclave de un ordenador determinado, en lugar de por un servidor central de Apple (como las actualizaciones de software).

Para ayudar a evitar la reproducción de cualquier archivo LocalPolicy anterior, el LLB debe buscar un [nonce](#) del componente de almacenamiento seguro asociado a Secure Enclave. Para ello, utiliza la ROM de arranque de Secure Enclave y se asegura de que el nonce de LocalPolicy se corresponda con el nonce del componente de almacenamiento seguro. Esto ayuda a impedir que un antiguo archivo LocalPolicy, que podría estar configurado para un nivel de seguridad inferior, vuelva a aplicarse al sistema después de actualizar la seguridad. En consecuencia, el arranque seguro de un Mac con chip de Apple ayuda a proteger no solo contra ataques que intentan restablecer versiones anteriores del sistema operativo, sino también contra posibles degradaciones de las políticas de seguridad.

El archivo LocalPolicy recoge si el sistema operativo está configurado para una seguridad total, reducida o permisiva:

- *Seguridad máxima:* El sistema se comporta como iOS y iPadOS, y solo permite el software de arranque más reciente en el momento de la instalación.
- *Seguridad reducida:* Se indica al LLB que confíe en firmas "globales", incluidas con el sistema operativo. Esto permite al sistema ejecutar versiones anteriores de macOS. A este nivel de seguridad se le llama *reducida* porque, inevitablemente, las versiones anteriores de macOS tienen vulnerabilidades sin correcciones. Este es también el nivel de política requerido para admitir el arranque de extensiones del kernel (kexts).
- *Seguridad permisiva:* Al igual que la seguridad reducida, el sistema utiliza la verificación de firmas globales para [iBoot](#) y más, pero también indica a iBoot que debe aceptar algunos objetos de arranque firmados por Secure Enclave con la misma clave utilizada para firmar LocalPolicy. Este nivel de política permite que los usuarios compilen, firmen y arranquen sus propios kernels XNU personalizados.

Si LocalPolicy indica al LLB que el sistema operativo seleccionado se está ejecutando en el modo de seguridad máxima, el LLB evalúa la firma personalizada para iBoot. Si se ejecuta con seguridad reducida o permisiva, el LLB evalúa la firma global. Cualquier error de verificación de la firma provocará que el sistema arranque en el sistema operativo de recuperación para ofrecer opciones de reparación.

Después de que el LLB traspase el control a iBoot, este carga firmware enlazado por macOS, como los del Neural Engine seguro, el procesador AOP y otro firmware. iBoot también consulta información del archivo LocalPolicy que le transfiere el LLB. Si LocalPolicy indica que debe haber una colección de kernel auxiliar (AuxKC), iBoot la busca en el sistema de archivos, verifica que está firmada por Secure Enclave con la misma clave que LocalPolicy y comprueba que su hash se corresponde con el almacenado en LocalPolicy. Si se verifica la AuxKC, iBoot la coloca en la memoria con la colección de kernel de arranque, antes de bloquear la región de memoria completa que cubre dicha colección y la AuxKC con la [protección de la integridad del coprocesador del sistema \(SCIP\)](#). Si la política indica que debe haber presente una AuxKC pero no se encuentra, el sistema sigue arrancando en macOS sin ella. iBoot también es responsable de verificar el hash de arranque para el volumen del sistema firmado (SSV), con el fin de garantizar que la integridad del sistema de archivos que montará el kernel está completamente verificada.

Modos de arranque para un Mac con chip de Apple

Un Mac con chip de Apple tiene los modos de arranque que se describen a continuación.

Modo	Combinación de teclas	Descripción
macOS	Desde el estado apagado, pulsa el botón de encendido y suéltalo .	<ol style="list-style-type: none"> 1. La ROM de arranque traspasa el control al LLB. 2. El LLB carga firmware enlazado por el sistema y el archivo LocalPolicy para el sistema operativo macOS seleccionado. 3. El LLB bloquea la indicación en el registro de progreso de arranque (BPR) de que arranca en macOS y traspasa el control a iBoot. 4. iBoot carga el firmware enlazado por macOS, la caché de confianza estática, el árbol del dispositivo y la colección de kernel de arranque. 5. Si el archivo LocalPolicy lo permite, iBoot carga la colección de kernel auxiliar (AuxKC) de kexts de terceros. 6. Si el archivo LocalPolicy no lo desactiva, iBoot verifica el hash de firma raíz del volumen del sistema firmado (SSV).
Sistema operativo de recuperación enlazado	Desde el estado apagado, mantén pulsado el botón de encendido.	<ol style="list-style-type: none"> 1. La ROM de arranque traspasa el control al LLB. 2. El LLB carga firmware enlazado por el sistema y el archivo LocalPolicy para el sistema operativo de recuperación. 3. El LLB bloquea la indicación en el registro de progreso de arranque de que arranca en el sistema operativo de recuperación enlazado y traspasa el control a iBoot para el sistema operativo de recuperación enlazado. 4. iBoot carga el firmware enlazado por macOS, la caché de confianza, el árbol del dispositivo y la colección de kernel de arranque. 5. Si falla el arranque del sistema operativo de recuperación enlazado, se intenta el arranque del sistema operativo de recuperación alternativo. <p><i>Nota:</i> No se permiten degradaciones de seguridad en el archivo LocalPolicy del sistema operativo de recuperación enlazado.</p>

Modo	Combinación de teclas	Descripción
Sistema operativo de recuperación alternativo	Desde el estado apagado, pulsa dos veces el botón de encendido y manténlo pulsado.	<ol style="list-style-type: none"> 1. La ROM de arranque traspasa el control al LLB. 2. El LLB carga firmware enlazado por el sistema y el archivo LocalPolicy para el sistema operativo de recuperación. 3. El LLB bloquea la indicación en el registro de progreso de arranque de que arranca en el sistema operativo de recuperación enlazado y traspasa el control a iBoot para el sistema operativo de recuperación. 4. iBoot carga el firmware enlazado por macOS, la caché de confianza, el árbol del dispositivo y la colección de kernel de arranque. <p><i>Nota:</i> No se permiten degradaciones de seguridad en el archivo LocalPolicy del sistema operativo de recuperación enlazado.</p>
Modo seguro	Arranca el sistema operativo de recuperación tal y como se ha descrito anteriormente y, a continuación, mantén pulsada la tecla Mayúsculas mientras seleccionas el volumen de arranque.	<ol style="list-style-type: none"> 1. Arranca el sistema operativo de recuperación tal y como se ha descrito anteriormente. 2. Al dejar pulsada la tecla Mayúsculas mientras seleccionas un volumen, la app BootPicker aprueba macOS para el arranque, como de costumbre; también define una variable nvram que indica a iBoot que no cargue la AuxKC en el siguiente arranque. 3. El sistema se reinicia y arranca en el volumen de destino, pero iBoot no carga la AuxKC.

Restricciones del sistema operativo de recuperación enlazado

En macOS 12.0.1 o posterior, cada nueva instalación de macOS también instala una versión de sistema operativo de recuperación enlazado en el grupo de volúmenes APFS correspondiente. Este diseño resulta familiar para los usuarios de ordenadores Mac basados en Intel, pero en un Mac con chip de Apple, proporciona garantías adicionales de seguridad y compatibilidad. Como cada instalación de macOS ahora tiene un sistema operativo de recuperación enlazado dedicado, esto ayuda a garantizar que solo ese sistema operativo de recuperación enlazado dedicado pueda realizar operaciones de degradaciones de seguridad. Esto ayuda a proteger las instalaciones de las versiones más nuevas de macOS de las manipulaciones iniciadas desde versiones anteriores de macOS, y viceversa.

Las restricciones de enlace se aplican de este modo:

- Todas las instalaciones de macOS 11 se enlazan al sistema operativo de recuperación. Si se selecciona el arranque de una instalación de macOS 11 por defecto, el sistema operativo de recuperación se arranca manteniendo pulsado el botón de encendido en el tiempo de arranque en un Mac con chip de Apple. El sistema operativo de recuperación puede degradar los ajustes de seguridad de las instalaciones de macOS 11, pero no los de las instalaciones de macOS 12.0.1.
- Si se selecciona el arranque de una instalación de macOS 12.0.1 o posterior por defecto, el sistema operativo de recuperación enlazado se arranca manteniendo pulsado el botón de encendido al arrancar el Mac. El sistema operativo de recuperación enlazado puede degradar los ajustes de seguridad de la instalación de macOS enlazada, pero no los de cualquier otra instalación de macOS.

Para arrancar en un sistema operativo de recuperación enlazado para cualquier instalación de macOS, es necesario seleccionar esa instalación como la instalación por defecto. Esto se hace usando Disco de Arranque en Preferencias del Sistema o iniciando cualquier sistema operativo de recuperación y manteniendo pulsada la tecla Opción mientras se selecciona un volumen.

Nota: El sistema operativo de recuperación enlazado no puede realizar degradaciones de ninguna instalación de macOS.

Control de la política de seguridad de Disco de Arranque para un Mac con chip de Apple

Descripción general

A diferencia de las políticas de seguridad de un ordenador Mac basado en Intel, las políticas de seguridad de un Mac con chip de Apple son para cada sistema operativo instalado. Esto significa que en el mismo Mac se admiten varias instancias de macOS instaladas con diferentes versiones y políticas de seguridad. Por este motivo, se ha añadido un *selector de sistema operativo* a Utilidad de Seguridad de Arranque.



En un Mac con chip de Apple, Utilidad de Seguridad del Sistema indica el estado de seguridad general de macOS configurado por el usuario, como el arranque de una *next* o la configuración de la protección de la integridad del sistema (SIP). Si el cambio del ajuste de seguridad degradara considerablemente la seguridad o permitiera poner en riesgo el sistema más fácilmente, los usuarios deben acceder al sistema operativo de recuperación manteniendo pulsado el botón de encendido (para que la señal no se pueda desencadenar mediante software malicioso y solo una persona con acceso físico pueda desencadenarla) para aplicar el cambio. Por este motivo, un Mac con chip de Apple tampoco requerirá (ni admitirá) una contraseña de firmware; todos los cambios críticos ya se gestionan mediante la autorización del usuario. Para obtener más información acerca de la SIP, consulta [Protección de la integridad del sistema](#).

La seguridad máxima o reducida puede establecerse mediante Utilidad de Seguridad de Arranque desde el sistema operativo de recuperación. Sin embargo, la seguridad permisiva solo es accesible desde herramientas de línea de comandos para usuarios que aceptan el riesgo de degradar considerablemente la seguridad de su Mac.

Política de seguridad máxima

“Seguridad máxima” es la opción por defecto y se comporta igual que en iOS y iPadOS. En el momento en que se descarga el software y está preparado para su instalación, en lugar de usar la firma global que viene con el software, macOS contacta con el mismo servidor de firmas de Apple que se usa para iOS y iPadOS y pide una nueva firma “personalizada”. Una firma está personalizada cuando incluye el [identificador único del dispositivo o ECID](#) (un identificador único específico de la CPU de Apple, en este caso) como parte de la petición de firma. La firma que devuelve el servidor de firmas es, por tanto, única y solo puede usarla esa CPU de Apple en concreto. Cuando se aplica la política “Seguridad máxima”, la ROM de arranque y el LLB contribuyen a garantizar que una determinada firma no solo esté firmada por Apple, sino que esté firmada para ese Mac concreto; en esencia, vinculan esa versión de macOS a ese Mac.



El uso de un servidor de firmas en línea también proporciona una mayor protección frente a los ataques que intentan restablecer versiones anteriores y que suelen utilizar firmas globales. En un sistema de firmas globales, la etapa de seguridad podría haberse restablecido muchas veces, pero esto no lo sabrá un sistema que nunca ha visto el último firmware. Por ejemplo, un ordenador que actualmente cree que se encuentra en la etapa 1 de seguridad acepta el software de la etapa 2 de seguridad, incluso si la etapa de seguridad actual es 5. Con un sistema de firmas en línea del chip de Apple, el servidor de firmas puede rechazar la creación de firmas para el software que no se encuentre en la etapa de seguridad más reciente.

Además, si un atacante descubre una vulnerabilidad después de un cambio de etapa de seguridad, no puede simplemente tomar el software vulnerable del sistema A de una etapa anterior y aplicarlo al sistema B para atacarlo. El hecho de que el software vulnerable de una etapa anterior estuviera personalizado para el sistema A ayuda a evitar que se pueda transferir y, por tanto, utilizar para atacar un sistema B. Todos estos mecanismos funcionan conjuntamente para ofrecer garantías mucho más sólidas de que los atacantes no pueden instalar software vulnerable en un Mac voluntariamente para burlar las protecciones proporcionadas por el software más reciente. Sin embargo, un usuario que tenga el nombre y la contraseña de un administrador del Mac siempre puede elegir la política de seguridad que mejor se adapte a su caso de uso.

Política de seguridad reducida

La seguridad reducida es similar al comportamiento de "Seguridad media" en un Mac basado en Intel con un chip T2, en el que un proveedor (en este caso, Apple) genera una firma digital para que el código pueda afirmar que procede del proveedor. Este diseño ayuda a impedir que los atacantes inserten código sin firmar. Apple se refiere a esta firma como firma "global" porque se puede usar en cualquier Mac, durante cualquier cantidad de tiempo, para un Mac que actualmente tiene establecida una política de seguridad reducida. La seguridad reducida no proporciona por sí sola protección contra ataques que intentan restablecer versiones anteriores (aunque los cambios no autorizados en el sistema operativo pueden provocar que los datos del usuario dejen de ser accesibles). Para obtener más información, consulta [Extensiones del kernel en un Mac con chip de Apple](#).



Además de permitir a los usuarios ejecutar versiones anteriores de macOS, la seguridad reducida se requiere para otras acciones que pueden poner en riesgo la seguridad del sistema del usuario, como la introducción de extensiones del kernel de terceros (kexts). Las kexts tienen los mismos privilegios que el kernel y, por lo tanto, cualquier vulnerabilidad en kexts de terceros puede poner en riesgo todo el sistema operativo. Por ello, se recomienda encarecidamente a los desarrolladores que adopten extensiones del sistema, antes de que se elimine la compatibilidad con las kexts de macOS en futuros ordenadores Mac con chips de Apple. Aunque las kexts de terceros estén permitidas, no se podrán cargar en el kernel a petición. En su lugar, se reunirán en una colección de kernel auxiliar (AuxKC), cuyo hash se almacena en el archivo LocalPolicy, por lo que requieren un reinicio. Para obtener más información sobre la generación de la AuxKC, consulta [Extensiones del kernel en macOS](#).

Política de seguridad permisiva

La seguridad permisiva es para aquellos usuarios que aceptan establecer el Mac en un estado mucho más inseguro. Este modo es distinto al modo “Sin seguridad” de los ordenadores Mac basados en Intel con chip T2. Con la seguridad permisiva, la verificación de firmas se sigue realizando a lo largo de toda la cadena de arranque seguro, pero al establecer la política en “Seguridad permisiva” se indica a iBoot que debe aceptar objetos de arranque firmados por Secure Enclave localmente, como una colección de kernel de arranque generada por el usuario compilada desde un kernel de XNU personalizado. De este modo, la seguridad permisiva también proporciona una capacidad arquitectónica para ejecutar un kernel del sistema operativo que no sea de confianza arbitrario. Cuando una colección de kernel de arranque personalizada o un sistema operativo que no sea de confianza se cargan en el sistema, algunas claves de descryptación dejan de estar disponibles. Esto está así diseñado para impedir que un sistema operativo que no sea de confianza acceda a datos de sistemas operativos de confianza.

Importante: Apple no proporciona ni admite kernels XNU personalizados.



La seguridad permisiva también se diferencia del modo “Sin seguridad” de los ordenadores Mac basados en Intel con el chip T2 en que es un requisito previo para algunas degradaciones de seguridad que anteriormente se controlaban de manera independiente. En particular, para desactivar la protección de la integridad del sistema (SIP) en un Mac con chip de Apple, un usuario debe reconocer que está cambiando el sistema al modo de seguridad permisiva. Este requisito se ha establecido debido a que la desactivación de la SIP siempre ha puesto al sistema en un estado que permite comprometer la seguridad del kernel mucho más fácilmente. En concreto, la desactivación de la SIP en ordenadores Mac con chip de Apple desactiva la obligación de firmar los kexts durante la generación de la AuxKC, lo que permite que cualquier kext arbitraria se cargue en la memoria del kernel. En un Mac con chip de Apple se ha realizado otra mejora en la SIP, al sacar el almacén de políticas de NVRAM y trasladarlo a LocalPolicy. Así, ahora al desactivar la SIP, se requiere que un usuario con acceso a la clave de firma de LocalPolicy se autentique desde el sistema operativo de recuperación, ejecutado tras mantener pulsado el botón de encendido. Esto dificulta considerablemente que un atacante del software o incluso físicamente presente pueda desactivar la SIP.

No es posible bajar al nivel de seguridad permisiva desde la app Utilidad de Seguridad de Arranque. Los usuarios solo pueden bajar el nivel de seguridad si ejecutan herramientas de línea de comandos desde Terminal en el sistema operativo de recuperación, como `csrutil` (para desactivar la SIP). Una vez que el usuario baja el nivel de seguridad, este hecho se refleja en Utilidad de Seguridad de Arranque, donde un usuario puede establecer la seguridad en un modo más seguro.

Nota: Un Mac con chip de Apple no requiere ni admite una política de arranque de soportes, ya que, técnicamente, todos los arranques se realizan localmente. Si un usuario decide arrancar desde un soporte externo, en primer lugar es necesario personalizar la versión del sistema operativo mediante un reinicio autenticado desde el sistema operativo de recuperación. Este reinicio crea un archivo LocalPolicy en la unidad interna que se usa para realizar un arranque de confianza desde el sistema operativo almacenado en el soporte externo. De esta forma, la configuración del arranque desde el soporte externo siempre está permitida explícitamente por sistema operativo, y ya requiere la autorización del usuario, con lo que no se necesita ninguna configuración segura adicional.

Creación y gestión de claves de firmas de LocalPolicy

Creación

Cuando macOS se instala por primera vez en fábrica o cuando se realiza una operación de borrado e instalación con conexión compartida, el Mac ejecuta código desde un disco RAM de restauración temporal para inicializar el estado por defecto. Durante este proceso, el entorno de restauración crea un nuevo par de claves pública y privada que se almacenan en Secure Enclave. La clave privada se denomina *clave de identidad del propietario (OIK)*. Si ya existe una OIK, se destruye como parte de este proceso. El entorno de restauración también inicializa la clave usada para el bloqueo de activación, la *clave de identidad del usuario (UIK)*. En una parte de este proceso, que es exclusivo de los Mac con chip de Apple, se solicita la certificación de la UIK para el bloqueo de activación y se incluye un conjunto de restricciones solicitadas que se aplicarán durante la validación en LocalPolicy. Si el dispositivo no puede obtener una UIK certificada para el bloqueo de activación (por ejemplo, porque el dispositivo está asociado actualmente a una cuenta de Buscar mi Mac y se ha notificado como perdido), no puede continuar con la creación de un archivo LocalPolicy. Si se emite un *certificado de identidad de usuario (ucrt)* para un dispositivo, dicho ucrt contiene restricciones de política impuestas por el servidor y restricciones de política solicitadas por el usuario en una extensión X.509 v3.

Cuando se recupera correctamente un ucrt o bloqueo de activación, se almacena en una base de datos en el servidor y también se devuelve al dispositivo. Una vez que el dispositivo tiene un ucrt, se envía una solicitud de certificación para la clave pública que corresponde a la OIK al servidor de la *autoridad de acreditación básica (BAA)*. La BAA verifica la solicitud de certificación de la OIK con la clave pública del ucrt almacenado en la base de datos accesible de la BAA. Si la BAA puede verificar la certificación, certifica la clave pública, devolviendo el *certificado de identidad del propietario (OIC)*, que está firmado por la BAA y contiene las restricciones almacenadas en el ucrt. El OIC se devuelve a Secure Enclave. Desde ese momento, siempre que Secure Enclave firme un nuevo archivo LocalPolicy, adjunta el OIC al archivo Image4. El LLB tiene confianza integrada en el certificado raíz de BAA, lo que hace que confíe en el OIC, lo que a su vez permite que confíe en la firma de LocalPolicy general.

Restricciones de RemotePolicy

Todos los archivos Image4, no solo los LocalPolicy, contienen restricciones en la evaluación del manifiesto Image4. Estas restricciones se codifican mediante identificadores de objetos especiales (OID) en el certificado terminal. La biblioteca de verificación de Image4 busca el OID de restricciones de certificado especiales de un certificado durante la evaluación de la firma y evalúa mecánicamente las restricciones especificadas en él. Las restricciones tienen estos formatos:

- X debe existir
- X no debe existir
- X debe tener un valor específico

Así que, por ejemplo, para las firmas "personalizadas", las restricciones de certificado contendrán "ECID debe existir", y para las firmas "globales", contendrán "ECID no debe existir". Estas restricciones están diseñadas para garantizar que todos los archivos Image4 firmados por una clave determinada deban ajustarse a ciertos requisitos para evitar la generación de manifiestos Image4 firmados erróneamente.

En el contexto de cada archivo LocalPolicy, a estas restricciones de certificados Image4 se les denomina *RemotePolicy*. Pueden existir RemotePolicy distintos para diferentes LocalPolicy de entornos de arranque. RemotePolicy se utiliza para restringir el archivo LocalPolicy del sistema operativo de recuperación, de forma que solo pueda comportarse como si se arrancara con seguridad máxima. Esto incrementa la confianza en la integridad del sistema operativo de recuperación como un lugar donde se puede modificar la política. RemotePolicy restringe el archivo LocalPolicy para que contenga el ECID del Mac en el que LocalPolicy se generó y el hash del nonce de RemotePolicy (rpnh) específico almacenado en el componente de almacenamiento seguro asociado de ese Mac. El rpnh y, por tanto, RemotePolicy solo cambian cuando se realizan acciones para Buscar mi Mac y el bloqueo de activación, como la inscripción, la anulación de la inscripción, el bloqueo remoto y el borrado remoto. Las restricciones de RemotePolicy se determinan y especifican en el momento de la certificación de la clave de identidad del usuario (UIK) y se firman en el certificado de identidad del usuario (ucrt) emitido. Algunas restricciones de RemotePolicy, como ECID, ChipID y BoardID, están determinadas por el servidor. Esto es así para impedir que un dispositivo firme archivos de LocalPolicy para otro dispositivo. El dispositivo puede especificar otras restricciones de RemotePolicy para ayudar a impedir que se degrade la seguridad de LocalPolicy sin proporcionar la autenticación local necesaria para acceder al OIK actual ni la autenticación remota de la cuenta para el bloqueo de activación del dispositivo.

Contenido de un archivo LocalPolicy para un Mac con chip de Apple

LocalPolicy es un archivo Image4 firmado por Secure Enclave. Image4 es un formato de estructura de datos codificado por la norma DER de ASN.1 (notación sintáctica abstracta 1) que se usa para describir información sobre objetos de la cadena de arranque seguro en plataformas de Apple. En un modelo de arranque seguro basado en Image4, se solicitan políticas de seguridad en el momento de la instalación del software mediante una solicitud de firma enviada a un servidor de firmas central de Apple. Si la directiva es aceptable, el servidor de firmas devuelve un archivo Image4 firmado, que contiene una serie de secuencias de códigos de 4 caracteres (4CC). Estos archivos Image4 firmados y los códigos de 4 caracteres se evalúan en el arranque mediante software como la ROM de arranque o el LLB.

Traspaso de propiedad entre sistemas operativos

El acceso a la clave de identidad del propietario se denomina "Propiedad". La propiedad se requiere para permitir a los usuarios invalidar el archivo LocalPolicy tras realizar cambios en la política o el software. La OIK está protegida por la misma jerarquía de claves que se describe en [Protección de clave sellada \(SKP\)](#), donde la OIK está protegida por la misma clave de encriptación de claves (KEK) que la clave de encriptación de volumen (VEK). Esto significa que normalmente se encuentra protegida por las contraseñas de usuario y las medidas del sistema operativo y la política. Solo hay una única OIK para todos los sistemas operativos del Mac. Por lo tanto, al instalar un segundo sistema operativo, se requiere el consentimiento explícito de los usuarios del primer sistema operativo para traspasar la propiedad a los usuarios del segundo sistema operativo. Sin embargo, aún no existen para el segundo sistema operativo cuando se ejecuta el instalador desde el primer sistema operativo. Por lo general, los usuarios de los sistemas operativos no se generan hasta que el sistema operativo se arranca y se ejecuta el asistente de configuración. Por tanto, se requieren dos nuevas acciones al instalar un segundo sistema operativo en un Mac con chip de Apple:

- Crear un archivo LocalPolicy para el segundo sistema operativo
- Preparar una instancia de "Instalar usuario" para traspasar la propiedad

Al ejecutar un asistente de instalación y establecer como destino para la instalación un volumen secundario en blanco, un mensaje pregunta al usuario si desea copiar un usuario del volumen actual para que sea el primer usuario del segundo volumen. Si el usuario responde afirmativamente, la instancia de "Instalar usuario" que se crea es, en realidad, una KEK que se obtiene a partir de la contraseña del usuario seleccionado y claves de hardware y que, a su vez, se utiliza para encriptar la OIK al transferirse al segundo sistema operativo. A continuación, desde el asistente de instalación del segundo sistema operativo, se solicita la contraseña de ese usuario, para permitir el acceso a la OIK de Secure Enclave para el nuevo sistema operativo. Si los usuarios deciden no copiar un usuario, la instancia de "Instalar usuario" se creará igualmente, pero se usará una contraseña vacía, en lugar de una contraseña del usuario. Este segundo flujo existe para ciertos escenarios de administración del sistema. No obstante, los usuarios que deseen tener instalaciones de varios volúmenes y realizar un traspaso de la propiedad de la manera más segura posible deben siempre optar por copiar un usuario del primer sistema operativo en el segundo.

LocalPolicy en un Mac con chip de Apple

En un Mac con chip de Apple, el control de las políticas de seguridad locales se ha delegado en una aplicación que se ejecuta en Secure Enclave. Este software puede utilizar las credenciales del usuario y el modo de arranque de la CPU principal para determinar quién puede cambiar la política de seguridad y desde qué entorno de arranque. Esto ayuda a impedir que el software malicioso utilice los controles de política de seguridad contra el usuario al reducir los niveles de seguridad para obtener más privilegios.

Propiedades del manifiesto de LocalPolicy

El archivo LocalPolicy contiene algunos 4CC arquitectónicos que se encuentran en la mayoría de los archivos Image4, como BORD (un identificador de placa o modelo), CHIP (que indica un chip determinado de Apple) o [ECID \(identificador único del dispositivo\)](#). Sin embargo, los 4CC siguientes solo abordan las políticas de seguridad que los usuarios pueden configurar.

Nota: Apple usa el término *Sistema operativo de recuperación auténtico enlazado (1TR)* para indicar un arranque en el sistema operativo enlazado manteniendo pulsado un botón de encendido físico una sola vez. Este es distinto del sistema operativo de recuperación normal, que se produce mediante NVRAM o manteniendo pulsado un botón dos veces, o que puede ocurrir cuando se producen errores en el arranque. La pulsación del botón físico de un tipo determinado genera una mayor confianza en que el entorno de arranque no sea accesible para un atacante del software que haya logrado acceder a macOS.

Hash del nonce de LocalPolicy (lpth)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El lpth se usa como mecanismo de antirreproducción de LocalPolicy. Se trata de un hash SHA384 del nonce de LocalPolicy (LPN) almacenado en el componente de almacenamiento seguro asociado y al que se puede acceder a través de la ROM de arranque de Secure Enclave o del sistema operativo de Secure Enclave. El nonce nativo nunca está visible para el procesador de aplicaciones, solo para sepOS. Un atacante que desee convencer al LLB de que un archivo LocalPolicy anterior que haya capturado sea válido necesitaría colocar un valor en el componente de almacenamiento seguro asociado que genere un hash para el mismo valor de lpth encontrado en el archivo LocalPolicy que quiera volver a reproducir. Por lo general, solo hay un LPN válido en el sistema, excepto durante las actualizaciones de software, cuando hay simultáneamente dos válidos, para permitir la posibilidad de arrancar de forma alternativa el software antiguo en caso de que se produzca un error de actualización. Cuando se modifica cualquier archivo LocalPolicy de cualquier sistema operativo, todas las políticas se vuelven a firmar con el nuevo valor de lpth correspondiente al nuevo LPN encontrado en el componente de almacenamiento seguro asociado. Este cambio ocurre cuando el usuario modifica los ajustes de seguridad o crea nuevos sistemas operativos con un nuevo archivo LocalPolicy para cada uno.

Hash del nonce de la política remota (rpth)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El rpth se comporta de la misma manera que lpth, pero solo se actualiza cuando se actualiza la política remota, como al cambiar el estado de registro de Buscar. Este cambio ocurre cuando el usuario modifica el estado de Buscar en su Mac.

Hash del nonce del sistema operativo de recuperación (ronh)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El ronh se comporta de la misma manera que lpnh, pero se encuentra exclusivamente en el archivo LocalPolicy del sistema operativo de recuperación. Se actualiza cuando también lo hace el sistema operativo de recuperación, como en las actualizaciones de software. Se usa un nonce independiente de lpnh de rpnh para que cuando Buscar establezca un dispositivo en el estado desactivado, se puedan desactivar los sistemas operativos existentes (mediante la eliminación de su LPN y RPN del componente del almacenamiento seguro), mientras que el sistema operativo de recuperación aún pueda arrancarse. De esta forma, los sistemas operativos podrán reactivarse cuando el propietario del sistema demuestre que tiene el control del sistema mediante la introducción de su contraseña de iCloud usada para la cuenta de Buscar. Este cambio ocurre cuando un usuario actualiza el sistema operativo de recuperación o crea nuevos sistemas operativos.

Hash del manifiesto Image4 de la próxima etapa (nsih)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El campo *nsih* representa un hash SHA384 de la estructura de datos del manifiesto Image4 que describe la instancia de macOS arrancada. El manifiesto Image4 de macOS contiene medidas de todos los objetos de arranque, como iBoot, la caché de confianza estática, el árbol del dispositivo, la colección de kernel de arranque y el hash raíz del volumen del sistema firmado (SSV). Cuando se indica al LLB que arranque una instancia de macOS determinada, esto está diseñado para garantizar que el hash del manifiesto Image4 de macOS unido a iBoot se corresponda con lo que se ha capturado en el campo *nsih* de LocalPolicy. De este modo, *nsih* captura la intención del usuario sobre para qué sistema operativo ha creado el usuario un archivo LocalPolicy. Los usuarios cambian el valor de *nsih* de forma implícita al realizar una actualización de software.

Hash de la política de la colección de kernel auxiliar (AuxKC) (auxp)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* macOS
- *Descripción:* El *auxp* es un hash SHA384 de la política de la lista de kexts autorizadas por el usuario (UAKL). Se utiliza durante la generación de la AuxKC para ayudar a garantizar que solo las kexts autorizadas por el usuario se incluyan en la AuxKC. *smb2* es un requisito previo para definir este campo. Los usuarios cambian el valor de *auxp* implícitamente cuando cambian la UAKL al aprobar una kext en el panel "Seguridad y privacidad" de Preferencias del Sistema.

Hash del manifiesto Image4 de la colección de kernel auxiliar (AuxKC) (auxi)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* macOS
- *Descripción:* Una vez que el sistema verifica que el hash de la UAKL se corresponde con lo que se encuentra en el campo auxp de LocalPolicy, solicita que la aplicación del procesador Secure Enclave responsable de la firma de LocalPolicy firme la AuxKC. A continuación, se coloca un hash SHA384 de la firma del manifiesto Image4 de la AuxKC en LocalPolicy, a fin de evitar una posible confusión de las AuxKC firmadas anteriormente en un sistema operativo al arrancar. Si iBoot encuentra el campo auxi en LocalPolicy, intenta cargar la AuxKC desde el almacenamiento y validar su firma. También verifica que el hash del manifiesto Image4 adjunto a la AuxKC se corresponde con el valor encontrado en el campo auxi. Si, por algún motivo, la AuxKC no se carga, el sistema sigue arrancando sin este objeto de arranque y, por lo tanto, sin cargar kexts de terceros. El campo auxp es un requisito previo para definir el campo auxi en LocalPolicy. Los usuarios cambian el valor de auxi implícitamente cuando cambian la UAKL al aprobar una kext en el panel "Seguridad y privacidad" de Preferencias del Sistema.

Hash de recibo de la colección de kernel auxiliar (AuxKC) (auxr)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* macOS
- *Descripción:* El auxr es un hash SHA384 de recibo de la AuxKC, que indica el conjunto exacto de kexts que estaban incluidas en la AuxKC. El recibo de la AuxKC puede ser un subconjunto de la UAKL, ya que las kexts pueden excluirse de la AuxKC aunque estén autorizadas por el usuario si se tiene constancia de que se utilizan para realizar ataques. Asimismo, algunas kexts que pueden usarse para romper el límite entre usuario y kernel pueden acarrear una disminución de las funcionalidades, como la incapacidad de usar Apple Pay o reproducir contenido HDR y 4K. Los usuarios que deseen contar con estas funciones aceptan una inclusión en la AuxKC más restrictiva. El campo auxp es un requisito previo para definir el campo auxr en LocalPolicy. Los usuarios cambian el valor de auxr implícitamente cuando compilan una nueva AuxKC desde el panel "Seguridad y privacidad" de Preferencias del Sistema.

Hash del manifiesto Image4 de CustomOS (coih)

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR
- *Descripción:* El coih es un hash SHA384 hash del manifiesto Image4 de CustomOS. iBoot utiliza la carga útil de ese manifiesto (en lugar del kernel de XNU) para transferir el control. Los usuarios cambian el valor del coih implícitamente al usar la herramienta de línea de comandos kmutil configure-boot en 1TR.

UUID del grupo de volúmenes APFS (vuid)

- *Tipo:* Cadena de octetos (16)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El vuid indica el grupo de volúmenes que el kernel debe usar como raíz. Este campo es principalmente informativo y no se utiliza para restricciones de seguridad. Es el usuario quien establece este vuid implícitamente al crear una nueva instalación del sistema operativo.

UUID del grupo de claves de encriptación de claves (KEK) (kuid)

- *Tipo:* Cadena de octetos (16)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El kuid indica el volumen que se ha arrancado. La clave de encriptación de claves generalmente se usa para Protección de datos. En cada archivo LocalPolicy, se utiliza para proteger la clave de firma de LocalPolicy. Es el usuario quien establece el kuid implícitamente al crear una nueva instalación del sistema operativo.

Medición de la política de arranque de confianza del sistema operativo de recuperación enlazado (prot).

- *Tipo:* Cadena de octetos (48)
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* Una medición de la política de arranque de confianza del sistema operativo de recuperación enlazado (TBPM) es un cálculo del hash SHA384 iterativo sobre el manifiesto Image4 de un archivo LocalPolicy, excepto los nonces, para ofrecer una medición coherente en el tiempo (ya que los nonces como l_{pnh} se actualizan con frecuencia). El campo prot, que solo se encuentra en cada archivo LocalPolicy de macOS, proporciona un emparejamiento para indicar el archivo LocalPolicy del sistema operativo de recuperación que se corresponde con el archivo LocalPolicy de macOS.

Tiene el archivo LocalPolicy del sistema operativo de recuperación firmado por Secure Enclave (hr1p)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* El hr1p indica si el valor prot anterior es la medición de un archivo LocalPolicy del sistema operativo de recuperación firmado por Secure Enclave o no. Si no, el servidor de firmas en línea de Apple, que firma los archivos Image4 de macOS entre otras cosas, firmará el archivo LocalPolicy del sistema operativo de recuperación.

Versión del sistema operativo local (love)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR, sistema operativo de recuperación, macOS
- *Descripción:* love indica la versión del sistema operativo para la que se crea el archivo LocalPolicy. La versión se obtiene del siguiente manifiesto de estado durante la creación del archivo LocalPolicy y se usa para aplicar las restricciones de enlazado del sistema operativo de recuperación.

Multiarranque seguro (smb0)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR, sistema operativo de recuperación
- *Descripción:* Si smb0 está presente y tiene el valor true, el LLB permite que el manifiesto Image4 de la siguiente etapa se firme globalmente, en lugar de requerir una firma personalizada. Los usuarios pueden cambiar este campo con Utilidad de Seguridad de Arranque o bputil para bajar al nivel de seguridad reducida.

Multiarranque seguro (smb1)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si smb1 está presente y tiene el valor true, iBoot permite que objetos como una colección de kernel personalizada se firmen con Secure Enclave con la misma clave que LocalPolicy. La presencia de smb0 es un requisito previo para la presencia de smb1. Los usuarios pueden cambiar este campo con herramientas de línea de comandos como `csrutil` o `bputil` para bajar al nivel de seguridad permisiva.

Multiarranque seguro (smb2)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si smb2 está presente y tiene el valor true, iBoot permite que la colección de kernel auxiliar se firme con Secure Enclave con la misma clave que LocalPolicy. La presencia de smb0 es un requisito previo para la presencia de smb2. Los usuarios pueden cambiar este campo con Utilidad de Seguridad de Arranque o `bputil` para bajar al nivel de seguridad reducida y permitir kexts de terceros.

Multiarranque seguro (smb3)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si smb3 está presente y tiene el valor true, un usuario en el dispositivo ha permitido el control de la [gestión de dispositivos móviles \(MDM\)](#) del sistema. La presencia de este campo permite que el archivo LocalPolicy que controla la aplicación del procesador Secure Enclave acepte la autenticación MDM en lugar de requerir la autenticación del usuario local. Los usuarios pueden cambiar este campo mediante Utilidad de Seguridad de Arranque `obputil` para permitir el control gestionado de kexts de terceros y actualizaciones de software. (En macOS 11.2 o posterior, MDM también puede iniciar una actualización a la versión más reciente de macOS si el modo de seguridad actual es "Seguridad máxima").

Multiarranque seguro (smb4)

- *Tipo:* Booleano
- *Entornos mutables:* macOS
- *Descripción:* Si smb4 está presente y tiene el valor true, el dispositivo ha permitido el control MDM del sistema operativo con [Apple School Manager](#), [Apple Business Manager](#) o Apple Business Essentials. La presencia de este campo permite que el archivo LocalPolicy que controla la aplicación Secure Enclave acepte la autenticación MDM en lugar de requerir la autenticación del usuario local. La solución MDM cambia este campo si detecta que el número de serie de un dispositivo aparece en cualquiera de estos tres servicios.

Protección de la integridad del sistema (sip0)

- *Tipo:* Entero sin firmar de 64 bits
- *Entornos mutables:* 1TR
- *Descripción:* El valor `sip0` contiene bits de la política de protección de la integridad del sistema (SIP) que anteriormente se almacenaban en NVRAM. Aquí se añaden los nuevos bits de la política de SIP (en lugar de usar campos de LocalPolicy como el que se muestra abajo), si solo se usan en macOS, no con el LLB. Los usuarios pueden cambiar este campo con `csrutil` desde 1TR para desactivar la SIP y bajar al nivel de seguridad permisiva.

Protección de la integridad del sistema (sip1)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si `sip1` está presente y tiene el valor `true`, iBoot permitirá errores para verificar el hash raíz del volumen del sistema firmado (SSV). Los usuarios pueden cambiar este campo con `csrutil` o `bputil` desde 1TR.

Protección de la integridad del sistema (sip2)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si `sip2` está presente y tiene el valor `true`, iBoot no bloqueará el registro de hardware de la *región de solo lectura del texto configurable (CTRR)* que marca la memoria de kernel como de no escritura. Los usuarios pueden cambiar este campo con `csrutil` o `bputil` desde 1TR.

Protección de la integridad del sistema (sip3)

- *Tipo:* Booleano
- *Entornos mutables:* 1TR
- *Descripción:* Si `sip3` está presente y tiene el valor `true`, iBoot no aplicará su lista autorizada integrada para la variable `boot-args` de NVRAM que, de lo contrario, podría filtrar las opciones pasadas al kernel. Los usuarios pueden cambiar este campo con `csrutil` o `bputil` desde 1TR.

Certificados y RemotePolicy

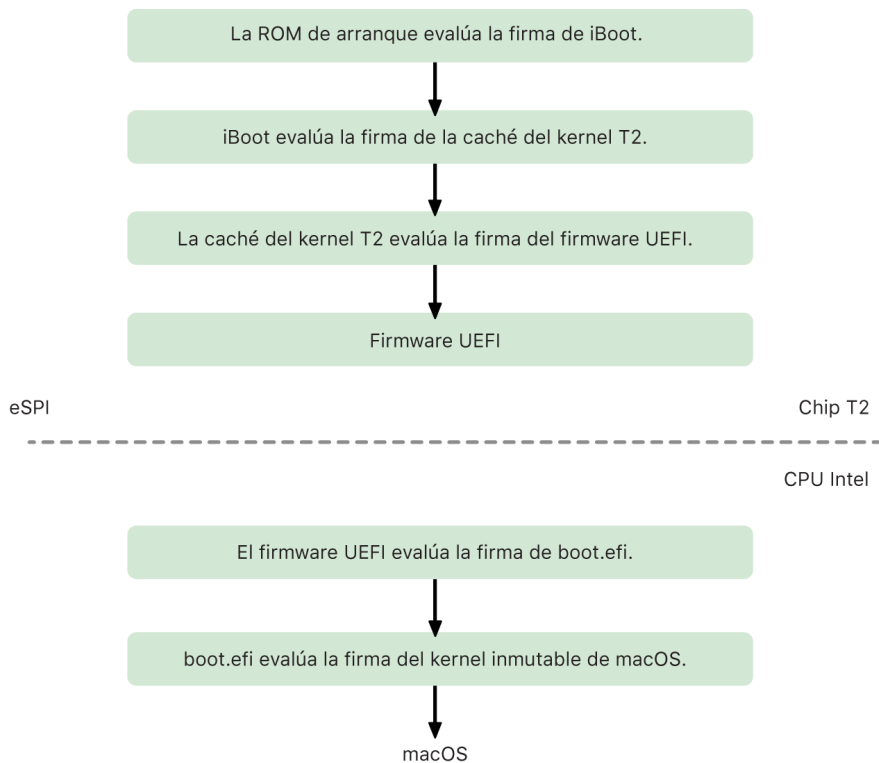
Tal y como se describe en [Creación y gestión de claves de firmas de LocalPolicy](#), el archivo Image4 de LocalPolicy también contiene el certificado de identidad del propietario (OIC) y el archivo RemotePolicy integrado.

Ordenadores Mac basados en Intel

Proceso de arranque para un Mac basado en Intel

Mac basado en Intel con un chip de seguridad T2 de Apple

Al encender un Mac basado en Intel con un chip de seguridad T2 de Apple, el chip realiza un arranque seguro desde su [ROM de arranque](#), de la misma forma que los iPhone, los iPad y los Mac con chip de Apple. Esto verifica el cargador de arranque de iBoot y es el primer paso de la cadena de confianza. [iBoot](#) comprueba el kernel y el código de extensión de kernel del chip T2, que después verifica el firmware de UEFI de Intel. El firmware de UEFI y la firma asociada en un principio solo están disponibles para el chip T2.



Después de la verificación, la imagen del firmware de UEFI se asigna a una porción de la memoria del chip T2. Esta memoria pasa a estar disponible para la CPU Intel a través de la interfaz de periféricos serie mejorada (eSPI). Cuando la CPU Intel arranca por primera vez, obtiene el firmware de UEFI a través de eSPI procedente de la copia asignada por la memoria y de integridad probada del firmware ubicado en el chip T2.

La evaluación de la cadena de confianza continúa en la CPU Intel: el firmware de UEFI evalúa la firma de boot.efi, que es el cargador de arranque de macOS. Las firmas de arranque seguro del macOS, que residen en el procesador Intel, se guardan en el mismo formato Image4 que se usa para iOS, iPadOS y el arranque seguro del chip T2. Además, el código que analiza los archivos Image4 es el mismo código bastionado de la actual implementación de arranque seguro de iOS y iPadOS. Boot.efi, a su vez, verifica la firma de un nuevo archivo llamado "immutablekernel". Cuando se activa el arranque seguro, el archivo immutablekernel representa el conjunto completo de extensiones del kernel de Apple necesarias para el arranque de macOS. La política de arranque seguro termina con el traspaso a immutablekernel y, después de eso, empiezan a aplicarse las políticas de seguridad de macOS (como la protección de la integridad del sistema y las extensiones del kernel firmadas).

Si se produce cualquier fallo o error en este proceso, el Mac entra en el [modo de recuperación](#), en el modo de recuperación del chip de seguridad T2 de Apple o en el modo de [actualización del firmware del dispositivo \(DFU\)](#) del chip de seguridad T2 de Apple.

Microsoft Windows en un Mac basado en Intel con un chip T2

Por defecto, un Mac basado en Intel compatible con el arranque seguro únicamente confía en contenido firmado por Apple. Sin embargo, para mejorar la seguridad de las instalaciones de Boot Camp, Apple también es compatible con el arranque seguro de Windows. El [firmware de la interfaz de firmware extensible unificada \(UEFI\)](#) incluye una copia del certificado de producción CA 2011 de Microsoft Windows, que se usa para autenticar los cargadores de arranque de Microsoft.

Nota: De momento no se ha proporcionado ninguna confianza al certificado CA 2011 de la UEFI de Microsoft Windows, lo que permitiría la verificación del código firmado por los socios de Microsoft. Este certificado de la autoridad de certificación de la UEFI se usa habitualmente para verificar la autenticación de los cargadores de arranque de otros sistemas operativos, como las variantes de Linux.

La compatibilidad con el arranque seguro de Windows no se activa por defecto; se activa mediante Asistente Boot Camp (BCA). Cuando un usuario ejecuta el BCA, macOS se reconfigura para confiar en el código original firmado por Microsoft durante el arranque. Después de completar el BCA, si macOS no puede llevar a cabo la evaluación de la confianza del código original de Apple durante el arranque seguro, el firmware de UEFI intenta evaluar la confianza del objeto según el formato de arranque seguro de la UEFI. Si la evaluación de la confianza se realiza correctamente, el Mac sigue adelante con el proceso de arranque de Windows. Si no, el Mac entra en el sistema operativo de recuperación e informa al usuario del error al evaluar la confianza.

Ordenadores Mac basados en Intel sin chip T2

Un Mac basado en Intel sin chip T2 no admite el arranque seguro. Por lo tanto, el [firmware de la interfaz de firmware extensible unificada \(UEFI\)](#) carga el software de arranque de macOS (boot.efi) desde el sistema de archivos sin verificación y el software de arranque carga el kernel (prelinkedkernel) desde el sistema de archivos sin verificación. Para proteger la integridad de la cadena de arranque, los usuarios deberían activar todos estos mecanismos de seguridad:

- *Protección de la integridad del sistema (SIP)*: Activado por defecto, protege el software de arranque y el kernel de escrituras malintencionadas desde el mismo macOS en ejecución.
- *FileVault*: Esto se puede activar de dos formas: por el usuario o por un administrador de una solución de [gestión de dispositivos móviles \(MDM\)](#). Esto protege frente a un atacante presente físicamente que utiliza la modalidad de disco de destino para sobrescribir el software de arranque.
- *Contraseña de firmware*: Esto se puede activar de dos formas: por el usuario o por un administrador de MDM. Esto ayuda a evitar que un atacante presente físicamente inicie modos de arranque alternativos (como el sistema operativo de recuperación, el modo de usuario único o la modalidad de disco de destino) desde los que el software de arranque se puede sobrescribir. Esto también ayuda a evitar el arranque desde soportes alternativos, por los que un atacante podría ejecutar códigos para sobrescribir el software de arranque.



Modos de arranque de un Mac basado en Intel con un chip de seguridad T2 de Apple

Un Mac basado en Intel con un chip de seguridad T2 de Apple tiene diversos modos de arranque a los que se puede acceder en el arranque pulsando unas combinaciones de teclas que el firmware de UEFI o el software de arranque reconocen. Algunos modos de arranque, como el modo de usuario único, no funcionan a no ser que la política de seguridad se cambie a "Sin seguridad" en Utilidad de Seguridad de Arranque.

Modo	Combinación de teclas	Descripción
Arranque de macOS	Ninguna	El firmware de UEFI traspasa el control al software de arranque de macOS (una aplicación de UEFI), que a su vez traspasa el control al kernel de macOS. Durante un arranque estándar de un Mac con FileVault activado, el software de arranque de macOS presenta la interfaz de la ventana de inicio de sesión que recibe la contraseña que descripta el almacenamiento.
Gestor de arranque	Opción (⌥)	El firmware de UEFI inicia la aplicación de UEFI integrada, que presenta al usuario con una interfaz de selección del dispositivo de arranque.
Modalidad de disco de destino (TDM)	T	El firmware de UEFI inicia la aplicación de UEFI integrada, que presenta el dispositivo de almacenamiento interno como un dispositivo de almacenamiento en formato nativo basado en bloques a través de FireWire, Thunderbolt, USB o cualquier combinación de las tres (dependiendo del modelo del Mac).
Modo de usuario único	Comando (⌘) + S	El kernel de macOS transfiere el indicador <code>-s</code> del vector de argumento de <code>launchd</code> y, a continuación, <code>launchd</code> crea el shell de usuario único en el <code>tty</code> de la app Consola. <i>Nota:</i> Si el usuario sale del shell, macOS continúa el proceso de arranque con la ventana de inicio de sesión.
Sistema operativo de recuperación	Comando (⌘) + R	El firmware de UEFI carga un macOS mínimo desde un archivo de imagen de disco (.dmg) firmado en el dispositivo de almacenamiento interno.
Sistema operativo de recuperación con conexión a internet	Opción (⌥) + Comando (⌘) + R	La imagen de disco firmada se descarga de internet mediante HTTP.
Diagnóstico	D	El firmware de UEFI carga un entorno de diagnóstico de UEFI mínimo desde un archivo de imagen de disco firmado en el dispositivo de almacenamiento interno.
Diagnóstico con conexión a internet	Opción (⌥) + D	La imagen de disco firmada se descarga de internet mediante HTTP.
Arranque de Windows	Ninguna	Si se ha instalado Windows mediante Boot Camp, el firmware de UEFI traspasa el control al software de arranque de Windows, que traspasa el control al kernel de Windows.

Utilidad de Seguridad de Arranque en un Mac con un chip de seguridad T2 de Apple

Descripción general

En un Mac basado en Intel con un chip de seguridad T2 de Apple, Utilidad de Seguridad de Arranque gestiona una serie de ajustes de políticas de seguridad. La utilidad, que es accesible al arrancar en el sistema operativo de recuperación y seleccionar Utilidad de Seguridad de Arranque desde el menú Utilidades, impide que un atacante pueda manipular con facilidad los ajustes de seguridad admitidos.



Los cambios en las políticas más importantes requieren autenticación, incluso en el [modo de recuperación](#). Cuando se abre Utilidad de Seguridad de Arranque por primera vez, pide al usuario que introduzca una contraseña de administrador para la instalación de macOS principal asociada con el sistema operativo de recuperación que se ha arrancado en ese momento. Si no hay ningún administrador, se debe crear uno antes de poder cambiar la política. El chip T2 requiere que el ordenador Mac esté arrancado en ese momento en el sistema operativo de recuperación y que se produzca una autenticación con credenciales respaldadas por Secure Enclave antes de poder realizar el cambio de dicha política. Los cambios en la política de seguridad tienen dos requisitos implícitos. El sistema operativo de recuperación se debe:

- Arrancar desde un dispositivo de almacenamiento conectado directamente al chip T2, puesto que las particiones de otros dispositivos no tienen credenciales respaldadas por Secure Enclave vinculadas al dispositivo de almacenamiento interno.
- Almacenar en un volumen [APFS](#), porque solo se pueden almacenar las credenciales de autenticación del modo de recuperación enviadas a Secure Enclave en el volumen APFS Prearranque de una unidad. Los volúmenes con formato HFS+ no pueden usar el arranque seguro.

Esta política solo se muestra en Utilidad de Seguridad de Arranque en los ordenadores Mac basados en Intel con un chip T2. Aunque en la mayoría de casos de uso la política de arranque seguro no debería requerir cambios, los usuarios son los que, en última instancia, tienen el control de los ajustes de su dispositivo y pueden optar (en función de sus necesidades) por desactivar o utilizar una opción menos segura de la funcionalidad de arranque seguro del Mac.

Los cambios a la política de arranque seguro llevados a cabo desde esta app solo se aplican a la evaluación de la cadena de confianza que se verifica en el procesador Intel. La opción "Arranque seguro del chip T2" siempre se aplica.

La política de arranque seguro se puede configurar en uno de estos tres ajustes: "Seguridad máxima", "Seguridad media", y "Sin seguridad". "Sin seguridad" desactiva la evaluación del arranque seguro por completo en el procesador Intel y permite que el usuario inicie el proceso de arranque con lo que quiera.

Política de arranque "Seguridad máxima"

"Seguridad máxima" es la política de arranque por defecto y se comporta de manera similar que en iOS y iPadOS o que "Seguridad máxima" en un Mac con chip de Apple. En el momento en el que se descarga el software y se prepara para su instalación, se personaliza con una firma que incluye el [identificador único del dispositivo o ECID](#) (un identificador único específico del chip T2, en este caso) como parte de la petición de firma. La firma que devuelve el servidor de firmas es, por tanto, única y solo puede usarla ese chip T2 en concreto. El [firmware de la interfaz de firmware extensible unificada \(UEFI\)](#) está diseñado para garantizar que, cuando la política "Seguridad máxima" está en vigor, una determinada firma no solo esté firmada por Apple, sino que esté firmada para ese Mac concreto, vinculando en la práctica esa versión de macOS a ese Mac. Esto ayuda a impedir ataques que intentan restablecer versiones anteriores, tal y como se describe para la seguridad máxima en un Mac con chip de Apple.

Política de arranque "Seguridad media"

La política de arranque "Seguridad media" es similar a un arranque seguro de la UEFI tradicional, en la que un proveedor (en este caso, Apple) genera una firma digital para que el código pueda afirmar que procede del proveedor. De esta forma se evita que los atacantes puedan insertar código sin firmar. Apple se refiere a esta firma como firma "global" porque se puede usar en cualquier Mac, durante cualquier cantidad de tiempo, para un Mac que actualmente tiene establecida una política de seguridad media. iOS, iPadOS y el chip T2 no son compatibles con las firmas globales. Este ajuste no intenta impedir los ataques que intentan restablecer versiones anteriores.

Política de arranque de soportes

Esta política de arranque de soportes solo existe en los Mac basados en Intel con un chip T2 y es independiente de la política de arranque seguro. Así, incluso si un usuario desactiva el arranque seguro, esto no cambia el comportamiento por defecto de impedir cualquier otra cosa que no sea el dispositivo de almacenamiento conectado directamente al chip T2 para arrancar el Mac (la política de arranque de soportes no es necesaria en un Mac con chip de Apple). Para más información, consulta [Control de la política de seguridad de Disco de Arranque](#).

Protección mediante contraseña de firmware en un Mac basado en Intel

macOS en ordenadores Mac basados en Intel con un chip de seguridad T2 de Apple admite el uso de una contraseña de firmware para ayudar a evitar modificaciones no deseadas de los ajustes del firmware en un Mac concreto. La contraseña de firmware está diseñada para evitar la selección de modos de arranque alternativos, como arrancar en un sistema operativo de recuperación o en el modo de usuario único, arrancar desde un volumen no autorizado o arrancar en la modalidad de disco de destino.

Nota: La contraseña de firmware no se requiere en un Mac con chip de Apple, ya que la funcionalidad de firmware crítica que restringía se ha trasladado al sistema operativo de recuperación y, cuando FileVault está activado, este sistema requiere que el usuario se autentique para que pueda accederse a la funcionalidad crítica.

El modo más básico de contraseña de firmware se puede localizar en la Utilidad de contraseña de firmware del sistema operativo de recuperación en un Mac basado en Intel *sin* chip de seguridad T2, y en la Utilidad de Seguridad de Arranque en un Mac basado en Intel *con* un chip T2. Las opciones avanzadas (como la posibilidad de pedir que se introduzca la contraseña en cada proceso de arranque) están disponibles en la herramienta de línea de comandos `firmwarepasswd` en macOS.

Establecer una contraseña de firmware resulta especialmente importante para reducir el riesgo de ataques en ordenadores Mac basados en Intel sin un chip T2 de un atacante presente físicamente. La contraseña de firmware puede ayudar a impedir que un atacante arranque el sistema operativo de recuperación, desde donde podría desactivar la protección de la integridad del sistema (SIP). Al restringir el proceso de arranque desde soportes alternativos, un atacante no puede ejecutar código privilegiado desde otro sistema operativo para atacar los firmwares periféricos.

Hay un mecanismo de restablecimiento de la contraseña de firmware para ayudar a los usuarios que han olvidado su contraseña. Los usuarios pulsan una combinación de teclas durante el proceso de arranque y se les presenta una cadena específica del modelo que deben proporcionar a AppleCare. AppleCare firma digitalmente un recurso y el [identificador uniforme de recursos \(URI\)](#) comprueba esta firma. Si se valida la firma y el contenido es para ese Mac concreto, el firmware de UEFI elimina la contraseña de firmware.

Para los usuarios que no quieren que otra persona elimine su contraseña de firmware mediante software, se ha añadido la opción `-disable-reset-capability` a la herramienta de línea de comandos `firmwarepasswd` en macOS 10.15. Antes de establecer esta opción, los usuarios deben reconocer que, si olvidan la contraseña y necesitan su eliminación, el usuario debe asumir el coste de la sustitución de la placa lógica, algo necesario para conseguirlo. Las organizaciones que quieren proteger sus ordenadores Mac de los ataques externos y de los empleados deben establecer una contraseña de firmware en los sistemas que pertenezcan a la organización. Esto puede realizarse en el dispositivo de las siguientes maneras:

- de forma manual, en el momento de la instalación, mediante la herramienta de línea de comandos `firmwarepasswd`;
- mediante herramientas de gestión de terceros que usan la herramienta de línea de comandos `firmwarepasswd`;
- usando la [gestión de dispositivos móviles \(MDM\)](#).

Sistema operativo de recuperación y entornos de diagnóstico de un Mac basado en Intel

Sistema operativo de recuperación

El sistema operativo de recuperación es totalmente independiente del macOS principal y todo el contenido se almacena en un archivo de imagen de disco llamado BaseSystem.dmg. También tiene asociado un archivo BaseSystem.chunklist, que se utiliza para verificar la integridad de BaseSystem.dmg. El archivo chunklist es una serie de hashes de fragmentos de 10 MB del archivo BaseSystem.dmg. El [firmware de la interfaz de firmware extensible unificada \(UEFI\)](#) evalúa la firma del archivo chunklist y, a continuación, evalúa de uno en uno el hash de cada fragmento del archivo BaseSystem.dmg. Esto ayuda a garantizar que coincide con el contenido firmado que hay en el archivo chunklist. Si alguno de esos hashes no coincide, se anula el proceso de arranque del sistema operativo de recuperación local y, en su lugar, el firmware de UEFI intenta arrancar desde el sistema operativo de recuperación con conexión a internet.

Si la verificación se completa correctamente, el firmware de UEFI monta la imagen BaseSystem.dmg como un disco de RAM e inicia el archivo boot.efi que contiene. No hace falta que el firmware de UEFI lleve a cabo ninguna comprobación específica de [boot.efi](#), ni que boot.efi compruebe el kernel, puesto que ya se ha comprobado la integridad del contenido completado del sistema operativo (del cual estos elementos son solo un subconjunto).

Diagnóstico Apple

El procedimiento de arranque del entorno de diagnóstico local es prácticamente el mismo que cuando se inicia el sistema operativo de recuperación. Se utilizan archivos AppleDiagnostics.dmg y AppleDiagnostics.chunklist independientes, pero se verifican de la misma forma que los archivos BaseSystem. En lugar de iniciar boot.efi, el firmware de UEFI inicia un archivo dentro de la imagen de disco (archivo .dmg) llamado diags.efi que, a su vez, se encarga de invocar distintos controladores de UEFI con los que puede comunicarse y comprobar si hay errores de hardware.

Sistema operativo de recuperación y entorno de diagnóstico con conexión a internet

Si se ha producido un error al iniciar los entornos de diagnóstico o de recuperación local, el firmware de UEFI intenta descargar las imágenes de internet (un usuario también puede solicitar específicamente que las imágenes se obtengan de internet utilizando unas secuencias especiales de teclas que se pulsan durante el arranque). La validación de la integridad de las imágenes de disco y de los archivos chunklist descargados del servidor del sistema operativo de recuperación se realiza del mismo modo que con las imágenes obtenidas de un dispositivo de almacenamiento.

Aunque la conexión al servidor del sistema operativo de recuperación se realiza mediante HTTP, se sigue comprobando la integridad del contenido completo descargado como se ha descrito anteriormente y, por tanto, está protegido frente a la manipulación por parte de un atacante que controle la red. En caso de que un determinado fragmento no supere la verificación de integridad, se vuelve a solicitar del servidor del sistema operativo de recuperación 11 veces antes de abandonar los intentos y mostrar un error.

Cuando se añadieron los modos de recuperación y diagnóstico con conexión a internet a los ordenadores Mac en 2011, se decidió que sería mejor utilizar el transporte HTTP más sencillo y gestionar la autenticación de contenido mediante el mecanismo de chunklist, en lugar de implementar la funcionalidad HTTPS más compleja en el firmware de UEFI, incrementando así la superficie de ataque del firmware.

Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS

En macOS 10.15, Apple introdujo el volumen del sistema de solo lectura, que es un volumen aislado y dedicado para el contenido del sistema. macOS 11 o posterior añade fuertes medidas de protección criptográfica para el contenido del sistema con un *volumen del sistema firmado* (SSV). El SSV incluye un mecanismo del kernel que verifica la integridad del contenido del sistema en tiempo de ejecución y rechaza todos los datos (de código o no) sin una firma criptográfica válida de Apple. A partir de iOS 15 y iPadOS 15, el volumen del sistema en un dispositivo iOS y iPadOS también obtiene la protección criptográfica de un volumen del sistema firmado.

El SSV no solo ayuda a evitar la manipulación del software de Apple que forma parte del sistema operativo, sino que también garantiza que las actualizaciones de software de macOS sean más fiables y mucho más seguras. Dado que el SSV utiliza instantáneas del [sistema de archivos de Apple \(APFS\)](#), si no se puede llevar a cabo una actualización, la antigua versión del sistema puede restaurarse sin necesidad de reinstalar.

Desde su introducción, APFS ha proporcionado integridad de metadatos del sistema de archivos mediante sumas de control no criptográficas en el dispositivo de almacenamiento interno. El SSV refuerza el mecanismo de integridad al añadir hashes criptográficos y ampliarlo para abarcar cada byte de los datos de archivos. Los datos del dispositivo de almacenamiento interno (incluidos los metadatos del sistema de archivos) se convierten en un hash criptográfico en la ruta de lectura y el hash se compara con un valor esperado en los metadatos del sistema de archivos. En caso de discrepancia, el sistema asume que los datos se han manipulado y no los devolverá al software que los solicite.

Cada hash SHA256 del SSV se almacena en el árbol de metadatos del sistema de archivos principal, que también se convierte en un hash. Dado que cada nodo del árbol verifica de forma recursiva la integridad de los hashes de sus elementos secundarios —como un árbol de hash binario (Merkle)—, el valor de hash del nodo raíz, denominado *sello*, abarca cada byte de datos en el SSV, de modo que la firma criptográfica cubre el volumen del sistema completo.

Durante la instalación y actualización de macOS, el sello se vuelve a calcular desde el sistema de archivos del dispositivo y esa medición se verifica con la medición que Apple ha firmado. En un Mac con chip de Apple, el cargador de arranque verifica el sello antes de transferir el control al kernel. En un Mac basado en Intel con un chip de seguridad T2 de Apple, el cargador de arranque reenvía la medición y la firma al kernel que, a su vez, verifica el sello directamente antes de montar el sistema de archivos raíz. En cada caso, si la verificación falla, el proceso de arranque se detendrá y se solicitará al usuario que reinstale macOS. Este procedimiento se repite en cada arranque a menos que el usuario elija acceder a un modo de seguridad inferior y haya decidido por separado desactivar el volumen del sistema firmado.

Durante las actualizaciones de software de iOS y iPadOS, el volumen del sistema se prepara y se vuelve a calcular de forma similar. Los cargadores de arranque de iOS y iPadOS verifican que el sello está intacto y que coincide con un valor firmado por Apple antes de permitir que el dispositivo inicie el kernel. Las discrepancias en el arranque piden al usuario que actualice el software del sistema en el dispositivo. Los usuarios no pueden desactivar la protección de un volumen de sistema firmado en iOS y iPadOS.

SSV y firma del código

La firma del código sigue vigente y el kernel exige su aplicación. El volumen del sistema firmado proporciona protección cuando se lee cualquier byte del dispositivo de almacenamiento interno. Por su parte, la firma de código proporciona protección cuando se asignan mediante la memoria objetos Mach como ejecutables. Tanto el SSV como la firma del código protegen código ejecutable en todas las rutas de lectura y ejecución.

SSV y FileVault

En macOS 11, el SSV proporciona una protección en reposo equivalente para el contenido del sistema y, por lo tanto, no es necesario que el volumen del sistema se encripte. El sistema de archivos detectará todas las modificaciones que se le realicen mientras está en reposo cuando estas se lean. Si el usuario ha activado FileVault, el contenido del usuario en el volumen de datos se seguirá encriptando con un secreto proporcionado por el usuario.

Si el usuario decide desactivar el SSV, el sistema en reposo será vulnerable a la manipulación y dicha manipulación podría permitir a un atacante extraer datos del usuario encriptados la próxima vez que arranque el sistema. Por lo tanto, el sistema no permitirá que se desactive el SSV si FileVault está activado. La protección en reposo debe activarse o desactivarse para ambos volúmenes de manera coherente.

En macOS 10.15 o versiones anteriores, FileVault protege el software del sistema operativo en reposo al encriptar el contenido del usuario y del sistema con una clave protegida por un secreto proporcionado por el usuario. Esto protege frente a un atacante con acceso físico al dispositivo, impidiéndole que acceda al sistema de archivos que contiene el software del sistema o lo modifique.

El SSV y un Mac con un chip de seguridad T2 de Apple

En un Mac con un chip de seguridad T2 de Apple, solo macOS está protegido por el SSV. El software que se ejecuta en el chip T2 y verifica macOS está protegido por el arranque seguro.

Actualizaciones seguras de software

La seguridad es un proceso. No basta con realizar un arranque de confianza de la versión del sistema operativo instalada de fábrica; también debe existir un mecanismo para obtener de forma rápida y segura las actualizaciones de seguridad más recientes. Apple publica periódicamente actualizaciones de software para resolver nuevos problemas de seguridad. Los usuarios de dispositivos iOS y iPadOS reciben notificaciones de actualizaciones en el dispositivo. Los usuarios de Mac pueden encontrar las actualizaciones disponibles en Preferencias del Sistema. Las actualizaciones se proporcionan por vía inalámbrica, para poder instalar rápidamente las correcciones de seguridad más recientes.

Proceso de actualización

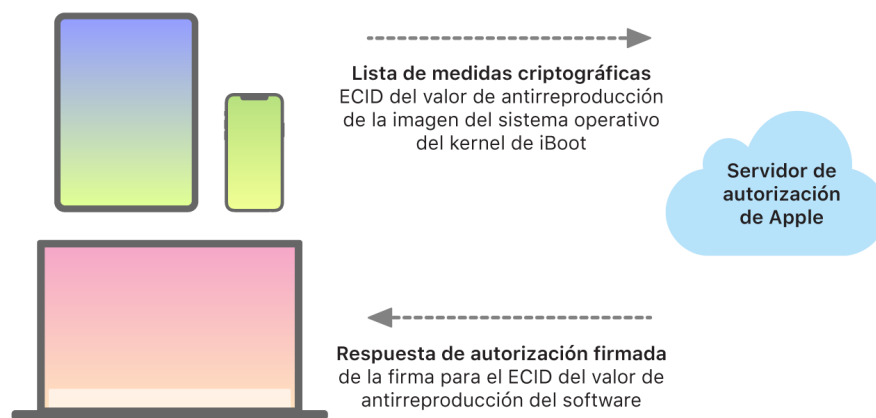
El proceso de actualización usa la misma raíz de confianza basada en hardware que utiliza el arranque seguro diseñada para instalar únicamente código firmado por Apple. El proceso de actualización también utiliza [autorización del software del sistema](#) para comprobar que únicamente las copias de las versiones del sistema operativo que Apple está firmando activamente se puedan instalar en los dispositivos iOS y iPadOS o en los ordenadores Mac con el ajuste "Seguridad máxima", configurado como la política de arranque seguro en Utilidad de Seguridad de Arranque. Con estos procesos seguros, Apple puede detener la firma de versiones anteriores del sistema operativo con vulnerabilidades conocidas y ayudar a impedir ataques que intentan restablecer versiones anteriores.

Para una mayor seguridad de las actualizaciones de software, cuando el dispositivo que se va a actualizar se conecta físicamente a un Mac, se descarga e instala una copia completa de iOS o iPadOS. Sin embargo, para las actualizaciones de software de forma remota (OTA) *solo se descargan los componentes necesarios para llevar a cabo la actualización*. Al no descargar todo el sistema operativo, se mejora la eficiencia de la red. Además, las actualizaciones de software se pueden almacenar en caché en un Mac en el que se ejecute macOS 10.13 o posterior con el almacenamiento en caché del contenido activado, de manera que los dispositivos iOS y iPadOS no tengan que volver a descargar de internet los datos de actualización necesarios (de todos modos, tendrán que ponerse en contacto con los servidores de Apple para completar el proceso de actualización).

Proceso de actualización personalizado

Durante las actualizaciones, se realiza una conexión con el servidor de autorización de instalaciones de Apple, que incluye una lista de medidas criptográficas para cada parte del paquete de instalación que se vaya a instalar (por ejemplo, iBoot, el kernel o una imagen del sistema operativo), un valor antirreproducción aleatorio (el nonce) y el [identificador único del dispositivo \(ECID\)](#).

El servidor de autorización coteja la lista de medidas presentada con las versiones cuya instalación se permite y, si encuentra una coincidencia, añade el ECID a la medida y firma el resultado. Como parte del proceso de actualización, el servidor envía un conjunto completo de datos firmados al dispositivo. La adición del ECID "personaliza" la autorización para el dispositivo que realiza la solicitud. El servidor solo autoriza y firma las medidas conocidas, de modo que ayuda a garantizar que la actualización se lleve a cabo de acuerdo con las especificaciones de Apple.



La evaluación de la cadena de confianza del arranque verifica que la firma procede de Apple y que la medida del ítem cargado desde el dispositivo de almacenamiento, en combinación con el ECID del dispositivo, coincide con lo que cubría la firma. Estos pasos están diseñados para garantizar que, en dispositivos que admiten la personalización, la autorización sea para un dispositivo determinado y que un sistema operativo o versión de firmware anterior de un dispositivo no se puede copiar en otro. El [nonce](#) ayuda a impedir que un atacante guarde la respuesta del servidor y la utilice para manipular un dispositivo o modificar el software del sistema de algún otro modo.

El proceso de personalización es el motivo por el que siempre se requiere una conexión de red con Apple para actualizar cualquier dispositivo con un chip diseñado por Apple, incluido un Mac basado en Intel con el chip de seguridad T2 de Apple.

Por último, el volumen de datos del usuario nunca se monta durante una actualización de software, lo que contribuye a impedir que se lea o se escriba nada en ese volumen durante las actualizaciones.

En los dispositivos con un procesador Secure Enclave, ese hardware usa de forma similar el proceso de [autorización del software del sistema](#) para comprobar la integridad de tu software y está diseñado para evitar la instalación de versiones anteriores.

Integridad del sistema operativo

El software del sistema operativo de Apple está diseñado pensando en la seguridad. Este diseño incluye una raíz de confianza de hardware (que se usa para activar el arranque seguro) y un proceso de actualización de software rápido y seguro. Los sistemas operativos de Apple también usan sus funciones específicas de hardware basadas en chips para ayudar a impedir que se aprovechen vulnerabilidades mientras el sistema se ejecuta. Estas funciones en tiempo de ejecución protegen la integridad del código de confianza mientras se ejecuta. En síntesis, el software de los sistemas operativos de Apple ayuda a mitigar técnicas de ataque tanto si se originan a partir de una app maliciosa como desde internet o a través de cualquier otro canal. Las funciones de protección indicadas aquí están disponibles en dispositivos con sistemas en chips (SoC) diseñados por Apple compatibles (lo que incluye a iOS, iPadOS, tvOS, watchOS y ahora también a macOS en un Mac con chip de Apple).

Función	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Familia M1
Protección de la integridad del kernel	✓	✓	✓	✓	✓	✓
Restricciones rápidas de permisos		✓	✓	✓	✓	✓
Protección de la integridad del coprocesador del sistema			✓	✓	✓	✓
Códigos de autenticación de puntero			✓	✓	✓	✓
Capa de protección de la página		✓	✓	✓	✓	Consulta la nota a continuación.

Nota: La capa de protección de la página (PPL) requiere que la plataforma *solo* ejecute código firmado y de confianza; este es un modelo de seguridad que no es aplicable para macOS.

Protección de la integridad del kernel

Una vez que se completa la inicialización de los kernels del sistema operativo, se activa la protección de la integridad del kernel (KIP) para ayudar a evitar las modificaciones del kernel y del código del controlador. El [controlador de memoria](#) proporciona una región de memoria física protegida que **iBoot** usa para cargar el kernel y las extensiones del kernel. Una vez completado el arranque, el controlador de memoria impide escribir en la región de memoria física protegida. La unidad de gestión de memoria (MMU) del procesador de aplicaciones está configurada para ayudar a impedir la asignación de código privilegiado de la memoria física fuera de la región de memoria protegida, así como para ayudar a impedir asignaciones grabables de la memoria física en la región de memoria del kernel.

Para impedir que se vuelva a configurar, el hardware utilizado para activar la KIP se bloquea cuando el proceso de arranque se completa.

Restricciones rápidas de permisos

A partir de los SoC S3 y A11 Bionic de Apple, se introdujo una nueva interfaz de hardware. Esta interfaz (Restricciones rápidas de permisos) incluye un registro de la CPU que restringe los permisos rápidamente, por hilos. Con Restricciones rápidas de permisos (también llamadas registros de APRR), los sistemas operativos compatibles pueden eliminar rápidamente los permisos de ejecución de la memoria sin la sobrecarga de una llamada del sistema y el recorrido o la alineación de la tabla de página. Estos permisos proporcionan un nivel más de mitigación para ataques desde internet, especialmente para código compilado en tiempo de ejecución, ya que la memoria no se puede ejecutar al mismo tiempo que se lee y se escribe.

Protección de la integridad del coprocesador del sistema

El firmware del coprocesador gestiona muchas tareas críticas del sistema, por ejemplo, Secure Enclave, el procesador del sensor de imágenes y el coprocesador de movimiento. Por lo tanto, su seguridad es clave para la seguridad general del sistema. Para impedir la modificación del firmware del coprocesador, Apple utiliza un mecanismo llamado *protección de la integridad del coprocesador del sistema (SCIP)*.

La SCIP funciona de forma similar a la protección de la integridad del kernel (KIP): en el arranque, iBoot carga el firmware del coprocesador en una región de memoria protegida, reservada y separada de la región de KIP. iBoot configura cada unidad de memoria del coprocesador para ayudar a impedir lo siguiente:

- Asignaciones ejecutables fuera de su parte de la región de memoria protegida.
- Asignaciones grabables dentro de su parte de la región de memoria protegida.

También en el arranque, para configurar la SCIP para Secure Enclave, se usa el sistema operativo de Secure Enclave. Cuando el proceso de arranque se completa, el hardware utilizado para activar la SCIP se bloquea. Esto está así diseñado para impedir que se vuelva a configurar.

Códigos de autenticación de puntero

Los códigos de autenticación de puntero (PAC) se usan para proteger el sistema frente a ataques que aprovechan fallos por corrupción de memoria. El software del sistema y las apps integradas usan estos códigos para ayudar a impedir que se modifiquen los punteros de funciones y las direcciones de retorno (punteros de código). Los PAC usan cinco valores secretos de 128 bits para firmar las instrucciones y los datos del kernel, y cada proceso del espacio del usuario tiene sus propias claves B. Los ítems contienen sal criptográfica y se firman como se indica a continuación.

Ítem	Clave	Sal
Dirección de retorno de funciones	IB	Dirección de almacenamiento
Punteros de funciones	IA	0
Función de invocación del bloqueo	IA	Dirección de almacenamiento
Caché del método Objective-C	IB	Dirección de almacenamiento + Clase + Selector
C++ V-Entradas de tabla	IA	Dirección de almacenamiento + Hash (nombre del método alterado)
Etiqueta goto calculada	IA	Hash (nombre de la función)
Estado del hilo del kernel	GA	.
Registros del estado del hilo del usuario	IA	Dirección de almacenamiento
C++ V-Punteros de tabla	DA	0

El valor de la firma se almacena en bits de relleno sin usar en la parte superior del puntero de 64 bits. La firma se verifica antes de su uso y el relleno se restaura para ayudar a garantizar que la dirección del puntero funcione. Si no se verifica, se produce una anulación. Esta verificación aumenta la dificultad de muchos ataques, como en el caso de un ataque de programación orientada al retorno (ROP), que intenta engañar al dispositivo para que ejecute código existente de manera maliciosa al manipular direcciones de retorno de funciones almacenadas en la pila.

Capa de protección de la página

La capa de protección de la página (PPL) en iOS, iPadOS y watchOS está diseñada para impedir que el código del espacio del usuario se modifique una vez completada la verificación de una firma de código. PPL, basándose en la protección de la integridad del kernel y las restricciones rápidas de permisos, gestiona las modificaciones de los permisos de la tabla de página para garantizar que únicamente la PPL pueda alterar las páginas protegidas que contienen el código de usuario y las tablas de página. El sistema ofrece una reducción drástica de la superficie de ataque al respaldar el cumplimiento de la integridad del código en todo el sistema, incluso si un kernel ha sido comprometido. Esta protección no se ofrece en macOS porque la PPL solo es aplicable en sistemas en los que todo el código ejecutado debe estar firmado.

Funciones de seguridad del sistema de macOS adicionales

Funciones de seguridad del sistema de macOS adicionales

macOS funciona en una gran variedad de soluciones de hardware (por ejemplo, CPU basadas en Intel, CPU basadas en Intel combinadas con el chip de seguridad T2 de Apple y SoC con chips de Apple) y es compatible con diversos escenarios de uso genéricos. Mientras que algunos usuarios solo usan las apps básicas preinstaladas o las disponibles en App Store, otros acceden al kernel y necesitan fundamentalmente desactivar todas las medidas de protección de la plataforma para poder ejecutar y probar su código en ejecución con los mayores niveles de confianza. La mayoría de los usuarios se encuentran en un punto intermedio, y muchos tienen periféricos y software que requieren distintos niveles de acceso. Apple ha diseñado la plataforma macOS mediante un enfoque que integra hardware, software y servicios; una plataforma que, por diseño, ofrece seguridad y que resulta sencilla de configurar, implementar y gestionar, al tiempo que mantiene la capacidad de configurarse que requieren los usuarios. macOS también incluye las principales tecnologías de seguridad que un profesional de la informática necesita para ayudar a proteger los datos corporativos en entornos de redes empresariales seguras.

Las siguientes funciones atienden y ayudan a proteger las diversas necesidades de los usuarios de macOS. Se incluyen las siguientes:

- Seguridad del volumen del sistema firmado
- Protección de la integridad del sistema
- Cachés de confianza
- Protección para periféricos
- Compatibilidad con Rosetta 2 (traducción automática) y seguridad para un Mac con chip de Apple
- Compatibilidad y protecciones DMA
- Compatibilidad y seguridad de extensiones del kernel (kexts)
- Compatibilidad y seguridad de ROM opcionales
- Seguridad del firmware de UEFI para ordenadores Mac basados en Intel

Protección de la integridad del sistema

macOS utiliza permisos del kernel para limitar la capacidad de escribir archivos críticos del sistema con una función llamada *protección de la integridad del sistema (SIP)*. Esta función es independiente de la protección de la integridad del kernel (KIP) basada en el hardware de un Mac con chip de Apple (que protege la modificación del kernel en la memoria), al que complementa. Se utiliza una tecnología de controles de acceso obligatorios para ofrecer esta función y una serie de protecciones a nivel del kernel adicionales, como el aislamiento y los almacenes seguros de datos.

Controles de acceso obligatorios

macOS usa los controles de acceso obligatorios, unas políticas que establecen restricciones de seguridad creadas por el desarrollador y que no se pueden anular. Este enfoque es diferente de los controles de acceso discrecional, que permiten a los usuarios anular las políticas de seguridad en función de sus preferencias.

Los controles de acceso obligatorios están ocultos para los usuarios, pero constituyen la tecnología subyacente que ayuda a activar muchas funciones importantes, incluyendo el aislamiento, los controles parentales, las preferencias gestionadas, las extensiones y la protección de la integridad del sistema.

Protección de la integridad del sistema

La *protección de la integridad del sistema* restringe los componentes a solo lectura en ubicaciones críticas del sistema de archivos para ayudar a evitar que un código malicioso los pueda modificar. La protección de la integridad del sistema es un ajuste específico de los ordenadores que se activa por defecto cuando un usuario actualiza a OS X 10.11 o posterior. En ordenadores Mac basados en Intel, si se desactiva, elimina la protección de todas las particiones del dispositivo de almacenamiento físico. macOS aplica esta política de seguridad a cada proceso que se ejecuta en el sistema, independientemente de si se ejecuta en una zona protegida o con privilegios de administrador.

Cachés de confianza

Uno de los objetos incluidos en la cadena de arranque seguro es la caché de confianza estática, un registro de confianza de todos los objetos binarios Mach-O que se controlan en el volumen del sistema firmado. Cada Mach-O se representa con un hash de directorio de código. Para una búsqueda eficaz, estos hashes se ordenan antes de insertarse en la caché de confianza. El directorio de código es el resultado de la operación de firma realizada por `codesign(1)`. Para aplicar la caché de confianza, la SIP debe permanecer activada. Para desactivar la aplicación de la caché de confianza en un Mac con chip de Apple, se debe establecer el arranque seguro en el modo de seguridad permisiva.

Cuando se ejecuta un archivo binario (ya sea para originar un nuevo proceso o para asignar código ejecutable a un proceso existente), su directorio de código se extrae y se convierte en un hash. Si el hash resultante se encuentra en la caché de confianza, se concederán privilegios de plataforma a las asignaciones ejecutables creadas para el archivo binario; es decir, pueden poseer cualquier autorización y ejecutarse sin verificación adicional en lo que respecta a la autenticidad de la firma. Esto contrasta con un Mac basado en Intel, donde el certificado de Apple que firma los archivos binarios transfiere los privilegios de plataforma al contenido del sistema operativo (este certificado no limita qué autorizaciones puede poseer el archivo binario).

Los archivos binarios que no son de plataforma (por ejemplo, código de terceros certificado) deben tener cadenas de certificados válidas para poder ejecutarse, y las autorizaciones que puedan poseer estarán restringidas por el perfil de firma emitido para el desarrollador por el programa para desarrolladores de Apple.

Todos los archivos binarios incluidos en macOS están firmados con un *identificador de plataforma*. En un Mac con chip de Apple, este identificador se usa para indicar que, aunque el archivo binario está firmado por Apple, el hash de su directorio de código debe estar presente en la caché de confianza para poder ejecutarse. En un Mac basado en Intel, el identificador de plataforma se usa para realizar una revocación específica de archivos binarios a partir de una versión anterior de macOS, lo que impide que esos archivos binarios se ejecuten en versiones más recientes.

La caché de confianza estática bloquea completamente un conjunto de archivos binarios en una versión de macOS determinada. Este comportamiento ayuda a impedir que los archivos binarios firmados legítimamente por Apple de sistemas operativos anteriores se introduzcan en versiones más recientes para que un atacante consiga ventaja.

Código de plataforma proporcionado fuera del sistema operativo

Apple proporciona archivos binarios (por ejemplo, Xcode y la pila de herramientas de desarrollo) que no están firmados con un identificador de plataforma. Incluso en este caso, se pueden ejecutar con privilegios de plataforma en un Mac con chip de Apple y en aquellos con un chip T2. Dado que este software de plataforma se proporciona independientemente de macOS, no se encuentra sujeto a los comportamientos de revocación impuestos por la caché de confianza estática.

Cachés de confianza cargables

Apple proporciona determinados paquetes de software con *cachés de confianza cargables*. Estas cachés tienen la misma estructura de datos que la caché de confianza estática. Sin embargo, aunque solo hay una caché de confianza estática y su contenido siempre está bloqueado en intervalos de solo lectura después de que se complete la inicialización temprana del kernel, se añaden cachés de confianza cargables al sistema en tiempo de ejecución.

Estas cachés de confianza se autentican mediante el mismo mecanismo que autentica el firmware de arranque (personalización que usa el servicio de firmas de confianza de Apple) o bien como objetos firmados globalmente (cuyas firmas no los vinculan a un servicio determinado).

Un ejemplo de una caché de confianza personalizada es la caché que se proporciona con la imagen de disco que se usa para realizar diagnósticos de campo en un Mac con chip de Apple. Esta caché de confianza está personalizada, junto con la imagen del disco, y se carga en el kernel del ordenador Mac mientras se arranca en un modo de diagnóstico. La caché de confianza permite al software de la imagen de disco ejecutarse con privilegio de plataforma.

Las actualizaciones de software de macOS incluyen un ejemplo de una caché de confianza firmada. Esta caché de confianza permite que un fragmento de código de la actualización de software (el *motor de actualización*) se ejecute con privilegio de plataforma. El motor de actualización realiza todo el trabajo para preparar la actualización de software, puesto que el sistema de host carece de la capacidad para ofrecer un rendimiento coherente entre las distintas versiones.

Seguridad del procesador de los periféricos en ordenadores Mac

Todos los sistemas informáticos modernos tienen muchos procesadores de periféricos integrados dedicados a tareas como las conexiones de red, los gráficos, la gestión de la energía, etc. A menudo, estos procesadores de periféricos tienen un solo propósito y son mucho menos potentes que la CPU principal. Los periféricos integrados que no implementan suficiente seguridad se convierten en un objetivo sencillo para los atacantes, a través del cual pueden infectar permanentemente el sistema operativo. Con un firmware del procesador de periféricos infectado, un atacante puede ir a por el software de la CPU principal, o bien captar datos sensibles directamente (por ejemplo, un dispositivo Ethernet podría ver el contenido de los paquetes que no están encriptados).

Siempre que es posible, Apple trabaja para reducir el número de procesadores de periféricos necesarios y para evitar diseños que requieran firmware. Pero cuando se necesitan procesadores independientes con su propio firmware, se hace todo lo posible para ayudar a garantizar que el atacante no pueda persistir en su ataque a ese procesador. Esto puede realizarse mediante la verificación del procesador de una de estas dos maneras:

- Ejecutando el procesador para que se descargue firmware verificado de la CPU principal durante el arranque.
- Haciendo que el procesador de periféricos implemente su propia cadena de arranque seguro para verificar el firmware del procesador de periféricos cada vez que el Mac arranque.

Apple trabaja con proveedores para supervisar sus implementaciones y mejorar sus diseños para incluir las propiedades deseadas, como las siguientes:

- Garantizar las fortalezas criptográficas mínimas.
- Ofrecer una revocación sólida del firmware malicioso conocido.
- Desactivar las interfaces de depuración.
- Firmar el firmware con claves criptográficas que se almacenan en módulos de seguridad de hardware (HSM) controlados por Apple.

En los últimos años, Apple ha trabajado con algunos proveedores externos para adoptar las mismas estructuras de datos "Image4", el mismo código de verificación y la misma infraestructura de firma que se usan en los chips de Apple.

Cuando el funcionamiento sin almacenamiento o el almacenamiento junto con un arranque seguro no son unas opciones viables, el diseño dicta que las actualizaciones de firmware se deben firmar criptográficamente y verificar antes de poder actualizar el almacenamiento persistente.

Rosetta 2 en un Mac con chip de Apple

Un Mac con chip de Apple puede ejecutar código compilado para el conjunto de instrucciones de x86_64 mediante un mecanismo de traducción denominado *Rosetta 2*. Se ofrecen dos tipos de traducciones: en tiempo de ejecución y antes de la ejecución.

Traducción en tiempo de ejecución

En la canalización de traducción en tiempo de ejecución (JIT), el objeto Mach de x86_64 se identifica de forma temprana en la ruta de ejecución de la imagen. Cuando se encuentran estas imágenes, el kernel transfiere el control a un stub de traducción de Rosetta especial, en lugar de a un editor de enlaces dinámicos, `dyld(1)`. A continuación, el stub de traducción traduce las páginas de x86_64 durante la ejecución de la imagen. Esta traducción se lleva a cabo completamente en el proceso. El kernel sigue verificando los hashes del código de cada página de x86_64 con la firma del código asociada al archivo binario. En el caso de que se detecte una discrepancia de hash, el kernel impone la política de corrección apropiada para ese proceso.

Traducción antes de la ejecución

En la ruta de traducción antes de la ejecución (AOT), se leen los archivos binarios de x86_64 del almacenamiento en los momentos en los que el sistema considera óptimos para la capacidad de respuesta de ese código. Los artefactos traducidos se escriben en el almacenamiento como un tipo especial de archivo de objeto Mach. Ese archivo es similar a una imagen ejecutable, pero está marcado para indicar que se trata del producto traducido de otra imagen.

En este modelo, el artefacto AOT obtiene toda su información de identidad de la imagen ejecutable x86_64 original. Para aplicar esta vinculación, una entidad del espacio del usuario con privilegios firma el artefacto de traducción mediante una clave específica del dispositivo que gestiona Secure Enclave. Esta clave solo se publica para la entidad del espacio del usuario con privilegios, que se identifica como tal mediante una autorización restringida. El directorio de código creado para el artefacto de traducción incluye el hash del directorio de código de la imagen ejecutable x86_64 original. La firma en el propio artefacto de traducción se denomina *firma complementaria*.

La canalización AOT comienza de manera similar a la canalización JIT, con el kernel que transfiere el control al tiempo de ejecución de Rosetta, en lugar de a un editor de enlaces dinámicos, `dyld(1)`. Sin embargo, en este caso el tiempo de ejecución de Rosetta envía una consulta de comunicación entre procesos (IPC) al servicio del sistema Rosetta, que pregunta si hay disponible una traducción AOT para la imagen ejecutable actual. Si la hay, el servicio Rosetta proporciona un identificador a esa traducción, que se asigna al proceso y se ejecuta. Durante la ejecución, el kernel aplica los hashes del directorio de código del artefacto de traducción, que se autentican mediante la firma radicada en la clave de firma específica del dispositivo. Los hashes del directorio de código de la imagen x86_64 original no están implicados en el proceso.

Los artefactos traducidos se almacenan en un almacén seguro de datos que no es accesible en tiempo de ejecución por ninguna entidad, salvo el servicio Rosetta. El servicio Rosetta gestiona el acceso a su caché mediante la distribución de descriptores de archivos de solo lectura entre los artefactos de traducción individuales, lo que limita el acceso a la caché de artefactos AOT. De manera intencionada, se restringe considerablemente la comunicación entre procesos de este servicio y la huella dependiente para limitar la superficie de ataque.

Si el hash del directorio de código de la imagen x86_64 original no coincide con el codificado en la firma del artefacto de traducción AOT, este resultado se considera equivalente a una firma de código no válida, y se toma la medida coercitiva correspondiente.

Si un proceso remoto consulta al kernel las autorizaciones u otras propiedades de identidad de código de un ejecutable traducido antes del tiempo de ejecución (AOT), se le devolverán las propiedades de identidad de la imagen x86_64 original.

Contenido de la caché de confianza estática

macOS 11 o posterior incluye archivos binarios Mach que contienen fragmentos de código informático de arm64 y x86_64. En un Mac con chip de Apple, un usuario puede optar por ejecutar el fragmento de x86_64 de un archivo binario del sistema mediante la canalización de Rosetta; por ejemplo, para cargar un módulo que no tenga una variante de arm64 nativa. Para respaldar esto, por normal general, la caché de confianza estática incluida con macOS contiene tres hashes de directorio de código por cada archivo de objeto Mach.

- Hash del directorio de código del fragmento de arm64
- Hash del directorio de código del fragmento de x86_64
- Hash del directorio de código de la traducción AOT del fragmento de x86_64

El procedimiento de traducción AOT de Rosetta es determinista ya que reproduce resultados idénticos para cualquier entrada dada, independientemente de cuándo o en qué dispositivo se realizó la traducción.

Durante la compilación de macOS, cada archivo de objeto Mach se ejecuta mediante la canalización de traducción AOT de Rosetta asociada con la versión de macOS compilada, y el hash del directorio de código resultante se registra en la caché de confianza. Los propios productos traducidos no se incluyen con el sistema operativo por motivos de eficiencia y se vuelven a constituir a petición cuando el usuario los solicita.

Cuando se ejecuta una imagen x86_64 en un Mac con chip de Apple, si el hash del directorio de código de esa imagen está en la caché de confianza estática, *también* se espera que el hash del directorio de código del artefacto AOT resultante esté en la caché de confianza estática. Estos productos no están firmados por la clave específica del dispositivo, ya que la autoridad de firma está radicada en la cadena de arranque seguro de Apple.

Código de x86_64 no firmado

Un Mac con chip de Apple no permite que se ejecute código de arm64 nativo a menos que haya asociada una firma válida. Esta firma puede ser tan sencilla como una firma de código ad hoc (cf. `codesign(1)`) que no contiene ninguna identidad de la mitad del secreto de un par de claves asimétricas (se trata simplemente de una medición no autenticada del archivo binario).

Para garantizar la compatibilidad con archivos binarios, se permite que se ejecute código de x86_64 traducido mediante Rosetta sin ninguna información de firma. No se transfiere ninguna identidad específica mediante el procedimiento de firma de Secure Enclave específico del dispositivo a este código, que se ejecuta exactamente con las mismas limitaciones que el código no firmado nativo que se ejecuta en un Mac basado en Intel.

Protecciones de acceso directo a memoria en los ordenadores Mac

Para obtener un rendimiento elevado en las interfaces de alta velocidad, como PCIe, FireWire, Thunderbolt y USB, los ordenadores deben admitir el acceso directo a memoria (DMA) desde los periféricos. Es decir, deben poder leer y escribir en la RAM sin que la CPU esté constantemente involucrada. Desde 2012, los ordenadores Mac han implementado un gran número de tecnologías para proteger el DMA, lo que hace que tengan el mejor conjunto de protecciones DMA de cualquier ordenador PC y el más completo.

Protecciones de acceso directo a memoria en un Mac con chip de Apple

Los sistemas en chips de Apple contienen una [unidad de gestión de memoria de entrada/salida \(IOMMU\)](#) para cada agente de DMA del sistema, incluidos los puertos PCIe y Thunderbolt. Dado que cada IOMMU tiene su propio conjunto de tablas de traducción de direcciones para traducir solicitudes de DMA, los periféricos conectados mediante PCIe o Thunderbolt solo pueden acceder a la memoria asignada explícitamente para su uso. Los periféricos no pueden acceder a memoria que pertenezca a otras partes del sistema, como el kernel o el firmware, ni a memoria asignada a otros periféricos. Si una IOMMU detecta un intento de un periférico de acceder a memoria que no ha sido asignada para el uso de ese periférico, desencadena un mensaje de pánico de kernel.

Protecciones de acceso directo a memoria para un Mac basado en Intel

En ordenadores Mac basados en Intel con tecnología Intel de virtualización para E/S dirigida (VT-d) inicializa la IOMMU, activando la reasignación de DMA y la reasignación de interrupciones en una fase muy temprana del proceso de arranque para mitigar diversas clases de vulnerabilidades de seguridad. El hardware de IOMMU de Apple inicia la operación con una política de denegación por defecto, de modo que, en el momento en que se enciende el sistema, empieza automáticamente a bloquear solicitudes de DMA de los periféricos. Las IOMMU, una vez inicializadas por el software, comienzan a permitir solicitudes de DMA de los periféricos a las regiones de memoria que han sido asignadas explícitamente para su uso.

Nota: La reasignación de interrupciones para PCIe no es necesaria en un Mac con chip de Apple, ya que cada IOMMU gestiona las interrupciones de mensajes señaladas (MSI) para sus propios periféricos.

Desde macOS 11, todos los ordenadores Mac con el chip de seguridad T2 de Apple ejecutan controladores de UEFI que facilitan el DMA en un entorno restringido del anillo 3 cuando estos controladores se enlazan con dispositivos externos. Esta propiedad ayuda a mitigar las vulnerabilidades de seguridad que pueden producirse cuando un dispositivo malicioso interactúa con un controlador de UEFI de forma imprevista en el arranque. En concreto, reduce el impacto de las vulnerabilidades en la gestión de los controladores de los búferes de DMA.

Extensiones del kernel en macOS

A partir de macOS 11, si se habilitan extensiones del kernel (kexts) de terceros, no se podrán cargar en el kernel a petición. En su lugar, se combinan en una *colección de kernel auxiliar (AuxKC)* que se carga durante el proceso de arranque. En un Mac con chip de Apple, la medición de la AuxKC se firma en el archivo LocalPolicy, mientras que en el hardware anterior, la AuxKC residía en el volumen de datos. Para volver a compilar la AuxKC se requiere la autorización del usuario y reiniciar macOS para cargar los cambios en el kernel, así como que el arranque seguro esté establecido en "Seguridad reducida".

Importante: Las kexts ya no se recomiendan para macOS. Las kexts ponen en riesgo la integridad y fiabilidad del sistema operativo, y Apple recomienda a los usuarios optar por soluciones que no requieran extender el kernel.

Extensiones del kernel en un Mac con chip de Apple

Las kexts deben activarse explícitamente en un Mac con chip de Apple, para lo que se debe mantener pulsado el botón de encendido en el arranque para acceder al Sistema operativo de recuperación auténtico (1TR), bajar al nivel de seguridad reducida y, a continuación, marcar la casilla para activar las extensiones del kernel. Esta acción también requiere introducir una contraseña de administrador para autorizar la bajada del nivel de seguridad. La combinación del modo 1TR y el requisito de la contraseña dificulta que los atacantes de software inyecten kexts en macOS partiendo desde el propio sistema operativo, lo que podrían aprovechar para obtener privilegios de kernel.

Después de que un usuario autorice la carga de las kexts, el flujo de carga de extensiones del kernel autorizadas por el usuario anterior se utiliza para autorizar la instalación de las kexts. La autorización que se usa para el flujo anterior también sirve para capturar un hash SHA384 de la lista de kexts autorizadas por el usuario (UAKL) en LocalPolicy. A continuación, el daemon de gestión del kernel (kmd) se encargará de validar solo aquellas kexts encontradas en la UAKL para su inclusión en la AuxKC.

- Si la protección de la integridad del sistema (SIP) está activada, la firma de cada kext se verifica antes de incluirla en la AuxKC.
- Si la SIP está desactivada, no se exige la firma de la kext.

Este enfoque permite flujos de seguridad permisiva, en los que desarrolladores o usuarios que no forman parte del programa para desarrolladores de Apple (Apple Developer Program) prueban kexts antes de que se firmen.

Una vez creada la AuxKC, su medición se envía a Secure Enclave para firmarse e incluirse en una estructura de datos Image4 que iBoot puede evaluar en el arranque. Como parte de la construcción de la AuxKC, también se genera un recibo de kexts. Este recibo contiene la lista de kexts incluidas realmente en la AuxKC, ya que el conjunto podría ser un subconjunto de la UAKL si se encontraran kexts prohibidas. En LocalPolicy se incluyen un hash SHA384 de la estructura de datos Image4 de la AuxKC y el recibo de kexts. El hash Image4 de la AuxKC se usa para que iBoot realice una verificación adicional en el arranque para ayudar a garantizar que no es posible arrancar un archivo Image4 anterior de la AuxKC firmado por Secure Enclave con un archivo LocalPolicy más reciente. Los subsistemas como Apple Pay utilizan el recibo de kexts para determinar si hay alguna kext cargada actualmente que pudiera interferir con la confianza de macOS. Si la hubiera, podrían desactivarse las funcionalidades de Apple Pay.

Alternativas a las kexts (macOS 10.15 o posterior)

macOS 10.15 permite a los desarrolladores extender las capacidades de macOS instalando y gestionando extensiones del sistema que se ejecutan en el espacio del usuario en lugar de hacerlo a nivel del kernel. Las extensiones del sistema, al ejecutarse en el espacio del usuario, aumentan la estabilidad y seguridad de macOS. Aunque las kexts tienen intrínsecamente acceso completo a todo el sistema operativo, a las extensiones que se ejecutan en el espacio del usuario solo se les concede los privilegios necesarios para llevar a cabo su función especificada.

Los desarrolladores pueden usar estructuras tecnológicas (como DriverKit, EndpointSecurity y NetworkExtension) para escribir controladores de interfaz humana y de USB, herramientas de seguridad de endpoint (como la prevención de pérdida de datos u otros agentes de endpoint) y herramientas de red y VPN sin tener que escribir kexts. Los agentes de seguridad de terceros solamente se deberían usar si aprovechan estas API o si tienen un plan de desarrollo sólido para hacer la transición hacia ellas y alejarse de las extensiones del kernel.

Carga de extensiones del kernel autorizadas por el usuario

Para mejorar la seguridad, se requiere el consentimiento del usuario para cargar las extensiones del kernel instaladas junto con macOS 10.13 o después de su instalación. Este proceso se conoce como *carga de extensión del kernel aprobada por el usuario*. Se requiere la autorización del administrador para aprobar una extensión del kernel. Las extensiones del kernel no requieren autorización si:

- se han instalado en un Mac con macOS 10.12 o anterior;
- sustituyen extensiones aprobadas previamente;
- se pueden cargar sin el consentimiento del usuario utilizando la herramienta de línea de comandos `spctl` disponible al arrancar un Mac desde el sistema operativo de recuperación;
- se pueden cargar con la configuración de una [solución de gestión de dispositivos móviles \(MDM\)](#).

A partir de macOS 10.13.2, los usuarios pueden usar una solución MDM para especificar una lista de extensiones del kernel que se cargan sin el consentimiento del usuario. Esta opción requiere que un Mac con macOS 10.13.2 esté inscrito en la solución MDM (mediante [Apple School Manager](#), [Apple Business Manager](#) o una inscripción en MDM realizada por el usuario).

Seguridad de las ROM opcionales en macOS

Nota: Actualmente, las ROM opcionales no son compatibles con un Mac con chip de Apple.

Seguridad de las ROM opcionales en un Mac con el chip de seguridad T2 de Apple

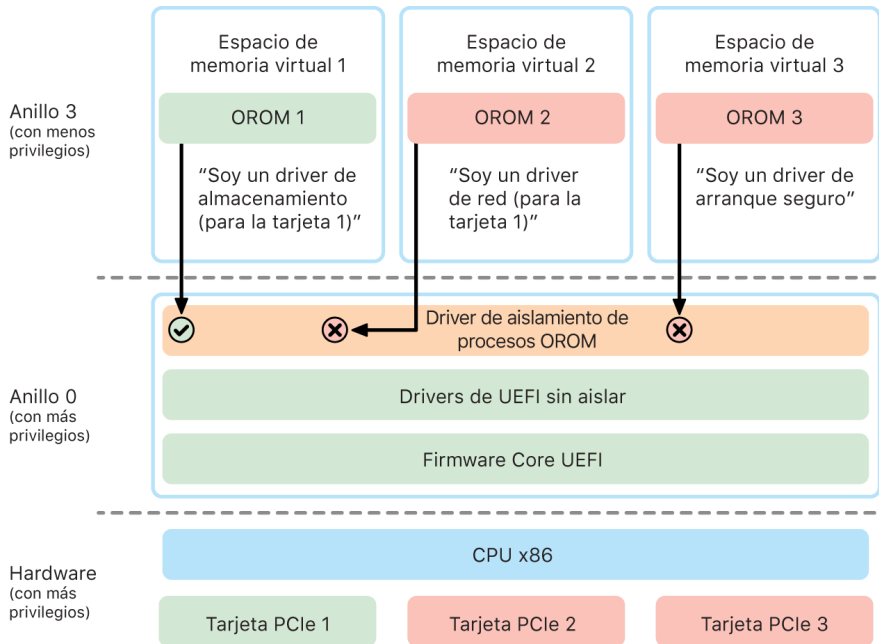
Los dispositivos Thunderbolt y PCIe tienen una "ROM opcional (OROM)" unida físicamente al dispositivo (normalmente no se trata de una verdadera ROM, sino de un chip reescribible que almacena firmware). En los sistemas basados en UEFI, ese firmware suele ser un controlador de UEFI, que lee el firmware de UEFI y lo ejecuta. El código ejecutado debe inicializar y configurar el hardware desde el que se ha obtenido, para que el resto del firmware pueda usar dicho hardware. Esta función es necesaria para que el hardware especializado de terceros se pueda cargar y funcionar durante las fases más tempranas del arranque, por ejemplo, para iniciar un proceso de arranque desde matrices RAID externas.

Sin embargo, dado que las OROM generalmente son reescribibles, si un atacante sobrescribe la OROM de un periférico legítimo, el código del atacante se ejecutará en un punto temprano del proceso de arranque y podrá manipular el entorno de ejecución y vulnerar la integridad del software cargado posteriormente. Del mismo modo, si el atacante introduce su propio dispositivo malicioso en el sistema, también podrá ejecutar código malicioso.

En macOS 10.12.3, el comportamiento de los ordenadores Mac vendidos después del 2011 se cambió para no ejecutar la OROM por defecto en el arranque del Mac, a menos que se pulsara una combinación especial de teclas. Esta combinación de teclas protegía frente a las OROM maliciosas que se podían introducir sin saberlo en la secuencia de arranque del macOS. El comportamiento por defecto de la Utilidad de contraseña de firmware también se cambió para que, cuando el usuario estableciera una contraseña de firmware, las OROM no se pudieran ejecutar, incluso si se pulsaba la combinación de teclas. Esto protegía frente a un atacante presente físicamente que introdujera una OROM maliciosa intencionadamente. Para los usuarios que todavía necesitan ejecutar OROM incluso después de establecer una contraseña de firmware, se puede configurar una opción mediante la herramienta de línea de comandos `firmwarepasswd` en macOS.

Seguridad de la zona protegida de la OROM

En macOS 10.15, el firmware de UEFI se actualizó para contener un mecanismo para aislar las OROM y quitarles privilegios. El firmware de UEFI normalmente ejecuta todo el código (incluidas las OROM) al nivel máximo de privilegios de la CPU, llamado anillo 0, y hay un único espacio de memoria virtual compartida para todo el código y los datos. El anillo 0 es el nivel de privilegios en el que se ejecuta el kernel de macOS, mientras que el nivel de privilegios más bajo, el anillo 3, es donde se ejecutan las apps. La zona protegida de la OROM elimina los privilegios de las OROM utilizando la separación de la memoria virtual al igual que lo hace el kernel y, a continuación, haciendo que las OROM se ejecuten en el anillo 3.



La zona protegida restringe significativamente las interfaces que pueden llamar las OROM (de forma similar al sistema de filtrado de llamadas de los kernels) y el tipo de dispositivo como el que una OROM puede registrarse (de forma similar a la autorización de apps). La ventaja de este diseño es que las OROM maliciosas ya no pueden escribir directamente en ninguna parte de la memoria del anillo 0. En su lugar, se restringen a una interfaz protegida muy limitada y bien definida. Esta interfaz ilimitada reduce significativamente la superficie de ataque y obliga a los atacantes a abandonar en primer lugar la zona protegida y a transferir los privilegios.

Seguridad del firmware de UEFI en un ordenador Mac basado en Intel

Un Mac basado en Intel con un chip de seguridad T2 de Apple ofrece seguridad gracias al firmware de UEFI (Intel).

Descripción general

Desde 2006, los ordenadores Mac con una CPU Intel utilizan un firmware de Intel basado en la versión 1 o la versión 2 del kit de desarrollo (EDK) de la interfaz de firmware extensible (EFI). El código basado en EDK2 se ajusta a las especificaciones de la interfaz de firmware extensible unificada (UEFI). En esta sección se hará referencia al firmware de Intel como el *firmware de UEFI*. El firmware de UEFI era el primer código que se ejecutaba en el chip de Intel.

Para un Mac basado en Intel sin el chip de seguridad T2 de Apple, la raíz de confianza del firmware de UEFI es el chip en el que se almacena el firmware. Apple firma digitalmente las actualizaciones del firmware de UEFI, que el firmware verifica antes de actualizar el almacenamiento. Para ayudar a evitar los ataques que intentan restablecer versiones anteriores, las actualizaciones siempre deben tener una versión más reciente que la versión existente. Sin embargo, un atacante con acceso físico al Mac podría usar hardware para atacar el chip de almacenamiento de firmware y actualizarlo para que albergue contenido malicioso. Del mismo modo, si existieran vulnerabilidades en un punto temprano del proceso de arranque del firmware de UEFI (antes de que se restrinja la escritura en el chip de almacenamiento) también podrían provocar una infección persistente del firmware de UEFI. Se trata de una limitación de la arquitectura del hardware común en la mayoría de ordenadores PC basados en Intel y que está presente en todos los ordenadores Mac basados en Intel sin el chip T2.

Para ayudar a impedir ataques físicos que puedan subvertir el firmware de UEFI, se ha modificado la arquitectura de los ordenadores Mac para radicar la confianza en el firmware de UEFI en el chip T2. En estos ordenadores Mac, la raíz de confianza del firmware de UEFI se encuentra específicamente en el firmware del chip T2, tal como se describe en [Proceso de arranque para un Mac basado en Intel](#).

Subcomponente del motor de gestión de Intel (ME)

El firmware del *motor de gestión de Intel (ME)* es un subcomponente que se almacena dentro del firmware de UEFI. El ME (un procesador y subsistema independiente en los chips de Intel) se usa principalmente para la protección de derechos de autor de audio y vídeo en un Mac que solo tenga gráficos basados en Intel. Para reducir la superficie de ataque de este subcomponente, un Mac basado en Intel ejecuta un firmware de ME personalizado en el que se han eliminado la mayoría de los componentes. Dado que el firmware de ME del Mac resultante es más pequeño que la compilación mínima por defecto publicada por Intel, muchos componentes que han sido objeto de ataques públicos por parte de investigadores de seguridad en el pasado ya no se encuentran presentes.

Modo de gestión del sistema (SMM)

Los procesadores Intel tienen un modo de ejecución especial que difiere del funcionamiento normal. Este se llamó *modo de gestión del sistema (SMM)* y originalmente se introdujo para gestionar operaciones urgentes, como la gestión de la energía. Sin embargo, para llevar a cabo dichas acciones, los ordenadores Mac han utilizado históricamente un microcontrolador discreto llamado *controlador de gestión del sistema (SMC)*. El SMC, que ya no es un microcontrolador independiente, se ha integrado en el chip T2.

Seguridad del sistema de watchOS

El Apple Watch usa muchas de las mismas funciones de seguridad de la plataforma basadas en hardware que iOS y iPadOS. Por ejemplo, el Apple Watch:

- Realiza arranques seguros y actualizaciones de software seguras.
- Mantiene la integridad del sistema operativo.
- Ayuda a proteger los datos, tanto en el dispositivo como al comunicarse con un iPhone enlazado o en internet.

Entre las tecnologías compatibles se encuentran aquellas indicadas en Seguridad del sistema (por ejemplo, KIP, SKP y SCIP), así como [Protección de datos](#), el llavero y tecnologías de red.

Actualizar watchOS

watchOS se puede configurar para que la actualización se instale durante la noche. Si quieres obtener más información acerca de cómo se almacena el código del Apple Watch y cómo se usa durante la actualización, consulta [Repositorios de claves](#).

Detección de muñeca

Si la detección de muñeca está activada, el dispositivo se bloquea automáticamente poco después de que el usuario se lo quite de la muñeca. Si la detección de muñeca está desactivada, el centro de control ofrece una opción para bloquear el Apple Watch. Cuando el Apple Watch se bloquea, solo se puede utilizar el servicio Apple Pay si se introduce el código en el Apple Watch. La detección de la muñeca se desactiva mediante la app Apple Watch del iPhone. Este ajuste también se puede aplicar a través de una solución de [gestión de dispositivos móviles \(MDM\)](#).

Bloqueo de activación

Cuando Buscar se activa en el iPhone, el Apple Watch enlazado puede usar el bloqueo de activación. El bloqueo de activación dificulta el uso o venta del Apple Watch en caso de pérdida o robo. El bloqueo de activación requiere el ID de Apple y la contraseña del usuario para desenlazar, borrar o reactivar el Apple Watch.

Enlace seguro con el iPhone

El Apple Watch solo se puede enlazar con un iPhone cada vez. Al desenlazar el Apple Watch, el iPhone comunica instrucciones para borrar todo el contenido y los datos del reloj.

El enlace entre el Apple Watch y el iPhone se asegura mediante un proceso de fuera de banda para intercambiar claves públicas, seguido del secreto compartido del enlace de Bluetooth de baja energía (BLE). El Apple Watch muestra un patrón animado, que captura la cámara del iPhone. Este patrón contiene un secreto codificado que se utiliza para el enlace fuera de banda de BLE 4.1. En caso necesario, el proceso estándar de Passkey Entry de BLE se utiliza como método de enlace alternativo.

Tras establecer la sesión de BLE y encriptarla mediante el protocolo de máxima seguridad disponible en Bluetooth Core Specification, el iPhone y el Apple Watch intercambian claves de una de estas maneras:

- Un proceso adaptado del [Servicio de identidad \(IDS\)](#) de Apple, tal y como se describe en la [Descripción general de la seguridad de iMessage](#).
- Un intercambio de claves mediante IKEv2/IPsec. El intercambio de claves inicial se autentica mediante la clave de la sesión Bluetooth (para escenarios de emparejamiento) o las claves de IDS (para escenarios de actualización del sistema operativo). Cada dispositivo genera un par de claves Ed25519 de 256 bits públicas y privadas y, durante el proceso de intercambio de claves inicial, se intercambian las claves públicas.

Nota: El mecanismo usado para el intercambio de claves y la encriptación varía en función de las versiones del sistema operativo del iPhone y el Apple Watch. Los dispositivos iPhone que usan iOS 13 o posterior al enlazarse con un Apple Watch con watchOS 6 o posterior solo usan IKEv2/IPsec para el intercambio de claves y la encriptación.

Una vez intercambiadas las claves:

- La clave de la sesión Bluetooth se descarta y todas las comunicaciones entre el iPhone y el Apple Watch se encriptan mediante uno de los métodos indicados anteriormente, con los enlaces encriptados de datos móviles, Bluetooth y wifi que proporcionan una capa de encriptación secundaria.
- (Solo IKEv2/IPsec) Las claves se almacenan en el llavero del sistema y se utilizan para autenticar futuras sesiones de IKEv2/IPsec entre los dispositivos. Todas las comunicaciones entre estos dispositivos están protegidas mediante la encriptación y el uso de AES-256-GCM o ChaCha20-Poly1305 (claves de 256 bits) en los dispositivos iPhone que usen iOS 15 o posterior enlazados con un Apple Watch Series 4 o posterior que use watchOS 8 o posterior.

La dirección del dispositivo Bluetooth de baja energía se cambia a intervalos de 15 minutos para reducir el riesgo de que se rastree localmente el dispositivo si alguien transmite un identificador persistente.

Para respaldar las apps que necesitan datos de transmisión en tiempo real, la encriptación se realiza mediante los métodos descritos en [Seguridad de FaceTime](#), que hacen uso del servicio de identidad (IDS) de Apple proporcionado por el iPhone enlazado o de una conexión directa a internet.

El Apple Watch implanta almacenamiento encriptado en el hardware y protección basada en clases de los archivos e ítems del llavero. Además, también se usan repositorios de claves con control de acceso para los ítems del llavero. Las [claves](#) que se utilizan para establecer comunicaciones entre el Apple Watch y el iPhone también se aseguran mediante la protección basada en clases. Para obtener más información, consulta [Repositorios de claves para Protección de datos](#).

Desbloqueo automático y el Apple Watch

Para mayor comodidad al usar varios dispositivos Apple, algunos dispositivos pueden desbloquear otros automáticamente en determinadas situaciones. El desbloqueo automático admite tres usos:

- Un iPhone puede desbloquear un Apple Watch.
- Un Apple Watch puede desbloquear un Mac.
- Un Apple Watch puede desbloquear un iPhone si se detecta que el usuario tiene la nariz y la boca tapadas.

Los tres casos se fundamentan sobre la misma base: un protocolo de estación a estación de autenticación mutua, con intercambio de claves a largo plazo en el momento de la activación de la función y claves de sesión efímeras únicas negociadas para cada solicitud. Independientemente del canal de comunicación subyacente, el túnel STS se negocia directamente entre los procesadores Secure Enclave de ambos dispositivos y todo el material criptográfico se conserva en ese dominio seguro (con la excepción de los ordenadores Mac sin Secure Enclave, que terminan el túnel STS en el kernel).

Desbloqueo

Una secuencia de desbloqueo completa puede dividirse en dos fases. En primer lugar, el dispositivo que se desbloquea (el "destino") genera un secreto de desbloqueo criptográfico y lo envía al dispositivo que realiza el desbloqueo (el "iniciador"). Después, el iniciador realiza el desbloqueo con el secreto generado previamente.

Para activar el desbloqueo automático, los dispositivos se conectan entre sí mediante una conexión BLE. A continuación, un secreto de desbloqueo de 32 bytes generado aleatoriamente por el dispositivo de destino se envía al iniciador a través del túnel STS. Durante el siguiente desbloqueo biométrico o con código, el dispositivo de destino encapsula su [clave derivada del código \(PDK\)](#) con el secreto de desbloqueo y descarta el secreto de desbloqueo de su memoria.

Para realizar el desbloqueo, los dispositivos inician una nueva conexión BLE y, a continuación, usan wifi P2P para estimar con seguridad la distancia entre sí. Si los dispositivos se encuentran dentro del alcance especificado y se cumplen las políticas de seguridad necesarias, el iniciador envía su secreto de desbloqueo al destino a través del túnel STS. A continuación, el destino genera un nuevo secreto de desbloqueo de 32 bytes que devuelve al iniciador. Si el secreto de desbloqueo actual enviado por el iniciador descifra correctamente el registro de desbloqueo, el dispositivo de destino se desbloquea y la PDK se vuelve a encapsular con un secreto de desbloqueo nuevo. Por último, el nuevo secreto de desbloqueo y la PDK se descartan de la memoria del destino.

Políticas de seguridad de desbloqueo automático del Apple Watch

Para mayor comodidad, un iPhone puede desbloquear el Apple Watch directamente después del arranque inicial, sin que sea necesario que el usuario introduzca primero el código en el propio Apple Watch. Para ello, se usa el secreto de desbloqueo aleatorio (generado durante la primera secuencia de desbloqueo tras la activación de la función) para crear un registro de custodia a largo plazo, que se almacena en el repositorio de claves del Apple Watch. El secreto del registro de custodia se almacena en el llavero del iPhone y sirve para arrancar una nueva sesión después de cada reinicio del Apple Watch.

Políticas de seguridad de desbloqueo automático del iPhone

Para el desbloqueo automático del iPhone con el Apple Watch se aplican políticas de seguridad adicionales. El Apple Watch no puede usarse en lugar de Face ID en el iPhone para otras operaciones, como para Apple Pay o para autorizaciones de apps. Cuando el Apple Watch desbloquea correctamente un iPhone enlazado, el reloj muestra una notificación y reproduce el patrón háptico asociado. Si el usuario pulsa el botón “Bloquear iPhone” de la notificación, el reloj envía al iPhone un comando de bloqueo a través de BLE. Cuando el iPhone recibe el comando de bloqueo, se bloquea y desactiva Face ID y el desbloqueo con el Apple Watch. El siguiente desbloqueo del iPhone deberá realizarse con el código del iPhone.

El correcto desbloqueo de un iPhone enlazado desde el Apple Watch (cuando está activado) requiere que se cumplan los siguientes criterios:

- El iPhone debe haberse desbloqueado con otro método al menos una vez desde que el Apple Watch asociado se haya puesto en la muñeca y desbloqueado.
- Los sensores deben poder detectar que la nariz y la boca están tapadas.
- La distancia medida debe ser de 2 a 3 metros o inferior.
- El Apple Watch no debe encontrarse en el modo Sueño.
- El Apple Watch o el iPhone deben haberse desbloqueado recientemente, o bien el Apple Watch debe haber experimentado movimiento físico, lo que indica que el usuario que lo lleva puesto está activo (por ejemplo, que no está dormido).
- El iPhone debe haberse desbloqueado al menos una vez en las últimas 6,5 horas.
- El iPhone debe encontrarse en un estado que permita realizar un desbloqueo del dispositivo con Face ID (para obtener más información, consulta [Face ID](#), [Touch ID](#), [códigos y contraseñas](#)).

Aprobar en macOS con el Apple Watch

Cuando se activa el desbloqueo automático con el Apple Watch, se puede usar el Apple Watch en lugar de o junto con Touch ID para aprobar las solicitudes de autorización y autenticación de:

- macOS y las apps de Apple que solicitan autorización
- Apps de terceros que solicitan autenticación
- Contraseñas guardadas de Safari
- Notas seguras

Uso seguro de wifi, datos móviles, iCloud y Gmail

Cuando el Apple Watch no se encuentre dentro del alcance de Bluetooth, se puede usar wifi o datos móviles en su lugar. El Apple Watch se conecta automáticamente a redes wifi a las que ya se ha unido anteriormente el iPhone enlazado y cuyas credenciales se hayan sincronizado con el Apple Watch mientras ambos dispositivos estaban dentro de su radio de alcance. Este comportamiento de conexión automática puede configurarse para cada red en la sección wifi de la app Ajustes del Apple Watch. En el caso de redes wifi a las que nunca se ha conectado ningún dispositivo, es posible acceder manualmente en la sección wifi de la app Ajustes del Apple Watch.

Si el Apple Watch y el iPhone no están en el mismo radio de alcance, el Apple Watch se conecta directamente a servidores de Gmail y iCloud para obtener el contenido de Mail, en lugar de sincronizar los datos de Mail con el iPhone enlazado a través de internet. Con cuentas de Gmail, el usuario debe autenticarse en Google en la sección Mail de la app Watch del iPhone. El identificador OAuth recibido de Google se envía al Apple Watch encriptado a través del servicio de identidad (IDS) de Apple, de forma que puede usarse para obtener el contenido de Mail. Este identificador OAuth nunca se utiliza para la conexión con el servidor de Gmail desde el iPhone enlazado.

Generación de números aleatorios

Los generadores pseudoaleatorios de números criptográficos (CPRNG) son un componente fundamental para un software seguro. Para ello, Apple proporciona un CPRNG de software de confianza que se ejecuta en los kernels de iOS, iPadOS, macOS, tvOS y watchOS. Se encarga de recopilar la entropía en formato nativo del sistema y proporcionar números aleatorios seguros a los consumidores, tanto en el kernel como en el espacio del usuario.

Fuentes de entropía

El CPRNG del kernel recibe semillas de software de varias fuentes de entropía durante el arranque y a lo largo de la vida útil del dispositivo. Entre ellas se incluyen (dependiendo de la disponibilidad):

- el generador de números aleatorios verdaderos del hardware de Secure Enclave;
- jitter basado en los tiempos recopilado durante el arranque;
- entropía recopilada de las interrupciones del hardware;
- un archivo de semilla de software que se usa para que la entropía no cambie de un arranque a otro;
- instrucciones aleatorias de Intel, como RDSEED y RDRAND (solo en un Mac basado en Intel).

El CPRNG del kernel

El CPRNG del kernel es un diseño derivado de Fortuna cuyo objetivo es conseguir un nivel de seguridad de 256 bits. Proporciona números aleatorios de alta calidad a los consumidores del espacio del usuario usando las siguientes API:

- la llamada al sistema `getentropy(2)`;
- el dispositivo aleatorio `(/dev/random)`.

El CPRNG del kernel acepta entropía proporcionada por el usuario a través de escrituras en el dispositivo aleatorio.

Dispositivo de investigación de seguridad de Apple

El dispositivo de investigación de seguridad de Apple es un iPhone especialmente configurado para permitir a los investigadores de seguridad llevar a cabo investigaciones en iOS sin tener que anular o desactivar las funciones de seguridad de la plataforma del iPhone. Con este dispositivo, un investigador puede realizar una carga lateral de contenido que ejecuta permisos equivalentes a la plataforma y, así, llevar a cabo una investigación sobre una plataforma que se asemeja a la de los dispositivos de producción.

Para ayudar a garantizar que los dispositivos de usuario no se vean afectados por la política de ejecución del dispositivo de investigación de seguridad, los cambios en la política se implementan en una variante de iBoot y en la colección de kernel de arranque, que no arrancan en hardware de usuario. La instancia de iBoot de investigación comprueba si hay un nuevo estado de configuración y entra en un bucle de kernel panic si se ejecuta en un hardware no configurado para investigación.

El subsistema cryptex permite a un investigador cargar una [caché de confianza](#) personalizada y una imagen de disco que contiene el contenido correspondiente. Se ha implementado una serie de medidas detalladas de defensa diseñadas para garantizar que este subsistema no permite la ejecución en dispositivos del usuario:

- launchd no carga la lista de propiedades launchd de cryptexd si detecta un dispositivo normal del usuario.
- cryptexd se anula si detecta un dispositivo normal del usuario.
- AppleImage4 no vende el [nonce](#) usado para verificar un cryptex de investigación en un dispositivo normal del usuario.
- El servidor de firmas rechaza personalizar una imagen de disco de cryptex para un dispositivo que no se encuentre en una lista autorizada explícita.

Para respetar la privacidad del investigador de seguridad, solo se envían a Apple las mediciones (por ejemplo, los hashes) de los ejecutables o de la caché del kernel y los identificadores de dispositivos de investigación de seguridad durante la personalización. Apple no recibe el contenido del cryptex que se carga en el dispositivo.

A fin de evitar que un tercero malicioso intente enmascarar un dispositivo de investigación como un dispositivo de usuario para engañar a un objetivo para que lo use a diario, el dispositivo de investigación de seguridad presenta las siguientes diferencias:

- El dispositivo de investigación de seguridad solo arranca mientras se carga. Para ello, puede utilizarse un cable Lightning o un cargador Qi compatible. Si el dispositivo no está cargando durante el arranque, entrará en el modo de recuperación. Si el usuario empieza a cargar el dispositivo y lo reinicia, arrancará con normalidad. Una vez que cargue el XNU, ya no será necesario que el dispositivo esté cargándose para seguir funcionando.
- El texto *Dispositivo de investigación de seguridad* se muestra debajo del logotipo de Apple durante el arranque de iBoot.
- El kernel XNU arranca en modo traza.
- El dispositivo tiene grabado un mensaje en el lateral: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125."

Las siguientes son medidas adicionales que están implementadas en el software que aparece después del arranque:

- El texto *Dispositivo de investigación de seguridad* se muestra durante la configuración del dispositivo.
- El texto *Dispositivo de investigación de seguridad* se muestra en la pantalla bloqueada y en la app Ajustes.

El dispositivo de investigación de seguridad ofrece a los investigadores las siguientes funciones que un dispositivo de usuario no proporciona. Los investigadores pueden:

- Realizar una carga lateral de código ejecutable en el dispositivo con autorizaciones arbitrarias en el mismo nivel de permiso que los componentes del sistema operativo Apple.
- Inicializar los servicios al arrancar.
- Utilizar contenido persistente entre reinicios.
- Usar `research.com.apple.license-to-operate` para permitir que un proceso depure cualquier otro proceso del sistema, incluidos los procesos del sistema.

El espacio de nombres `research.` solo es respetado por la variante RESEARCH de la extensión del kernel `AppleMobileFileIntegrity`; cualquier proceso con esta autorización se termina en un dispositivo del cliente durante la validación de la firma.

- Personalizar y restaurar la caché de un kernel personalizado.

Encriptación y Protección de datos

Descripción general de la encriptación y Protección de datos

La cadena de arranque seguro, la seguridad del sistema y las funciones de seguridad de las apps ayudan a verificar que, en un dispositivo, solo se puedan ejecutar apps y código que sean de confianza. Los dispositivos Apple disponen de otras funciones de encriptación para proteger los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad están en peligro (por ejemplo, si se pierde un dispositivo o si se ejecuta código que no sea de confianza). Todas estas funciones benefician tanto a los usuarios como a los administradores de TI, puesto que la información personal y corporativa está protegida y se proporcionan métodos para un borrado remoto, inmediato y completo, en caso de robo o pérdida del dispositivo.

Los dispositivos iOS y iPadOS usan una metodología de encriptación de archivos llamada *Protección de datos*, mientras que los datos de los ordenadores Mac basados en Intel se protegen con una tecnología de encriptación del volumen llamada *FileVault*. Un Mac con chip de Apple utiliza un modelo híbrido que admite Protección de datos, con dos advertencias: La clase de nivel de protección más bajo (D) no se admite, y el nivel por defecto (clase C) usa una clave de volumen que actúa igual que FileVault en un Mac basado en Intel. En todos los casos, las jerarquías de gestión de claves están radicadas de manera similar en el chip de Secure Enclave, y un motor AES dedicado permite encriptar a velocidad de línea y garantizar que nunca sea necesario proporcionar las claves de encriptación de larga duración al sistema operativo o la CPU del kernel (donde podrían estar en riesgo) (un Mac basado en Intel con un chip T1 o que no tenga Secure Enclave no utilizará el chip dedicado para proteger sus claves de encriptación de FileVault).

Además de usar Protección de datos y FileVault para ayudar a evitar el acceso no autorizado a los datos, Apple usa los *kernels de los sistemas operativos* para aplicar medidas de protección y seguridad. El kernel utiliza controles de acceso para aislar apps en una zona protegida (lo que restringe los datos a los que puede acceder una app) y un mecanismo llamado [almacén seguro de datos](#) (que en lugar de restringir las llamadas que puede hacer una app, restringe el acceso a los datos de una app desde las demás apps que lo soliciten).

Códigos y contraseñas

Para proteger los datos de los usuarios de ataques malintencionados, Apple usa códigos en iOS y iPadOS, y contraseñas en macOS. Cuanto mayor sea la longitud de un código o contraseña, más seguros serán (y más fácil será desalentar los ataques de fuerza bruta). A fin de desalentar aún más los ataques, Apple aplica tiempos de demora (para iOS y iPadOS) y un número limitado de intentos de introducción de contraseña (para Mac).

En iOS y iPadOS, al configurar el código o la contraseña de un dispositivo, el usuario activa la [protección de datos](#) automáticamente. La protección de datos también se activa en otros dispositivos que tienen un sistema en un chip (SoC) de Apple (como el Mac con chip de Apple, el Apple TV y el Apple Watch). En macOS, Apple usa el programa *FileVault* de encriptación del volumen integrada.

Cómo aumentan la seguridad los códigos y contraseñas seguros

iOS y iPadOS admiten códigos alfanuméricos de cuatro dígitos, de seis dígitos y de longitud arbitraria. Además de desbloquear el dispositivo, un código o contraseña proporciona entropía para determinadas claves de encriptación. Esto significa que un atacante que se haya hecho con un dispositivo no podrá acceder a los datos de clases de protección específicas si no dispone del código.

Dado que el código o contraseña está [vinculado](#) al UID del dispositivo, sería necesario realizar ataques de fuerza bruta en el dispositivo atacado. Para que cada intento sea más lento, se utiliza un recuento de iteraciones elevado. El recuento de iteraciones se calibra de manera que un intento tarde alrededor de 80 milisegundos. Así, se tardarían más de cinco años y medio en intentar todas las combinaciones de un código alfanumérico de seis caracteres con letras minúsculas y números.

Cuanto más seguro sea el código del usuario, más segura será la clave de encriptación. Asimismo, mediante el uso de Face ID y Touch ID, el usuario puede establecer y usar fácilmente un código mucho más seguro. Un código más seguro aumenta la entropía real que protege las claves de encriptación utilizadas para Protección de datos, sin que se vea perjudicada la experiencia del usuario al desbloquear un dispositivo muchas veces a lo largo del día.

Si se introduce una contraseña larga compuesta únicamente por números, se mostrará un teclado numérico en la pantalla bloqueada en lugar de un teclado completo. Es posible que sea más fácil introducir un código numérico largo que un código alfanumérico corto, aunque ambos proporcionen un nivel de seguridad parecido.

Los usuarios pueden especificar un código alfanumérico de mayor longitud seleccionando "Código alfanumérico personalizado" en las "Opciones de código" de Ajustes > "Touch ID y código" o "Face ID y código".

Cómo los tiempos de demora cada vez mayores desalientan los ataques de fuerza bruta (iOS, iPadOS)

En iOS y iPadOS, a fin de desalentar aún más los posibles ataques de fuerza bruta, existen tiempos de demora cada vez mayores tras la introducción de un código no válido en la pantalla bloqueada, tal y como se muestra en la siguiente tabla.

Intentos	Demora aplicada
1-4	Ninguna
5	1 minuto
6	5 minutos
7-8	15 minutos
9	1 hora

Si la opción "Borrar datos" está activada (en Ajustes > Touch ID y código), tras 10 intentos incorrectos consecutivos de introducir el código, todo el contenido y los ajustes se eliminarán del almacenamiento. Para este límite no se cuentan los intentos consecutivos al introducir el mismo código incorrecto. Este ajuste, que se puede definir con un umbral inferior, también está disponible como política de administración a través de una solución de [gestión de dispositivos móviles \(MDM\)](#) compatible con esta función y mediante Microsoft Exchange ActiveSync.

En dispositivos con Secure Enclave, las demoras se aplican mediante Secure Enclave. Si el dispositivo se reinicia durante un tiempo de demora, la demora aún se aplica, con el temporizador empezando de nuevo para el periodo actual.

Cómo los tiempos de demora cada vez mayores desalientan los ataques de fuerza bruta (macOS)

Para ayudar a evitar los ataques de fuerza bruta, cuando el Mac arranca, no se permiten más de 10 intentos de introducción de la contraseña en la ventana de inicio de sesión o el uso de la modalidad de disco de destino. Además, se imponen tiempos de demora cada vez mayores tras un número determinado de intentos erróneos consecutivos. Las demoras se aplican mediante Secure Enclave. Si el Mac se reinicia durante un tiempo de demora, la demora aún se aplica, con el temporizador empezando de nuevo para el periodo actual.

En la tabla siguiente se muestran demoras entre intentos de introducción de contraseña en un Mac con chip de Apple y un Mac con un chip T2.

Intentos	Demora aplicada
5	1 minuto
6	5 minutos
7	15 minutos
8	15 minutos
9	1 hora
10	Desactivado

Para ayudar a evitar que el software malicioso provoque pérdidas de datos permanentes al intentar atacar la contraseña del usuario, estos límites no se aplican una vez que el usuario ha iniciado sesión correctamente en el Mac, pero se vuelven a imponer después del reinicio. Si se agotan los 10 intentos, hay 10 intentos más disponibles después de arrancar en el sistema operativo de recuperación. Y si esos también se agotan, entonces hay 10 intentos adicionales disponibles para cada mecanismo de recuperación de FileVault (recuperación de iCloud, clave de recuperación de FileVault y clave a nivel de la institución). En total habrá 30 intentos adicionales. Una vez agotados esos intentos adicionales, Secure Enclave ya no procesa ninguna solicitud para descifrar el volumen o verificar la contraseña y los datos de la unidad no se pueden recuperar.

Para ayudar a proteger los datos en un entorno empresarial, el departamento de TI debería definir y aplicar las políticas de configuración de FileVault con una solución MDM. Las organizaciones tienen varias opciones para gestionar volúmenes encriptados, incluidas claves de recuperación a nivel de la institución, claves de recuperación personales (que de forma opcional se pueden almacenar con la solución MDM para su custodia) o una combinación de ambas. La rotación de las claves también se puede establecer como política en la solución MDM.

En un Mac con el chip de seguridad T2 de Apple, la contraseña cumple una función similar, excepto que la clave generada se usa para la encriptación de FileVault en lugar de para Protección de datos. macOS también ofrece opciones de recuperación de contraseña adicionales:

- Recuperación de iCloud
- Recuperación de FileVault
- Clave a nivel de la institución de FileVault

Protección de datos

Descripción general de Protección de datos

Apple usa una tecnología llamada [Protección de datos](#) para proteger los datos almacenados en el almacenamiento flash de los dispositivos que tienen un SoC de Apple, como los iPhone, iPad, Apple Watch, Apple TV y los ordenadores Mac con chip de Apple. Con la protección de datos, un dispositivo puede responder ante eventos habituales, como las llamadas de teléfono entrantes y, al mismo tiempo, proporcionar un alto nivel de encriptación para los datos de usuario. Algunas apps del sistema (como Mensajes, Mail, Calendario, Contactos y Fotos) y los valores de los datos de la app Salud utilizan Protección de datos por defecto. Las apps de terceros reciben esta protección automáticamente.

Implementación

Protección de datos se implementa mediante la creación y gestión de una jerarquía de claves, y se basa en las tecnologías de encriptación de hardware integradas en los dispositivos Apple. Protección de datos se controla por archivo, asignando cada archivo a una clase. La accesibilidad se determina en función de si las claves de clase se han desbloqueado o no. [El sistema de archivos de Apple \(APFS\)](#) permite al sistema de archivos subdividir las claves aún más por área (donde distintas partes de un archivo pueden tener claves diferentes).

Cada vez que se crea un archivo en el volumen de datos, Protección de datos crea una nueva clave de 256 bits (la *clave "por archivo"*) y se la proporciona al motor AES de hardware, que utiliza la clave para encriptar el archivo como si se hubiese escrito en el almacenamiento flash. En dispositivos A14, A15 y de la familia M1, la encriptación usa AES-256 en modo XTS, donde la clave "por archivo" de 256 bits pasa por una función de derivación de clave (publicación especial del NIST 800-108) para obtener una clave de ajuste de 256 bits y una clave de cifrado de 256 bits. Las generaciones de hardware A9 a A13, S5, S6 y S7 utilizan AES-128 en modo XTS, donde la clave "por archivo" de 256 bits se divide para proporcionar una clave de ajuste de 128 bits y una clave de cifrado de 128 bits.

En un Mac con chip de Apple, Protección de datos establece por defecto la clase C (consulta [Clases de Protección de datos](#)) pero utiliza una clave de volumen en lugar de una clave por archivo o por área, de forma que vuelve a crear el modelo de seguridad de FileVault para los datos del usuario. Los usuarios aún deben aceptar el uso de FileVault para recibir la máxima protección al vincular la jerarquía de claves de encriptación con su contraseña. Los desarrolladores también pueden optar por una clase de protección superior que utiliza una clave por archivo o por área.

Protección de datos en dispositivos Apple

En dispositivos Apple con Protección de datos, cada archivo está protegido con una clave por archivo (o por área) única. La clave, encapsulada con el algoritmo de encapsulación de claves NIST AED, se encapsula adicionalmente con una clave de clase determinada, en función de cómo vaya a accederse al archivo. La [clave por archivo](#) encapsulada se almacena en los metadatos del archivo.

Los dispositivos que usen el formato APFS podrán clonar archivos (copias de coste cero que usan la tecnología de copia al escribir). Si se clona un archivo, cada mitad del clon obtiene una clave nueva para aceptar las escrituras entrantes, de modo que los datos nuevos se escriben en el medio con una clave nueva. Con el tiempo, el archivo podría contar con varias áreas (o fragmentos), cada una de ellas con una clave distinta asignada. Sin embargo, la misma clave de clase guarda todas las áreas que componen un archivo.

Al abrir un archivo, sus metadatos se descifran con la [clave del sistema de archivos](#) y de este modo se muestra la clave por archivo encapsulada y una anotación sobre la clase que lo protege. La clave por archivo (o por área) se desencapsula con la clave de clase y, después, se proporciona al motor AES de hardware, que descifra el archivo cuando se lee en el almacenamiento flash. La gestión de claves de archivos encapsulados se realiza en Secure Enclave; la clave de archivo nunca se expone directamente al procesador de aplicaciones. En el arranque, Secure Enclave negocia una clave efímera con el motor AES. Cuando Secure Enclave desencapsula las claves de un archivo, estas vuelven a encapsularse con la clave efímera y se envían de vuelta al procesador de aplicaciones.

Los metadatos de todos los archivos del sistema de archivos del volumen de datos se encriptan con una clave de volumen aleatoria, que se crea la primera vez que se instala el sistema operativo o cuando un usuario borra el contenido del dispositivo. Mediante una clave de encapsulación de claves que solo Secure Enclave conoce, se encripta y encapsula la clave para el almacenamiento a largo plazo. La clave de encapsulación de claves cambia cada vez que un usuario borra su dispositivo. En el SoC A9 y posteriores, Secure Enclave depende de la entropía, respaldada por sistemas antirreproducción, para lograr la capacidad de borrado y proteger su clave de encapsulación de claves, entre otros componentes. Para obtener más información, consulta [Almacenamiento seguro no volátil](#).

Al igual que las claves por archivo o por área, la clave de los metadatos del volumen de datos nunca se expone directamente al procesador de aplicaciones, sino que Secure Enclave proporciona una versión efímera por arranque. Cuando se guarda, la clave encriptada del sistema de archivos se vuelve a encapsular con una “clave borrable” almacenada en el [almacenamiento borrable](#) o con una clave de encapsulación de contenido protegida por el mecanismo de antirreproducción de Secure Enclave. Esta clave no se ha diseñado para que los datos sean más confidenciales, sino para que se pueda borrar rápidamente por petición (los usuarios pueden hacerlo con la opción “Borrar contenidos y ajustes”, y los administradores o usuarios, mediante un comando de borrado remoto desde una solución de [gestión de dispositivos móviles \(MDM\)](#), desde Microsoft Exchange ActiveSync o desde iCloud). Al borrar la clave de esta manera, se deja de poder acceder a todos los archivos encriptados.

Puede que el contenido de un archivo esté encriptado con una o más claves por archivo (o por área) encapsuladas con una clave de clase y almacenadas en los metadatos del archivo, que a su vez está encriptado con la clave del sistema de archivos. La clave de clase se protege con el UID de hardware y, en el caso de algunas clases, con el código del usuario. Esta jerarquía proporciona flexibilidad y rendimiento. Por ejemplo, para cambiar la clase de un archivo, basta con volver a encapsular su clave por archivo y un cambio del código volverá a encapsular la clave de clase.

Clases de Protección de datos

Cuando se crea un archivo nuevo en dispositivos compatibles con Protección de datos, la app que lo crea le asigna una clase. Cada clase utiliza una política diferente para determinar si se puede acceder a los datos. En las secciones siguientes, se describen las clases y políticas básicas. Los ordenadores Mac con chips de Apple no son compatibles con "Clase D: Sin protección" y se establece un límite de seguridad en torno al inicio y el cierre de sesión (no el bloqueo o desbloqueo, como en los iPhone, iPad y iPod touch).

Clase	Tipo de protección
Clase A: Protección completa	NSFileProtectionComplete
Clase B: Protegido a menos que se abra	NSFileProtectionCompleteUnlessOpen
Clase C: Protegido hasta la primera autenticación del usuario <i>Nota:</i> macOS usa una clave de volumen para recrear las características de protección de FileVault.	NSFileProtectionCompleteUntilFirstUserAuthentication
Clase D: Sin protección <i>Nota:</i> No compatible en macOS.	NSFileProtectionNone

Protección completa

NSFileProtectionComplete: La clave de clase está protegida con una clave creada a partir del código o la contraseña de usuario y el UID del dispositivo. Poco después de que el usuario bloquee un dispositivo (10 segundos, si el ajuste "Solicitar contraseña" está en "De inmediato"), la clave de clase descryptada se descarta, de manera que se deja de poder acceder a todos los datos de esta clase hasta que el usuario vuelva a introducir el código o desbloquee (inicie sesión en) el dispositivo con Face ID o Touch ID.

En macOS, poco después de que el último usuario haya cerrado la sesión, la clave de clase descryptada se descarta, de manera que se deja de poder acceder a todos los datos de esta clase hasta que un usuario vuelva a introducir el código o inicie sesión en el dispositivo con Touch ID.

Protegido a menos que se abra

NSFileProtectionCompleteUnlessOpen: Puede que sea necesario escribir algunos archivos mientras el dispositivo está bloqueado o la sesión del usuario no esté iniciada. Por ejemplo, al descargar un archivo adjunto de correo en segundo plano. Este comportamiento se consigue con la [criptografía de curva elíptica asimétrica \(ECDH sobre Curve25519\)](#). Las [claves por archivo](#) normales están protegidas con una clave obtenida según el protocolo criptográfico de Diffie-Hellman de un paso, tal como se describe en la publicación NIST SP 800-56A.

La clave pública efímera del protocolo se almacena junto a la clave por archivo encapsulada. KDF es el acrónimo de "Concatenation Key Derivation Function" (función de derivación de claves de concatenación) (Alternativa aprobada 1), tal como se describe en la sección 5.8.1 de la publicación NIST SP 800-56A. AlgorithmID se omite; PartyUInfo y PartyVInfo son las claves públicas efímera y estática, respectivamente; y SHA256 se utiliza como función hash. En cuanto se cierra el archivo, la clave por archivo se borra de la memoria. Para volver a abrir el archivo, se vuelve a crear el secreto compartido con la clave privada de la clase "Protegido a menos que se abra" y la clave pública efímera del archivo, que se utilizan para desencapsular la clave por archivo, que después se utiliza para descifrar el archivo.

En macOS, la parte privada de `NSFileProtectionCompleteUnlessOpen` es accesible siempre que alguno de los usuarios del sistema haya iniciado sesión o se haya autenticado.

Protegido hasta la primera autenticación del usuario

NSFileProtectionCompleteUntilFirstUserAuthentication: Esta clase se comporta del mismo modo que "Protección completa", con la diferencia de que la clave de clase descifrada no se elimina de la memoria al bloquear el dispositivo o cuando se cierra la sesión del usuario. La protección de esta clase tiene propiedades similares a la encriptación de volumen completo de escritorio y protege los datos frente a ataques que impliquen un reinicio. Esta es la clase por defecto para todos los datos de apps de terceros que no tengan una clase de [Protección de datos](#) asignada por otra vía.

En macOS, esta clase utiliza una clave de volumen que es accesible siempre que el volumen esté montado, y actúa igual que FileVault.

Sin protección

NSFileProtectionNone: Esta clave de clase solo está protegida con el UID y se guarda en el [almacenamiento borrable](#). Dado que todas las claves necesarias para descifrar los archivos de esta clase se almacenan en el dispositivo, la encriptación solo añade la ventaja del borrado remoto rápido. Aunque un archivo no tenga asignada una clase de Protección de datos, se almacena en formato encriptado (igual que todos los datos de un dispositivo iOS y iPadOS).

Esto no se admite en macOS.

Nota: En macOS, en el caso de los volúmenes que no correspondan a un sistema operativo que se haya arrancado, todas las clases de protección de datos serán accesibles siempre que el volumen esté montado. La clase de protección de datos por defecto es `NSFileProtectionCompleteUntilFirstUserAuthentication`. La funcionalidad de claves por área está disponible tanto en Rosetta 2 como en las apps nativas.

Repositorios de claves para Protección de datos

Las claves de las clases de [Protección de datos](#) de archivo y de llavero se recopilan y gestionan en repositorios de claves en iOS, iPadOS, watchOS y tvOS. Estos sistemas operativos usan los siguientes repositorios de claves: usuario, dispositivo, copia de seguridad, custodia y copia de seguridad en iCloud.

Repositorio de claves del usuario

El repositorio de claves del usuario es el lugar en el que se almacenan las claves de clase encapsuladas que se utilizan durante el funcionamiento normal del dispositivo. Por ejemplo, cuando se introduce un código, se carga *NSFileProtectionComplete* del repositorio de claves del usuario y se desencapsula. Se trata de un archivo de lista de propiedades binario (.plist) almacenado en la clase No Protection.

En el caso de los dispositivos con SoC anteriores al A9, el contenido del archivo .plist está encriptado con una clave que se guarda en el [almacenamiento borrrable](#). Con el fin de proporcionar mayor seguridad a los repositorios de claves, esta clave se borra y se vuelve a generar cada vez que un usuario cambia el código.

En el caso de los dispositivos con el SoC A9 y posteriores, el archivo .plist contiene una clave que indica que el repositorio de claves está guardado en un depósito protegido por el [nonce](#) antirreproducción controlado por Secure Enclave.

Secure Enclave gestiona el repositorio de claves del usuario y admite consultas relativas al estado de bloqueo del dispositivo. Solo indica que el dispositivo está desbloqueado si se puede acceder a todas las claves de clase del repositorio de claves del usuario y si se han desencapsulado correctamente.

Repositorio de claves del dispositivo

El repositorio de claves del dispositivo sirve para almacenar las claves de clase encapsuladas que se utilizan en operaciones en las que se requieren datos específicos del dispositivo. Los dispositivos iPadOS configurados para un uso compartido necesitan, en algunas ocasiones, acceso a las credenciales antes de que los usuarios hayan iniciado sesión. Así, será necesario un repositorio de claves que no esté protegido con un código del usuario.

iOS y iPadOS no son compatibles con la separación criptográfica del contenido del sistema de archivos por usuario, lo cual significa que el sistema utilizará claves de clase del repositorio de claves del dispositivo para encapsular [claves por archivo](#). Sin embargo, el llavero utiliza claves de clase del repositorio de claves del usuario para proteger los ítems del llavero del usuario. En los dispositivos iOS y iPadOS configurados para que solo los utilice un usuario (configuración por defecto), el repositorio de claves del dispositivo y el del usuario son el mismo, y están protegidos mediante el código del usuario.

Repositorio de claves de copia de seguridad

El repositorio de claves de copia de seguridad se crea cuando iTunes (en macOS 10.14 o anterior) o el Finder (en macOS 10.15 o posterior) realiza una copia de seguridad encriptada y la almacena en el ordenador donde se efectúa la copia de seguridad del dispositivo. Se crea un repositorio de claves nuevo con un conjunto de claves nuevo, y los datos de la copia de seguridad se vuelven a encriptar en estas claves nuevas. Tal como se ha explicado anteriormente, los ítems del llavero no migrables permanecen encapsulados con la clave derivada del UID, lo cual hace posible su restauración en el dispositivo en el que se haya realizado la copia de seguridad original, pero impide el acceso a ellos en un dispositivo diferente.

El repositorio de claves (protegido por la contraseña definida) se ejecuta a través de 10 millones de iteraciones de la función de derivación de claves PBKDF2. A pesar de la gran cantidad de iteraciones, no existen vínculos a un dispositivo específico y, por lo tanto, los ataques de fuerza bruta realizados en paralelo en muchos ordenadores tendrían lugar, teóricamente, en el repositorio de claves de copia de seguridad. Esta amenaza se puede mitigar con una contraseña suficientemente segura.

Si un usuario opta por no encriptar la copia de seguridad, los archivos de copia de seguridad no se encriptan, sea cual sea su clase de Protección de datos, pero el llavero sigue estando protegido con una clave derivada del UID. Por este motivo, los ítems del llavero solo migran a un dispositivo nuevo cuando se establece una contraseña de copia de seguridad.

Repositorio de claves de custodia

El repositorio de claves de custodia se usa para la sincronización con el Finder (macOS 10.15 o posterior) o con iTunes (macOS 10.14 o anterior) a través de USB y [gestión de dispositivos móviles \(MDM\)](#). Este repositorio de claves permite que iTunes o el Finder realice una copia de seguridad y la sincronización sin necesidad de que el usuario introduzca un código, y permite que una solución MDM borre de forma remota el código de un usuario. Se almacena en el ordenador utilizado para la sincronización con iTunes o el Finder, o bien en la solución MDM que gestiona de forma remota el dispositivo.

El repositorio de claves de custodia mejora la experiencia del usuario durante la sincronización del dispositivo, que podría requerir el acceso a todas las clases de datos. La primera vez que un dispositivo bloqueado con contraseña se conecta a iTunes o el Finder, el usuario tiene que introducir un código. Entonces, el dispositivo crea un repositorio de claves de custodia que contiene las mismas claves de clase que se utilizan en el dispositivo, y se protege con una clave recién creada. El repositorio de claves de custodia y la clave que lo protege se reparten entre el dispositivo y el host o servidor; los datos almacenados en el dispositivo residen en la clase "Protegido hasta la primera autenticación del usuario". Por eso, es necesario introducir el código del dispositivo antes de que el usuario realice la primera copia de seguridad con iTunes o el Finder después de un reinicio.

En caso de una actualización de software remota (OTA), el usuario tiene que introducir su código al inicio del proceso. Este se utiliza para crear de forma segura un identificador de desbloqueo de un solo uso, que desbloquea el repositorio de claves del usuario después de la actualización. Este identificador no se puede generar si no se introduce el código de usuario; todos los identificadores generados anteriormente quedan invalidados si se cambia el código de usuario.

Los identificadores de desbloqueo de un solo uso sirven para instalar con o sin supervisión una actualización de software. Se encriptan con una clave derivada del valor actual de un contador monótono de Secure Enclave, el UUID del repositorio de claves y el UID de Secure Enclave.

En el SoC A9 (y posteriores), el identificador de desbloqueo puntual ya no se basa en contadores ni en el almacenamiento borrrable. En su lugar, se protege mediante el nonce antirreproducción controlado por Secure Enclave.

El identificador de desbloqueo de un solo uso para actualizaciones de software con supervisión caduca a los 20 minutos. En iOS 13 y iPadOS 13.1 o posterior, el identificador se guarda en un depósito protegido por Secure Enclave. Antes de iOS 13, este identificador se exportaba desde Secure Enclave y se escribía en el [almacenamiento borrrable](#) o se protegía mediante el mecanismo de antirreproducción de Secure Enclave. Un temporizador de políticas incrementaba el contador si el dispositivo no se había reiniciado en 20 minutos.

Las actualizaciones de software automáticas se realizan cuando el sistema detecta que hay disponible una actualización y se dan una de las siguientes situaciones:

- Las actualizaciones automáticas están configuradas en iOS 12 o versiones posteriores.
- El usuario selecciona "Instalar más tarde" cuando recibe la notificación de la actualización.

Después de que el usuario introduzca su código, se genera un identificador de desbloqueo puntual que puede ser válido en Secure Enclave hasta 8 horas. Si la actualización aún no se ha producido, este identificador de desbloqueo puntual se destruye cada vez que se bloquea el dispositivo y se vuelve a crear con cada desbloqueo posterior. Cada desbloqueo reinicia el límite de 8 horas. Transcurridas 8 horas, un temporizador de política invalida el identificador de desbloqueo puntual.

Repositorio de claves de copia de seguridad de iCloud

El repositorio de claves de copia de seguridad de iCloud es similar al de claves de copia de seguridad. Todas las claves de clase de este repositorio son asimétricas (utilizan Curve25519, como la clase de Protección de datos "Protegido a menos que se abra"). También se utiliza un repositorio de claves asimétrico para la copia de seguridad en el aspecto de recuperación de llaveros del llavero de iCloud.

Protección de claves en modos de arranque alternativos

Protección de datos está diseñada para proporcionar acceso a los datos de usuario solo después de una autenticación correcta y únicamente al usuario autorizado. Las clases de protección de datos están diseñadas para respaldar diversos escenarios de uso, como la capacidad de leer y escribir algunos datos incluso si un dispositivo está bloqueado (pero después del primer desbloqueo). Durante los modos de arranque alternativos, se toman medidas adicionales para proteger el acceso a los datos de usuario, como las que se emplean en el modo de actualización del firmware del dispositivo (DFU), el modo de recuperación, Diagnóstico Apple o incluso durante las actualizaciones de software. Estas funciones se basan en una combinación de características de hardware y software y se han ido ampliando a medida que los chips diseñados por Apple han evolucionado.

Función	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Recuperación todas las clases de Protección de datos	✓	✓	✓	✓	✓
Arranques alternativos del modo DFU, recuperación y las actualizaciones de software: Protección de datos de clase A, B y C		✓	✓	✓	✓

El motor AES de Secure Enclave está equipado con [bits semilla de software](#) que se pueden bloquear. Cuando se crean claves a partir del UID, estos bits semilla se incluyen en la función de derivación de claves para crear jerarquías de claves adicionales. Cómo varía el bit semilla usado según el sistema en un chip:

- A partir de los SoC A10 y S3 de Apple, un bit semilla se dedica a distinguir claves protegidas por el código del usuario. El bit semilla se establece para claves que requieren el código del usuario (incluidas las claves de clase A, clase B y clase C de Protección de datos) y se borra para claves que no requieren el código del usuario (como la clave de metadatos del sistema de archivos y las claves de clase D).
- En iOS 13 o posterior y iPadOS 13.1 o posterior, en dispositivos con un SoC A10 o posterior, se deja de poder acceder a todos los datos del usuario encriptados cuando los dispositivos se arrancan en el modo de diagnóstico. Esto se consigue introduciendo un bit semilla adicional cuyos ajustes rigen la capacidad de acceder a la clave de contenido, que a su vez es necesaria para acceder a los metadatos (y, por tanto, al contenido de todos los archivos) del volumen de datos encriptado con Protección de datos. Esta protección incluye los archivos protegidos en todas las clases (A, B, C y D), no solo aquellas que requieren el código del usuario.

- En los SoC A12, la [ROM de arranque](#) de Secure Enclave bloquea el bit semilla del código si el procesador de aplicaciones entra en [modo de actualización del firmware del dispositivo \(DFU\)](#) o [modo de recuperación](#). Cuando el bit semilla del código se bloquea, no se permite ninguna operación de cambio. Esto está así diseñado para impedir el acceso a los datos protegidos con el código del usuario.

Restaurar un dispositivo una vez que entra en modo DFU hace que vuelva a un estado anterior en buenas condiciones con la certeza de que solo hay código firmado por Apple no modificado. Se puede entrar en modo DFU manualmente.

Consulta los siguientes artículos de soporte técnico de Apple sobre cómo hacer que un dispositivo entre en modo DFU.

Dispositivo	Artículo
iPhone, iPad, iPod touch	Si has olvidado el código del iPhone
Apple TV	Si ves un símbolo de advertencia en el Apple TV
Mac con chip de Apple	Restablecer o restaurar un Mac con chip de Apple

Protección de los datos de usuario ante un ataque

Los atacantes que intentan extraer datos de usuario suelen probar diversas técnicas: extraer los datos encriptados en otro soporte para un ataque de fuerza bruta, manipular la versión del sistema operativo o bien cambiar o reducir la política de seguridad del dispositivo para facilitar el ataque. Para atacar los datos de un dispositivo, suele ser necesario comunicarse con el dispositivo mediante interfaces físicas, como un cable Lightning o USB. Los dispositivos Apple incluyen funciones para impedir tales ataques.

Los dispositivos Apple son compatibles con una tecnología llamada *Protección de clave sellada (SKP)* que está diseñada para garantizar que el material criptográfico no esté disponible fuera del dispositivo, o que se usa si se manipula la versión del sistema operativo o los ajustes de seguridad sin la correspondiente autorización del usuario. Secure Enclave *no* proporciona esta función; en su lugar, se basa en registros de hardware que existen en un nivel inferior para ofrecer un nivel adicional de protección a las claves necesarias para descifrar los datos de usuario independiente de Secure Enclave.

Nota: SKP solo está disponible en dispositivos con SoC diseñados por Apple.

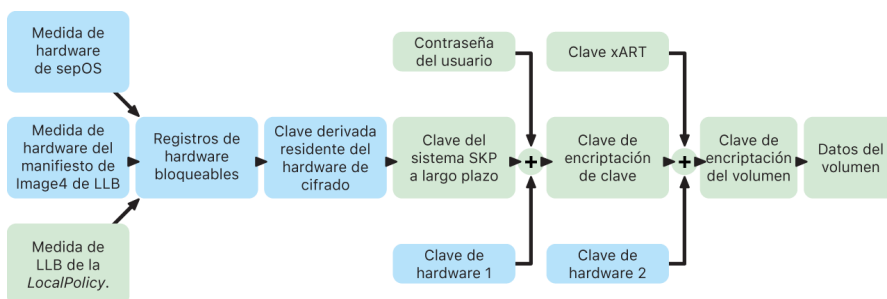
Función	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, familia M1
Protección de clave sellada	✓	✓	✓	✓	✓

El iPhone y el iPad también se pueden configurar para activar las conexiones de datos solo en aquellas condiciones en las que sea más probable que se indique que el dispositivo permanece bajo el control físico del propietario autorizado.

Protección de clave sellada (SKP)

En dispositivos Apple compatibles con Protección de datos, la clave de encriptación de claves (KEK) se protege (o se sella) mediante mediciones del software del sistema y se vincula al UID disponible únicamente desde Secure Enclave. En un Mac con chip de Apple, la protección de la clave de encriptación de claves (KEK) se refuerza con la incorporación de información sobre la política de seguridad en el sistema, puesto que macOS admite cambios críticos en la política de seguridad (por ejemplo, desactivar el arranque seguro o la SIP) que no se permiten en otras plataformas. En un Mac con chip de Apple, esta protección abarca claves de FileVault, ya que FileVault se implementa mediante Protección de datos (clase C).

La clave resultante de intrincar la contraseña del usuario, la clave SKP a largo plazo y la clave 1 de hardware (el UID de Secure Enclave) se denomina *clave derivada de la contraseña*. Esta clave se usa para proteger el repositorio de claves del usuario (en todas las plataformas compatibles) y la KEK (solo en macOS), y activar a continuación el desbloqueo biométrico o el desbloqueo automático con otros dispositivos, como el Apple Watch.



El monitor de arranque de Secure Enclave captura la medición del sistema operativo de Secure Enclave que se carga. Cuando la ROM de arranque del procesador de aplicaciones mide el manifiesto Image4 conectado al LLB, ese manifiesto contiene una medición del resto del firmware enlazado por el sistema que también se carga. El archivo LocalPolicy contiene las configuraciones de seguridad principales de macOS que se cargan. LocalPolicy también incluye el campo `ns1h`, que es un hash del manifiesto Image4 de macOS. El manifiesto Image4 de macOS contiene tanto mediciones del firmware enlazado con macOS y objetos de arranque troncales de macOS, como la colección de kernel de arranque o el hash raíz del volumen del sistema firmado (SSV).

Si un atacante es capaz de cambiar inesperadamente cualquiera de los componentes anteriormente medidos del firmware, el software o la configuración de seguridad, se modifican las mediciones almacenadas en los registros de hardware. La modificación de las mediciones hace que la *clave raíz de la medición del sistema (SMRK)* derivada del criptohardware derive en un valor diferente, lo que rompe el sello de la jerarquía de claves. Esto provoca que la *clave de dispositivo de la medición del sistema (SMDK)* sea inaccesible, lo que a su vez hace que la KEK y, por lo tanto, los datos sean igualmente inaccesibles.

Sin embargo, cuando el sistema no es atacado, debe tener en cuenta las actualizaciones de software legítimas que modifican las mediciones del firmware y el campo `nsih` de LocalPolicy para apuntar a nuevas mediciones de macOS. En otros sistemas que intentan incorporar mediciones del firmware, pero que no tienen una fuente de verdad conocida, el usuario está obligado a desactivar la seguridad, actualizar el firmware y, a continuación, volver a activarla para que se pueda capturar una nueva línea base de medición. Esto aumenta significativamente el riesgo de que un atacante pueda alterar el firmware durante una actualización de software. El hecho de que los manifiestos Image4 contengan todas las mediciones necesarias ayuda al sistema. El hardware que descripta el SMDK con el SMRK cuando las mediciones coinciden durante un arranque normal también puede encriptar el SMDK a un futuro SMRK propuesto. Al especificar las mediciones que se esperan después de una actualización de software, el hardware puede encriptar un SMDK que sea accesible en un sistema operativo actual y que lo siga siendo en un sistema operativo futuro. Del mismo modo, cuando un cliente cambia legítimamente sus ajustes de seguridad en LocalPolicy, el SMDK debe encriptarse en el futuro SMRK en función de la medición de LocalPolicy que el LLB calcula en el siguiente arranque.

Activar las conexiones de datos de forma segura en iOS y iPadOS

En dispositivos iOS o iPadOS, si no se ha establecido recientemente ninguna conexión de datos, los usuarios deben utilizar Face ID, Touch ID o un código para activar las conexiones de datos mediante una interfaz Smart Connector, USB o Lightning. Esto limita la superficie de ataque de dispositivos conectados físicamente, como cargadores malintencionados, al tiempo que permite usar otros accesorios dentro de unos periodos de tiempo razonables. Si ha transcurrido más de una hora desde que se ha bloqueado el dispositivo iOS o iPadOS, o desde que se ha desconectado un accesorio USB, el dispositivo no permitirá nuevas conexiones hasta que se desbloquee. Durante dicho periodo de una hora, solo se permitirán las conexiones de datos procedentes de accesorios que se hayan conectado al dispositivo con anterioridad mientras estaba desbloqueado. Los dispositivos recuerdan estos accesorios durante un plazo de 30 días desde su última conexión. Hasta que el dispositivo vuelva a desbloquearse, todo intento por parte de un accesorio desconocido de abrir una conexión de datos durante este periodo desactivará las conexiones de los datos procedentes de accesorios por Lightning, USB y Smart Connector. Este periodo de una hora:

- Ayuda a garantizar que los usuarios habituales de conexiones a un Mac o PC, a accesorios o por cable a CarPlay no tengan que introducir sus códigos cada vez que conectan su dispositivo.
- Es necesario porque el ecosistema de accesorios no ofrece una manera fiable desde el punto de vista de la encriptación de identificar los accesorios antes de establecer una conexión de datos.

Además, si han transcurrido más de tres días desde que se ha establecido una conexión de datos con un accesorio, el dispositivo paralizará las nuevas conexiones de datos inmediatamente después de bloquearse. De este modo, se mejora la protección para los usuarios que no suelen utilizar esos accesorios. Las conexiones de datos a través de Lightning, USB y Smart Connector también se desactivan cuando el dispositivo está en un estado que requiere introducir un código para reactivar la autenticación biométrica.

El usuario puede elegir reactivar las conexiones de datos siempre activadas en Ajustes (la configuración de algunos dispositivos de asistencia hace esto de forma automática).

La función del sistema de archivos de Apple

El sistema de archivos de Apple (APFS) es un sistema de archivos protegido por derechos de propiedad intelectual que se ha diseñado teniendo en cuenta la encriptación. El sistema de archivos de Apple (APFS) funciona en todas las plataformas de Apple (iPhone, iPad, iPod touch, Mac, Apple TV y Apple Watch). Optimizado para el almacenamiento flash/SSD, cuenta con una encriptación de alta seguridad, metadatos de copia al escribir, uso compartido de espacio, clonado de archivos y directorios, instantáneas, reajuste rápido del tamaño del directorio, primitivas atómicas de seguridad-guardado y mejoras en los fundamentos del sistema de archivos, así como un diseño único de copia al escribir que utiliza la fusión de E/S para ofrecer el máximo rendimiento al tiempo que se garantiza la fiabilidad de los datos.

Uso compartido del espacio

El sistema APFS asigna el espacio de almacenamiento por petición. Cuando un único contenedor APFS tiene varios volúmenes, el espacio libre del contenedor se comparte y se puede asignar a cualquiera de los volúmenes individuales, según sea necesario. Cada volumen solo usa parte de todo el contenedor, por lo que el espacio disponible es el tamaño total del contenedor menos el espacio usado en todos los volúmenes del contenedor.

Varios volúmenes

En macOS 10.15 o posterior, un contenedor APFS usado para arrancar el Mac debe contener al menos cinco volúmenes, los tres primeros de los cuales están ocultos al usuario:

- *Volumen de prearranque*: Este volumen no está encriptado y contiene los datos necesarios para arrancar cada volumen del sistema del contenedor.
- *Volumen VM*: Este volumen no está encriptado y macOS lo usa para almacenar archivos de intercambio encriptados.
- *Volumen de recuperación*: Este volumen no está encriptado y debe estar disponible sin desbloquear un volumen del sistema para poder arrancar en el sistema operativo de recuperación.
- *Volumen del sistema*: Contiene lo siguiente:
 - todos los archivos necesarios para arrancar el Mac;
 - todas las apps instaladas de forma nativa por macOS (las apps que solían almacenarse en la carpeta /Aplicaciones están ahora en /Sistema/Aplicaciones).

Nota: Por defecto, ningún proceso puede escribir en el volumen del sistema, ni siquiera los procesos del sistema Apple.

- *Volumen de datos*: Contiene datos sujetos a cambios, como los siguientes:
 - Todos los datos guardados en la carpeta del usuario (fotos, música, vídeos, documentos, etc.).
 - Apps que ha instalado el usuario, incluyendo aplicaciones de AppleScript y Automator.
 - Daemons y estructuras personalizados instalados por el usuario, la organización o apps de terceros.
 - Otras ubicaciones que son propiedad del usuario y en las que puede escribir, como /Aplicaciones, /Biblioteca, /Usuarios, /Volúmenes, /usr/local, /private, /var y /tmp.

Se crea un volumen de datos por cada volumen del sistema adicional. El volumen de prearranque, el volumen VM y el volumen de recuperación son volúmenes compartidos y no duplicados.

En macOS 11 o posterior, el volumen del sistema se encuentra en una instantánea. El sistema operativo arranca a partir de una instantánea del volumen del sistema, no solo de una instalación de solo lectura del volumen del sistema mutable.

En iOS y iPadOS, el almacenamiento está dividido por lo menos en dos volúmenes APFS:

- Volumen del sistema
- Volumen de datos

Protección de datos de llavero

Muchas apps necesitan gestionar contraseñas y otros datos de pequeño tamaño pero sensibles, como las claves o los identificadores de inicio de sesión. El **llavero** constituye un sistema seguro para almacenar estos ítems. Los diversos sistemas operativos de Apple utilizan distintos mecanismos para aplicar las garantías asociadas con las diferentes clases de protección del llavero. En macOS (incluidos los Mac con chip de Apple), Protección de datos no se usa directamente para aplicar estas garantías.

Descripción general

Los ítems del llavero se encriptan con dos claves AES-256-GCM distintas, una clave de tabla (metadatos) y una clave por fila (clave secreta). Los metadatos del llavero (todos los atributos excepto `kSecValue`) se encriptan con la clave de metadatos para agilizar las búsquedas, mientras que el valor secreto (`kSecValueData`) se encripta con la clave secreta. La clave de metadatos está protegida por Secure Enclave, pero se almacena en caché en el procesador de aplicaciones para permitir realizar consultas rápidas del llavero. La clave secreta siempre requiere un ciclo de ida y vuelta por Secure Enclave.

El llavero se implementa como una base de datos SQLite, almacenada en el sistema de archivos. Solo hay una base de datos y el daemon `securityd` determina a qué ítems del llavero puede acceder cada proceso o app. Las API de acceso a llaveros generan llamadas al daemon, que envía una consulta a las autorizaciones “`Keychain-access-groups`”, “`application-identifier`” y “`application-group`” de la app. En lugar de limitar el acceso a un solo proceso, los grupos de acceso permiten que los ítems del llavero se compartan entre apps.

Los ítems del llavero solo se pueden compartir entre las apps de un mismo desarrollador. Para compartir los ítems del llavero, las apps de terceros utilizan grupos de acceso con un prefijo asignado a través del programa para desarrolladores de Apple (Apple Developer Program) en sus grupos de aplicaciones. El requisito de prefijo y la exclusividad del grupo de aplicaciones se aplican mediante la firma de código, [perfiles de datos](#) y el [programa para desarrolladores de Apple](#).

Los datos de llavero se protegen con una estructura de clases similar a la utilizada en la protección de datos de archivo. Estas clases tienen comportamientos equivalentes a las clases de protección de datos de archivo, pero utilizan claves y funciones distintas.

Disponibilidad	Protección de datos de archivo	Protección de datos de llavero
Cuando está desbloqueado	<code>NSFileProtectionComplete</code>	<code>kSecAttrAccessibleWhenUnlocked</code>
Cuando está bloqueado	<code>NSFileProtectionCompleteUnlessOpen</code>	N/A
Tras el primer desbloqueo	<code>NSFileProtectionCompleteUntilFirstUserAuthentication</code>	<code>kSecAttrAccessibleAfterFirstUnlock</code>
Siempre	<code>NSFileProtectionNone</code>	<code>kSecAttrAccessibleAlways</code>
Código activado	N/A	<code>kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly</code>

Las apps que usan servicios de actualización en segundo plano pueden usar *kSecAttrAccessibleAfterFirstUnlock* para los ítems del llavero a los que es necesario acceder durante este tipo de actualizaciones.

La clase *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* muestra el mismo comportamiento que *kSecAttrAccessibleWhenUnlocked*, pero solo está disponible cuando el dispositivo está configurado con un código. Estas clases solo existen en el [repositorio de claves](#) del sistema y:

- No se sincronizan con el llavero de iCloud.
- No se realiza una copia de seguridad de ellas.
- No se incluyen en repositorios de claves de custodia.

Si se elimina o restablece el código, se descartan las claves de clase y los ítems dejan de ser útiles.

Otras clases de llavero tienen un equivalente a "Solo este dispositivo", que siempre está bajo la protección del UID cuando se copia del dispositivo durante la copia de seguridad, de modo que deja de ser útil si se restaura en un dispositivo diferente. Apple ha equilibrado la seguridad y la usabilidad cuidadosamente mediante la selección de clases de llavero que dependen del tipo de información que se esté protegiendo y de cuándo la necesite iOS y iPadOS. Por ejemplo, un certificado VPN debe estar disponible en todo momento para que el dispositivo esté continuamente conectado, pero se clasifica como "no migrable" para evitar que se pueda trasladar a otro dispositivo.

Protecciones de clase de los datos de llavero

Las protecciones de clase indicadas a continuación se aplican para ítems del llavero.

Ítem	Accesible
Contraseñas wifi	Tras el primer desbloqueo
Cuentas de Mail	Tras el primer desbloqueo
Cuentas de Microsoft Exchange ActiveSync	Tras el primer desbloqueo
Contraseñas VPN	Tras el primer desbloqueo
LDAP, CalDAV y CardDAV	Tras el primer desbloqueo
Identificadores de cuentas de redes sociales	Tras el primer desbloqueo
Claves de encriptación de anuncios de Handoff	Tras el primer desbloqueo
Identificador de iCloud	Tras el primer desbloqueo
Claves de iMessage	Tras el primer desbloqueo
Contraseña de "Compartir en casa"	Cuando está desbloqueado
Contraseñas de Safari	Cuando está desbloqueado
Marcadores de Safari	Cuando está desbloqueado
Copia de seguridad del Finder/iTunes	Cuando está desbloqueado, no migrable
Claves privadas instaladas por un perfil de configuración	Cuando está desbloqueado, no migrable

Ítem	Accesible
Certificados VPN	Siempre, no migrable
Claves de Bluetooth®	Siempre, no migrable
Identificador del servicio de notificaciones push (APNs) de Apple	Siempre, no migrable
Clave privada y certificados de iCloud	Siempre, no migrable
PIN de la SIM	Siempre, no migrable
Certificados instalados por un perfil de configuración	Siempre
Identificador de Buscar	Siempre
Buzón de voz	Siempre

Control de acceso a llaveros

Los llaveros pueden utilizar listas de control de acceso (ACL) para establecer políticas de accesibilidad y requisitos de autenticación. Los ítems pueden establecer condiciones que requieran la presencia del usuario al especificar que no se puede acceder a ellos a menos que se lleve a cabo una autenticación con Face ID, Touch ID o que se introduzca el código o la contraseña del dispositivo. El acceso a los ítems también se puede limitar si se especifica que el registro de Face ID o Touch ID no ha cambiado desde que se ha añadido el ítem. Esta limitación ayuda a impedir que un atacante añada sus propias huellas para acceder a un ítem del llavero. Las ACL se evalúan en Secure Enclave y solo se comparten con el kernel si se cumplen las restricciones especificadas.

Arquitectura de llavero en macOS

macOS también proporciona acceso al llavero para guardar de manera sencilla y segura nombres y contraseñas, incluyendo las identidades digitales, las claves de encriptación y las notas seguras. Se puede acceder abriendo la app Acceso a Llaveros en /Aplicaciones/Utilidades. El uso de un llavero elimina la necesidad de introducir (o incluso de recordar) las credenciales de cada recurso. Para cada usuario del Mac se crea un llavero inicial por defecto, aunque los usuarios pueden crear otros llaveros con fines específicos.

Además de los llaveros del usuario, macOS utiliza una serie de llaveros a nivel de sistema que mantienen los componentes de autenticación que no son específicos del usuario, como las credenciales de red y las identidades de la infraestructura de clave pública (PKI). Uno de estos llaveros, "Raíz del sistema", es inmutable y almacena los certificados raíz de la autoridad de certificación de PKI de internet para facilitar tareas comunes como la banca en línea y el comercio electrónico. De manera similar, el usuario puede implementar certificados de la autoridad de certificación suministrados internamente a ordenadores Mac gestionados para ayudar a validar sitios y servicios internos.

FileVault

Encriptación de volúmenes con FileVault en macOS

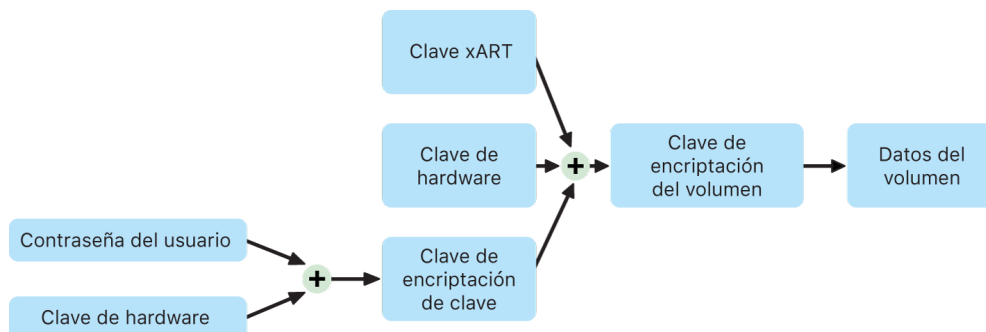
Los ordenadores Mac ofrecen FileVault, una función de encriptación integrada para proteger todos los datos en reposo. FileVault usa el algoritmo de encriptación de datos AES-XTS para proteger volúmenes completos en dispositivos de almacenamiento internos y extraíbles.

En un Mac con chip de Apple, FileVault se implanta con la clase C de Protección de datos con una clave de volumen. En un Mac con el chip de seguridad T2 de Apple y en un Mac con chip de Apple, los dispositivos de almacenamiento interno encriptados conectados directamente a Secure Enclave aprovechan las funciones de seguridad del hardware del chip y las del motor AES. Una vez que un usuario activa FileVault en un Mac, debe introducir sus credenciales durante el proceso de arranque.

Almacenamiento interno con FileVault activado

Sin unas credenciales de inicio de sesión válidas o una clave de recuperación criptográfica, los volúmenes APFS internos permanecen encriptados y están protegidos del acceso no autorizado, incluso si se retira el dispositivo de almacenamiento físico y se conecta a otro ordenador. En macOS 10.15, esto incluye tanto al volumen del sistema como al de datos. A partir de macOS 11, el volumen del sistema está protegido mediante la función de volumen del sistema firmado (SSV), pero el volumen de datos sigue protegido mediante encriptación. La encriptación del volumen interno en un Mac con chip de Apple y en aquellos con el chip T2 se implementa mediante la creación y gestión de una jerarquía de claves, y se basa en las tecnologías de encriptación de hardware integradas en el chip. Esta jerarquía de claves está diseñada para conseguir cuatro objetivos simultáneamente:

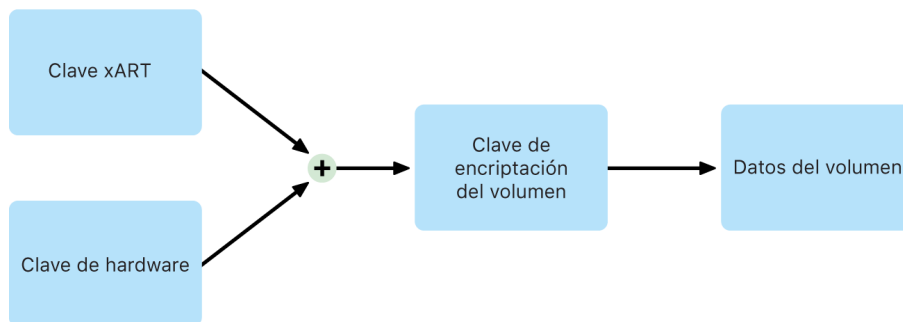
- Requerir la contraseña del usuario para la desencriptación.
- Proteger el sistema frente a un ataque de fuerza bruta llevado a cabo directamente sobre un soporte de almacenamiento extraído del Mac.
- Proporcionar un método rápido y seguro para borrar contenido mediante la eliminación del material de encriptación necesario.
- Permitir a los usuarios cambiar su contraseña (y, a su vez, las claves criptográficas utilizadas para proteger sus archivos) sin tener que volver a encriptar todo el volumen.



En un Mac con chip de Apple y en aquellos con el chip T2, toda la gestión de claves de FileVault se realiza en Secure Enclave; las claves de encriptación nunca se exponen directamente a la CPU de Intel. Todos los volúmenes APFS se crean con una clave de encriptación de volumen por defecto. El contenido del volumen y los metadatos se encriptan con esta clave de encriptación de volumen, que está encapsulada con la clave de clase. Con FileVault activado, la clave de clase se protege con una combinación de la contraseña del usuario y el UID de hardware.

Almacenamiento interno con FileVault desactivado

Si FileVault no está activado en un Mac con chip de Apple o en un Mac con el chip de seguridad T2 durante el proceso inicial del asistente de configuración, el volumen se seguirá encriptando, pero la clave de encriptación de volumen solo está protegida por el UID de hardware en Secure Enclave.



Si se activa FileVault posteriormente —un proceso inmediato, puesto que los datos ya se han encriptado— un mecanismo de antirreproducción ayuda a evitar que la clave antigua (basada únicamente en el UID de hardware) se utilice para desencriptar el volumen. A continuación, el volumen se protege con una combinación de la contraseña del usuario y el UID de hardware, como se ha descrito anteriormente.

Eliminar volúmenes FileVault

Al eliminar un volumen, Secure Enclave elimina su clave de encriptación de volumen de forma segura. Esto ayuda a evitar que en un futuro se pueda acceder con esta clave, incluso para Secure Enclave. Además, todas las claves de encriptación de volumen están encapsuladas con una clave de contenido. La clave de contenido no se ha diseñado para que los datos sean más confidenciales, sino para permitir que los datos se borren de forma rápida y segura porque, sin ella, la desencriptación es imposible.

En un Mac con chip de Apple y en aquellos con el chip T2, la clave de contenido se borrará mediante la tecnología compatible de [Secure Enclave](#), como, por ejemplo, comandos de MDM remotos. Al borrar la clave de contenido de esta manera, se deja de poder acceder a los volúmenes encriptados.

Dispositivos de almacenamiento extraíbles

La encriptación de los dispositivos de almacenamiento extraíbles no utiliza las funciones de seguridad de Secure Enclave y su encriptación se realiza del mismo modo que en un Mac basado en Intel sin el chip T2.

Gestión de FileVault en macOS

En macOS, las organizaciones pueden gestionar FileVault mediante el identificador seguro o el identificador Bootstrap.

Usar el identificador seguro

El sistema de archivos de Apple (APFS) en macOS 10.13 o posterior cambia el modo en que FileVault genera las claves de encriptación. En los volúmenes CoreStorage de las versiones anteriores de macOS, las claves utilizadas en el proceso de encriptación de FileVault se creaban cuando un usuario o una organización activaba FileVault en un Mac. En los volúmenes APFS de macOS, las claves se generan durante la creación del usuario, al definir la primera contraseña del usuario o durante la primera vez que un usuario inicia sesión en el Mac. Esta implementación de las claves de encriptación, cuándo se generan y cómo se almacenan forman parte de una característica llamada *identificador seguro*. En concreto, un identificador seguro es una versión encapsulada de una clave de encriptación de claves (KEK) protegida por la contraseña de un usuario.

Al implementar FileVault en APFS, el usuario puede seguir haciendo lo siguiente:

- Usar los procesos y las herramientas existentes, como una clave de recuperación personal (PRK) que se puede almacenar con una solución de [gestión de dispositivos móviles \(MDM\)](#) para custodia.
- Crear y usar una clave de recuperación a nivel de la institución (IRK).
- Posponer la activación de FileVault hasta que un usuario inicia o cierra sesión del Mac.

En macOS 11, al definir la primera contraseña del primer usuario en el Mac, se le asigna un identificador seguro a ese usuario. En algunos flujos de trabajo, es posible que este no sea el comportamiento deseado, ya que, anteriormente, la asignación del primer identificador seguro hubiera requerido el inicio de sesión con la cuenta de usuario. Para impedir que esto ocurra, añade `;DisabledTags;SecureToken` al atributo `AuthenticationAuthority` del usuario creado mediante programación antes de definir la contraseña del usuario, tal y como se muestra a continuación:

```
sudo dscl . append /Users/<user name> AuthenticationAuthority  
";DisabledTags;SecureToken"
```

Usar el identificador Bootstrap

macOS 10.15 ha introducido una nueva función, el *identificador Bootstrap*, para ayudar a otorgar un identificador seguro a las cuentas móviles y a la cuenta opcional de administrador del dispositivo creada por el programa de inscripción (“administrador gestionado”). En macOS 11, un identificador Bootstrap puede otorgar un identificador seguro a cualquier usuario que inicie sesión en un ordenador Mac, incluidas cuentas de usuarios locales. El uso de la función de identificador Bootstrap de macOS 10.15 o posterior requiere:

- Inscripción del Mac en una solución MDM utilizando Apple School Manager o Apple Business Manager, que hace que el Mac esté supervisado.
- Compatibilidad con el proveedor de MDM.

En macOS 10.15.4 o versiones posteriores, se genera un identificador Bootstrap que estará custodiado por la solución MDM al iniciar sesión por primera vez por parte de cualquier usuario que tenga activado el identificador seguro, si la solución MDM es compatible con esta función. En caso necesario, también se podría generar un identificador Bootstrap que estuviera custodiado por la solución MDM mediante la herramienta de línea de comandos `profiles`.

En macOS 11, también puede usarse un identificador Bootstrap para algo más que otorgar un identificador seguro a cuentas de usuario. En un Mac con chip de Apple, si hay un identificador Bootstrap disponible, puede usarse para autorizar la instalación tanto de extensiones del kernel como de actualizaciones de software si los ordenadores están gestionados con MDM.

Cómo protege Apple los datos personales de los usuarios

Protección del acceso de las apps a los datos de usuario

Además de encriptar los datos que contienen, los dispositivos Apple evitan que las apps puedan acceder sin permiso a la información personal del usuario mediante distintas técnicas, entre ellas la del [almacén seguro de datos](#). En Ajustes (iOS y iPadOS) o en Preferencias del Sistema (macOS), los usuarios pueden ver cuáles son las apps a las que han otorgado acceso a determinada información, así como conceder o revocar permisos para cualquier acceso futuro. El acceso se aplica a lo siguiente:

- *iOS, iPadOS y macOS*: Calendarios, Cámara, Contactos, Micrófono, Fotos, Recordatorios, reconocimiento de voz.
- *iOS y iPadOS*: Bluetooth, Casa, contenido multimedia, apps de contenido multimedia y Apple Music y Actividad física.
- *iOS y watchOS*: Salud.
- *macOS*: Monitorización de entrada (por ejemplo, las pulsaciones del teclado), indicaciones, grabación de pantalla (por ejemplo, vídeo y capturas de una pantalla estática), Preferencias del Sistema.

En iOS 13.4 y iPadOS 13.4 o versiones posteriores, todas las apps de terceros tienen todos sus datos protegidos automáticamente en un [almacén seguro de datos](#). Este almacén seguro de datos es una medida de protección frente a accesos no autorizados a los datos, incluso los procedentes de procesos que no están aislados en zonas protegidas. Las clases adicionales en iOS 15 o posterior incluyen "Red local", "Interacciones cercanas", "Datos de uso y de los sensores de la app Investigación" y el modo de concentración.

Si el usuario inicia sesión en iCloud, las apps en iOS y iPadOS tienen permiso de acceso a iCloud Drive por defecto. Los usuarios pueden controlar el acceso de cada app en Ajustes, en iCloud. Además, iOS y iPadOS proporcionan restricciones diseñadas para impedir la transferencia de datos entre las apps y las cuentas que se hayan instalado mediante una solución de [gestión de dispositivos móviles \(MDM\)](#) y aquellas que haya instalado el usuario.

Protección del acceso a los datos de salud del usuario

HealthKit proporciona un repositorio donde se centralizan los datos de salud y actividad física del iPhone y el Apple Watch. Asimismo, HealthKit funciona directamente con dispositivos de salud y de actividad física, como los monitores de frecuencia cardiaca Bluetooth LE y el coprocesador de movimiento integrado en muchos dispositivos iOS. Toda interacción de HealthKit con las apps de salud y forma física, las instituciones sanitarias y los dispositivos de salud y forma física requiere el permiso del usuario. Estos datos se almacenan en la clase de [Protección de datos](#) "Protegido a menos que se abra". 10 minutos después de que el dispositivo se bloquee, los datos dejan de ser accesibles. La siguiente vez que el usuario introduzca su código o use Face ID o Touch ID para desbloquear el dispositivo, los datos volverán a estar accesibles.

Recopilación y almacenamiento de los datos de salud y de actividad física

HealthKit también recopila y almacena datos de gestión, como permisos de acceso para apps, nombres de dispositivos conectados a HealthKit e información de programación utilizada para abrir apps cuando hay datos nuevos disponibles. Estos datos se almacenan en la clase de Protección de datos "Protegido hasta la primera autenticación del usuario". Los archivos de registro temporales almacenan los datos de salud que se generan cuando el dispositivo está bloqueado, por ejemplo, cuando el usuario está haciendo ejercicio. Estos datos se almacenan en la clase de Protección de datos "Protegido a menos que se abra". Cuando el dispositivo está desbloqueado, los archivos de registro temporales se importan en las bases de datos de salud principales y, una vez que ha terminado la importación, se eliminan.

Los datos de salud se pueden guardar en iCloud. La encriptación de punto a punto de los datos de Salud requiere iOS 12 (o versiones posteriores) y la autenticación de doble factor. De lo contrario, los datos del usuario permanecerán encriptados durante la transmisión y el almacenamiento, pero no se encriptarán de punto a punto. Una vez que el usuario activa la autenticación de doble factor y actualiza el sistema a iOS 12 o a una versión posterior, los datos de salud del usuario se migran a la encriptación de punto a punto.

Si el usuario hace una copia de seguridad de su dispositivo con el Finder (en macOS 10.15 o posterior) o con iTunes (macOS 10.14 o anterior), los datos de salud solo se almacenarán en el caso de que la copia de seguridad esté encriptada.

Historiales clínicos

Los usuarios pueden iniciar sesión en sistemas sanitarios admitidos desde la app Salud para obtener una copia de su historial clínico. Cuando un usuario se conecta a un sistema sanitario, se autentica con credenciales de cliente OAuth 2. Después de conectarse, los datos del historial clínico se descargan directamente desde la institución sanitaria a través de una conexión protegida con TLS 1.3. Una vez descargado, el historial clínico se guarda con seguridad junto con otros datos de salud.

Integridad de los datos de la app Salud

En la base de datos, también se almacenan metadatos para hacer un seguimiento de la procedencia de cada registro de datos. Estos metadatos incluyen un identificador de apps que identifica la app que ha almacenado el registro. Además, otros metadatos opcionales pueden contener una copia del registro con firma digital. El objetivo es proporcionar integridad de datos para los registros generados por un dispositivo de confianza. La firma digital está en el formato de sintaxis de mensajes criptográficos (CMS) que se especifica en la [RFC 5652](#).

Acceso de apps de terceros a los datos de la app Salud

El acceso a la API de HealthKit se controla mediante autorizaciones; las apps deben respetar las restricciones relativas al uso de los datos. Por ejemplo, las apps no pueden usar los datos de salud para fines publicitarios. Además, las apps tienen que proporcionar a los usuarios una política de privacidad donde se especifique el uso que hacen de los datos de salud.

El acceso de las apps a los datos de salud se controla con los ajustes de privacidad del usuario. Los usuarios tienen que conceder acceso a los datos de salud cuando las apps lo solicitan, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS. Sin embargo, en el caso de los datos de salud, las apps reciben acceso independiente para la lectura y escritura de datos y para cada tipo de datos de salud. Los usuarios pueden ver y revocar los permisos que se les haya concedido para el acceso a datos de salud en Ajustes > Salud > Acceso de datos y dispositivos.

Si disponen de permiso para escribir datos, las apps también pueden leer los datos que escriban. Si disponen de permiso para leer datos, las apps pueden leer los datos que escriban todas las fuentes. Sin embargo, las apps no pueden saber el acceso que tienen otras apps. Además, las apps no pueden saber con seguridad si disponen de acceso de lectura a los datos de salud. Cuando una app no tiene acceso de lectura, las consultas no devuelven datos, al igual que sucede cuando una base de datos está vacía. Esto está diseñado para evitar que las apps infieran el estado de salud del usuario al conocer el tipo de datos que este registra.

“Datos médicos” para los usuarios

La app Salud permite a los usuarios rellenar un formulario con sus datos médicos e información que pueda ser importante durante una emergencia médica. La información se introduce o actualiza manualmente y no se sincroniza con la información de las bases de datos de salud.

Para ver la información de “Datos médicos”, basta con pulsar el botón SOS de la pantalla bloqueada. La información se almacena en el dispositivo con la clase de Protección de datos “Sin protección”, de modo que se pueda acceder a ella sin necesidad de introducir el código del dispositivo. “Datos médicos” es una función opcional que permite a los usuarios decidir cómo conseguir un equilibrio entre seguridad y privacidad. Con iOS 13 o versiones anteriores, se guarda una copia de estos datos en la copia de seguridad de iCloud. En iOS 14, los datos médicos se sincronizan en todos los dispositivos mediante CloudKit con las mismas características de encriptación que el resto de los datos de salud.

Función de compartir los datos de salud

En iOS 15, la app Salud ofrece a los usuarios la opción de compartir sus datos de la app Salud con otros usuarios. Los datos de la app Salud se comparten entre los dos usuarios usando la encriptación de punto a punto de iCloud y Apple no puede acceder a los datos que se envían a través de la función de compartir los datos de salud. Para usar la función, tanto el usuario que envía como el que recibe deben utilizar iOS 15 o posterior y tener activada la autenticación de doble factor.

Los usuarios también pueden optar por compartir sus datos de la app Salud con su proveedor de servicios sanitarios usando la función “Compartir con el proveedor” de la app Salud. Los datos compartidos mediante esta función se ponen a disposición solo de las instituciones sanitarias seleccionadas por el usuario mediante una encriptación de punto a punto y Apple no mantiene ni tiene acceso a las claves de encriptación para desencriptar, ver o acceder de otro modo a los datos de la app Salud compartidos a través de la función “Compartir con el proveedor”. Puedes encontrar más detalles sobre cómo el diseño de este servicio protege los datos de la app Salud de los usuarios en la [sección Seguridad y privacidad](#) del Manual de registro de Apple para organizaciones sanitarias.

Encriptación y firma digital

Listas de control de acceso

Los datos del llavero se separan y protegen con listas de control de acceso (ACL). Como resultado, las credenciales almacenadas por las apps de terceros no son accesibles por las apps con otras identidades, a menos que el usuario las haya aprobado de forma explícita. Esta protección proporciona un mecanismo para proteger las credenciales de autenticación en los dispositivos Apple de una amplia variedad de apps y servicios dentro de la organización.

Mail

En la app Mail, los usuarios pueden enviar mensajes encriptados y firmados digitalmente. Mail descubre automáticamente la correspondiente dirección de correo electrónico compatible con [RFC 5322](#) (con distinción entre mayúsculas y minúsculas) y el asunto o los nombres alternativos del asunto en la firma digital y los certificados de encriptación en los identificadores de verificación de identificación personal (PIV) adjuntos en las tarjetas inteligentes compatibles. Si una cuenta de correo electrónico configurada coincide con una dirección de correo electrónico en una firma digital o certificado de encriptación en un identificador PIV adjunto, Mail muestra automáticamente el botón de inicio de sesión en la barra de herramientas de la ventana de un nuevo mensaje. Si Mail tiene el certificado de encriptación de correo electrónico del destinatario o puede descubrirlo en la lista global de direcciones (GAL) de Microsoft Exchange, aparece un icono de candado desbloqueado en la barra de herramientas de nuevo mensaje. Un icono del candado bloqueado indica que el mensaje se enviará encriptado con la clave pública del destinatario.

S/MIME por mensaje

iOS, iPadOS y macOS son compatibles con S/MIME por mensaje. Esto significa que los usuarios de S/MIME pueden optar por firmar y encriptar los mensajes siempre por defecto o firmar y encriptar los mensajes individuales de forma selectiva.

Las identidades que se usan con S/MIME se pueden entregar a los dispositivos Apple mediante un perfil de configuración, una solución de [gestión de dispositivos móviles \(MDM\)](#), el protocolo de inscripción de certificados simple (SCEP) o la autoridad de certificación Microsoft Active Directory.

Tarjetas inteligentes

macOS 10.12 o posterior incluye compatibilidad nativa con las tarjetas de verificación de la identidad personal (PIV). Esta tarjeta se utiliza mucho en organizaciones comerciales y gubernamentales para la autenticación de doble factor, la firma digital y la encriptación.

Las tarjetas inteligentes incluyen una o más identidades digitales que tienen un par de claves públicas y privadas y un certificado asociado. Al desbloquear una tarjeta inteligente con el número de identificación personal (PIN), se obtiene acceso a las claves privadas que se usan para las operaciones de autenticación, encriptación y firma. El certificado determina para qué se puede usar una clave, qué atributos están asociados a ella y si está validada (firmada) por una autoridad de certificación (CA).

Las tarjetas inteligentes se pueden usar para la autenticación de doble factor. Los dos factores necesarios para desbloquear una tarjeta son “algo que el usuario tiene” (la tarjeta) y “algo que el usuario conoce” (el PIN). macOS 10.12 o posterior también incluye compatibilidad nativa con la autenticación mediante la ventana de inicio de sesión de la tarjeta inteligente y la autenticación mediante el certificado de cliente para acceder a sitios web en Safari. También es compatible con la autenticación basada en Kerberos mediante el uso de pares de claves (PKINIT) para llevar a cabo un inicio de sesión único en servicios compatibles con Kerberos. Para obtener más información acerca de las tarjetas inteligentes y macOS, consulta [Introducción a la integración de tarjetas inteligentes](#) en *Implementación de las plataformas de Apple*.

Imágenes de disco encriptadas

En macOS, las imágenes de disco encriptadas hacen la función de contenedores seguros en los que los usuarios pueden almacenar o transferir documentos sensibles y otros archivos. Las imágenes de disco encriptadas se crean mediante Utilidad de Discos, que se encuentra en /Aplicaciones/Utilidades/. Las imágenes de disco se pueden encriptar mediante encriptación AES de 128 bits o 256 bits. Dado que una imagen de disco montada se trata como un volumen local conectado a un Mac, los usuarios pueden copiar, trasladar y abrir los archivos y carpetas que se han almacenado en ella. Al igual que ocurre con FileVault, el contenido de una imagen de disco se encripta y desencripta en tiempo real. Con las imágenes de disco encriptadas, los usuarios pueden intercambiar documentos, archivos y carpetas de forma segura guardando una imagen de disco encriptada en un soporte extraíble, enviándola como archivo adjunto de un mensaje de correo o guardándola en un servidor remoto. Si quieres obtener más información acerca de las imágenes de disco encriptadas, consulta el [Manual de uso de Utilidad de Discos](#).

Seguridad de las apps

Descripción general de la seguridad de las apps

Actualmente, las apps son unos de los elementos más importantes de una arquitectura de seguridad. Sus ventajas en cuanto a productividad son increíbles, pero si no se gestionan bien, también pueden repercutir negativamente en la seguridad y estabilidad del sistema o en los datos de usuario.

Por esta razón, Apple añade capas de protección para ayudar a garantizar que las apps están libres de software malicioso conocido y que no se han manipulado. La protección adicional hace que el acceso de las apps a los datos del usuario esté cuidadosamente mediado. Estos controles de seguridad proporcionan una plataforma estable y segura para las apps, donde miles de desarrolladores pueden ofrecer sus apps para iOS, iPadOS y macOS sin que la integridad del sistema se vea afectada. Además, los usuarios pueden acceder a estas apps en sus dispositivos Apple sin temor a los virus, el software malicioso o los ataques no autorizados.

En el iPhone, iPad y iPod touch, todas las apps se obtienen de App Store (y todas las apps se "aislan") para ofrecer los controles más estrictos.

En el Mac, muchas apps se obtienen de App Store, pero los usuarios del Mac también descargan y usan apps de internet. Para poder realizar descargas de internet de forma segura, macOS añade controles adicionales. En primer lugar, por defecto en macOS 10.15 o posterior, todas las apps para Mac deben estar certificadas por Apple para poder abrirlas. Este requisito ayuda a garantizar que las apps estén libres de software malicioso conocido sin que las apps deban proporcionarse a través de App Store. Además, macOS incluye un sistema de protección antivirus de última generación para bloquear (y, si es necesario, eliminar) el software malicioso.

Como control adicional en todas las plataformas, el aislamiento ayuda a proteger los datos del usuario frente a un acceso no autorizado por parte de las apps. Adicionalmente, en macOS, los datos de las áreas más importantes están, en sí mismos, protegidos. Esto ayuda a garantizar que los usuarios mantengan el control de acceso a los archivos en las carpetas Escritorio, Documentos y Descargas (entre otras) con respecto a todas las apps, tanto si las apps que intentan acceder están aisladas como si no.

Función nativa	Equivalente en otros desarrolladores
Lista de módulos no aprobada, lista de extensiones de Safari no aprobada	Definiciones de virus/software malicioso
Archivos en cuarentena	Definiciones de virus/software malicioso
Firmas XProtect/YARA	Definiciones de virus/software malicioso; protección del punto final
Gatekeeper	Protección de endpoint; requiere la firma de código de las apps para ayudar a garantizar que solo se ejecuta software de confianza
efiheck (necesario para un Mac sin un chip de seguridad T2 de Apple)	Protección de endpoint; detección de rootkit
Firewall de aplicaciones	Protección de endpoint; uso de firewalls
Filtrado de paquetes (pf)	Soluciones de firewall
Protección de la integridad del sistema	Integrado en macOS
Controles de acceso obligatorios	Integrado en macOS
Lista de exclusión de kexts	Integrado en macOS
Firma de código de apps obligatoria	Integrado en macOS
Certificación de apps	Integrado en macOS

Seguridad de las apps en iOS y iPadOS

Introducción a la seguridad de las apps para iOS y iPadOS

A diferencia de otras plataformas móviles, iOS y iPadOS no permiten a los usuarios instalar apps procedentes de sitios web que no estén firmadas y puedan ser maliciosas, ni ejecutar apps que no sean de confianza. Durante la ejecución, la firma de código comprueba que se realicen todas las páginas de la memoria ejecutable a medida que se cargan para ayudar a garantizar que una app no se haya modificado desde la última vez que se instaló o actualizó.

Una vez que se ha comprobado que una app procede de una fuente aprobada, iOS y iPadOS ponen en marcha medidas de seguridad diseñadas para impedir que ponga en peligro otras apps o el resto del sistema.

Proceso de firma de código de apps en iOS y iPadOS

En iOS y iPadOS, Apple garantiza la seguridad de las apps mediante mecanismos como la firma de código obligatoria y el inicio de sesión estricto para desarrolladores, entre otros.

Firma de código obligatoria

Una vez que se ha iniciado, el kernel de iOS o iPadOS controla los procesos y apps del usuario que se pueden ejecutar. Para ayudar a garantizar que todas las apps proceden de una fuente conocida y aprobada y no se han manipulado, iOS y iPadOS requieren que todo el código ejecutable se firme con un certificado emitido por Apple. Las apps proporcionadas con el dispositivo, como Mail y Safari, están firmadas por Apple. Las apps de terceros también se deben validar y firmar con un certificado emitido por Apple. La firma de código obligatoria extiende el concepto de cadena de confianza del sistema operativo a las apps y contribuye a impedir que aplicaciones de terceros carguen código sin firmar o utilicen código que se modifique automáticamente.

Cómo firman los desarrolladores sus apps

Los desarrolladores pueden firmar sus apps mediante la validación de un certificado (a través del programa para desarrolladores Apple Developer Program). También pueden incorporar en sus apps estructuras cuyo código se valide mediante un certificado emitido por Apple (a través de un identificador de equipo).

- *Validación del certificado:* Para desarrollar e instalar apps en dispositivos iOS y iPadOS, los desarrolladores deben registrarse en Apple y unirse al Apple Developer Program. Apple verifica la identidad real de cada desarrollador, ya sea una persona individual o una empresa, antes de emitir su certificado. Este certificado permite a los desarrolladores firmar apps y enviarlas a la tienda App Store para su distribución. Así, todas las apps de App Store han sido enviadas por personas u organizaciones identificables, lo cual funciona como elemento disuasorio para la creación de apps maliciosas. Además, Apple las ha revisado para ayudar a garantizar que normalmente funcionan según lo esperado y que no contienen errores ni otros problemas evidentes. Este proceso de revisión, organización y distribución, que se suma a la tecnología ya comentada, da confianza a los usuarios en cuanto a la calidad de las apps que compran.

- *Validación de la firma de código:* iOS y iPadOS permiten a los desarrolladores incorporar en sus apps marcos de desarrollo que las propias apps o las extensiones incorporadas en ellas pueden utilizar. Para proteger el sistema y otras apps frente a la carga de código de terceros en su espacio de direcciones, el sistema valida la firma de código en todas las bibliotecas dinámicas a las que un proceso ofrezca un enlace al iniciarse. Esta verificación se consigue mediante el identificador de equipo (ID de equipo), que se extrae de un certificado emitido por Apple. Un identificador de equipo es una cadena de 10 caracteres alfanuméricos, como 1A2B3C4D5F. Un programa puede tener un enlace a cualquier biblioteca de plataformas proporcionada con el sistema o a cualquier biblioteca que tenga el mismo identificador de equipo en su firma de código como ejecutable principal. Los ejecutables que se envían con el sistema no cuentan con un identificador de equipo, por lo que solo pueden contener enlaces a bibliotecas que se envíen con el propio sistema.

Verificar las apps internas propias

Las empresas aptas también pueden crear apps internas propias para utilizarlas dentro de la organización y distribuirlas a sus empleados. Las empresas y organizaciones pueden solicitar el registro en el Programa Enterprise para desarrolladores de Apple (ADEP). Para obtener más información y para revisar los requisitos de idoneidad, consulta el [sitio web del Programa Enterprise para desarrolladores de Apple](#). Una vez que una organización es miembro de ADEP, puede registrarse para obtener un [perfil de datos](#) que permita la ejecución de apps internas propias en los dispositivos autorizados.

Los usuarios deben tener instalado el perfil de datos para poder ejecutar estas apps. Esto ayuda a garantizar que solo los usuarios que elija la organización pueden cargar las apps en sus dispositivos iOS y iPadOS. Se confía implícitamente en las apps instaladas con una solución de [gestión de dispositivos móviles \(MDM\)](#), dado que la relación entre la organización y el dispositivo ya está establecida. De lo contrario, los usuarios tienen que aprobar el perfil de datos de la app en Ajustes. Las organizaciones también pueden restringir a los usuarios para que no aprueben apps de desarrolladores desconocidos. En la primera apertura de cualquier app interna propia, el dispositivo debe recibir la confirmación positiva de Apple de que se permite ejecutar la app.

Seguridad del proceso de ejecución en iOS y iPadOS

iOS y iPadOS ayudan a garantizar la seguridad en tiempo de ejecución mediante una "zona protegida", autorizaciones declaradas y la aleatorización del espacio de direcciones (ASLR).

Aislamiento

Todas las apps de terceros se "aislan" para impedir que accedan a los archivos almacenados por otras apps o que realicen cambios en el dispositivo. El aislamiento está diseñado para evitar que las apps recopilen o modifiquen la información almacenada por otras apps. Cada una tiene un directorio de inicio único para sus archivos, que se asigna de forma aleatoria al instalarla. Si una app de terceros necesita acceder a información ajena, utiliza únicamente los servicios que iOS y iPadOS proporcionan de forma explícita.

Los archivos y recursos del sistema también están protegidos de las apps del usuario. La mayoría de los recursos y archivos del sistema de iOS y iPadOS se ejecutan como el usuario sin privilegios "mobile", igual que todas las apps de terceros. Toda la partición del sistema operativo se instala como de solo lectura. Las herramientas innecesarias, como los servicios de inicio de sesión remoto, no se incluyen en el software del sistema y las API no permiten que las apps transfieran sus privilegios para modificar otras apps o iOS y iPadOS.

Uso de autorizaciones

El acceso de apps de terceros a información del usuario y a funciones como iCloud, así como su extensibilidad, se controla mediante autorizaciones declaradas. Las autorizaciones son pares de clave-valor que se utilizan para acceder a una app y permiten la autenticación más allá de los factores en tiempo de ejecución, como un ID de usuario UNIX. Las autorizaciones llevan una firma digital, por lo que no se pueden modificar. Los daemons y las apps del sistema las utilizan mucho para realizar operaciones con privilegios específicos que, de otro modo, requerirían la ejecución del proceso como root. Esto reduce considerablemente la posibilidad de que un daemon o app del sistema en peligro transfiera sus privilegios.

Además, las apps solo pueden realizar procesos en segundo plano a través de las API proporcionadas por el sistema. De esta manera, las apps siguen funcionando sin que su rendimiento o la duración de la batería se vean mermados.

Aleatorización del espacio de direcciones

La aleatorización del espacio de direcciones (ASLR) ayuda a proteger el sistema frente a los ataques que aprovechan los fallos por corrupción de memoria. Al abrirse, las apps integradas utilizan la ASLR para ayudar a aleatorizar todas las regiones de la memoria. Además de funcionar al abrirse, la ASLR ordena aleatoriamente las direcciones de memoria de código ejecutable, las bibliotecas del sistema y las estructuras de programación relacionadas, reduciendo aún más la probabilidad de que tengan lugar muchos ataques. Por ejemplo, en el caso de un ataque "return-to-libc" en el que se intenta engañar a un dispositivo para que ejecute código malicioso mediante la manipulación de las direcciones de memoria de la pila y las bibliotecas del sistema, la aleatorización en su colocación dificulta la ejecución del ataque, especialmente en varios dispositivos. Xcode y los entornos de desarrollo de iOS o iPadOS compilan automáticamente programas de terceros que tengan activada la compatibilidad con la ASLR.

La función Execute Never

iOS y iPadOS aumentan el nivel de protección con la función Execute Never (XN) de ARM, que marca las páginas de memoria como no ejecutables. Solo las apps en condiciones muy controladas pueden utilizar las páginas de memoria marcadas como grabables y ejecutables: el kernel comprueba la presencia de la autorización de firma de código dinámica exclusiva de Apple. Incluso entonces, solo se puede realizar una única llamada mmap para solicitar una página ejecutable y grabable, a la que se proporciona una dirección aleatorizada. Safari utiliza esta funcionalidad para su compilador Just-in-Time (JIT) de JavaScript.

Extensiones compatibles en iOS, iPadOS y macOS

iOS, iPadOS y macOS permiten a las apps proporcionar funcionalidad a otras apps mediante el uso de extensiones. Las extensiones son binarios ejecutables firmados para fines específicos y empaquetados en una app. Durante la instalación, el sistema detecta las extensiones automáticamente y las pone a disposición de otras apps utilizando un sistema de coincidencias.

Puntos de extensión

Las áreas del sistema que admiten extensiones se conocen como *puntos de extensión*. Cada punto de extensión proporciona API y aplica políticas para el área correspondiente. El sistema determina qué extensiones están disponibles en función de las reglas de coincidencia específicas de cada punto de extensión. El sistema inicia los procesos de extensión automáticamente cuando es necesario y gestiona su duración. Las autorizaciones se pueden utilizar para restringir la disponibilidad de las extensiones a apps específicas del sistema. Por ejemplo, un widget de la vista Hoy solo aparece en el centro de notificaciones, y la extensión para compartir solo está disponible en el panel Compartir. Algunos ejemplos de puntos de extensión son los widgets Hoy, Compartir, Acciones, "Edición de fotos", "Proveedor de archivos" y "Teclado personalizado".

Cómo se comunican las extensiones

Las extensiones se ejecutan en su propio espacio de direcciones. Para la comunicación entre la extensión y la app desde la que se ha activado, se utiliza la comunicación entre procesos mediada por la estructura del sistema. Las extensiones no tienen acceso a los archivos o espacios de memoria de las otras extensiones. Se han diseñado de forma que estén aisladas entre sí, de las apps contenedoras y de las apps que las utilizan. Se aíslan igual que cualquier otra app de terceros y tienen un contenedor diferente al de la app que las contiene. Sin embargo, comparten el mismo acceso a los controles de privacidad que la app contenedora. De este modo, si un usuario concede el acceso a Contactos a una app, las extensiones incorporadas en la app también gozarán del acceso, pero no así las extensiones activadas por ella.

Cómo se utilizan los teclados personalizados

Los teclados personalizados son un tipo de extensión especial, puesto que el usuario los activa para todo el sistema. Una vez activados, se utiliza una extensión de teclado para cualquier campo de texto, salvo el de la introducción del código y cualquier vista de texto seguro. Con el fin de restringir la transferencia de datos del usuario, los teclados personalizados se ejecutan por defecto en una zona protegida muy restrictiva que bloquea el acceso a la red, los servicios que realizan operaciones de red en nombre de un proceso y las API que permiten que la extensión filtre los datos introducidos. Los desarrolladores de teclados personalizados pueden solicitar que su extensión tenga acceso abierto, lo cual permite que el sistema ejecute la extensión en la zona protegida por defecto tras obtener el consentimiento del usuario.

MDM y extensiones

En el caso de los dispositivos inscritos en una solución de [gestión de dispositivos móviles \(MDM\)](#), las extensiones de teclado y documentos obedecen a las reglas de gestión de aperturas de archivos. Por ejemplo, la solución MDM puede ayudar a impedir que los usuarios exporten un documento de una app gestionada a un proveedor de documentos sin gestionar o que utilicen un teclado sin gestionar con una app gestionada. Además, los desarrolladores de apps pueden impedir el uso de extensiones de teclado de terceros en su aplicación.

Protección de apps y grupos de apps en iOS y iPadOS

En iOS y iPadOS, las organizaciones pueden proteger las apps de forma segura mediante el SDK de iOS y uniéndose a los grupos de apps en el portal para desarrolladores de Apple.

Adoptar la protección de datos en apps

El kit de desarrollo de software (SDK) de iOS y iPadOS ofrece un conjunto completo de API que facilita a los desarrolladores internos y de terceros la adopción de la [protección de datos](#) y contribuye a garantizar el máximo nivel de protección en sus apps. La protección de datos está disponible para las API de archivo y de base de datos, como NSFileManager, CoreData, NSData y SQLite.

La base de datos de la app Mail (archivos adjuntos incluidos), los libros gestionados, los marcadores de Safari, las imágenes de apertura de apps y los datos de ubicación también se almacenan mediante encriptación, con claves protegidas por el código del usuario en su dispositivo. Las apps Calendario (archivos adjuntos no incluidos), Contactos, Recordatorios, Notas, Mensajes y Fotos implementan la autorización de protección de datos "Protegido hasta la primera autenticación del usuario".

Las apps instaladas por el usuario que no activan una clase de protección de datos específica reciben por defecto la clase "Protegido hasta la primera autenticación del usuario".

Unirse a los grupos de apps

Las apps y las extensiones que sean propiedad de una cuenta de desarrollador determinada pueden compartir contenido una vez que se hayan configurado como parte de un grupo de apps. El desarrollador puede crear los grupos de apps apropiados en el portal para desarrolladores de Apple e incluir el conjunto de apps y extensiones que desee. Una vez que se han configurado como parte de un grupo de apps, las apps tienen acceso a lo siguiente:

- Un contenedor en el volumen compartido para el almacenamiento, que permanece en el dispositivo mientras al menos una de las apps del grupo esté instalada.
- Preferencias compartidas.
- Ítems del [llavero](#) compartidos.

El portal para desarrolladores de Apple contribuye a garantizar que los [identificadores de grupo \(GID\)](#) de apps sean únicos en todo el ecosistema de apps.

Verificación de los accesorios en iOS y iPadOS

El programa de licencias Made for iPhone, iPad y iPod touch (MFi) proporciona a los fabricantes de accesorios aprobados acceso al Protocolo de accesorios para iPod (iAP) y los componentes de hardware necesarios.

Cuando un accesorio MFi se comunica con un dispositivo iOS o iPadOS mediante un conector Lightning o USB-C o por Bluetooth, el dispositivo pide al accesorio que responda con un certificado proporcionado por Apple, que el dispositivo verifica, para demostrar que cuenta con la autorización de Apple. Entonces, el dispositivo envía un reto, que el accesorio debe contestar con una respuesta firmada. Este proceso está totalmente gestionado por un [circuito integrado \(IC\)](#) personalizado que Apple proporciona a los fabricantes de accesorios aprobados y es transparente para el accesorio.

Los accesorios pueden solicitar acceso a funcionalidades y métodos de transporte diferentes; por ejemplo, acceso a secuencias de audio digital a través del cable Lightning o USB-C, o información de ubicación proporcionada por Bluetooth. Un circuito integrado de autenticación está diseñado para garantizar que solo tienen acceso total al dispositivo los accesorios aprobados. Si un accesorio no es compatible con la autenticación, su acceso queda limitado al audio analógico y a un pequeño subconjunto de controles de reproducción de audio serie (UART).

AirPlay también usa el circuito integrado de autenticación para verificar si los receptores cuentan con la aprobación de Apple. Las secuencias de audio de AirPlay y de vídeo de CarPlay usan el Protocolo de asociación segura (SAP) MFi, que encripta la comunicación entre el accesorio y el dispositivo con AES128 en modo de contador (CTR). Las claves efímeras se intercambian mediante el intercambio de claves de ECDH (Curve25519) y se firman con la clave RSA de 1024 bits del circuito integrado de autenticación, como parte del protocolo de estación a estación (STS).

Seguridad de las apps en macOS

Introducción a la seguridad de las apps para macOS

La seguridad de las apps en macOS consta de una serie de capas superpuestas. La primera de ellas es la opción de ejecutar únicamente las apps de confianza y firmadas de App Store. Además, Apple añade capas de protección para ayudar a garantizar que las apps descargadas de internet están libres de software malicioso conocido. macOS ofrece tecnologías para detectar y eliminar software malicioso y ofrece protecciones adicionales diseñadas para impedir que apps que no sean de confianza accedan a los datos del usuario. Los servicios de Apple, como la certificación y las actualizaciones de XProtect están diseñados para impedir la instalación de software malicioso. Cuando sea necesario, estos servicios localizan el software malicioso que haya podido evitar la detección inicialmente y lo eliminan de forma rápida y eficaz. En última instancia, los usuarios de macOS pueden utilizar el ordenador libremente con el modelo de seguridad que prefieran, incluso si ello implica ejecutar código que no esté firmado y que no sea de confianza.

Proceso de firma de código de apps en macOS

Todas las apps de App Store están firmadas por Apple. Esta firma está diseñada para garantizar que no se han manipulado ni alterado. Apple firma todas las apps proporcionadas con los dispositivos Apple.

En macOS 10.15, todas las apps distribuidas fuera de App Store deben estar firmadas por el desarrollador con un certificado de ID de desarrollador emitido por Apple (en combinación con una clave privada) y estar certificadas por Apple para ejecutarse bajo los ajustes por defecto de Gatekeeper. Las apps desarrolladas internamente también deberían estar firmadas con un ID de desarrollador emitido por Apple para que los usuarios puedan validar su integridad.

En macOS, la firma de código y la certificación funcionan de forma independiente (y pueden llevarlas a cabo diferentes agentes) para diferentes propósitos. La firma de código la lleva a cabo el desarrollador que utiliza su certificado de ID de desarrollador (emitido por Apple) y la verificación de esta firma sirve para probar al usuario que el software de un desarrollador no se ha manipulado desde que el desarrollador compiló y firmó ese software. La certificación puede realizarla cualquier persona de la cadena de distribución del software y sirve para probar que Apple ha recibido una copia del código para comprobar la existencia de software malicioso y que no se ha encontrado ningún software malicioso conocido. El resultado de la certificación es un tique que se almacena en los servidores de Apple y que se puede adjuntar a la app (por cualquier persona) sin invalidar la firma del desarrollador.

Los controles de acceso obligatorios (MAC) requieren la firma de código para permitir las autorizaciones protegidas por el sistema. Por ejemplo, las apps que requieren acceso a través del firewall deben tener un código firmado con la autorización MAC correspondiente.

Gatekeeper y la protección durante la ejecución en macOS

macOS ofrece la tecnología Gatekeeper y protección durante la ejecución para ayudar a garantizar que solo se ejecute software de confianza en el Mac de un usuario.

Gatekeeper

macOS incluye una tecnología de seguridad llamada *Gatekeeper* que está diseñada para ayudar a garantizar que solo se ejecute software de confianza en el Mac de un usuario. Cuando un usuario descarga y abre una app, un módulo o un paquete de instalador desde fuera de App Store, Gatekeeper verifica que el software proviene de un desarrollador identificado, está certificado por Apple como libre de contenido malicioso conocido y no se ha alterado. Gatekeeper también solicita la aprobación del usuario antes de abrir un software descargado por primera vez para asegurarse de que el usuario no ha sido engañado para que ejecute código creyendo que simplemente es un archivo de datos.

Por defecto, Gatekeeper ayuda a garantizar que todo el software descargado está firmado por App Store o por un desarrollador registrado y certificado por Apple. El proceso de revisión de App Store y la canalización de certificación están diseñados para garantizar que las apps no contienen ningún software malicioso conocido. Por lo tanto, por defecto *todo el software de macOS se comprueba en busca de contenido malicioso conocido la primera vez que se abre, independientemente de cómo ha llegado al Mac.*

Los usuarios y organizaciones tienen la opción de permitir únicamente el software instalado de App Store. Alternativamente, los usuarios pueden anular las políticas de Gatekeeper para abrir cualquier software, a menos que esté restringido por una solución de [gestión de dispositivos móviles \(MDM\)](#). Las organizaciones pueden usar una solución MDM para configurar los ajustes de Gatekeeper, incluso permitir el software firmado con identidades alternativas. Gatekeeper también se puede desactivar por completo, si es necesario.

Gatekeeper también protege frente a la distribución de módulos maliciosos con apps benignas. En este caso, mediante la app se desencadena la carga de un módulo malicioso sin conocimiento del usuario. Cuando resulte necesario, Gatekeeper abre apps desde ubicaciones aleatorizadas de solo lectura. De este modo, se impide la carga automática de módulos distribuidos junto con la app.

Protección durante la ejecución

Los archivos y recursos del sistema, y el kernel están protegidos del espacio de las apps de un usuario. Todas las apps de App Store están aisladas para restringir el acceso a los datos almacenados por otras apps. Si una app de App Store necesita acceder a los datos de otra app, solo puede hacerlo mediante las API y los servicios proporcionados por macOS.

Protección frente al software malicioso en macOS

Apple utiliza un proceso de inteligencia frente a amenazas para identificar y bloquear rápidamente el software malicioso.

Tres niveles de defensa

Las defensas contra el software malicioso se estructuran en tres capas:

1. *Impedir el lanzamiento o la ejecución de software malicioso:* App Store, o Gatekeeper junto con el servicio de certificación
2. *Impedir que el software malicioso se ejecute en los sistemas del cliente:* Gatekeeper, certificación y XProtect
3. *Corregir los problemas ocasionados por el software malicioso ejecutado:* XProtect

El primer nivel de defensa está diseñado para impedir la distribución del software malicioso y evitar que se inicie; este es el objetivo de App Store y Gatekeeper junto con el servicio de certificación.

El siguiente nivel de defensa es ayudar a garantizar que, si el software malicioso aparece en cualquier Mac, se identifique y bloquee rápidamente, tanto para detener su propagación como para solucionar los problemas de los sistemas Mac en los que ya se haya establecido. XProtect refuerza esta defensa, junto con Gatekeeper y el servicio de certificación.

Por último, XProtect actúa para corregir los problemas causados por el software malicioso que haya conseguido ejecutarse.

Estas medidas, descritas a continuación, se combinan para ofrecer una protección óptima frente a virus y software malicioso. Existen medidas de protección adicionales, especialmente en un Mac con chip de Apple, para limitar los daños potenciales del software malicioso que logre ejecutarse. Consulta [Protección del acceso de las apps a los datos de usuario](#) para ver cómo puede ayudar macOS a proteger los datos de usuario del software malicioso, e [Integridad del sistema operativo](#) para ver cómo puede limitar macOS las acciones que puede realizar el software malicioso en el sistema.

Certificación

La *certificación* es un servicio de análisis de software malicioso proporcionado por Apple. Los desarrolladores que quieran distribuir apps para macOS fuera de App Store, envían sus apps para que se analicen como parte del proceso de distribución. Apple analiza este software en busca de software malicioso conocido y, si no encuentra nada, emite un tique de certificación. Habitualmente, los desarrolladores adjuntan este tique a su app para que Gatekeeper pueda verificar e iniciar la app, incluso sin conexión.

Apple también puede emitir un tique de revocación para apps consideradas maliciosas, incluso si anteriormente se habían certificado. macOS comprueba periódicamente si hay nuevos tiques de revocación para que Gatekeeper disponga de la información más reciente y pueda impedir que se inicien esos archivos. Este proceso permite bloquear muy rápidamente apps maliciosas, ya que las actualizaciones se producen en segundo plano con una frecuencia mucho mayor que incluso las actualizaciones en segundo plano que insertan nuevas firmas de XProtect. Además, esta medida de protección se puede aplicar tanto a apps que se han certificado anteriormente como a las que no.

XProtect

macOS incluye una tecnología antivirus integrada denominada *XProtect* para la detección y eliminación mediante firmas de software malicioso. El sistema usa firmas YARA, una herramienta para la detección de software malicioso basada en firmas, que Apple actualiza periódicamente. Apple supervisa las nuevas infecciones de software malicioso y sus diferentes versiones, y actualiza las firmas automáticamente (independientemente de las actualizaciones del sistema) para ayudar a defender un Mac frente a las infecciones de software malicioso. XProtect detecta y bloquea automáticamente la ejecución del software malicioso conocido. En macOS 10.15 o posterior, XProtect comprueba si hay contenido malicioso conocido cada vez que:

- se inicia una app por primera vez;
- se modifica una app (en el sistema de archivos);
- se actualizan las firmas de XProtect.

Cuando XProtect detecta software malicioso conocido, se bloquea y el usuario recibe una notificación, y se le ofrece la opción de trasladar el software a la Papelera.

Nota: La certificación es eficaz con archivos (o hashes de archivo) conocidos y se puede usar en apps que se han iniciado anteriormente. Las reglas basadas en firmas de XProtect son más genéricas que un hash de archivo específico, para poder encontrar variantes que Apple no haya detectado. XProtect solo analiza las apps que se han modificado o las apps en su primera apertura.

En caso de que el software malicioso encuentre las formas de acceder a un Mac, XProtect también incluye tecnología para solucionar las infecciones. Por ejemplo, incluye un motor que permite reparar las infecciones mediante actualizaciones proporcionadas automáticamente por Apple (como parte de las actualizaciones automáticas de los archivos de datos del sistema y las actualizaciones de seguridad). También elimina el software malicioso en cuanto recibe información actualizada y sigue buscando infecciones periódicamente. XProtect no reinicia automáticamente el Mac.

Actualizaciones de seguridad de XProtect automáticas

Apple publica las actualizaciones para XProtect automáticamente en función de la última información sobre amenazas disponible. Por defecto, macOS comprueba estas actualizaciones a diario. Las actualizaciones de certificación, que se distribuyen mediante la sincronización de CloudKit, son mucho más frecuentes.

Cómo responde Apple cuando se detecta un nuevo software malicioso

Cuando se detecta un nuevo software malicioso, se toman una serie de medidas:

- Todos los certificados de ID de desarrollador asociados se revocan.
- Se emiten tiques de revocación de certificación para todos los archivos (apps y archivos asociados).
- Se desarrollan y publican firmas de XProtect.

Estas firmas también se aplican con efectos retroactivos a software certificado con anterioridad y, si se detecta algo nuevo, pueden producirse una o varias de las acciones anteriores.

En última instancia, la detección de un software malicioso pone en marcha una serie de pasos durante los segundos, horas y días siguientes para propagar las mejores medidas de protección posibles para los usuarios de Mac.

Controlar el acceso de las apps a los archivos en macOS

Apple cree que los usuarios deberían disponer de la transparencia, el consentimiento y el control totales sobre lo que las apps hacen con sus datos. En macOS 10.15, el sistema aplica este modelo para ayudar a garantizar que todas las apps deban obtener el consentimiento del usuario antes de acceder a los archivos en Documentos, Descargas, Escritorio, iCloud Drive y en los volúmenes de red. En macOS 10.13 o posterior, las apps que requieren acceso a todo el almacenamiento del dispositivo deben añadirse de forma explícita en Preferencias del Sistema. Además, las funciones de accesibilidad y automatización requieren el permiso del usuario para ayudar a garantizar que no burlen otras protecciones. En función de la política de acceso, puede que se solicite o requiera a los usuarios que cambien el ajuste en Preferencias del Sistema > Seguridad y privacidad > Privacidad:

Ítem	Usuario preguntado por una app	El usuario debe editar los ajustes de privacidad del sistema
Accesibilidad		✓
Acceso a todo el almacenamiento interno		✓
Archivos y carpetas <i>Nota:</i> Incluye Escritorio, Documentos, Descargas, volúmenes de red y volúmenes extraíbles	✓	
Automatización (eventos de Apple)	✓	

Los ítems de la Papelera del usuario están protegidos de las apps que utilizan el acceso completo al disco; no se le preguntará al usuario por el acceso de la app. Si el usuario quiere que las apps puedan acceder a los archivos, se deben trasladar de la Papelera a otra ubicación.

Al usuario que activa FileVault en un Mac se le solicitará que proporcione credenciales válidas antes de continuar con el proceso de arranque y obtener acceso a modos de arranque especializados. Sin unas credenciales de inicio de sesión válidas o una clave de recuperación, todo el volumen permanece encriptado y está protegido del acceso no autorizado, incluso si se retira el dispositivo de almacenamiento físico y se conecta a otro ordenador.

Para proteger los datos en un entorno empresarial, el departamento de TI debería definir y aplicar las políticas de configuración de FileVault con una solución de [gestión de dispositivos móviles \(MDM\)](#). Las organizaciones tienen varias opciones para gestionar volúmenes encriptados, incluidas claves de recuperación a nivel de la institución, claves de recuperación personales (que de forma opcional se pueden almacenar con la solución MDM para su custodia) o una combinación de ambas. La rotación de las claves también se puede establecer como política en la solución MDM.

Funciones de seguridad en la app Notas

La app Notas incluye la función de notas seguras (en el iPhone, iPad, Mac y el sitio web de iCloud), que permite a los usuarios proteger el contenido de determinadas notas. Los usuarios también pueden compartir notas con otras personas de forma segura.

Notas seguras

Las notas seguras están encriptadas de punto a punto con una contraseña definida por el usuario que es necesaria para ver las notas en dispositivos iOS, iPadOS, macOS y el sitio web de iCloud. Cada cuenta de iCloud (incluidas las cuentas del dispositivo propio) puede tener una contraseña independiente.

Cuando un usuario protege una nota, se deriva una clave de 16 bits de la contraseña del usuario con PBKDF2 y SHA256. La nota y todos sus archivos adjuntos se encriptan mediante AES en modo Galois/Counter (AES-GCM). Se generan nuevos registros en Core Data y CloudKit para guardar la nota encriptada, los archivos adjuntos, la etiqueta y el vector de inicialización. Después de crear los nuevos registros, los datos originales sin encriptar se eliminan. Los archivos adjuntos compatibles con la encriptación pueden ser imágenes, dibujos, tablas, mapas y sitios web. Las notas que contienen otros tipos de archivos adjuntos no se pueden encriptar y los que no son compatibles no se pueden añadir a las notas seguras.

Para ver una nota segura, el usuario debe introducir su contraseña o autenticarse con Face ID o Touch ID. Una vez que el usuario se ha autenticado correctamente, tanto para ver como para crear una nota segura, la aplicación Notas abre una sesión segura. Mientras la sesión segura está abierta, el usuario puede ver o proteger otras notas sin tener que autenticarse de nuevo. Sin embargo, la sesión segura se aplicará solo a las notas protegidas con la contraseña proporcionada. El usuario todavía tendrá que autenticarse para las notas protegidas con una contraseña diferente. La sesión segura se cierra cuando:

- El usuario pulsa el botón “Bloquear ahora” en Notas.
- Notas pasa a estar en segundo plano durante más de tres minutos (8 minutos en macOS).
- El dispositivo iOS o iPadOS se bloquea.

Para cambiar la contraseña de una nota segura, el usuario debe introducir la contraseña actual, ya que Face ID y Touch ID no están disponibles al cambiar la contraseña. Después de elegir una nueva contraseña, la app Notas vuelve a encapsular las claves de todas las notas existentes en la misma cuenta que estaban encriptadas por la contraseña anterior.

Si un usuario escribe de forma incorrecta la contraseña tres veces seguidas, Notas muestra una indicación proporcionada por el usuario, si el usuario introdujo una durante la configuración. Si el usuario sigue sin recordar su contraseña, puede restablecerla en los ajustes de Notas. Esta función permite a los usuarios crear otras notas seguras con una contraseña nueva, pero no les permite ver las notas protegidas anteriormente, a las cuales podrán acceder solamente si recuerdan la contraseña antigua. Para poder restablecer la contraseña, se necesita la contraseña de la cuenta de iCloud del usuario.

Notas compartidas

Las notas que no están encriptadas de punto a punto con una contraseña se pueden compartir con otras personas. Las notas compartidas pueden seguir usando el tipo de datos encriptados de CloudKit para cualquier texto que el usuario ponga en una nota o para cualquier archivo que le adjunte. Los componentes siempre se encriptan con una clave encriptada en el [CKRecord](#). Los metadatos, como las fechas de creación y modificación, no se encriptan. CloudKit gestiona el proceso mediante el cual cada uno de los participantes puede encriptar y desencriptar los datos de los demás.

Funciones de seguridad en la app Atajos

En la app Atajos, los atajos se pueden sincronizar opcionalmente entre dispositivos Apple mediante iCloud. También pueden compartirse atajos con otros usuarios mediante iCloud. Los atajos se guardan localmente en un formato encriptado.

Los atajos personalizados son versátiles, del mismo modo que un script o un programa. Al descargar atajos de internet, se avisa al usuario de que Apple no ha revisado el atajo y se le da la oportunidad de inspeccionar el atajo. Para proteger frente a atajos malintencionados, se descargan definiciones de software malicioso actualizadas para identificar atajos malintencionados durante la ejecución.

Los atajos personalizados también pueden ejecutar JavaScript especificado por el usuario en sitios web en Safari cuando se les invoca desde la hoja para compartir. Para proteger frente a JavaScript malintencionado que, por ejemplo, intente que el usuario ejecute un script en el sitio web de una red social para recopilar sus datos, se coteja el JavaScript con las definiciones de software malicioso mencionadas anteriormente. La primera vez que un usuario ejecuta JavaScript en un dominio, se solicita al usuario que permita que se ejecuten atajos con JavaScript en la página web actual para ese dominio.

Seguridad de los servicios

Descripción general de la seguridad de los servicios

Apple ha creado un robusto conjunto de servicios para ayudar a los usuarios a aprovechar todavía más la utilidad y productividad de sus dispositivos. Estos servicios ofrecen unas capacidades potentes para el almacenamiento en la nube, la sincronización, el almacenamiento de contraseñas, la autenticación, los pagos, los mensajes, las comunicaciones y mucho más, y todo ello mientras protegen la privacidad de los usuarios y la seguridad de sus datos.

Este capítulo abarca las tecnologías de seguridad que se usan en iCloud, "Iniciar sesión con Apple", Apple Pay, iMessage, Apple Messages for Business, FaceTime, Buscar y Continuidad.

Nota: No todos los contenidos ni servicios de Apple están disponibles en todos los países o regiones.

ID de Apple e ID de Apple gestionado

Descripción general de la seguridad del ID de Apple

Un ID de Apple es la cuenta que se usa para iniciar sesión en los servicios de Apple. Es importante que el usuario proteja su ID de Apple para ayudar a evitar que se produzca un acceso no autorizado a sus cuentas. Con el fin de ayudarle a conseguirlo, los ID de Apple exigen el uso de contraseñas seguras que:

- deben estar compuestas, al menos, de ocho caracteres;
- deben combinar números y letras;
- no deben contener tres o más caracteres idénticos consecutivos;
- no sean de uso común.

Se recomienda a los usuarios que aumenten el grado de protección indicado añadiendo más caracteres o signos de puntuación para que sus contraseñas resulten aún más seguras.

Apple también envía notificaciones a los usuarios por mensajes de correo electrónico, por notificaciones push o por ambos métodos cuando se producen cambios importantes en sus cuentas. Por ejemplo, si se ha modificado una contraseña o la información de facturación, o bien si el ID de Apple se ha utilizado para iniciar sesión en un dispositivo nuevo. Si los usuarios detectan algo extraño, deben cambiar la contraseña de su ID de Apple inmediatamente.

Además, Apple utiliza diversas políticas y procedimientos diseñados para proteger las cuentas de los usuarios. Entre ellos, se incluyen la limitación del número de veces que se puede intentar iniciar sesión y restablecer la contraseña, la supervisión activa de fraudes para ayudar a identificar los ataques mientras se están produciendo, y las revisiones periódicas de las políticas que permiten a Apple adaptarse a cualquier información nueva que pueda afectar a la seguridad del usuario.

Nota: La política de contraseña del ID de Apple gestionado la establece un administrador en [Apple School Manager](#) o [Apple Business Manager](#).

Autenticación de doble factor

Para ayudar a los usuarios a proteger más sus cuentas, por defecto Apple usa la *autenticación de doble factor* (una capa adicional de seguridad para los ID de Apple). Está diseñado para garantizar que solo el propietario de la cuenta pueda acceder a ella, aunque otra persona conozca la contraseña. Con la autenticación de doble factor, solo se puede acceder a la cuenta de un usuario desde dispositivos de confianza (como el iPhone, iPad, iPod touch o Mac del usuario) o desde otros dispositivos (después de completar una verificación desde uno de estos dispositivos de confianza) o desde un número de teléfono de confianza. Para iniciar sesión por primera vez en un dispositivo nuevo, se necesita la contraseña del ID de Apple y un código de verificación de seis dígitos que se muestra en los dispositivos de confianza del usuario o que se envía a un número de teléfono de confianza. Al introducir el código, el usuario confirma que el dispositivo nuevo es de confianza y que es seguro iniciar sesión en él. Puesto que para acceder a la cuenta de un usuario ya no basta con una contraseña, la autenticación de doble factor mejora la seguridad del ID de Apple del usuario y de toda la información personal que este guarda en Apple. Está integrada directamente en iOS, iPadOS, macOS, tvOS, watchOS y los sistemas de autenticación que utilizan los sitios web de Apple.

Cuando un usuario inicia sesión en un sitio web de Apple con un navegador web, se envía una solicitud de segundo factor a todos los dispositivos de confianza asociados a la cuenta de iCloud del usuario para solicitar la aprobación de la sesión web. Si el usuario está iniciando sesión en un sitio web de Apple desde un navegador web de un dispositivo de confianza, verá el código de verificación que se muestra de forma local en el dispositivo que está usando. Cuando el usuario introduzca el código en ese dispositivo, se aprobará la sesión web.

Restablecimiento de la contraseña y recuperación de la cuenta

Si se olvida la contraseña de una cuenta de ID de Apple, un usuario puede restablecerla en un dispositivo de confianza. Si no hay ningún dispositivo de confianza disponible, pero se conoce la contraseña, un usuario puede usar un número de teléfono de confianza para autenticarse mediante la verificación por SMS. Además, para poder recuperar de forma inmediata un ID de Apple, se puede utilizar un código usado con anterioridad para restablecerlo junto con un SMS. Si ninguna de estas opciones es posible, entonces es necesario seguir los pasos del proceso de recuperación de la cuenta. Para más información, consulta el artículo de soporte técnico de Apple [Cómo usar la función Recuperación de cuenta cuando no puedes restablecer la contraseña del ID de Apple](#).

Seguridad del ID de Apple gestionado

Los ID de Apple gestionados funcionan de forma muy similar a un ID de Apple, pero son propiedad de una organización empresarial o educativa, que es la que los controla. Estas organizaciones pueden restablecer las contraseñas, limitar las compras y las comunicaciones como FaceTime y Mensajes, y configurar permisos basados en funciones para los empleados, el cuerpo docente, los profesores y los alumnos.

Algunos servicios están desactivados para los ID de Apple gestionados (por ejemplo, Apple Pay, el llavero de iCloud, HomeKit y Buscar).

Inspecciones de los ID de Apple gestionados

Los ID de Apple gestionados también son compatibles con las *inspecciones*, que permiten a las organizaciones cumplir la legislación y las normas en materia de privacidad. Un administrador, director o profesor de [Apple School Manager](#) puede inspeccionar las cuentas específicas de ID de Apple gestionados.

Los inspectores pueden supervisar solo las cuentas de usuarios con menos privilegios en la jerarquía escolar. Por ejemplo, los profesores pueden supervisar a los alumnos; los directores pueden inspeccionar a los profesores y a los alumnos, y los administradores, a los directores, a los profesores y a los alumnos.

Cuando se solicitan credenciales de inspección con Apple School Manager, se emite una cuenta especial que tiene acceso solo al ID de Apple gestionado para el que se haya solicitado la inspección. El inspector puede entonces leer y modificar el contenido del usuario guardado en iCloud o en apps en las que el servicio CloudKit está activado. Cada solicitud de acceso de auditoría se registra en Apple School Manager. Los registros muestran quién ha sido el inspector, para qué ID de Apple gestionado el inspector ha solicitado acceso, cuándo se ha realizado la solicitud y si la inspección se ha llevado a cabo o no.

ID de Apple gestionados y dispositivos personales

Los ID de Apple gestionados también se pueden utilizar con dispositivos iOS y iPadOS, y ordenadores Mac personales. Los alumnos pueden iniciar sesión en iCloud con el ID de Apple gestionado emitido por la institución y una contraseña adicional de uso personal que sirve de segundo factor en el proceso de autenticación de doble factor del ID de Apple. Cuando los alumnos utilizan un ID de Apple gestionado en un dispositivo personal, el llavero de iCloud no está disponible y la institución puede restringir otras prestaciones como FaceTime o Mensajes. Todos los documentos de iCloud creados por alumnos con su sesión iniciada se someterán a una auditoría, tal y como se ha descrito anteriormente en este apartado.

iCloud

Descripción general de la seguridad de iCloud

iCloud almacena los contactos, calendarios, fotos, documentos y otra información del usuario, y la mantiene al día automáticamente en todos sus dispositivos. Además, las apps de terceros también pueden usar iCloud para almacenar y sincronizar documentos, así como datos clave-valor para datos de apps según las indicaciones del desarrollador. Los usuarios configuran iCloud iniciando sesión con un ID de Apple y seleccionando qué servicios quieren usar. Los administradores de TI pueden desactivar ciertas funciones de iCloud, como iCloud Drive y la copia de seguridad de iCloud, mediante perfiles de configuración de [gestión de dispositivos móviles \(MDM\)](#).

iCloud utiliza métodos de seguridad robustos y emplea políticas estrictas para proteger los datos del usuario. Antes de cargarse a los servidores de iCloud, la mayoría de los datos de iCloud se encriptan en el dispositivo del usuario mediante unas claves de iCloud generadas por el dispositivo. En el caso de los datos sin encriptación de punto a punto, el dispositivo del usuario carga estas claves de iCloud de forma segura a unos módulos de seguridad de hardware de iCloud que se encuentran en los centros de datos de Apple. Esto permite a Apple ayudar al usuario a recuperar sus datos y desencriptarlos cuando lo necesita (por ejemplo, cuando inicia sesión en un nuevo dispositivo, restaura datos desde una copia de seguridad o accede a sus datos de iCloud a través de un navegador web). Los datos que se transfieren entre los dispositivos del usuario y los servidores de iCloud se encriptan aparte durante su transmisión con TLS, y los servidores de iCloud almacenan los datos del usuario con una capa de encriptación adicional en reposo.

Las claves de encriptación, cuando Apple dispone de ellas, se protegen en los centros de datos de Apple. Cuando se procesan datos almacenados en un centro de datos de terceros, solo se accede a estas claves de encriptación mediante el software de Apple que se ejecuta en servidores seguros, y solo mientras se realiza el procesamiento necesario. Para una mayor privacidad y seguridad, muchos servicios de Apple utilizan la encriptación de punto a punto, lo que significa que los datos de iCloud solo son accesibles para los propios usuarios y solo en los dispositivos de confianza en los que hayan iniciado sesión con su ID de Apple.

Apple ofrece a los usuarios dos opciones para encriptar y proteger los datos que almacenan en iCloud:

- **Protección de datos estándar (el ajuste por defecto):** Los datos de iCloud del usuario se encriptan, las claves de encriptación se almacenan en los centros de datos de Apple y Apple solo puede ayudar a recuperar datos y cuentas. Solo tienen encriptación de punto a punto determinados datos de iCloud (14 categorías de datos, entre los que se incluyen los datos de Salud y las contraseñas del llavero de iCloud).
- **Protección de datos avanzada para iCloud:** Un ajuste opcional que ofrece el máximo nivel de la seguridad de los datos en la nube de Apple. Si un usuario decide activar la protección de datos avanzada, solo es posible acceder a las claves de encriptación de la mayoría de los datos de iCloud desde los dispositivos de confianza del usuario, donde se protegen mediante encriptación de punto a punto. Cuando se activa la protección de datos avanzada, el número de categorías de datos que utilizan la encriptación de punto a punto aumenta a 23 e incluye la copia de seguridad de iCloud, Fotos y Notas, entre otras.

En el artículo de soporte técnico de Apple [Información general sobre la seguridad de los datos de iCloud](#), se especifican las categorías de datos de iCloud protegidas con encriptación de punto a punto.

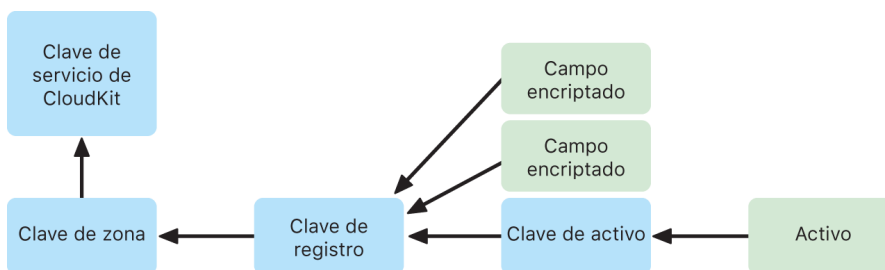
Encriptación de iCloud

La encriptación de datos en iCloud está directamente relacionada con el modelo de almacenamiento de datos, empezando por las API y estructuras de CloudKit que permiten que las apps y el software del sistema almacenen datos en iCloud en nombre del usuario y mantienen todo actualizado en todos los dispositivos y en la web.

Encriptación de CloudKit

CloudKit es una estructura que permite a los desarrolladores de apps almacenar en iCloud datos de clave-valor, datos estructurados y activos (datos de gran tamaño almacenados fuera de la base de datos, como imágenes y vídeos). CloudKit es compatible con bases de datos tanto públicas como privadas, agrupadas en contenedores. Las bases de datos públicas, que suelen utilizarse para activos genéricos, se comparten de forma global y no están encriptadas. Los datos de iCloud del usuario se almacenan en las bases de datos privadas.

CloudKit utiliza una jerarquía de claves que coincide con la estructura de los datos. La base de datos privada de cada contenedor está protegida por una jerarquía de claves, con una raíz de clave asimétrica llamada *clave de servicio de CloudKit*. Estas claves son únicas para cada usuario de iCloud y se generan en el dispositivo de confianza. Cuando los datos se escriben en CloudKit, todas las claves de registro se generan en el dispositivo de confianza del usuario y, antes de subir ningún dato, se encapsulan con la jerarquía de claves adecuada.



Muchos servicios de Apple, enumerados en el artículo de soporte de Apple [Información general sobre la seguridad de los datos de iCloud](#), emplean la encriptación de punto a punto con una clave de servicio de CloudKit protegida por la sincronización del llavero de iCloud. Para estos contenedores de CloudKit, las claves de servicio se almacenan en el llavero de iCloud del usuario y comparten las características de seguridad del llavero de iCloud: las claves están disponibles únicamente en los dispositivos de confianza del usuario y ni Apple ni ningún tercero pueden acceder a ellas. Si pierden su dispositivo, los usuarios pueden recuperar los datos del llavero de iCloud a través de la [recuperación segura del llavero de iCloud](#), los [contactos de recuperación de la cuenta](#) o una clave de recuperación de cuenta.

Gestión de claves de encriptación

La seguridad de los datos encriptados en CloudKit depende de la seguridad de las correspondientes claves de encriptación. Las claves del servicio CloudKit se dividen en dos categorías: con encriptación de punto a punto y disponibles tras la autenticación.

- **Claves de servicio con encriptación de punto a punto:** Para los servicios de iCloud con encriptación de punto a punto, las claves privadas de servicio de iCloud pertinentes nunca están disponibles para los servidores de Apple. Las parejas de claves de servicio, incluidas las privadas, se crean en local en un dispositivo de confianza del usuario y se transfieren a los otros dispositivos del usuario mediante el uso de la [seguridad del llavero de iCloud](#). Aunque los flujos de recuperación y sincronización del llavero de iCloud están mediados por los servidores de Apple, estos servidores tienen el acceso a cualquiera de los datos del llavero del usuario bloqueado por medios criptográficos. En el caso extremo de que el usuario perdiera el acceso al llavero de iCloud y a todos los mecanismos de recuperación, perdería los datos con encriptación de punto a punto de CloudKit. Apple no puede ayudar a recuperar estos datos.
- **Claves de servicio disponibles tras la autenticación:** Para otros servicios, como Fotos y iCloud Drive, las claves de servicio se almacenan en los módulos de seguridad de hardware de iCloud de los centros de datos de Apple y son accesibles para algunos servicios de Apple. Cuando un usuario inicia sesión en iCloud desde un nuevo dispositivo y autentica su ID de Apple, estas claves son accesibles para los servidores de Apple sin la intervención del usuario. Por ejemplo, el usuario puede ver sus fotos en línea nada más iniciar sesión en iCloud.com. Estas claves de servicio son *claves disponibles tras la autenticación*.

Protección de datos avanzada para iCloud

La protección de datos avanzada para iCloud es un ajuste opcional que ofrece el máximo nivel de seguridad de los datos en la nube de Apple. Cuando un usuario decide activar la protección de datos avanzada, solo es posible acceder a las claves de encriptación de la mayoría de los datos de iCloud desde los dispositivos de confianza del usuario, donde se protegen con *encriptación de punto a punto*. Para los usuarios que activen la protección de datos avanzada, el número total de categorías de datos protegidos por la encriptación de punto a punto aumenta de 14 a 23 e incluye la copia de seguridad de iCloud, Fotos y Notas, entre otras.

La protección de datos avanzada para iCloud estará disponible para los usuarios de Estados Unidos a finales de 2022 y empezará a llegar al resto del mundo a principios de 2023.

Conceptualmente, la protección de datos avanzada es muy sencilla: todas las claves de servicio de CloudKit que se generaron en el dispositivo y, después, se subieron a los módulos de seguridad de hardware (HSM) de iCloud *disponibles tras la autenticación* de los centros de datos de Apple, se eliminan de dichos módulos y, en su lugar, se conservan íntegros en el dominio de protección del llavero de iCloud de la cuenta. Estas se gestionan como las claves de servicio *con encriptación de punto a punto* existentes, lo que significa que Apple ya no puede leer ni acceder a las claves.

La protección de datos avanzada también protege automáticamente los campos de CloudKit que los desarrolladores de terceros eligen marcar como encriptados, así como todos los activos de CloudKit.

Activar la protección de datos avanzada

Cuando el usuario activa la protección de datos avanzada, su dispositivo de confianza ejecuta dos acciones: en primer lugar, comunica la intención del usuario de activar la protección de datos avanzada en el resto de sus dispositivos que participen en la encriptación de punto a punto. Para ello, escribe un nuevo valor, firmado por las claves locales del dispositivo, en los metadatos del dispositivo del llavero de iCloud. Los servidores de Apple no pueden eliminar ni modificar esta acreditación mientras se sincronizan con el resto de los dispositivos del usuario.

En segundo lugar, el dispositivo inicia la eliminación de las claves de servicio *disponibles tras la autenticación* de los centros de datos de Apple. Dado que los HSM protegen estas claves, esta eliminación es inmediata, permanente e irrevocable. Una vez eliminadas las claves, Apple no puede seguir accediendo a *ninguno* de los datos protegidos por las claves de servicio del usuario. A partir de ese instante, el dispositivo comienza una operación de rotación de claves asíncrona que crea una nueva clave de servicio para cada uno de los servicios cuya clave haya estado disponible alguna vez para los servidores de Apple. Si la rotación de claves falla, debido a una caída de la red o a cualquier otro error, el dispositivo seguirá intentando rotar las claves hasta conseguirlo.

Una vez que haya conseguido rotar las claves, los datos nuevos que se escriban en el servicio no podrán desencriptarse con la clave de servicio antigua. Está protegida por la clave nueva que está bajo el control exclusivo de los dispositivos de confianza del usuario y que nunca estuvo disponible para Apple.

Protección de datos avanzada y acceso web a iCloud.com

Cuando un usuario activa la protección de datos avanzada por primera vez, el acceso web a los datos que tiene alojados en iCloud.com queda desactivado automáticamente. Esto se debe a que los servidores web de iCloud dejan de tener acceso a las claves necesarias para desencriptar y mostrar los datos del usuario. El usuario puede elegir activar de nuevo el acceso web y utilizar la participación de su dispositivo de confianza para acceder a sus datos de iCloud encriptados en la web.

Una vez activado el acceso web, el usuario tendrá que autorizar el inicio de sesión web en uno de sus dispositivos de confianza cada vez que visite iCloud.com. La autorización "arma" al dispositivo para el acceso web. Durante la hora inmediatamente posterior, este dispositivo aceptará las solicitudes de ciertos servidores de Apple para cargar determinadas claves de servicio, pero solo aquellas que estén incluidas en una lista de servicios permitidos accesibles normalmente en iCloud.com. En otras palabras, aun después de que el usuario autorice un inicio de sesión web, una solicitud de servidor será incapaz de inducir al dispositivo del usuario a cargar claves de servicio para datos que no se vean en iCloud.com (por ejemplo, los datos de Salud o las contraseñas del llavero de iCloud). Los servidores de Apple solo solicitan las claves de servicio necesarias para desencriptar los datos concretos que el usuario está solicitando para acceder a la web. Cada vez que se carga una clave de servicio, esta se encripta a través de un vínculo de clave efímero a la sesión web autorizada por el usuario, y se muestra una autorización en el dispositivo del usuario que muestra el servicio de iCloud cuyos datos están disponibles para los servidores de Apple de forma temporal.

Preservar las elecciones del usuario

El usuario es el único que puede modificar los ajustes de la protección de datos avanzada y el acceso web a iCloud.com. Estos valores se almacenan en los metadatos del dispositivo del llavero de iCloud del usuario y solo pueden cambiarse desde uno de sus dispositivos de confianza. Los servidores de Apple no pueden modificar estos ajustes por el usuario ni pueden devolverlos a una configuración anterior.

Implicaciones para la seguridad del intercambio de datos y la colaboración

En la mayoría de los casos, cuando los usuarios comparten contenido para colaborar entre ellos —por ejemplo, con Notas compartidas, Recordatorios compartidos, carpetas compartidas en iCloud Drive o la fototeca compartida de iCloud— y todos los usuarios tienen activada la protección de datos avanzada, los servidores de Apple solo se utilizan para establecer el intercambio pero no tienen acceso a las claves de encriptación de los datos compartidos. El contenido sigue teniendo encriptación de punto a punto y solo es accesible desde los dispositivos de confianza de los participantes. Para cada operación de intercambio, Apple podría almacenar un título y una imagen en miniatura representativa con la protección de datos estándar para mostrar una previsualización a los receptores de los datos.

Cuando, al permitir la colaboración, se selecciona la opción “cualquiera que tenga un enlace”, el contenido se pone a disposición de los servidores de Apple con la protección de datos estándar, ya que los servidores necesitan poder proporcionar acceso a cualquiera que abra la URL.

La colaboración con iWork y la función de álbumes compartidos de Fotos no son compatibles con la protección de datos avanzada. Cuando los usuarios colaboran en un documento de iWork o abren un documento de iWork desde una carpeta compartida en iCloud Drive, las claves de encriptación del documento se cargan de forma segura a los servidores de iWork de los centros de datos de Apple. Esto es así debido a que la colaboración en tiempo real en iWork requiere la mediación del lado del servidor para coordinar los cambios en los documentos entre los participantes. Las fotos añadidas a los álbumes compartidos se almacenan con la protección de datos estándar debido a que la función permite que los álbumes se compartan públicamente en la web.

Desactivar la protección de datos avanzada

El usuario puede desactivar la protección de datos avanzada en cualquier momento. Si decide hacerlo:

1. El dispositivo del usuario graba su nueva elección en los metadatos de participación del llavero de iCloud y el ajuste se sincroniza de forma segura en todos sus dispositivos.
2. El dispositivo del usuario carga las claves de servicio de forma segura para todos los servicios *disponibles tras la autenticación* a los HSM de iCloud de los centros de datos de Apple. Esto nunca incluye las claves de servicio con encriptación de punto a punto con la protección de datos estándar, como el llavero de iCloud y los datos de Salud.

El dispositivo carga tanto las claves de servicio originales, generadas antes de haber activado la protección de datos avanzada, como las claves de servicio nuevas que se generaron cuando el usuario activó la función. Esto hace que todos los datos de estos servicios sean accesibles tras la autenticación y devuelve la cuenta a la protección de datos estándar, donde Apple puede volver a ayudar al usuario a recuperar la mayoría de sus datos en caso de perder el acceso a su cuenta.

Datos de iCloud que no están cubiertos por la protección de datos avanzada

Dada la necesidad de interoperar con los sistemas globales de correo electrónico, contactos y calendarios, Mail, Contactos y Calendario de iCloud no tienen encriptación de punto a punto.

iCloud almacena algunos datos sin la protección de las claves de servicio de CloudKit específicas del usuario, aunque la protección de datos avanzada esté activada. Para recibir protección, los campos de registro de CloudKit deben estar declarados como “encriptados” expresamente en el esquema del contenedor, y la lectura y escritura de campos encriptados requiere el uso de [API](#) independientes. La fecha y hora de modificación de un archivo u objeto se utiliza para ordenar la información del usuario, y las sumas de control de los datos de los archivos y fotos se utilizan para ayudar a Apple a deduplicar y optimizar el almacenamiento del usuario en iCloud y su dispositivo. Todo ello, sin tener acceso a los propios archivos y fotos. En el artículo de soporte técnico de Apple [Información general sobre la seguridad de los datos de iCloud](#), encontrarás información sobre cómo se utiliza la encriptación para determinadas categorías de datos.

Decisiones como el uso de sumas de control para la deduplicación de datos —una conocida técnica llamada *encriptación convergente*— formaron parte del diseño original de los servicios de iCloud cuando se presentaron por primera vez. Estos metadatos siempre están encriptados, pero Apple almacena las claves de encriptación con protección de datos estándar. Para seguir reforzando los mecanismos de protección de la seguridad para todos los usuarios, Apple se ha comprometido a que, cuando se active la protección de datos avanzada, se encripten más datos de punto a punto, incluidos estos metadatos.

Requisitos de la protección de datos avanzada

Estos son los requisitos para activar la protección de datos avanzada para iCloud:

- La cuenta del usuario debe ser compatible con la encriptación de punto a punto. La encriptación de punto a punto requiere que el usuario haya configurado la autenticación de doble factor para su ID de Apple y un código de acceso o contraseña en sus dispositivos de confianza. Para obtener más información, consulta el artículo de soporte técnico de Apple [Autenticación de doble factor para el ID de Apple](#).
- Los dispositivos en los que el usuario haya iniciado sesión con su ID de Apple deben estar actualizados a iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 y la versión más reciente de iCloud para Windows. Este requisito evita que una versión previa de iOS, iPadOS, macOS, tvOS o watchOS utilice indebidamente las claves de servicio recién creadas volviéndolas a cargar a los HSM *disponibles tras la autenticación* en un intento errado de reparar el estado de la cuenta.
- El usuario debe configurar al menos un método de recuperación alternativo —uno o más contactos de recuperación o una clave de recuperación— que puedan utilizar para recuperar sus datos de iCloud si pierden el acceso a su cuenta.

Si los métodos de recuperación fallan —por ejemplo, si la información del contacto de configuración está desactualizada o el usuario la olvida—, Apple no puede ayudar a recuperar los datos de iCloud con encriptación de punto a punto del usuario.

La protección de datos avanzada para iCloud solo puede activarse para los ID de Apple. Los ID de Apple gestionados y las cuentas secundarias (varía en función del país o región) no son compatibles.

Seguridad de la copia de seguridad de iCloud

iCloud guarda copias de seguridad de la información —incluidos los ajustes del dispositivo, los datos de las apps, las fotos y los vídeos del carrete y las conversaciones de la app Mensajes— todos los días por wifi. La copia de seguridad de iCloud solo se hace cuando el dispositivo está bloqueado y enchufado a una fuente de alimentación y tiene acceso wifi a internet. Debido a la encriptación del almacenamiento que se usa en iOS y iPadOS, la copia de seguridad de iCloud en iOS y iPadOS se ha diseñado para mantener protegidos los datos y, al mismo tiempo, permitir que se realicen copias de seguridad progresivas y desatendidas, y restauraciones. Por defecto, la clave de servicio de la copia de seguridad de iCloud se guarda en una copia de seguridad segura en los módulos de seguridad de hardware de iCloud de los centros de datos de Apple, y está incluida en la categoría de datos disponibles tras la autenticación. Para los usuarios que activen la protección de datos avanzada para iCloud, la clave de servicio de la copia de seguridad de iCloud está protegida con encriptación de punto a punto, y solo está disponible para los usuarios en sus dispositivos de confianza.

Cuando los archivos se crean en clases de [protección de datos](#) a las que no se puede acceder cuando el archivo está bloqueado, las [claves por archivo](#) correspondientes se encriptan con las claves de clase del [repositorio de claves](#) de la copia de seguridad de iCloud y se realiza una copia de seguridad de los archivos en iCloud en su estado encriptado original. Todos los archivos se encriptan durante el transporte y, cuando se almacenan, se encriptan usando claves basadas en las cuentas, como se describe en [Encriptación de CloudKit](#).

El repositorio de claves de la copia de seguridad de iCloud contiene claves asimétricas (Curve25519) para las clases de protección de datos que no son accesibles cuando el dispositivo está bloqueado. El conjunto de copias de seguridad se almacena en la cuenta de iCloud del usuario y consiste en una copia de los archivos del usuario y el repositorio de claves de la copia de seguridad de iCloud. Este repositorio está protegido mediante una clave aleatoria, que también está almacenada en el conjunto de copias de seguridad. La contraseña de iCloud del usuario no se usa para la encriptación. De este modo, el cambio de contraseña de iCloud no invalida las copias de seguridad existentes.

Al restaurarlo, los archivos de los que se ha realizado la copia de seguridad, el repositorio de claves de la copia de seguridad de iCloud y la clave para el repositorio de claves se recuperan de la cuenta de iCloud del usuario. El repositorio de claves de la copia de seguridad de iCloud se desencripta usando su clave, a continuación, las claves por archivo del repositorio de claves se usan para desencriptar los archivos del conjunto de copias de seguridad, que se escriben como archivos nuevos en el sistema de archivos y, de este modo, se vuelven a encriptar según la clase de protección de datos correspondiente.

Con la copia de seguridad de iCloud se guarda una copia del siguiente contenido:

- Los registros de música, vídeos, programas de televisión, apps y libros comprados. La copia de seguridad de iCloud de un usuario incluye información sobre el contenido comprado en el dispositivo del usuario, pero no el propio contenido comprado. Cuando el usuario restaura contenido a partir de una copia de seguridad de iCloud, lo que ha comprado se descarga automáticamente de iTunes Store, App Store, la app Apple TV o la app Libros. Algunos tipos de contenido no se descargan automáticamente en todos los países o regiones y es posible que haya compras antiguas que no estén disponibles si se ha reembolsado su importe o si ya no están disponibles en su respectiva tienda. El historial completo de compra está asociado al ID de Apple de un usuario.

- Las fotos y vídeos guardados en los dispositivos de un usuario. Ten en cuenta que si un usuario activa "Fotos en iCloud" en iOS 8.1, iPadOS 13.1 u OS X 10.10.3, o posterior, las fotos y los vídeos ya estarán almacenados en iCloud, de modo que no se incluirán en la copia de seguridad de iCloud del usuario.
- Los contactos, eventos de calendario, recordatorios y notas.
- Los ajustes de los dispositivos.
- Los datos de las apps.
- La organización de la pantalla de inicio y las apps.
- La configuración de HomeKit.
- Datos médicos.
- La contraseña de Notas de Voz (en caso necesario, se requiere la tarjeta SIM física que se estaba utilizando durante la copia de seguridad).
- Mensajes, Apple Messages for Business, los mensajes de texto (SMS) y MMS (en caso necesario, se requiere la tarjeta SIM física que se estaba utilizando durante la copia de seguridad).

La copia de seguridad de iCloud también se utiliza para hacer una copia de seguridad de la cadena de claves local del dispositivo, encriptada con una clave derivada de la clave criptográfica raíz UID del Secure Enclave del dispositivo. Esta clave es única del dispositivo y Apple no la conoce. Esto permite que la base de datos solo se pueda restaurar en el mismo dispositivo en el que se originó, es decir, nadie (ni siquiera Apple) podrá leerla. Para obtener más información, consulta [Secure Enclave](#).

Mensajes en iCloud

Mensajes en iCloud mantiene actualizado el historial de mensajes del usuario, que está disponible en todos los dispositivos.

Con la protección de datos estándar, Mensajes en iCloud se encripta de punto a punto cuando se desactiva la copia de seguridad de iCloud. Cuando se activa la copia de seguridad de iCloud, incluye una copia de la clave de encriptación de Mensajes en iCloud para que Apple pueda ayudar al usuario a recuperar sus mensajes aunque haya perdido el acceso al llavero de iCloud y sus dispositivos de confianza. Si el usuario desactiva la copia de seguridad de iCloud, se genera una nueva clave en el dispositivo para proteger Mensajes en iCloud en el futuro. La nueva clave solo se almacena en el llavero, al que solo puede acceder el usuario en sus dispositivos de confianza, y los nuevos datos que se escriban en el contenedor no pueden desencriptarse con la clave de contenedor antigua.

Con la protección de datos avanzada, Mensajes en iCloud siempre se encripta de punto a punto. Cuando la copia de seguridad de iCloud se activa, todo lo que hay dentro tiene encriptación de punto a punto, incluida la clave de encriptación de Mensajes en iCloud. Cuando el usuario activa la protección de datos avanzada, se sustituyen tanto la clave de servicio de la copia de seguridad de iCloud como la clave de contenedor de Mensajes en iCloud. Para obtener más información, consulta el artículo de soporte técnico de Apple [Información general sobre la seguridad de los datos de iCloud](#).

Seguridad del contacto de recuperación de la cuenta

Los usuarios pueden añadir hasta cinco personas de su confianza como contactos de recuperación de la cuenta para que les ayuden a recuperar su cuenta y sus datos de iCloud, incluidos los datos con encriptación de punto a punto, tengan o no activada la protección de datos avanzada. Ni Apple ni el contacto de recuperación tienen la información necesaria individualmente para recuperar los datos de iCloud con encriptación de punto a punto del usuario.

Los contactos de recuperación se han diseñado teniendo en cuenta la privacidad del usuario. Apple desconoce los contactos de recuperación elegidos por el usuario. Los servidores de Apple solo conocen información sobre un contacto de recuperación al final de un intento de recuperación, cuando el usuario ha pedido ayuda al contacto y su contacto ya ha empezado a ayudarlo con la recuperación. Una vez concluida la recuperación, esa información no se retiene.

Proceso de seguridad del contacto de recuperación

Cuando un usuario configura un contacto de recuperación de cuenta, la clave para acceder a los datos de iCloud del usuario —incluidos los datos de CloudKit con encriptación de punto a punto— se encripta con una clave aleatoria segura. Esta clave aleatoria se divide, entonces, entre el contacto de recuperación y Apple. En el momento de la recuperación, solo se puede recuperar la clave original y acceder a los datos de iCloud del usuario cuando se vuelven a combinar ambas partes.

Para configurar un contacto de recuperación de cuenta, el dispositivo del usuario se comunica con los servidores de Apple para subir la parte de la información de la clave que tendrá Apple. A continuación, establece un contenedor de CloudKit con encriptación de punto a punto con el contacto de recuperación para compartir la parte que el contacto de recuperación necesita. Tanto Apple como el contacto de recuperación reciben el mismo secreto de autorización del usuario, que luego es necesario para la recuperación. La comunicación para invitar y aceptar a los contactos de recuperación tiene lugar a través de un canal de IDS autenticado mutuamente. El contacto de recuperación almacena automáticamente la información recibida en su llavero de iCloud. Apple no puede acceder al contenido del contenedor de CloudKit ni al llavero de iCloud que almacena esta información. Cuando se comparte esa parte, los servidores de Apple solo ven un ID anónimo para el contacto de recuperación.

Más adelante, cuando un usuario necesite recuperar su cuenta y sus datos de iCloud, podrá solicitar ayuda a su contacto de recuperación. En ese momento, el dispositivo del contacto de recuperación genera un código de recuperación, que el contacto de recuperación proporciona al usuario fuera de red (por ejemplo, en persona o mediante una llamada telefónica). A continuación, el usuario introduce este código de recuperación en su dispositivo para establecer una conexión segura entre dispositivos mediante el protocolo SPAKE2+, cuyo contenido no es accesible para Apple. Esta interacción está orquestada por los servidores de Apple, pero Apple no puede iniciar el proceso de recuperación.

Una vez establecida la conexión segura y completadas todas las comprobaciones de seguridad necesarias, el dispositivo del contacto de recuperación devuelve al usuario que solicita la recuperación su parte de la información de la clave y el secreto de autorización establecido anteriormente. El usuario presenta este secreto de autorización a un servidor de Apple, lo cual otorga acceso a la información de la clave que Apple almacena. La presentación del secreto de autorización también autoriza el restablecimiento de la contraseña de la cuenta para restaurar el acceso a la misma.

Por último, el dispositivo del usuario vuelve a combinar la información de la clave recibida de Apple y el contacto de recuperación de cuenta, y después lo usa para descifrar y recuperar sus datos de iCloud.

Existen medidas de seguridad para impedir que un contacto de recuperación inicie la recuperación sin el consentimiento del usuario, que incluyen un control de vivacidad en la cuenta del usuario. Si la cuenta se está usando activamente, la recuperación empleando un contacto de recuperación también requiere conocer un código del dispositivo reciente o el código de seguridad de iCloud.

Seguridad del representante digital

Si un usuario quiere que sus datos de iCloud sean accesibles para los beneficiarios designados después de su muerte, puede establecer representantes digitales en su cuenta. Un beneficiario de representante digital obtiene acceso a todos los datos de iCloud de la persona fallecida, incluidos casi todos los datos con encriptación de punto a punto pero no los datos del llavero de iCloud, como las contraseñas de las cuentas. La tecnología que subyace al representante digital es similar al funcionamiento del contacto de recuperación una clave aleatoria segura se divide entre Apple y el representante digital para que ninguno de los dos puedan descifrar ningún dato por sí mismo. Un beneficiario recibe las mismas clases de datos, con independencia de si el usuario activó o no la protección de datos avanzada.

La información de clave que recibe un beneficiario se denomina "clave de acceso" en la documentación dirigida al usuario final, y se guarda automáticamente en los dispositivos compatibles, pero también puede imprimirse y almacenarse sin conexión para su uso. Para obtener más información, consulta el artículo de soporte técnico de Apple [Cómo añadir un representante digital al ID de Apple](#).

Tras el fallecimiento del usuario, los representantes digitales se registran en el sitio web de reclamaciones de Apple para iniciar el acceso. Esto requiere un certificado de defunción y se autoriza en parte con el secreto de autorización mencionado en la sección anterior. Una vez completadas todas las comprobaciones de seguridad, Apple emite un nombre de usuario y una contraseña para la nueva cuenta y entrega la información de la clave necesaria al representante digital.

Para facilitar la introducción de la clave de acceso cuando sea necesario, esta se presenta como un código alfanumérico con un código QR asociado. Una vez introducida, la clave de acceso se usa para restaurar los datos de iCloud de la persona fallecida. Esto puede realizarse en un dispositivo, o el acceso puede establecerse en línea. Para obtener más información, consulta el artículo de soporte técnico de Apple [Solicitar acceso a una cuenta de Apple como representante digital](#).

Seguridad del relay privado de iCloud

El relay privado de iCloud ayuda a proteger a los usuarios principalmente cuando navegan por la web con Safari, pero también incluye todas las solicitudes de resolución de nombres DNS. Esto ayuda a impedir que ningún tercero, ni siquiera Apple, pueda correlacionar la dirección IP del usuario y su actividad de navegación. Lo hace usando diferentes proxies, un proxy de entrada, gestionado por Apple, y un proxy de salida, gestionado por un proveedor de contenidos. Para usar el relay privado de iCloud, el usuario debe utilizar iOS 15, iPadOS 15 o macOS 12.0.1, o posterior, y haber iniciado sesión en su cuenta de iCloud+ con su ID de Apple. El relay privado de iCloud se puede activar en Ajustes > iCloud o Ajustes del Sistema > iCloud.

Para obtener más información, consulta [Introducción al relay privado de iCloud](#).

Gestión del código y de la contraseña

Descripción general de la seguridad de la contraseña

iOS, iPadOS y macOS permiten a los usuarios autenticarse de manera sencilla en sitios web y apps de terceros que usan contraseñas. La mejor manera de gestionar las contraseñas es no tener que usar una. “Iniciar sesión con Apple” permite a los usuarios iniciar sesión en sitios web y apps de terceros sin tener que crear ni gestionar una cuenta o contraseña adicional con la protección que proporciona la autenticación de doble factor del ID de Apple. Para los sitios que no son compatibles con “Iniciar sesión con Apple”, la función “Contraseñas seguras automáticas” permite que los dispositivos de un usuario puedan crear, sincronizar e introducir de forma automática contraseñas seguras y únicas para sitios y apps. En iOS y iPadOS, las contraseñas se guardan en el llavero especial “Autorrelleno de contraseñas” controlado por el usuario que se puede gestionar en Ajustes > Contraseñas.

En macOS, las contraseñas guardadas se pueden gestionar en las preferencias de “Contraseñas de Safari”. Este sistema de sincronización también se puede usar para sincronizar las contraseñas creadas manualmente por el usuario.

Seguridad de “Iniciar sesión con Apple”

“Iniciar sesión con Apple” es una alternativa a otros sistemas de inicio de sesión único que respeta la privacidad. Ofrece la comodidad y eficacia de iniciar sesión con un solo toque mientras que el usuario obtiene más transparencia y control sobre sus datos personales.

“Iniciar sesión con Apple” permite a los usuarios configurar una cuenta e iniciar sesión en apps y sitios web con el ID de Apple que ya tienen, lo cual les da más control sobre sus datos personales. Las apps solo piden el nombre y la dirección de correo electrónico del usuario a la hora de configurar una cuenta y el usuario siempre tiene la posibilidad de elegir: puede compartir su dirección de correo electrónico personal con la app, o bien optar por mantener esa dirección en privado y usar en su lugar el nuevo servicio de transmisión de correos electrónicos privados de Apple. De este modo, el servicio de transmisión de correos electrónicos comparte una dirección de correo electrónico única y anónima que reenviará los correos electrónicos a la dirección personal del usuario para que puedan seguir recibiendo comunicación útil del desarrollador al tiempo que mantienen cierto grado de privacidad y control sobre su información personal.

“Iniciar sesión con Apple” se ha creado teniendo en cuenta la seguridad. Cada usuario de “Iniciar sesión con Apple” debe tener activada la autenticación de doble factor para su ID de Apple. La autenticación de doble factor ayuda a proteger el ID de Apple y también las cuentas que establecen con sus apps. Además, Apple ha desarrollado e integrado en “Iniciar sesión con Apple” una señal antifraude que respeta la privacidad. Esta señal da a los desarrolladores la seguridad de que los nuevos usuarios que obtienen son personas reales y no bots ni cuentas de scripts.

Contraseñas seguras automáticas

Cuando el llavero de iCloud está activado, iOS, iPadOS y macOS crean contraseñas seguras, aleatorias y únicas cuando los usuarios se registran en un sitio web en Safari o cambian su contraseña en él. En iOS y iPadOS, la generación de contraseñas seguras automáticas también está disponible en las apps. Para dejar de utilizar contraseñas seguras, los usuarios deben desactivar esta función. Las contraseñas generadas se guardan en el llavero y se mantienen actualizadas entre dispositivos con el llavero de iCloud cuando está activado.

Por defecto, las contraseñas generadas por iOS y iPadOS tienen 20 caracteres de longitud. Contienen un dígito, un carácter en mayúscula, dos guiones y 16 caracteres en minúscula. Estas contraseñas generadas son seguras y contienen 71 bits de entropía.

Las contraseñas se generan basándose en una heurística que determina que una experiencia con un campo de contraseña es para crear una contraseña. Si la heurística no logra reconocer una contraseña contextual usada para crear una contraseña, los desarrolladores de apps pueden establecer `UITextContentType.newPassword` en su campo de texto y los desarrolladores web pueden establecer `autocomplete= "new-password"` en sus elementos `<input>`.

Para ayudar a garantizar que las contraseñas generadas son compatibles con el servicio en cuestión, las apps y los sitios web pueden proporcionar reglas. Los desarrolladores proporcionan estas reglas mediante `UITextFieldPasswordRules` o el atributo `passwordrules` de sus elementos `input`. A continuación, los dispositivos generan la contraseña más segura posible que cumple estas reglas.

Seguridad de "Autorrelleno de contraseñas"

"Autorrelleno de contraseñas" rellena automáticamente las credenciales almacenadas en el llavero. El gestor de contraseñas del llavero de iCloud y "Autorrelleno de contraseñas" proporcionan las siguientes funciones:

- Rellenar credenciales en apps y sitios webs.
- Generar contraseñas seguras.
- Guardar contraseñas en apps y sitios web en Safari.
- Compartir contraseñas de manera segura con los contactos de un usuario.
- Proporcionar contraseñas a un Apple TV cercano que solicite credenciales.

Solo se pueden generar y guardar contraseñas desde las apps, además de proporcionar contraseñas al Apple TV, en iOS y iPadOS.

Autorrelleno de contraseñas en apps

iOS y iPadOS permiten a los usuarios introducir en los campos de las credenciales presentes en apps los nombres de usuario y contraseñas guardados. Su funcionamiento es similar al de "Autorrelleno de contraseñas" en Safari. Para ello, en iOS y iPadOS, los usuarios pulsán una llave en la barra QuickType del teclado. En macOS, para las apps creadas con Mac Catalyst, aparece el menú desplegable Contraseñas debajo de los campos de las credenciales.

Cuando una app se asocia a un sitio web de forma segura con el mismo mecanismo de apple-app-site-association, gracias al mismo archivo apple-app-site-association, en la barra QuickType de iOS y iPadOS y en el menú desplegable de macOS aparecerán directamente como sugerencias las credenciales para la app, si se ha guardado alguna en el llavero "Autorrelleno de contraseñas". Esto permite a los usuarios decidir si quieren compartir o no las credenciales guardadas en Safari con las apps que tengan las mismas propiedades de seguridad sin que esas apps tengan que adoptar una API.

"Autorrelleno de contraseñas" no revela ninguna información sobre credenciales a una app hasta obtener el consentimiento del usuario para revelar una credencial. La lista de credenciales se presenta o se extrae del proceso de la app.

Cuando una app y un sitio web tienen una relación de confianza y un usuario envía credenciales desde una app, iOS y iPadOS pueden preguntar al usuario si quiere guardar esas credenciales en el llavero "Autorrelleno de contraseñas" para usarlas en el futuro.

Acceso de las apps a las contraseñas guardadas

Las apps de iOS, iPadOS y macOS pueden solicitar la ayuda del llavero "Autorrelleno de contraseñas" con el inicio de sesión de un usuario mediante `ASAuthorizationPasswordProvider` y `SecAddSharedWebCredential`. El proveedor de la contraseña y su solicitud se pueden usar junto con "Iniciar sesión con Apple" para que se llame a la misma API para ayudar a los usuarios a iniciar sesión en una app, independientemente de si la cuenta de usuario se basa en una contraseña o se creó mediante "Iniciar sesión con Apple".

Las apps solo pueden acceder a las contraseñas guardadas si tanto el desarrollador de la app como el administrador del sitio web han dado su aprobación y el usuario, su consentimiento. Los desarrolladores de apps incluyen una autorización en su app para expresar su intención de acceder a las contraseñas guardadas de Safari. La autorización enumera los nombres de dominio completos de los sitios web asociados. Por su parte, los sitios web deben colocar un archivo en su servidor en el que figuren los identificadores de apps únicos de las apps que Apple ha aprobado.

Cuando se instala una app con la autorización `com.apple.developer.associated-domains`, iOS y iPadOS envían una solicitud de TLS a cada sitio web de la lista para solicitar uno de los archivos siguientes:

- `apple-app-site-association`
- `.well-known/apple-app-site-association`

Si el archivo incluye el identificador de apps de la app que se está instalando, iOS y iPadOS marcarán que el sitio web y la app tienen una relación de confianza. Las llamadas a estas dos API solo generan una solicitud para el usuario cuando existe una relación de confianza; para que se lleve a cabo la entrega de contraseñas a la app o para que se actualicen o eliminen, es necesaria la aceptación del usuario.

Recomendaciones de seguridad de contraseñas

La lista de contraseñas de "Autorrelleno de contraseñas" en iOS, iPadOS y macOS indica qué contraseñas guardadas del usuario se han *reutilizado* en otros sitios web, cuáles de esas contraseñas se consideran *poco seguras* y cuáles se han visto comprometidas debido a una *filtración de datos*.

Descripción general

Usar la misma contraseña para más de un servicio puede hacer que esas cuentas sean vulnerables a un ataque de relleno de credenciales. Si se vulnera la seguridad de un servicio y hay una fuga de contraseñas, los atacantes pueden probar las mismas credenciales en otros servicios para poner en riesgo la seguridad de más cuentas.

- Las contraseñas se marcan como *reutilizadas* si se detecta que la misma contraseña se ha utilizado para más de una contraseña guardada en diferentes dominios.
- Las contraseñas se marcan como *poco seguras* si un atacante puede adivinarlas fácilmente. iOS, iPadOS y macOS detectan los patrones comunes que se usan para crear contraseñas fáciles de recordar, como usar las palabras de un diccionario, la sustitución de caracteres comunes (como el uso de "c0ntr4señ4" en lugar de "contraseña"), los patrones de un teclado (como "q12we34r" de un teclado QWERTY) o las secuencias repetidas (como "123123"). Estos patrones se suelen usar para crear contraseñas que cumplan los requisitos mínimos de contraseña de los servicios, pero también suelen utilizarlos los atacantes que intentan obtener una contraseña por fuerza bruta.

Dado que muchos servicios solicitan específicamente un código PIN de cuatro o seis dígitos, estos códigos cortos se evalúan con normas diferentes. Los códigos PIN se consideran poco seguros si son uno de los códigos PIN más comunes, si son una secuencia creciente o decreciente (como "1234" o "8765") o si siguen un patrón de repetición (como "123123" o "123321").

- Las contraseñas se marcan como *filtradas* si la función de supervisión de contraseñas puede demostrar que han estado presentes en una filtración de datos. Para obtener más información, consulta [Supervisión de contraseñas](#).

Las contraseñas poco seguras, reutilizadas y filtradas se indican en la lista de contraseñas (macOS) o están presentes en la interfaz dedicada de recomendaciones de seguridad (iOS y iPadOS). Si el usuario inicia sesión en un sitio web en Safari con una contraseña guardada anteriormente que es muy poco segura o que ha aparecido en una filtración de datos, se muestra una alerta conminándole a que la actualice a una contraseña segura automática.

Actualizar la seguridad de autenticación de la cuenta en iOS y iPadOS

Las apps que implementan una extensión de modificación de autenticación de cuentas (en la estructura de los servicios de autenticación) pueden ofrecer actualizaciones sencillas con solo pulsar un botón de las cuentas que usan contraseñas; en concreto, pueden cambiar a "Iniciar sesión con Apple" o empezar a utilizar una contraseña segura automática. Este punto de extensión está disponible en iOS y iPadOS.

Si una app ha implementado el punto de extensión y está instalada en el dispositivo, los usuarios verán opciones de actualización de la extensión al visualizar las recomendaciones de seguridad de las credenciales asociadas con la app en el gestor de contraseñas del llavero de iCloud en Ajustes. Las actualizaciones también se ofrecen cuando los usuarios inician sesión en la app con la credencial en riesgo. Las apps tienen la capacidad de indicar al sistema que no muestre a los usuarios opciones de actualización después de iniciar sesión. Con la nueva API AuthenticationServices, las apps también pueden invocar sus extensiones y realizar actualizaciones, idealmente desde los ajustes de la cuenta o la pantalla de gestión de la cuenta de la app.

Las apps pueden elegir si admiten actualizaciones de contraseña segura, actualizaciones de "Iniciar sesión con Apple" o ambas cosas. En una actualización de contraseña segura, el sistema generará una contraseña segura automática para el usuario. Si es necesario, la app puede proporcionar reglas de contraseña personalizadas que se deben seguir al generar la nueva contraseña. Cuando un usuario cambia una cuenta para dejar de usar una contraseña y utilizar "Iniciar sesión con Apple" en su lugar, el sistema proporciona una nueva credencial de "Iniciar sesión con Apple" a la extensión con la que asociar la cuenta. El correo electrónico del ID de Apple del usuario no se proporciona como parte de la credencial. Tras una actualización correcta de "Iniciar sesión con Apple", el sistema elimina la credencial de contraseña utilizada anteriormente del llavero del usuario si estaba guardada allí.

Las extensiones de modificación de autenticación de cuentas tienen la oportunidad de realizar una autenticación de usuario adicional antes de realizar una actualización. Para las actualizaciones iniciadas en el gestor de contraseñas o después de iniciar sesión en una app, la extensión proporciona el nombre de usuario y la contraseña de la cuenta que actualizar. En el caso de las actualizaciones dentro de la app, solo se proporciona el nombre de usuario. Si la extensión requiere que el usuario se vuelva a autenticar, puede solicitar que se muestre una interfaz de usuario personalizada antes de continuar con la actualización. El caso de uso previsto para mostrar esta interfaz de usuario es solicitar al usuario que introduzca un segundo factor de autenticación para autorizar la actualización.

Supervisión de contraseñas

La supervisión de contraseñas es una función que compara las contraseñas almacenadas en el llavero “Autorrelleno de contraseñas” del usuario con una lista seleccionada y actualizada continuamente de contraseñas de las que se tiene constancia que han aparecido en filtraciones de diferentes organizaciones de internet. Si esta función está activada, el protocolo de supervisión compara continuamente las contraseñas del llavero “Autorrelleno de contraseñas” del usuario con la lista seleccionada.

Funcionamiento de la supervisión

El dispositivo del usuario realiza continuamente comprobaciones por turnos (round robin) de las contraseñas del usuario, realizando consultas a un intervalo que es independiente de las contraseñas del usuario o de los patrones de uso de su gestor de contraseñas. Esto ayuda a garantizar que los estados de verificación permanezcan actualizados con las listas más recientes de contraseñas filtradas. A fin de ayudar a evitar que se filtre información sobre la cantidad de contraseñas únicas que tiene el usuario, las solicitudes se agrupan por lotes y se realizan en paralelo. En cada comprobación se verifica un número fijo de contraseñas en paralelo y, si el usuario tiene menos contraseñas que dicho número, se generarán contraseñas aleatorias y se añadirán a las consultas para compensar la diferencia.

Comparación de las contraseñas

La comparación de contraseñas es un proceso de dos partes. Las contraseñas más filtradas se incluyen en una lista local en el dispositivo del usuario. Si la contraseña del usuario aparece en esta lista, el usuario recibe inmediatamente una notificación sin ninguna interacción externa. Esto está diseñado para garantizar que no se filtre información sobre las contraseñas que tiene un usuario que están más comprometidas debido a una filtración de contraseñas.

Si la contraseña no está incluida en la lista de contraseñas más frecuentes, se comparará con otras contraseñas filtradas con menos frecuencia.

Comparación de contraseñas de los usuarios con una lista seleccionada

Para comprobar si la contraseña que no está presente en la lista local coincide, se requiere cierta interacción con los servidores de Apple. A fin de ayudar a garantizar que no se envíen a Apple contraseñas de usuarios legítimos, se implementa un tipo de *intersección de conjunto privado* criptográfica que compara las contraseñas de los usuarios con un gran conjunto de contraseñas filtradas. De este modo, para las contraseñas con menor riesgo de filtración, se compartirá muy poca información con Apple. Para la contraseña de un usuario, esta información se limita a un prefijo de 15 bits de un hash criptográfico. La eliminación de las contraseñas filtradas con más frecuencia de este proceso interactivo mediante la lista local de contraseñas más filtradas reduce el delta en la frecuencia relativa de contraseñas en los cubos del servicio web, por lo que inferir contraseñas de usuario a partir de estas búsquedas no resulta práctico.

El protocolo subyacente crea particiones de la lista de contraseñas seleccionadas, que contenía aproximadamente 1500 millones de contraseñas en el momento de redactar este manual, en 2^{15} cubos distintos. El cubo al que pertenece la contraseña se basa en los primeros 15 bits del valor del hash SHA256 de la contraseña. Además, cada contraseña filtrada, pw , se asocia con un punto de curva elíptica en la curva P256 de NIST: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, donde α es una clave aleatoria de secreto conocida solo por Apple, y H_{SWU} es una función de Oracle aleatoria que asigna contraseñas a puntos de curva según el método Shallue-van de Woestijne-Ulas. Esta transformación está diseñada para ocultar computacionalmente los valores de contraseñas y contribuye a impedir que se muestren nuevas contraseñas filtradas mediante la función de supervisión de contraseñas.

Para calcular la intersección del conjunto privado, el dispositivo del usuario determina el cubo al que pertenece la contraseña del usuario mediante λ , el prefijo de 15 bits de SHA256(upw), donde upw es una de las contraseñas del usuario. El dispositivo genera su propia constante aleatoria, β , y envía el punto $P_c = \beta \cdot H_{SWU}(upw)$ al servidor, junto con una solicitud para el cubo correspondiente a λ . Aquí, β oculta información sobre la contraseña del usuario y limita a λ la información expuesta de la contraseña a Apple. Por último, el servidor toma el punto enviado por el dispositivo del usuario, calcula $\alpha P_c = \alpha \beta \cdot H_{SWU}(upw)$, y lo devuelve, junto con el cubo de puntos correspondiente $B_\lambda = \{P_{pw} \mid \text{SHA256}(pw) \text{ comienza con el prefijo } \lambda\}$ — al dispositivo.

La información devuelta permite al dispositivo calcular $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ y confirma que la contraseña del usuario se ha filtrado si $\alpha P_c \in B'_\lambda$.

Envío de contraseñas a otros usuarios o dispositivos Apple

Apple envía contraseñas de forma segura a otros usuarios o dispositivos Apple con AirDrop y en el Apple TV.

Cómo guardar credenciales en otro dispositivo con AirDrop

Cuando iCloud está activado, los usuarios pueden usar AirDrop para enviar una credencial guardada a otro dispositivo. La credencial incluye el nombre de usuario y la contraseña y los sitios web para los que está guardada. El envío de credenciales con AirDrop siempre se realiza con el modo "Solo contactos", independientemente de los ajustes del usuario. En el dispositivo receptor, después de que el usuario acepte la transferencia, las credenciales se guardan en el llavero "Autorrelleno de contraseñas" del usuario.

Cómo rellenar credenciales en apps en el Apple TV

En el Apple TV, el autorrelleno de contraseñas está disponible para rellenar credenciales en apps. Cuando el usuario selecciona un campo de texto de nombre de usuario o contraseña en tvOS, el Apple TV empieza a realizar una solicitud de autorrelleno de contraseña a través de Bluetooth de baja energía (BLE).

Cualquier iPhone, iPad o iPod touch cercano mostrará un mensaje invitando al usuario a compartir una credencial con el Apple TV. El método de encriptación se establece del siguiente modo:

- Si el dispositivo y el Apple TV usan la misma cuenta de iCloud, la encriptación entre los dispositivos se produce automáticamente.
- Si el dispositivo ha iniciado sesión en una cuenta de iCloud diferente a la que usa el Apple TV, se le pide al usuario que establezca una conexión encriptada mediante el uso de un código PIN. Para recibir esta solicitud, el iPhone debe estar desbloqueado y cerca del Siri Remote enlazado con el Apple TV.

Una vez establecida la conexión encriptada mediante la encriptación de enlace de BLE, la credencial se envía al Apple TV y se rellena automáticamente en los campos de texto pertinentes de la app.

Extensiones de proveedor de credenciales

En iOS, iPadOS y macOS, los usuarios pueden designar una app de terceros participante como proveedor de credenciales para el autorrelleno de contraseñas en los ajustes de Contraseñas (iOS y iPadOS) o en los ajustes de Extensiones en Preferencias del Sistema (macOS). Este mecanismo se basa en extensiones de apps. La extensión del proveedor de credenciales debe proporcionar una vista para seleccionar credenciales y, opcionalmente, puede proporcionar metadatos sobre credenciales guardadas, que podrán ofrecerse directamente en la barra QuickType (iOS y iPadOS) o en una sugerencia de autocompletar (macOS). Los metadatos incluyen el sitio web de la credencial y el nombre de usuario asociado, pero no su contraseña. iOS, iPadOS y macOS se comunicarán con la extensión para obtener la contraseña cuando el usuario decida introducir una credencial de manera automática en una app o un sitio web en Safari. Los metadatos de credenciales se almacenan dentro del contenedor de apps del proveedor de credenciales y se eliminan automáticamente al desinstalar una app.

Llavero de iCloud

Descripción general de la seguridad del llavero de iCloud

El llavero de iCloud permite a los usuarios sincronizar de forma segura sus contraseñas entre los dispositivos iOS y iPadOS y los ordenadores Mac sin revelar esa información a Apple. Además de un alto grado de privacidad y seguridad, existen otros objetivos que han influido notablemente en el diseño y la arquitectura del llavero de iCloud como, por ejemplo, su facilidad de uso y la posibilidad de recuperarlo. El llavero de iCloud consta de dos servicios: la sincronización del llavero y la recuperación del llavero.

Apple diseñó el llavero de iCloud y la recuperación del llavero para que las contraseñas del usuario se mantuvieran protegidas en las siguientes circunstancias:

- La cuenta de iCloud de un usuario está en peligro.
- iCloud está en peligro a causa de un empleado o ataque externo.
- Terceras personas acceden a las cuentas del usuario.

Integración del gestor de contraseñas con el llavero de iCloud

iOS, iPadOS y macOS pueden generar automáticamente contraseñas aleatorias seguras por criptografía para usarlas como contraseñas de cuentas en Safari. iOS y iPadOS también pueden generar contraseñas seguras para apps. Las contraseñas generadas se almacenan en el [llavero](#) y se sincronizan con otros dispositivos. Los ítems del llavero se transfieren de un dispositivo a otro a través de los servidores de Apple. Sin embargo, están encriptados de manera que ni Apple ni otros dispositivos pueden leer su contenido.

Sincronización segura del llavero

Cuando un usuario activa el llavero de iCloud por primera vez, el dispositivo establece un círculo de confianza y crea una identidad de sincronización para sí mismo. La identidad de sincronización consta de una clave privada y una clave pública, y se almacena en el llavero del dispositivo. La clave pública de la identidad de sincronización se coloca en el círculo y este se firma dos veces: primero, lo firma la clave privada de la identidad de sincronización y, después, una clave de curva elíptica asimétrica (con P-256) derivada de la contraseña de la cuenta de iCloud del usuario. Junto con el círculo, se almacenan los parámetros (sal aleatoria e iteraciones), usados para crear la clave que se basa en la contraseña de iCloud del usuario.

Para las cuentas de autenticación de doble factor, se crea un círculo de sincronización adicional similar que se almacena en CloudKit. Las identidades de los dispositivos en este sistema consisten en dos pares de claves elípticas asimétricas (usando P-384), también almacenadas en el llavero. Cada dispositivo mantiene su propia lista de identidades en las que confía y firma esta lista usando una de sus claves de identidad.

Almacenamiento en iCloud del círculo de sincronización

El círculo de sincronización firmado se almacena en el área de almacenamiento de datos clave-valor de iCloud del usuario. No se puede leer sin conocer la contraseña de iCloud del usuario y no se puede modificar de forma válida sin disponer de la clave privada de la identidad de sincronización de su miembro.

Para las cuentas de autenticación de doble factor, la lista de sincronización de cada dispositivo se almacena en CloudKit. Las listas no se pueden leer sin conocer la contraseña de iCloud del usuario y no se pueden modificar sin disponer de las claves privadas del dispositivo que las posea.

Cómo se añaden los otros dispositivos de un usuario al círculo de sincronización

Los nuevos dispositivos, al iniciar sesión en iCloud, se unen al círculo de sincronización del llavero de iCloud de una de las dos maneras siguientes: emparejándose con un dispositivo del llavero de iCloud existente y siendo patrocinado por él, o usando la recuperación del llavero de iCloud.

Durante los flujos de emparejamiento, el dispositivo solicitante crea nuevas identidades de sincronización tanto para el círculo de sincronización como para las listas de sincronización (para las cuentas de autenticación de doble factor) y las presenta al patrocinador. El patrocinador añade la clave pública del nuevo miembro al círculo de sincronización y vuelve a firmarlo con la identidad de sincronización correspondiente y la clave derivada de la contraseña de iCloud del usuario. El nuevo círculo de sincronización se ubica en iCloud, donde el nuevo miembro lo firma de manera similar. En las cuentas de autenticación de doble factor, el dispositivo patrocinador también proporciona al dispositivo que accede un *comprobante* firmado por sus claves de identidad, que muestra que se debe confiar en el dispositivo solicitante. A continuación, actualiza su lista individual de identidades de sincronización de confianza para incluir al solicitante.

Así, el círculo de sincronización tiene dos miembros y cada uno de ellos dispone de la clave pública del otro. Estos empiezan a intercambiar ítems individuales del llavero mediante el almacenamiento de datos clave-valor de iCloud o los almacenan en CloudKit, usando lo más adecuado en función de la situación. Si ambos miembros del círculo tienen actualizaciones para el mismo ítem, se elige uno u otro, lo que da lugar a una eventual uniformidad. Cada ítem que se sincroniza se encripta de modo que únicamente lo pueda descryptar un dispositivo que esté dentro del círculo de confianza del usuario; ni Apple ni ningún otro dispositivo pueden descryptarlo.

Este “proceso de acceso” se repite a medida que se unen nuevos dispositivos al círculo de sincronización. Por ejemplo, si se une un tercer dispositivo, se puede enlazar con cualquiera de los dispositivos existentes. A medida que se añaden nuevos pares, cada par se sincroniza con el nuevo. Esto está diseñado para garantizar que todos los miembros tengan los mismos ítems del llavero.

Solo se sincronizan ciertos ítems

Algunos ítems del llavero son específicos del dispositivo, como las claves de iMessage, por lo que deben permanecer en el dispositivo. En consecuencia, cada ítem que se sincronice debe estar marcado explícitamente con el atributo `kSecAttrSynchronizable`.

Apple establece este atributo para los datos de usuario de Safari (que incluyen los nombres de usuario, contraseñas y números de tarjetas de crédito), así como para las contraseñas de redes wifi, las claves de encriptación de HomeKit y otros ítems del llavero que admiten la encriptación de punto a punto en iCloud.

Además, por defecto, los ítems del llavero que hayan añadido apps de terceros no se sincronizan. Los desarrolladores deben definir el atributo `kSecAttrSynchronizable` al añadir ítems al llavero.

Recuperación segura del llavero de iCloud

El llavero de iCloud custodia los datos del llavero de los usuarios con Apple, *sin* permitir que Apple lea sus contraseñas u otros datos que contenga. Incluso si el usuario solamente dispone de un dispositivo, la recuperación del llavero le proporciona una red de seguridad frente a la pérdida de datos. Esto es especialmente importante cuando Safari se usa para generar contraseñas seguras y aleatorias para cuentas web, ya que el único registro de esas contraseñas está en el llavero.

Dos de los conceptos básicos de la recuperación del llavero son la autenticación secundaria y el servicio de custodia segura, ambos creados por Apple específicamente para admitir esta función. El llavero del usuario se encripta mediante un código seguro y el servicio de custodia proporciona una copia del llavero únicamente si se cumple una serie de condiciones estrictas.

Uso de la autenticación secundaria

Existen varias maneras de establecer un código seguro:

- Si la cuenta del usuario tiene activada la autenticación de doble factor, se utiliza el código del dispositivo para recuperar el llavero custodiado.
- Si no se ha configurado la autenticación de doble factor, se solicitará al usuario que proporcione un valor de seis dígitos para el código de seguridad de iCloud. Opcionalmente, sin la autenticación de doble factor, los usuarios pueden especificar un código propio más largo o permitir que sus dispositivos generen un código aleatorio de encriptación, que pueden registrar y guardar.

Proceso de custodia del llavero

Una vez establecido el código, el llavero se custodia con Apple. El dispositivo iOS, iPadOS o macOS exporta primero una copia del llavero del usuario, lo encripta encapsulado con claves en un [repositorio de claves](#) asimétrico y lo coloca en el área de almacenamiento de datos clave-valor de iCloud del usuario. El repositorio de claves se encapsula con el código de seguridad de iCloud del usuario y con la clave pública del clúster del [módulo de seguridad de hardware \(HSM\)](#), que almacena el registro de la custodia, convirtiéndose así en el *registro de la custodia de iCloud* del usuario. Para las cuentas de autenticación de doble factor, el llavero se almacena en CloudKit y se encapsula con claves intermedias que solo se pueden recuperar con el contenido del registro de la custodia de iCloud, lo que proporciona el mismo nivel de protección.

El contenido del registro de la custodia también permite al dispositivo que se está recuperando volver a unirse al llavero de iCloud, lo que demuestra a cualquier dispositivo existente que el dispositivo que se está recuperando ha realizado correctamente el proceso de custodia y, por tanto, está autorizado por el propietario de la cuenta.

Nota: Si el usuario decide aceptar un código de seguridad aleatorio de encriptación en lugar de especificar el suyo propio o utilizar un valor de cuatro dígitos, el registro de la custodia no será necesario, puesto que el código de seguridad de iCloud se utilizará para encapsular directamente la clave aleatoria.

Además de establecer un código de seguridad, los usuarios deben registrar un número de teléfono. Esto proporciona un nivel de autenticación secundario durante la recuperación del llavero. El usuario recibe un mensaje SMS al que debe responder para que la recuperación pueda continuar.

Seguridad de la custodia para el llavero de iCloud

iCloud proporciona una infraestructura segura para custodias de [llaveros](#) para ayudar a garantizar que solo los usuarios y los dispositivos autorizados pueden realizar una recuperación. Para proteger los registros de custodia, hay clústeres de [módulos de seguridad de hardware \(HSM\)](#) topográficamente situados tras iCloud. Tal como se ha descrito anteriormente, cada uno tiene una clave que sirve para encriptar los registros de la custodia bajo su supervisión.

Para recuperar el llavero, los usuarios deben autenticarse con su cuenta de iCloud y su contraseña, y deben responder a un SMS que se envía al teléfono que hayan registrado. Una vez hecho esto, los usuarios deben introducir su código de seguridad de iCloud. El clúster de HSM verifica que el usuario conoce el código de seguridad de iCloud, que no se envía a Apple, mediante el protocolo de contraseña remota segura (SRP). Cada miembro del clúster verifica de manera independiente que el usuario no ha superado el número máximo de intentos permitidos para recuperar el registro, como se indica a continuación. Si la mayoría está de acuerdo, el clúster desencapsula el registro de la custodia y lo envía al dispositivo del usuario.

A continuación, el dispositivo usa el código de seguridad de iCloud para desencapsular la clave aleatoria que se ha usado para encriptar el llavero del usuario. Con esa clave, el llavero, que se ha recuperado del almacenamiento de datos clave-valor de iCloud y CloudKit, se desencripta y se restaura en el dispositivo. iOS, iPadOS y macOS solo permiten 10 intentos para autenticar y recuperar un registro de la custodia. Tras varios intentos erróneos, el registro se bloquea y el usuario debe ponerse en contacto con el servicio de soporte de Apple para que se le concedan más intentos. Tras el décimo intento erróneo, el clúster del HSM destruye el registro de la custodia y el llavero se pierde para siempre. Este sistema ofrece protección frente a los ataques de fuerza bruta para intentar recuperar el registro aunque conlleve el sacrificio de los datos de llavero.

Estas políticas se codifican en el firmware del HSM. Las tarjetas de acceso administrativo que permiten que el firmware se modifique se han destruido. Cualquier intento de alterar el firmware o de acceder a la clave privada provoca que el clúster del HSM elimine dicha clave. Si esto sucede, el propietario de cada llavero al que protege el clúster recibe un mensaje en el que se indicará que el registro de la custodia se ha perdido. A continuación, podrán decidir si quieren volver a inscribirse.

Apple Pay

Descripción general de la seguridad de Apple Pay

Con Apple Pay, los usuarios pueden utilizar los dispositivos iPhone, iPad, Mac y Apple Watch compatibles para pagar de forma sencilla, segura y privada en tiendas, apps e internet en Safari. Los usuarios también pueden añadir tarjetas de transporte, de estudiante y tarjetas de acceso compatibles con Apple Pay a Cartera. Es un sistema fácil para los usuarios que incluye seguridad integrada tanto en el hardware como en el software.

Además, Apple Pay se ha diseñado para proteger la información personal del usuario. Apple Pay no recopila información de las transacciones que se pueda vincular al usuario. Las transacciones de pago quedan entre el usuario, el beneficiario y la entidad emisora de la tarjeta.

Seguridad de los componentes de Apple Pay

Apple Pay usa varias características de hardware y software para ofrecer compras seguras y fiables.

Secure Element

Secure Element es un chip estándar certificado en el que se ejecuta la plataforma Java Card, que cumple con los requisitos del sector financiero en cuanto a pagos electrónicos. El circuito integrado de Secure Element y la plataforma Java Card están certificados de acuerdo con el proceso de evaluación de seguridad EMVCo. Una vez completada correctamente la evaluación de seguridad, EMVCo emite certificados únicos para el circuito integrado y la plataforma.

El circuito integrado de Secure Element ha recibido la certificación del estándar de Criterios Comunes. Para obtener más información, consulta [Certificaciones de seguridad para servicios de procesador Secure Enclave](#) en Certificaciones de las plataformas de Apple.

Controlador NFC

El controlador de comunicación de campo cercano (NFC) gestiona los protocolos NFC y dirige la comunicación entre el procesador de aplicaciones y Secure Element, y entre Secure Element y el terminal del punto de venta.

Cartera

Cartera se utiliza para añadir y gestionar tarjetas de crédito, débito o cliente para hacer pagos con Apple Pay. Los usuarios pueden ver sus tarjetas y posiblemente información adicional proporcionada por la entidad emisora de la tarjeta, como la política de privacidad de la entidad emisora de la tarjeta, las transacciones recientes y otros datos en Cartera. También pueden añadir tarjetas a Apple Pay en:

- El asistente de configuración y en Ajustes para iOS y iPadOS.
- La app Watch para el Apple Watch.
- Cartera y Apple Pay en Preferencias del Sistema para ordenadores Mac con Touch ID.

Además, Cartera permite a los usuarios añadir y gestionar tarjetas de transporte, tarjetas de bonificación, tarjetas de embarque, tarjetas regalo, carnés de estudiante, tarjetas de acceso, etc.

Secure Enclave

En el iPhone, iPad, Apple Watch, ordenadores Mac con Touch ID y ordenadores Mac con chip de Apple que usan el teclado Magic Keyboard con Touch ID, Secure Enclave gestiona el proceso de autenticación y permite realizar transacciones de pago.

En el caso del Apple Watch, el dispositivo debe estar desbloqueado y el usuario debe pulsar el botón lateral dos veces. Esta doble pulsación se detecta y se transfiere directamente a Secure Element, o a Secure Enclave si está disponible, sin pasar por el procesador de aplicaciones.

Servidores de Apple Pay

Los servidores de Apple Pay gestionan la configuración y la adición de las tarjetas de crédito, débito, transporte, acceso y carnés de estudiante en la app Cartera. Los servidores también gestionan los números de cuenta del dispositivo almacenados en Secure Element. Se comunican tanto con el dispositivo como con los servidores de la entidad emisora de la tarjeta o la red de pagos. Los servidores de Apple Pay también son los responsables de volver a encriptar las credenciales de pago para los pagos realizados desde las apps o en internet.

Cómo protege Apple Pay las compras del usuario

Secure Element

Secure Element aloja un applet diseñado específicamente para gestionar Apple Pay. También incluye applets certificados por entidades emisoras de tarjetas o redes de pagos. Los datos de las tarjetas de crédito, débito o prepago se envían a estos applets desde la red de pago o la entidad emisora de la tarjeta, encriptados con claves que solo conocen la red de pago o la entidad emisora de la tarjeta y el dominio de seguridad de los applets. Estos datos se almacenan en los applets y se protegen con las funciones de seguridad de Secure Element. Durante una transacción, el terminal se comunica directamente con Secure Element a través del controlador NFC mediante un bus de hardware dedicado.

Controlador NFC

Como puerta de enlace a Secure Element, el controlador NFC ayuda a garantizar que todas las transacciones de pago sin contacto se realizan a través de un terminal del punto de venta que esté cerca del dispositivo. El controlador NFC solo marca como transacciones sin contacto aquellas solicitudes de pago procedentes de un terminal situado dentro del área.

Una vez que el titular de la tarjeta autoriza el pago con tarjeta de crédito, débito o prepago (incluidas tarjetas de cliente) mediante Face ID, Touch ID o un código, o bien al pulsar dos veces el botón lateral de un Apple Watch desbloqueado, el controlador dirige las respuestas sin contacto preparadas por los applets de pago de Secure Element al campo de NFC de forma exclusiva. En consecuencia, los datos de autorización de pagos para las transacciones de pago sin contacto se incluyen en el campo local de NFC y nunca se exponen al procesador de aplicaciones. En comparación, los datos de autorización de pagos realizados en las apps y en internet se dirigen al procesador de aplicaciones, pero siempre después de que Secure Element los encripte en el servidor de Apple Pay.

Tarjetas de crédito, débito y prepago

Descripción general de la seguridad del envío de datos de tarjetas

Cuando un usuario añade una tarjeta de crédito, débito o prepago (incluidas las tarjetas de cliente) a Cartera, Apple envía la información de la tarjeta, junto con otra información sobre la cuenta y el dispositivo del usuario, a la entidad emisora de la tarjeta o al proveedor de servicios autorizado de la entidad emisora de la tarjeta de forma segura. La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba la adición de la tarjeta a Cartera. Como parte del proceso de envío de datos de tarjetas, Apple Pay utiliza tres llamadas de servidor para la comunicación con la entidad emisora de la tarjeta o la red:

- Campos obligatorios
- Comprobar tarjeta
- Enlazar y provisionar

La entidad emisora de la tarjeta o la red utilizan estas llamadas para verificar, aprobar y añadir tarjetas a Cartera. Estas sesiones de servidor cliente usan TLS 1.2 para transferir los datos.

Los números de tarjeta completos no se almacenan ni en el dispositivo ni en los servidores de Apple Pay, sino que se crea un número de cuenta de dispositivo encriptado que después se almacena en Secure Element. Este número único se encripta de forma que Apple no pueda acceder a él. El número de cuenta del dispositivo es único y diferente de la mayoría de los números de tarjeta de crédito o débito; la entidad emisora de la tarjeta o la red de pagos pueden impedir su uso en tarjetas de banda magnética, por teléfono o en sitios web. El número de cuenta del dispositivo de Secure Element nunca se almacena en los servidores de Apple Pay ni se incluye en las copias de seguridad de iCloud y está aislado de los dispositivos iOS, iPadOS y watchOS y de los ordenadores Mac con Touch ID.

Las tarjetas que se utilizan con el Apple Watch se transmiten a Apple Pay mediante la app Apple Watch del iPhone o con la app para el iPhone de la entidad emisora de la tarjeta. Para añadir una tarjeta al Apple Watch es necesario que el reloj esté dentro del radio de alcance de Bluetooth. Las tarjetas están registradas específicamente para utilizarlas con el Apple Watch y disponen de sus propios números de cuenta del dispositivo almacenados en Secure Element en el Apple Watch.

Al añadir tarjetas de crédito, débito o prepago (incluidas tarjetas de cliente), estas se muestran en una lista de tarjetas en el asistente de configuración en dispositivos en los que se haya iniciado sesión con la misma cuenta de iCloud. Estas tarjetas permanecerán en la lista mientras sigan activas en al menos un dispositivo. Las tarjetas desaparecerán de la lista cuando se hayan eliminado de todos los dispositivos durante siete días. Esta función requiere que la autenticación de doble factor esté activada en la cuenta de iCloud correspondiente.

Añadir tarjetas de crédito o débito a Apple Pay

Se pueden añadir tarjetas de crédito manualmente a Apple Pay en los dispositivos Apple.

Añadir tarjetas de crédito o débito manualmente

Para añadir una tarjeta manualmente, se utilizan el nombre, el número de la tarjeta, la fecha de caducidad y el código CVV con el fin de facilitar el proceso de envío de datos. Desde Ajustes, la app Cartera o la app Apple Watch, los usuarios pueden introducir dicha información mediante el teclado o usando la cámara del dispositivo. Cuando la cámara captura la información de la tarjeta, Apple intenta rellenar los campos de nombre, número de tarjeta y fecha de caducidad. La foto no se guarda nunca en el dispositivo ni se almacena en la fototeca. Una vez completados todos los campos, en el proceso "Comprobar tarjeta" se verifican todos excepto el código CVV. A continuación, esta información se encripta y se envía al servidor de Apple Pay.

Si se devuelve un identificador de condiciones de uso con el proceso "Comprobar tarjeta", Apple descarga las condiciones de la entidad emisora de la tarjeta y se las muestra al usuario. Si el usuario las acepta, Apple envía el identificador de las condiciones aceptadas y el código CVV al proceso "Enlazar y provisionar". De forma adicional y como parte del proceso "Enlazar y provisionar", Apple comparte información desde el dispositivo con la entidad emisora de la tarjeta o la red. Esto incluye información acerca de (a) la actividad del usuario en iTunes Store y App Store (por ejemplo, si dispone de un amplio historial de transacciones dentro de iTunes), (b) el dispositivo del usuario (por ejemplo, el número de teléfono, el nombre y el modelo del dispositivo, así como de cualquier dispositivo Apple con el que está enlazado y que es necesario para configurar Apple Pay) y (c) su ubicación aproximada en el momento de añadir su tarjeta (si tiene activada la localización). La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba la adición de la tarjeta a Apple Pay.

El proceso "Enlazar y provisionar" tiene dos consecuencias:

- El dispositivo empieza a descargar el archivo de Cartera correspondiente a la tarjeta de crédito o débito.
- El dispositivo empieza a vincular la tarjeta al Secure Element.

El archivo de la tarjeta contiene varias URL para descargar imágenes y metadatos de la tarjeta (p. ej., los datos de contacto), la app de la entidad emisora de la tarjeta correspondiente y otras funciones compatibles. También contiene su estado, que incluye información como, por ejemplo, si se ha completado la personalización de Secure Element, si la entidad emisora de la tarjeta ha suspendido su uso, o bien si es necesario realizar otra verificación antes de poder pagar con la tarjeta mediante Apple Pay.

Añadir tarjetas de crédito o débito desde una cuenta de iTunes Store

Para añadir una tarjeta de crédito o débito registrada en iTunes, puede que el usuario deba volver a introducir la contraseña de su ID de Apple. El número de la tarjeta se obtiene desde iTunes y se inicia el proceso "Comprobar tarjeta". Si la tarjeta es compatible con Apple Pay, el dispositivo descarga y muestra las condiciones de uso y, a continuación, enviará la información sobre el ID y el código de seguridad de la tarjeta para pasar al proceso "Enlazar y provisionar". Puede que se realice una verificación adicional en el caso de las tarjetas de las cuentas de iTunes registradas.

Añadir tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta

Cuando una app está registrada para su uso con Apple Pay, se establecen claves para el servidor de la entidad emisora de la tarjeta y para la app. Estas claves se usan para encriptar la información de la tarjeta que se envía al emisor de la tarjeta. Esto impide que el dispositivo Apple lea la información. El flujo de envío de datos es similar al que se utiliza para tarjetas añadidas de forma manual, descrito anteriormente, exceptuando que se utilizan contraseñas de un solo uso en lugar del código CVV.

Añadir tarjetas de crédito o débito desde el sitio web de la entidad emisora de la tarjeta

Algunos emisores de tarjetas ofrecen la posibilidad de iniciar el proceso de añadir las tarjetas para Cartera directamente desde sus sitios web. En este caso, el usuario inicia la tarea seleccionando una tarjeta para añadirla en el sitio web del emisor de la tarjeta. A continuación, se dirige al usuario a una experiencia autónoma de inicio de sesión de Apple (dentro del dominio de Apple) y se le pide que inicie sesión con su ID de Apple. Una vez iniciada la sesión correctamente, el usuario elige uno o más dispositivos a los que añadir la tarjeta y se le pide que confirme el resultado del envío de datos de la tarjeta en cada dispositivo de destino.

Añadir una verificación adicional

La entidad emisora de la tarjeta puede decidir si una tarjeta de crédito o débito requiere una verificación adicional. En función de la oferta de la entidad emisora de la tarjeta, es posible que el usuario pueda elegir entre diferentes opciones para realizar la verificación adicional. Tales opciones pueden ser, entre otras, un mensaje de texto, un mensaje de correo electrónico, una llamada del servicio de atención al cliente o un método para finalizar la verificación en la app aprobada de un tercero. Para los mensajes de texto o de correo electrónico, el usuario selecciona la información de contacto entre los datos que la entidad emisora de la tarjeta tiene registrados. A continuación, se envía un código que el usuario necesita introducir en la app Cartera, Ajustes o la app Apple Watch. En el caso de servicio al cliente o de la verificación con una app, la entidad emisora lleva a cabo su propio proceso de comunicación.

Autorización de pagos con Apple Pay

En el caso de los dispositivos que tienen Secure Enclave, se puede realizar un pago solo tras recibir la autorización de Secure Enclave. En el iPhone o iPad, este proceso conlleva la confirmación de que el usuario se ha autenticado con Face ID, Touch ID o con el código del dispositivo. Face ID o Touch ID es el método por defecto (si está disponible), pero, si se prefiere, siempre se puede usar el código. Tras tres intentos erróneos de reconocimiento de la huella digital o dos intentos erróneos de reconocer una cara, se ofrece la posibilidad de insertar el código. Tras cinco intentos erróneos, la inserción del código es obligatoria. Además, el código también es necesario si Face ID o Touch ID no se ha configurado o activado para Apple Pay. Para realizar un pago en el Apple Watch, el dispositivo se debe desbloquear con el código y el botón lateral se debe pulsar dos veces.

Usar una clave de enlace compartida

La comunicación entre Secure Enclave y Secure Element se realiza mediante una interfaz serie, con Secure Element conectado al controlador NFC que, a su vez, se conecta al procesador de aplicaciones. Aunque no estén directamente conectados, Secure Enclave y Secure Element se pueden comunicar de forma segura gracias a una clave de enlace suministrada durante el proceso de fabricación. La encriptación y la autenticación de la comunicación se basan en el estándar AES, con **nonces** criptográficos que usan ambas partes para protegerse de los ataques de reproducción. La clave de enlace se genera dentro de Secure Enclave a partir de la clave UID y el identificador único de Secure Element. Después, se transfiere de Secure Enclave a un **módulo de seguridad de hardware (HSM)** en la fábrica, que dispone del material necesario para introducir, a continuación, la clave de enlace en Secure Element.

Autorizar una transacción segura

Cuando el usuario autoriza una transacción, que requiere un gesto físico que se comunica a Secure Enclave directamente, Secure Enclave envía datos firmados acerca del tipo de autenticación e información detallada sobre el tipo de transacción (sin contacto o desde apps) a Secure Element, que está vinculado a un valor de autorización aleatorio (AR). Este valor AR se genera en Secure Enclave cuando un usuario facilita por primera vez una tarjeta de crédito, y no cambia mientras Apple Pay está activado. La encriptación de Secure Enclave y el mecanismo antirretroceso protegen este valor, que se envía de forma segura a Secure Element mediante la clave de enlace. Al recibir un valor AR nuevo, Secure Element marca como eliminada cualquier tarjeta añadida previamente.

Usar un criptograma de pago para seguridad dinámica

Todas las transacciones de pago que se originan en los applets de pago incluyen un criptograma de pago junto con un número de cuenta del dispositivo. Este criptograma, que es un código de un solo uso, se calcula con la ayuda de un contador de transacciones y una clave. El contador de transacciones se incrementa con cada nueva transacción. La clave se proporciona en el applet de pago durante su personalización y es conocida por la red de pago, por la entidad emisora de la tarjeta o por ambas. En función del sistema de pago, puede que también se usen otros datos para el cálculo, entre los que se incluyen:

- Un Número Impredecible de Terminal para transacciones de comunicación de campo cercano (NFC).
- Un nonce del servidor de Apple Pay (para las transacciones dentro de apps).

Estos códigos de seguridad se proporcionan tanto a la red de pago como a la entidad emisora de la tarjeta, lo que permite a la entidad emisora verificar cada transacción. La longitud de esos códigos de seguridad puede variar en función del tipo de transacción.

Pago con tarjetas mediante Apple Pay

Apple Pay permite pagar compras en tiendas, en apps y en sitios web.

Pagar con tarjetas en tiendas

Si el iPhone o el Apple Watch está encendido y detecta un campo NFC, muestra al usuario la tarjeta solicitada (si la selección automática está activada para esa tarjeta), o la tarjeta por defecto, que se gestiona en Ajustes. El usuario también puede ir a Cartera y seleccionar una tarjeta o, si el dispositivo está bloqueado, puede:

- Pulsar dos veces el botón lateral en dispositivos con Face ID.
- Pulsar dos veces el botón de inicio en dispositivos con Touch ID.
- Utilizar las funciones de accesibilidad que permiten el uso de Apple Pay desde la pantalla bloqueada.

A continuación, antes de que se transmita la información relativa al pago, el usuario deberá autenticarse mediante Face ID, Touch ID o su código. Si el Apple Watch está desbloqueado, al pulsar dos veces el botón lateral, se activa la tarjeta por defecto para realizar el pago. No se envía ninguna información relativa al pago sin la autenticación del usuario.

Al procesar el pago una vez que el usuario se ha autenticado, se utiliza el número de cuenta del dispositivo y un código de seguridad dinámico específico para cada transacción. Ni Apple ni ningún dispositivo del usuario enviarán los números completos de la tarjeta de crédito o débito a los beneficiarios. Puede que Apple reciba información anónima relacionada con la transacción como, por ejemplo, la ubicación y la hora aproximada en la que se ha realizado. Esta información sirve de ayuda para mejorar Apple Pay, así como otros productos y servicios de Apple.

Pagar con tarjetas en apps

Apple Pay también se puede utilizar para realizar pagos en apps del iPhone, iPad, Mac y Apple Watch. Cuando los usuarios pagan de esta manera con Apple Pay, Apple recibe información encriptada de la transacción. Antes de que esa información se envíe al desarrollador o al beneficiario, Apple vuelve a encriptar la transacción con una clave específica del desarrollador. Apple Pay guarda información sobre la transacción de forma anónima como, por ejemplo, el importe aproximado de la compra. Esta información no se puede relacionar con el usuario y nunca incluye qué ha comprado.

Cuando una app inicia una transacción de pago de Apple Pay, los servidores de Apple Pay reciben la transacción encriptada desde el dispositivo antes de que el beneficiario la reciba. A continuación, los servidores de Apple Pay vuelven a encriptar la transacción con la clave específica del beneficiario antes de transmitirla al beneficiario.

Cuando una app solicita un pago, llama a una API para determinar si el dispositivo es compatible con Apple Pay y si la tarjeta de crédito o débito del usuario puede utilizarse para realizar pagos en una red de pago que acepte el beneficiario. La app solicita todos los datos que necesita para procesar y completar la transacción como, por ejemplo, las direcciones de envío y facturación o los datos de contacto. A continuación, la app pide a iOS, iPadOS o watchOS que presente la hoja de Apple Pay, que solicita información para la app, así como otra información necesaria, como la tarjeta que se va a utilizar.

Es entonces cuando la app muestra la información relacionada con la ciudad, el país y el código postal para calcular los gastos de envío finales. Sin embargo, no recibe toda la información solicitada hasta que el usuario autoriza el pago mediante Face ID, Touch ID o el código del dispositivo. Una vez autorizado, la información que se muestra en la hoja de Apple Pay se envía al beneficiario.

Autorizar pagos de la app

Cuando el usuario autoriza el pago, se envía un aviso a los servidores de Apple Pay para obtener un **nonce** criptográfico, similar al valor que devuelve el terminal NFC y que se utiliza para realizar transacciones en las tiendas. El nonce, junto con otros datos de la transacción, se transfiere a Secure Element para computar una credencial de pago que se encripta mediante una clave de Apple. La credencial de pago encriptada se devuelve a los servidores de Apple Pay, que la desencriptan, cotejan su nonce con el que han enviado originalmente los servidores de Apple Pay y la encriptan de nuevo con la clave del beneficiario asociada a su ID. Después, el pago vuelve al dispositivo, que se encarga de devolverlo a la app mediante la API. A continuación, la app se la facilita al sistema del beneficiario para que la procese. En ese momento, el beneficiario ya puede desencriptar la credencial de pago con la ayuda de su clave privada para procesarla. Esto, en combinación con la firma de los servidores de Apple, permite que el beneficiario verifique que él es el destinatario de la transacción.

Las API requieren una autorización en la que se indiquen los ID compatibles del beneficiario. Al poder enviar también datos adicionales (como, por ejemplo, el número de pedido o la identidad del cliente) al Secure Element para que los firme, una app garantiza que la transacción no se puede desviar a otro cliente. El desarrollador de la app se encarga de realizar esta tarea y es quien puede especificar `applicationData` en `PKPaymentRequest`. En los datos de pago encriptados, se incluye un hash de estos datos. A continuación, el beneficiario será responsable de verificar que su hash de `applicationData` coincide con el de los datos de pago.

Pagar con tarjetas en sitios web

Apple Pay permite realizar pagos en sitios web con el iPhone, el iPad, el Apple Watch y ordenadores Mac con Touch ID. Asimismo, pueden iniciarse transacciones de Apple Pay en un Mac y acabarse en un iPhone o Apple Watch compatible con Apple Pay utilizando la misma cuenta de iCloud.

Para pagar con Apple Pay en internet, es necesario que todos los sitios web participantes estén registrados en Apple. Una vez registrado el dominio, se realiza la validación del nombre de dominio solo después de que Apple emita un certificado de cliente TLS. Los sitios web compatibles con Apple Pay deben ofrecer su contenido mediante el protocolo HTTPS. Por cada transacción de pago, los sitios web deben obtener una sesión comercial segura y única con un servidor de Apple mediante el uso de un certificado de cliente TLS emitido por Apple. Apple también se encarga de firmar los datos de la sesión comercial. Una vez verificada la firma de la sesión comercial, el sitio web puede preguntar si el usuario dispone de un dispositivo compatible con Apple Pay y si en ese dispositivo hay activada una tarjeta de crédito, débito o prepago. No se comparte ninguna otra información. Si el usuario no quiere compartir esa información, puede desactivar las preguntas de Apple Pay en los ajustes de privacidad de Safari en los dispositivos iPhone, iPad y Mac.

Una vez validada la sesión comercial, las medidas de privacidad y seguridad son las mismas que cuando un usuario paga desde una app.

Si el usuario transmite información relacionada con el pago desde un Mac a un iPhone o Apple Watch, mediante Handoff, Apple Pay utiliza el protocolo del [servicio de identidad \(IDS\) de Apple](#) encriptado de punto a punto para transmitir la información relacionada con el pago entre el Mac del usuario y el dispositivo autorizador. El cliente IDS del Mac utiliza las claves del dispositivo del usuario (no disponibles para Apple) con el fin de realizar la encriptación, de manera que ningún otro dispositivo pueda desencriptar esa información. Al detectar el dispositivo que se utiliza para continuar con la operación de Apple Pay mediante Handoff, se obtiene el tipo y el identificador único de las tarjetas de crédito del usuario junto con otros metadatos. El número de cuenta específico del dispositivo correspondiente a la tarjeta del usuario no se comparte y sigue estando almacenado de forma segura en el iPhone o Apple Watch del usuario. Apple también transfiere de forma segura las direcciones de contacto, envío y facturación del usuario utilizadas recientemente mediante el llavero de iCloud.

Cuando el usuario autoriza el pago mediante Face ID, Touch ID o el código, o pulsa dos veces el botón lateral del Apple Watch, se transmite de forma segura un identificador de pago encriptado exclusivamente para el certificado comercial de cada sitio web desde el iPhone o Apple Watch del usuario hasta su Mac y, a continuación, se envía al sitio web del beneficiario.

Solo los dispositivos que se encuentran a poca distancia entre sí pueden solicitar un pago completo. La proximidad se determina mediante avisos de Bluetooth de baja energía (BLE).

Tarjetas sin contacto en Apple Pay

Para transmitir datos de tarjetas admitidas a terminales NFC compatibles, Apple usa el protocolo de servicio de valor añadido de Apple (Apple VAS). El protocolo VAS puede implementarse en terminales de pago sin contacto o en las apps del iPhone y utiliza NFC para establecer la comunicación con dispositivos Apple compatibles. El protocolo VAS funciona a una distancia reducida y puede utilizarse para presentar tarjetas sin contacto independientemente o como parte de una transacción con Apple Pay.

Al sostener el dispositivo cerca del terminal NFC, el terminal inicia la recepción de la información de la tarjeta al enviar una solicitud de tarjeta. Si el usuario dispone de una tarjeta con el identificador del proveedor de la tarjeta, se le solicita que autorice su uso mediante Face ID, Touch ID o un código. La información de la tarjeta, una fecha y una clave P-256 de ECDH aleatoria de un solo uso se utilizan junto con la clave pública del proveedor para derivar una clave de encriptación para los datos de la tarjeta, que se envían al terminal.

Desde iOS 12.0.1 y hasta iOS 13 inclusive, los usuarios pueden seleccionar una tarjeta manualmente antes de presentarla al terminal NFC del beneficiario. En iOS 13.1 o posterior, las entidades emisoras de las tarjetas pueden configurar las tarjetas seleccionadas manualmente para que requieran o no la autenticación del usuario.

Inhabilitar las tarjetas con Apple Pay

Las tarjetas de crédito, débito y prepago que se hayan añadido a Secure Element solamente se pueden usar si este muestra una autorización con la misma clave de enlace y el mismo valor de autorización aleatorio (AR) que cuando se añadió la tarjeta. Al recibir un valor AR nuevo, Secure Element marca como eliminada cualquier tarjeta añadida previamente. Esto permite que el sistema operativo dé instrucciones a Secure Enclave para que inhabilite las tarjetas marcando su copia del valor AR como no válida en las siguientes circunstancias:

Método	Dispositivo
Si se desactiva el código.	iPhone, iPad, Apple Watch
Si se desactiva la contraseña.	Mac
Si el usuario cierra su sesión en iCloud.	iPhone, iPad, Mac, Apple Watch
Si el usuario selecciona "Borrar contenidos y ajustes".	iPhone, iPad, Mac, Apple Watch
Si el dispositivo se restaura desde el modo de recuperación.	iPhone, iPad, Mac, Apple Watch
Si se desenlaza el dispositivo.	Apple Watch

Suspensión, eliminación y borrado de tarjetas

Los usuarios pueden suspender el servicio Apple Pay en el iPhone, iPad y Apple Watch al activar el modo Perdido en sus dispositivos mediante Buscar. Los usuarios también tienen la posibilidad de eliminar y borrar sus tarjetas de Apple Pay mediante Buscar o iCloud.com, o bien directamente en sus dispositivos mediante Cartera. En el Apple Watch, las tarjetas se pueden eliminar mediante los ajustes de iCloud, la app Apple Watch del iPhone, o bien directamente en el reloj. La entidad emisora de la tarjeta o la red de pago correspondiente puede suspender o eliminar la posibilidad de realizar pagos mediante las tarjetas del dispositivo con Apple Pay, aunque el dispositivo no esté en línea ni conectado a una red móvil o wifi. Los usuarios también pueden llamar a la entidad emisora de la tarjeta para suspender o eliminar tarjetas de Apple Pay.

Cuando un usuario borra el contenido de todo el dispositivo con "Borrar contenidos y ajustes", con Buscar o restaurando el dispositivo, los dispositivos iPhone, iPad, iPod touch, Mac y Apple Watch solicitan a Secure Element que marque todas las tarjetas como eliminadas. El resultado inmediato es que las tarjetas dejan de poder utilizarse hasta que se consiga establecer contacto con los servidores de Apple Pay para solicitarles que eliminen las tarjetas de Secure Element por completo. Independientemente, Secure Enclave marca el valor AR como no válido para impedir cualquier autorización de pago con las tarjetas registradas previamente. Cuando el dispositivo está conectado a internet, intenta ponerse en contacto con los servidores de Apple Pay para ayudar a cerciorarse de que todas las tarjetas se han borrado de Secure Element.

Seguridad de Apple Card

En modelos compatibles de iPhone y Mac, un usuario puede solicitar una tarjeta Apple Card de forma segura.

Solicitar la tarjeta Apple Card

En iOS 12.4 o posterior, macOS 10.14.6 o posterior y watchOS 5.3 o posterior, Apple Card se puede usar con Apple Pay para realizar pagos en tiendas, en apps y en internet.

Para solicitar una Apple Card, el usuario debe haber iniciado sesión en su cuenta de iCloud desde un dispositivo iOS o iPadOS compatible con Apple Pay y haber configurado la autenticación de doble factor en la cuenta de iCloud. Cuando se aprueba la solicitud, la tarjeta Apple Card está disponible en la app Cartera o desde Ajustes > "Cartera y Apple Pay" en cualquiera de los dispositivos válidos en los que el usuario haya iniciado sesión con su ID de Apple.

Cuando un usuario solicita una Apple Card, la información de identidad se verifica de forma segura por los proveedores de identidad asociados de Apple. A continuación, se comparte con Goldman Sachs Bank USA a efectos de identidad y de evaluación del crédito.

La información, como el número de la seguridad social o la imagen del documento de identidad proporcionados durante la solicitud, se encripta con sus correspondientes claves y se transmite de forma segura a los proveedores de identidad asociados de Apple o a Goldman Sachs Bank USA. Apple no puede descifrar estos datos.

La información de ingresos proporcionada durante la solicitud y la información del número de cuenta bancaria que se utilizará para el pago de las facturas se encriptan con su clave y se transmiten de forma segura a Goldman Sachs Bank USA. La información del número de cuenta bancaria se guarda en el llavero. Apple no puede descifrar estos datos.

Al añadir la tarjeta Apple Card a la app Cartera, es posible que se comparta la misma información que al añadir una tarjeta de crédito o débito con el banco asociado de Apple, Goldman Sachs Bank USA, y con Apple Payments Inc. Esta información únicamente se utiliza para solucionar problemas, evitar fraudes y para fines normativos.

En iOS 14.6 o posterior, iPadOS 14.6 o posterior y watchOS 7.5 o posterior, el organizador de una familia de iCloud que tenga una tarjeta Apple Card puede compartir su tarjeta con los miembros de la familia de iCloud mayores de 13 años. El usuario debe autenticarse para confirmar la invitación. La app Cartera usa una clave en Secure Enclave para computar una firma que vincula al propietario y al invitado. Esa firma se valida en los servidores de Apple.

Opcionalmente, el organizador puede establecer un límite de transacciones para los participantes. Las tarjetas de los participantes también pueden bloquearse para detener su gasto en cualquier momento a través de la app Cartera. Cuando un copropietario o participante mayor de 18 años acepta la invitación y la solicita, pasa por el mismo proceso de solicitud definido en la sección de solicitud de la tarjeta Apple Card en la app Cartera.

Uso de la tarjeta Apple Card

En la app Cartera se puede pedir una tarjeta Apple Card física. Cuando el usuario recibe la tarjeta física, la tarjeta se activa con la etiqueta NFC que hay en el sobre de la tarjeta física. La etiqueta es única para cada tarjeta y no se puede usar para activar la tarjeta de otro usuario. Opcionalmente, la tarjeta se puede activar manualmente en los ajustes de la app Cartera. Además, el usuario también puede bloquear o desbloquear la tarjeta física en cualquier momento desde la app Cartera.

Pagos con Apple Card y detalles de la tarjeta en Cartera

Los pagos pendientes en la cuenta de la tarjeta Apple Card se pueden realizar desde la app Cartera en iOS con Apple Cash y una cuenta bancaria. El pago de las facturas se puede programar como recurrente o como pago único en una fecha específica con Apple Cash y una cuenta bancaria. Cuando un usuario realiza un pago, se envía una llamada a los servidores de Apple Pay para obtener un nonce criptográfico, similar a lo que ocurre con Apple Cash. El nonce, junto con otros datos de la configuración de pago, se transfiere a Secure Element para computar una firma. A continuación, la firma se devuelve a los servidores de Apple Pay, que verifican la autenticación, integridad y exactitud del pago mediante la firma de pago y el nonce. A continuación, se pasa la orden a Goldman Sachs Bank USA para que la procese.

La app Cartera recupera el número de la tarjeta Apple Card presentando un certificado. El servidor de Apple Pay valida el certificado para confirmar que la clave se ha generado en Secure Enclave. A continuación, usa esta clave para encriptar el número de la tarjeta Apple Card antes de devolverla a la app Cartera, de modo que solo pueda descifrarla el iPhone que solicitó el número de la tarjeta Apple Card. Después de la descifración, el número de la tarjeta Apple Card se guarda en el llavero de iCloud.

Para mostrar el número de la tarjeta Apple Card al usarla en la app Cartera se requiere la autenticación del usuario con Face ID, Touch ID o un código. El usuario puede sustituirlo en la sección de información de la tarjeta, desactivando el anterior.

Protección antifraude avanzada

En iOS 15 o posterior y iPadOS 15 o posterior, el usuario de la tarjeta Apple Card puede activar la función "Protección antifraude avanzada" en la app Cartera. Cuando está activada, el código de seguridad de la tarjeta se actualiza cada pocos días.

Seguridad de Apple Cash

En iOS 11.2, iPadOS 13.1 y watchOS 4.2 o versiones posteriores, se puede utilizar Apple Pay en un iPhone, iPad o Apple Watch para enviar, recibir y solicitar dinero de otros usuarios. Cuando un usuario recibe dinero, se añade a una cuenta de Apple Cash a la que se puede acceder desde la app Cartera o desde Ajustes > "Cartera y Apple Pay" en cualquiera de los dispositivos válidos en los que el usuario haya iniciado sesión con su ID de Apple.

En iOS 14, iPadOS 14 y watchOS 7, el organizador de una familia de iCloud que haya verificado su identidad con Apple Cash puede activar Apple Cash para los miembros de la familia menores de 18 años. El organizador también puede limitar las funciones de envío de dinero de estos usuarios solo a miembros de la familia o contactos. Si se recupera la cuenta del ID de Apple de un miembro de la familia menor de 18 años, el organizador de la familia debe volver a activar manualmente la tarjeta de Apple Cash para ese usuario. Si el miembro de la familia menor de 18 años deja de formar parte de la familia de iCloud, su saldo de Apple Cash se transfiere automáticamente a la cuenta del organizador.

Cuando el usuario configura Apple Cash, es posible que se comparta la misma información que al añadir una tarjeta de crédito o débito con nuestro banco asociado Green Dot Bank y con Apple Payments Inc., una filial totalmente participada y creada para proteger tu privacidad, ya que la información se guarda y procesa por separado del resto de Apple y de una forma que el resto de Apple desconoce. Esta información únicamente se utiliza para solucionar problemas, evitar fraudes y para fines normativos.

Cómo usar Apple Cash en iMessage

Para realizar pagos entre personas y utilizar Apple Cash, el usuario debe haber iniciado sesión en su cuenta de iCloud desde un dispositivo compatible con Apple Cash y haber configurado la autenticación de doble factor en la cuenta de iCloud. Las solicitudes de dinero y transferencias entre usuarios se inician desde la app Mensajes o pidiéndoselo a Siri. Cuando un usuario intenta enviar dinero, iMessage muestra la hoja de Apple Pay. Siempre se utiliza primero el saldo de Apple Cash. Si es necesario, se utilizan fondos adicionales de una segunda tarjeta de crédito o débito que el usuario ha añadido a la app Cartera.

Usar Apple Cash en tiendas, apps e internet

La tarjeta Apple Cash de la app Cartera se puede utilizar con Apple Pay para realizar pagos en tiendas, en apps y en internet. El dinero de la cuenta de Apple Cash también se puede transferir a una cuenta bancaria. Además de recibir dinero de otro usuario, se puede añadir dinero a la cuenta de Apple Cash desde una tarjeta de débito o prepago en la app Cartera.

Apple Payments Inc. guarda los datos de la transacción del usuario y puede que los utilice para solucionar problemas, evitar fraudes y para fines normativos una vez completada la transacción. El resto de Apple desconoce a quién ha enviado dinero el usuario, de quién ha recibido dinero o dónde ha realizado una compra con su tarjeta Apple Cash.

Cuando el usuario envía dinero con Apple Pay, lo añade a una cuenta de Apple Cash o lo transfiere a una cuenta bancaria, se envía un aviso a los servidores de Apple Pay para obtener un **nonce** criptográfico, similar al valor que se devuelve para Apple Pay desde las apps. El nonce, junto con otros datos de la transacción, se transfiere a Secure Element para computar una firma de pago. La firma se devuelve a los servidores de Apple Pay, que verifican la autenticación, integridad y exactitud de la transacción mediante la firma de pago y el nonce. A continuación, se inicia la transferencia de dinero y el usuario recibe una notificación de que la transacción se ha completado.

Si la transacción implica:

- Una tarjeta de débito para añadir dinero a Apple Cash.
- La aportación de una cantidad de dinero adicional si el saldo de Apple Cash es insuficiente.

También se produce una credencial de pago encriptada que se envía a los servidores de Apple Pay, de manera similar a cómo funciona Apple Pay en apps y sitios web.

Cuando el saldo de la cuenta de Apple Cash supera una cierta cantidad, o si se detecta una actividad inusual, se le pide al usuario que verifique su identidad. La información proporcionada para verificar la identidad del usuario, como el número de la seguridad social o las respuestas a preguntas (por ejemplo, confirmar el nombre de la calle donde el usuario ha residido anteriormente) se transmite de forma segura al socio de Apple y se encripta utilizando su clave. Apple no puede descifrar estos datos. Se solicitará al usuario que verifique su identidad de nuevo si realiza una recuperación de la cuenta del ID de Apple para poder volver a acceder a su saldo de Apple Cash.

Seguridad de “Tap to Pay on iPhone”

“Tap to Pay on iPhone”, disponible en iOS 15.4, permite que los comercios estadounidenses acepten Apple Pay y otros métodos de pago sin contacto usando el iPhone y una app iOS habilitada por el asociado. Con este servicio, los usuarios con dispositivos iPhone compatibles pueden aceptar de forma segura los pagos sin contacto y los pases compatibles con NFC de *Apple Pay*. Con “Tap to Pay on iPhone”, los beneficiarios no necesitan hardware adicional para aceptar los pagos sin contacto.

“Tap to Pay on iPhone” se ha diseñado para proteger la información personal de la persona que paga. Este servicio no recopila información de las transacciones que se pueda vincular a la persona que paga. La información de la tarjeta de pago, como el número de la tarjeta de crédito/débito (PAN), está protegida por Secure Element y no está disponible para el comercio. La información de la tarjeta de pago se mantiene entre el proveedor de servicios de pago del beneficiario, la persona que paga y la entidad emisora de la tarjeta. Además, el servicio Tap to Pay no recopila el nombre, la dirección ni el número de teléfono de la persona que paga.

“Tap to Pay on iPhone” ha sido evaluado externamente por un laboratorio de seguridad acreditado y aprobado por American Express, Discover, Mastercard y Visa.

Seguridad del componente de pago sin contacto

- *Secure Element*: Secure Element [enlace a la sección Secure Element de Apple Pay] aloja los kernels de pago que leen y protegen los datos de las tarjetas de pago sin contacto.
- *Controlador NFC*: El controlador de comunicación de campo cercano (NFC) gestiona los protocolos NFC y dirige la comunicación entre el procesador de aplicaciones y Secure Element, y entre Secure Element y la tarjeta de pago sin contacto.
- *Servidores de "Tap to Pay on iPhone"*: Los servidores de "Tap to Pay on iPhone" gestionan la configuración y el envío de datos de los kernels de pago en el dispositivo. Los servidores también monitorizan la seguridad de los dispositivos "Tap to Pay on iPhone" de una manera compatible con la norma Contactless Payments on COTS (CPoC) del Payment Card Industry Security Standards Council (PCI SSC) y cumplen con el PCI DSS.

Cómo Tap to Pay lee las tarjetas de crédito, débito y prepago

Descripción general de la seguridad del envío de datos

Al usar por primera vez "Tap to Pay on iPhone" utilizando una app con suficiente derecho, el servidor de "Tap to Pay on iPhone" determina si el dispositivo cumple los criterios de idoneidad, como el modelo de dispositivo, la versión de iOS y si se ha establecido un código. Una vez completada esta verificación, el applet de aceptación del pago se descarga desde el servidor de "Tap to Pay on iPhone" y se instala en Secure Element, junto con la configuración del kernel de pago asociado. Esta operación se realiza de forma segura entre los servidores de "Tap to Pay on iPhone" y Secure Element. Secure Element valida la integridad y autenticidad de estos datos antes de la instalación.

Descripción general de la seguridad de la lectura de tarjetas

Cuando una app de "Tap to Pay on iPhone" solicita la lectura de una tarjeta desde la estructura ProximityReader, se muestra una hoja (controlada por iOS) que pide al usuario que toque una tarjeta de pago. iOS inicializa el lector de tarjetas de pago y, a continuación, solicita a los kernels de pago de Secure Element que inicien la lectura de la tarjeta.

En este momento, Secure Element asume el control del controlador NFC en modo lectura. Este modo solo permite el intercambio de datos de la tarjeta entre la tarjeta de pago y Secure Element a través del controlador NFC. Las tarjetas de pago solo se pueden leer mientras este modo esté activo.

Después de que el applet de aceptación de pagos en Secure Element haya completado la lectura de la tarjeta, encripta y firma los datos de la tarjeta. Los datos de la tarjeta permanecen encriptados y autenticados hasta que llegan al proveedor de servicios de pago. Solo el proveedor de servicios de pago usado por la app para solicitar la lectura de la tarjeta puede desencriptar los datos de la tarjeta. El proveedor de servicios de pago debe solicitar la clave de desencriptación de los datos de la tarjeta al servidor de "Tap to Pay on iPhone". El servidor de "Tap to Pay on iPhone" emite las claves de desencriptado al proveedor de servicios de pago después de validar la integridad y autenticidad de los datos, y después de verificar que la lectura de la tarjeta se produjo en menos de 60 segundos desde la lectura de la tarjeta en el dispositivo.

Este modelo ayuda a garantizar que los datos de la tarjeta no puedan ser desencriptados por nadie más que el proveedor de servicios de pago, que procesa esta transacción para el beneficiario.

Usar la app Cartera

Acceder mediante la app Cartera

En la app Cartera de los dispositivos iPhone y Apple Watch compatibles, los usuarios pueden guardar las llaves de sus casas, coches y habitaciones de hotel. Incluso pueden guardar las tarjetas de identificación de las empresas y los carnés de estudiante. Cuando un usuario llega a una puerta, se presentará automáticamente la llave adecuada, de forma que podrá entrar con un solo toque mediante la comunicación de campo cercano (NFC).

Comodidad para el usuario

Al añadir una llave, un pase, un carné de estudiante o una tarjeta de identificación de la empresa a la app Cartera, el modo exprés se activa por defecto. Las tarjetas en el modo exprés interactúan con las terminales que los acepten sin tener que autenticarse con Face ID, Touch ID, un código o haciendo doble clic en el botón lateral del Apple Watch. El usuario puede desactivar el modo exprés tocando el botón Más en el anverso de la tarjeta en la app Cartera. Para volver a activar el modo exprés, debe usar Face ID, Touch ID o un código.

Privacidad y seguridad

Las llaves en la app Cartera aprovechan al máximo la privacidad y la seguridad integradas en el iPhone y en el Apple Watch. Nunca se comparte con Apple cuándo o dónde usa una persona sus llaves en la app Cartera ni se almacenan en los servidores de Apple. Además, las credenciales se almacenan de forma segura dentro de Secure Element (SE) de los dispositivos compatibles. SE aloja applets especialmente diseñados para gestionar y almacenar de forma segura las llaves de acceso, garantizando que esas llaves no se puedan extraer.

Antes de añadir cualquier llave de acceso, un usuario debe haber iniciado sesión en su cuenta de iCloud en un iPhone compatible y tener activada la autenticación de doble factor para su cuenta de iCloud, con la excepción de un carné de estudiante, que no requiere que la autenticación de doble factor esté activada.

Cuando un usuario inicia el proceso de envío de datos, se siguen pasos similares a los que se realizan en el envío de datos de tarjetas de crédito y débito, como el de [enlazar y provisionar](#). Durante una transacción, el lector se comunica con Secure Element a través del controlador NFC mediante un canal seguro establecido.

El número de dispositivos, incluidos el iPhone y el Apple Watch, a los que se puede añadir una llave de acceso está definido y controlado por cada asociado y puede variar de un asociado a otro. Este enfoque permite a cada asociado tener control sobre el número máximo de llaves de acceso añadidas por tipo de dispositivo para adaptarse a sus necesidades específicas. Para ello, Apple proporciona a los asociados el tipo de dispositivo y los identificadores anónimos del mismo. Los identificadores son diferentes para cada asociado por motivos de privacidad y seguridad.

Las llaves se pueden desactivar o eliminar mediante las siguientes acciones:

- Borrar el dispositivo remotamente con Buscar.
- Activar el modo Perdido con Buscar.

- Recibir un comando de borrado remoto de la solución de [gestión de dispositivos móviles \(MDM\)](#).
- Eliminar todas las tarjetas de la página de la cuenta del ID de Apple.
- Eliminar todas las tarjetas de iCloud.com.
- Eliminar todas las tarjetas de la app Cartera.
- Eliminar la tarjeta en la app de la entidad emisora.

En iOS 15.4 o posterior, cuando un usuario pulsa dos veces el botón lateral de un iPhone con Face ID o pulsa dos veces el botón de inicio de un iPhone con Touch ID, los detalles de sus pases y llaves de acceso no se muestran hasta que se autenticuen en el dispositivo. Se requiere una autenticación mediante Face ID, Touch ID o código antes de que la información específica del pase, incluyendo los detalles de la reserva del hotel, aparezca en la app Cartera.

Tipos de credenciales de acceso

Hay diferentes tipos de acceso desde Cartera, como tarjetas de acceso de hostelería, tarjetas de identificación de las empresas, carnés de estudiante, las llaves de casa y las llaves del coche.

Hostelería

Las llaves de las habitaciones de los hoteles en Cartera ayudan a ofrecer una experiencia fácil y sin contacto desde el registro de entrada hasta el de salida, a la vez que proporcionan ventajas adicionales de privacidad y seguridad para los huéspedes que se suman a las de las tradicionales llaves de los hoteles en forma de tarjetas de plástico. Los huéspedes del hotel en los establecimientos admitidos pueden tocar para desbloquear con las llaves de la habitación en Cartera en sus [iPhone](#) compatibles y en el Apple Watch Series 4 o posterior.

Estas funciones en la app Cartera se han diseñado específicamente para reducir las dificultades para el cliente:

- Adición previa a la llegada desde la app del hotel, para añadir un pase a la app Cartera antes de la estancia.
- Mosaicos del pase de registro de entrada, para iniciar los registros de entrada y las asignaciones de habitación desde la app Cartera.
- Actualizaciones clave posteriores a la adición, para poder ampliar o modificar las estancias actuales.
- Posibilidad de tener las llaves de varias habitaciones en un solo pase en la app Cartera.
- Archivo automático de las llaves caducadas en la app Cartera.

Tarjetas de identificación de las empresas

Las tarjetas de identificación de los empleados de los socios admitidos pueden añadirse a la app Cartera en el iPhone y el Apple Watch, lo que permite a los empleados de todo el mundo acceder sin contacto a sus lugares de trabajo. Para añadir una tarjeta de identificación, un empleado debe tener activada la autenticación multifactor para la cuenta utilizada para iniciar sesión en la app proporcionada por su empresa.

La tarjeta de identificación del empleado aprovecha las funciones de acceso de Apple, permitiendo a los usuarios:

- añadir automáticamente una tarjeta de identificación del empleado a su Apple Watch enlazado a través de la adición push que no requiere la instalación de la app de un socio;
- acceder sin problemas a los servicios de la oficina utilizando el modo exprés;
- acceder al lugar de trabajo incluso si el iPhone se queda sin batería.

Carnés de estudiante

En iOS 12 o posterior, los estudiantes, el profesorado y el personal de campus participantes pueden añadir sus carnés de estudiante a la app Cartera en modelos compatibles de iPhone y Apple Watch para acceder a ciertas ubicaciones y pagar allí donde se acepte su tarjeta.

El usuario puede añadir el carné de estudiante a la app Cartera mediante una app proporcionada por la entidad emisora de la tarjeta o por la institución participante. El proceso técnico para ello es el mismo que el descrito en [Añadir tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta](#). Además, las apps emisoras deben admitir la autenticación de doble factor en las cuentas que protegen el acceso a los carnés de estudiante. Una tarjeta puede estar configurada simultáneamente en hasta dos dispositivos Apple compatibles cualesquiera en los que se haya iniciado sesión con el mismo ID de Apple.

Hogares multifamiliares

Los inquilinos y el personal de las instalaciones asociadas admitidas pueden utilizar la llave de su casa en la app Cartera para acceder al edificio, al apartamento y a las zonas comunes. La llave de casa se puede añadir desde la app proporcionada por el socio. En el caso de los socios que admiten la adición sin fricción, los administradores de propiedades pueden enviar a los inquilinos un enlace para iniciar el envío mediante su canal de mensajería preferido (por ejemplo, correo electrónico o SMS), de modo que el inquilino solo tenga que pulsar el enlace para obtener la llave. Los clips de apps también proporcionan una experiencia segura y sin problemas, con lo que se puede enviar una llave sin instalar la aplicación de un socio. Para obtener más información, consulta el artículo de soporte técnico de Apple [Usar clips de apps en el iPhone](#).

Llave de casa

Una llave de casa en la app Cartera puede utilizarse con cerraduras compatibles con NFC con un simple toque de un iPhone o Apple Watch. Para más información sobre cómo un usuario puede configurar y utilizar una llave de casa, consulta el artículo de soporte técnico de Apple [Abrir la puerta con una llave de casa en el iPhone](#).

Cuando un usuario configura una llave de casa, todos los residentes de su hogar también reciben automáticamente la llave de casa. Para seguir compartiendo una llave de casa o eliminar a un miembro de una casa compartida, el propietario de una casa puede usar la app Casa para gestionar las invitaciones y los miembros. Cuando un usuario decide aceptar una invitación para unirse a una casa con una llave de casa, se inicia la adición de la llave de casa en la app Cartera en sus dispositivos. Si un usuario decide abandonar una casa o si el propietario de la casa le retira el acceso, estas acciones también eliminan la llave de la casa de la app Cartera.

Llave del coche

Ciertos modelos de dispositivos iPhone, así como los Apple Watch enlazados, ofrecen compatibilidad nativa con el almacenamiento digital de las llaves del coche en Cartera. Las llaves del coche aparecen representadas como tarjetas en la app Cartera (creadas por Apple en nombre del fabricante del automóvil) y son compatibles con todas las funciones de las tarjetas de Apple Pay (el modo Perdido de iCloud, el borrado remoto, la eliminación local de tarjetas y la opción "Borrar contenidos y ajustes"). Además de la gestión estándar de tarjetas de Apple Pay, las llaves del coche compartidas se pueden eliminar del iPhone del propietario, de su Apple Watch y de la interfaz de usuario del vehículo.

La función de llaves del coche se puede usar para abrir y cerrar el vehículo, arrancar el motor o poner el modo de conducción. La "transacción estándar" ofrece autenticación mutua y es obligatoria para arrancar el motor. Las transacciones de apertura y cierre pueden utilizar la "transacción rápida" cuando sea necesario para optimizar el rendimiento.

Las llaves se crean al enlazar un iPhone con un vehículo propio compatible. Todas las llaves se crean en el chip Secure Element integrado basadas en la generación incorporada de claves de curva elíptica (NIST P-256) (ECC-OBKG) y en el caso de las llaves privadas nunca salen de Secure Element. Para la comunicación entre los dispositivos y el vehículo se utiliza NFC, o una combinación de Bluetooth LE y UWB, y para la gestión de las llaves se usa una API entre Apple y el servidor del fabricante del vehículo con TLS con autenticación mutua. Después de enlazar una llave con un iPhone, cualquier Apple Watch que esté enlazado con ese iPhone también podrá recibir una llave. Si se elimina una llave en el vehículo o en el dispositivo, no se podrá restaurar. Las llaves de dispositivos perdidos o robados pueden suspenderse y reactivarse, pero para volver a proporcionarlas en un nuevo dispositivo es necesario enlazarlas o compartirlas de nuevo.

Seguridad de la función de llave del coche en iOS

Los desarrolladores pueden ofrecer compatibilidad con funciones de acceso seguro sin llave al vehículo en determinados modelos de iPhone y en los Apple Watch enlazados.

Proceso de enlace por parte del propietario

El propietario debe probar que el vehículo es suyo (el método depende del fabricante del vehículo) y puede iniciar el proceso de enlace en la app del fabricante del vehículo, mediante un enlace de correo electrónico que le enviará el fabricante o a través del menú del vehículo. En cualquiera de los casos, el propietario debe presentar una contraseña confidencial de enlace única en el iPhone, que servirá para generar un canal de enlace seguro mediante el protocolo SPAKE2+ con la curva NIST P-256. Si se usa la app o el enlace de correo electrónico, la contraseña se transferirá automáticamente al iPhone, donde la contraseña deberá introducirse manualmente si se inicia el enlace desde el vehículo.

Llaves compartidas

El iPhone enlazado del propietario puede compartir las llaves con los dispositivos iPhone compatibles de familiares y amigos (y con los correspondientes Apple Watch enlazados) enviando una invitación específica para dicho dispositivo mediante iMessage y el [servicio de identidad \(IDS\)](#) de Apple. Todos los comandos para compartir llaves se intercambian mediante la función IDS con encriptación de punto a punto. El iPhone enlazado del propietario impide que el canal IDS cambie durante el proceso de compartir las llaves para protegerlo frente al reenvío de la invitación.

Tras aceptar la invitación, el iPhone del familiar o amigo crea una llave digital y envía la cadena de certificados de creación de la llave al iPhone enlazado del propietario para verificar que la llave se ha creado en un dispositivo Apple auténtico. El iPhone enlazado del propietario firma la clave pública ECC del iPhone del otro familiar o amigo y devuelve la firma al iPhone de este. La operación de firma en el dispositivo del propietario requiere que el usuario se autentique (mediante Face ID, Touch ID o código) y una intención del usuario segura descrita en [Usos de Face ID y Touch ID](#). La autorización se solicita al enviar la invitación y se almacena en Secure Element para utilizarla cuando el dispositivo del amigo devuelva la solicitud de firma. Las autorizaciones de la llave se proporcionan al vehículo bien en línea por el servidor del fabricante del vehículo o durante el primer uso de la llave compartida en el vehículo.

Eliminación de una llave

Las llaves pueden eliminarse del dispositivo llavero desde el dispositivo del propietario y del vehículo. La eliminación de llaves en el iPhone llavero son inmediatas, incluso si el llavero está utilizando la llave. Por ello, se muestra una advertencia importante antes de la eliminación. Es posible que la eliminación de llaves en el vehículo se pueda realizar en cualquier momento o solo cuando el vehículo esté conectado a internet.

En ambos casos, la eliminación en el dispositivo llavero o en el vehículo se notifica a un servidor de inventario de llaves (KIS) del fabricante del vehículo, que registra las llaves generadas para un vehículo con fines relacionados con el seguro del coche.

El propietario puede solicitar la eliminación de una llave desde el reverso de la tarjeta de propietario. La solicitud se enviará en primer lugar al fabricante del vehículo para eliminar la llave en el vehículo. El fabricante del vehículo establece las condiciones para la eliminación de la llave en el vehículo. Solo cuando la llave se haya eliminado del vehículo, el servidor del fabricante del automóvil enviará una solicitud de anulación remota al dispositivo llavero.

Una vez anulada una llave en el dispositivo, el applet que gestiona las llaves de coche digitales crea una acreditación de anulación firmada criptográficamente, que sirve como prueba de la eliminación por parte del fabricante del vehículo y que se usa para eliminar la llave del KIS.

Transacciones con el estándar NFC

Para los vehículos que usan una llave NFC, se establece un canal seguro entre el lector y un iPhone mediante la generación de pares de claves efímeras en el lector y en el iPhone. Mediante un método de concordancia de claves, se puede obtener un secreto compartido en ambos lados que se usa para generar una clave simétrica compartida mediante el protocolo Diffie-Hellman, una función de derivación de claves y firmas a partir de la clave duradera establecida durante el enlace.

La clave pública efímera generada en el vehículo se firma con la clave privada duradera del lector, lo que permite que el iPhone autentique el lector. Desde la perspectiva del iPhone, este protocolo está diseñado para impedir que se revelen datos sensibles de privacidad a un atacante que intercepte la comunicación.

Por último, el iPhone utiliza el canal seguro establecido para encriptar su identificador de clave pública junto con la firma calculada en un reto derivado de los datos del lector y determinados datos adicionales específicos de la app. Esta verificación de la firma del iPhone que hace el lector permite que este autentique el dispositivo.

Transacciones rápidas

El iPhone genera un criptograma basado en un secreto compartido anteriormente durante una transacción estándar. Este criptograma permite al vehículo autenticar rápidamente el dispositivo en escenarios en los que es necesario optimizar el rendimiento. Opcionalmente, se establece un canal seguro entre el vehículo y el dispositivo mediante la derivación de claves de sesión a partir de un secreto previamente compartido durante una transacción estándar y un nuevo par de claves efímeras. La capacidad del vehículo de establecer el canal seguro autentica el vehículo en el iPhone.

Transacciones con el estándar BLE/UWB

Para los vehículos que usan una llave UWB, se establece una sesión Bluetooth LE entre el vehículo y el iPhone. De forma similar a la transacción NFC, se obtiene un secreto compartido por ambas partes y se usa para establecer una sesión segura. Esta sesión se usa para derivar y acordar posteriormente una clave secreta de alcance UWB (URSK). La clave URSK se proporciona a las radios UWB del dispositivo del usuario y del vehículo para permitir la localización precisa del dispositivo del usuario en una posición específica cerca o dentro del vehículo. El vehículo usa entonces la posición del dispositivo para tomar decisiones sobre el desbloqueo o el arranque del vehículo. Las claves URSK tienen un TTL predefinido. Para evitar que se interrumpa el alcance cuando expira un TTL, las claves URSK se pueden predefinir en el SE del dispositivo y en el HSM/SE del vehículo mientras el alcance seguro no está activo pero el BLE está conectado. Esto evita la necesidad de una transacción estándar para derivar una nueva URSK en una situación crítica en el tiempo. La URSK prederivada puede transferirse muy rápidamente a las radios UWB del coche y del dispositivo para evitar la interrupción del alcance UWB.

Privacidad

El servidor de inventario de llaves (KIS) del fabricante del vehículo no almacena el identificador del dispositivo, el SEID ni el ID de Apple. Tan solo almacena un identificador mutable, el identificador de la autoridad de certificación de la instancia. Este identificador no está vinculado a datos privados concretos del dispositivo ni por el servidor, y se elimina cuando el usuario borra el dispositivo completamente (mediante "Borrar contenidos y ajustes").

Añadir tarjetas de transporte y de dinero electrónico a la app Cartera

En muchos mercados globales, los usuarios pueden añadir tarjetas de transporte y tarjetas de dinero electrónico admitidas a la app Cartera en modelos compatibles de iPhone y Apple Watch. En función del operador, esto puede hacerse bien al transferir el saldo o el abono de transporte (o ambas cosas) de una tarjeta física a su representación digital en Cartera, o bien al enviar los datos de una tarjeta de transporte nueva o tarjeta de dinero electrónico desde Cartera o desde la app de la entidad emisora de la tarjeta. Después de añadir las tarjetas de transporte a la app Cartera, los usuarios pueden tomar el transporte público con solo acercar el iPhone o el Apple Watch al lector de tarjetas de transporte. Algunas tarjetas de transporte también sirven para realizar pagos.

Cómo funcionan las tarjetas de transporte y de dinero electrónico

Las tarjetas de transporte y tarjetas de dinero electrónico añadidas se asocian a una cuenta de iCloud del usuario. Si el usuario añade más de una tarjeta a la app Cartera, es posible que Apple o la entidad emisora de la tarjeta pueda enlazar la información personal del usuario y la información de la cuenta asociada entre las tarjetas. Las tarjetas de transporte y de dinero electrónico y las transacciones están protegidas por un conjunto de claves jerárquicas criptográficas.

Durante el proceso de transferencia del saldo de la tarjeta física a la app Cartera, los usuarios deben introducir la información específica de la tarjeta. Los usuarios también pueden proporcionar información personal para demostrar que son los propietarios de la tarjeta. Al transferir abonos de transporte del iPhone al Apple Watch, ambos dispositivos deben tener conexión a internet.

El saldo se puede recargar con fondos de tarjetas de crédito, débito y prepago a través de Cartera o desde la app de la entidad emisora de la tarjeta de transporte o de dinero electrónico. Para comprender la seguridad de la recarga del saldo al usar Apple Pay, consulta [Pagar con tarjetas en apps](#). Para obtener información acerca de cómo se añade la tarjeta desde la app del emisor de la tarjeta, consulta [Añadir tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta](#).

Si se admite el envío de datos desde una tarjeta física, la entidad emisora de la tarjeta de transporte o de dinero electrónico dispone de las claves criptográficas necesarias para autenticar la tarjeta física y verificar los datos que ha introducido el usuario. Una vez verificados los datos, el sistema puede crear un número de cuenta del dispositivo para Secure Element y activar el abono recién añadido en la app Cartera con el saldo transferido. Para algunas tarjetas, una vez enviados los datos de la tarjeta física, esta se desactiva.

Al finalizar cualquier tipo de envío de datos, si el saldo de la tarjeta se almacena en el dispositivo, los datos se encriptan y se almacenan en un applet determinado en Secure Element. El operador dispone de las claves para llevar a cabo operaciones de encriptación en los datos de la tarjeta para las transacciones de saldo.

Por defecto, los usuarios de las tarjetas de transporte se benefician de una experiencia fluida con la tarjeta exprés que les permite pagar y viajar sin necesidad de identificarse con Face ID, Touch ID o un código. Cualquier lector de tarjetas sin contacto cercano en modo exprés puede acceder a información, como las estaciones visitadas recientemente, el historial de transacciones y los billetes adicionales. Los usuarios pueden activar el requisito de autorización mediante Face ID, Touch ID o el código en los ajustes de "Cartera y Apple Pay" si desactivan la tarjeta exprés. Las tarjetas de dinero electrónico no son compatibles con el modo exprés.

Al igual que ocurre con otras tarjetas de Apple Pay, los usuarios pueden suspender o eliminar las tarjetas de dinero electrónico si realizan las acciones siguientes:

- Borrar el dispositivo remotamente con Buscar.
- Activar el modo Perdido con Buscar.
- Introducir un comando de borrado remoto de la solución de [gestión de dispositivos móviles \(MDM\)](#).
- Eliminar todas las tarjetas de la página de la cuenta del ID de Apple.
- Eliminar todas las tarjetas de iCloud.com.
- Eliminar todas las tarjetas de la app Cartera.
- Eliminar la tarjeta en la app de la entidad emisora.

Los servidores de Apple Pay notificarán al operador de la tarjeta que suspenda o desactive esas tarjetas. Si un usuario elimina su tarjeta de transporte o de dinero electrónico desde un dispositivo con conexión a internet, el saldo se puede recuperar si añade la tarjeta a un dispositivo en el que hayan iniciado sesión con el mismo ID de Apple. Si un dispositivo está desconectado de internet, apagado o inhabilitado, es posible que no se pueda recuperar.

Añadir tarjetas de transporte y de dinero electrónico al Apple Watch de un miembro de la familia

En iOS 15 y watchOS 8, el organizador de una familia de iCloud puede añadir tarjetas de tránsito y de dinero electrónico a los dispositivos Apple Watch de los miembros de la familia a través de la app Apple Watch de su iPhone. Cuando se añade una de estas tarjetas al Apple Watch de un miembro de la familia, se requiere que el reloj esté cerca y conectado al iPhone del organizador mediante wifi o Bluetooth. Para que esto ocurra, los miembros de la familia deben tener activada la autenticación de doble factor para su ID de Apple.

Los miembros de la familia pueden enviar una solicitud para añadir dinero a una tarjeta de transporte o de dinero electrónico desde su Apple Watch usando iMessage. El contenido del mensaje está protegido por una encriptación de punto a punto, como se describe en [Descripción general de la seguridad de iMessage](#). Se puede añadir dinero a una tarjeta en el Apple Watch de un miembro de la familia de forma remota usando una conexión wifi o de datos móviles. No es necesario estar cerca.

Nota: Puede que esta función no esté disponible en todos los países o regiones.

Tarjetas de crédito y débito

En algunas ciudades, los lectores de tarjetas de transporte aceptan tarjetas (inteligentes) EMV para pagar los viajes de transporte público. Cuando los usuarios presentan una tarjeta de crédito o débito a esos lectores, el usuario debe autenticarse, del mismo modo que en "Pagos con tarjetas de crédito y débito en tiendas".

En iOS 12.3 o posterior, algunas tarjetas EMV de crédito o débito existentes en la app Cartera pueden habilitarse como tarjeta exprés. La tarjeta exprés permite a los usuarios pagar un viaje en los operadores de transporte compatibles sin necesidad de identificarse con Face ID, Touch ID o un código. Cuando un usuario facilita una tarjeta EMV de crédito o débito, la primera tarjeta facilitada a la app Cartera se activa para la tarjeta exprés. El usuario puede pulsar el botón Más en el anverso de la tarjeta en la app Cartera y desactivar la tarjeta exprés para esa tarjeta si establece "Ajustes de la tarjeta exprés" en Ninguno. El usuario también puede seleccionar una tarjeta de crédito o débito diferente como su tarjeta exprés usando la app Cartera. Para volver a activar o para seleccionar una tarjeta exprés diferente, se requiere Face ID, Touch ID o el código.

Se puede usar Apple Card y Apple Cash con la tarjeta exprés.

Documentos de identidad en Cartera

En el iPhone 8 o posterior con iOS 15.4 o posterior y en el Apple Watch Series 4 o posterior con watchOS 8.4 o posterior, los usuarios pueden añadir su documento de identidad o el carné de conducir a la app Cartera y tocar su iPhone o Apple Watch para presentarlo sin problemas y de forma segura en los establecimientos participantes.

Nota: Esta función solo está disponible en los estados participantes de EE. UU.

Los documentos de identidad en la app Cartera usan funciones de seguridad integradas en el hardware y el software del dispositivo del usuario para ayudar a proteger su identidad y ayudar a mantener la seguridad de su información personal.

Añadir un carné de conducir o documento de identidad a la app Cartera

En el iPhone, los usuarios solo tienen que tocar el botón Añadir (+) en la parte superior de la pantalla de la app Cartera para empezar a añadir su carné de conducir o documento de identidad. Si los usuarios tienen un Apple Watch enlazado en el momento de la configuración, se les pedirá que añadan también su carné de conducir o documento de identidad a la app Cartera del Apple Watch.

En primer lugar, se pide a los usuarios que usen su iPhone para escanear el anverso y el reverso del permiso de conducir físico o del documento de identidad. El iPhone evalúa la calidad y el tipo de imágenes para ayudar a garantizar que las imágenes proporcionadas son aceptables por la autoridad estatal emisora. Estas imágenes del carné de identidad se encriptan con la clave de la autoridad estatal emisora en el dispositivo y luego se envían a la autoridad estatal emisora.

A continuación, se pide al usuario que complete una serie de movimientos faciales y de la cabeza. Estos movimientos son evaluados por el dispositivo del usuario y por Apple para ayudar a reducir el riesgo de que alguien use una fotografía, un vídeo o una máscara para intentar añadir el documento de identidad de otra persona a la app Cartera. Los resultados del análisis de estos movimientos se envían a la autoridad estatal emisora, pero no el vídeo de los movimientos en sí.

Para ayudar a garantizar que la persona que añade el documento de identidad a la app Cartera es la misma a la que pertenece el documento de identidad, se pide a los usuarios que se hagan un selfie. Antes de que la foto del usuario se envíe a la autoridad estatal emisora, los servidores de Apple y el dispositivo del usuario comparan la foto con el aspecto de la persona que realizó la serie de movimientos faciales y de la cabeza y ayudan a garantizar que la foto que se envía es de una persona viva con el mismo aspecto físico que el del documento de identidad. Una vez realizada la comparación, la foto se encripta en el dispositivo y se envía a la autoridad estatal emisora para que la compare con la imagen registrada de su documento de identidad.

Por último, se pide a los usuarios que realicen una autenticación mediante Face ID o Touch ID. El dispositivo del usuario vincula este único Face ID o Touch ID biométrico coincidente con el documento de identidad para ayudar a garantizar que solo la persona que añadió el documento de identidad a este iPhone pueda presentarlo; no se puede usar otra información biométrica inscrita para autorizar la presentación del documento de identidad. Esto ocurre estrictamente en el dispositivo y no se envía a la autoridad estatal emisora.

La autoridad estatal emisora recibirá la información necesaria para configurar el documento de identidad digital. Esto incluye imágenes del anverso y el reverso del documento de identidad del usuario, datos leídos del código de barras PDF417, así como el selfie que el usuario se hizo como parte del proceso de verificación del documento de identidad. El estado emisor también recibe un valor de un solo dígito, utilizado para ayudar a evitar el fraude, que se basa en los patrones de uso del dispositivo del usuario, los datos de configuración y la información sobre su ID de Apple personal. En última instancia, es el estado emisor el que decide aprobar o rechazar que el documento de identidad se añada a la app Cartera.

Después de que la autoridad estatal emisora autorice añadir el documento de identidad o el permiso de conducir a la app Cartera, se genera un par de claves en el Secure Element del iPhone que ancla el documento de identidad del usuario a ese dispositivo específico. Si se añade al Apple Watch, se genera un par de claves en el Secure Element del Apple Watch.

Una vez que el documento de identidad está en el iPhone, la información reflejada en el documento de identidad del usuario en la app Cartera se almacena en un formato encriptado y protegido por Secure Enclave.

Usar un carné de conducir o documento de identidad en la app Cartera

Para usar su documento de identidad en la app Cartera, los usuarios tienen que autenticarse mediante el Face ID o Touch ID del dispositivo asociado al documento de identidad en la app Cartera antes de que el iPhone presente la información al lector de identidad.

Para usar su documento de identidad en la app Cartera en el Apple Watch, los usuarios tienen que desbloquear su iPhone usando el aspecto de Face ID o la huella digital de Touch ID asociados cada vez que se pongan el Apple Watch. Entonces, pueden usar su documento de identidad en la app Cartera sin autenticarse hasta que se quiten el Apple Watch de nuevo. Esta función aprovecha las capacidades básicas del desbloqueo automático detalladas en [Seguridad del sistema en watchOS](#).

Cuando los usuarios acercan el iPhone o Apple Watch al lector de identidad, ven una indicación en el dispositivo que muestra qué información específica se está solicitando, por quién, y si tienen intención de almacenarla. Tras autorizar con el Face ID o Touch ID asociado, la información de identidad solicitada se libera del dispositivo.

Importante: Los usuarios no necesitan desbloquear, mostrar o entregar su dispositivo para presentar su documento de identidad.

Si los usuarios tienen una función de accesibilidad, como el control por voz, el control por botón o AssistiveTouch, pueden usar su código para acceder y presentar su información en lugar de activar Face ID o Touch ID.

La transmisión de los datos de identidad al lector de identidad sigue los estándares ISO/IEC 18013-5, que prevén varios mecanismos de seguridad disponibles capaces de detectar, disuadir y mitigar los riesgos de seguridad. Estos consisten en medidas para evitar las falsificaciones y preservar la integridad de los datos de identidad, la vinculación del dispositivo, el consentimiento informado y la confidencialidad de los datos del usuario a través de enlaces de radio.

Medidas para evitar las falsificaciones y preservar la integridad de los datos de identidad

Los documentos de identidad en la app Cartera usan una firma proporcionada por el emisor para que cualquier lector compatible con los estándares ISO/IEC 18013-5 pueda verificar el documento de identidad de un usuario en la app Cartera. Además, todos los elementos de datos del documento de identidad en la app Cartera están protegidos individualmente frente a la falsificación. Esto permite que el lector de identidad solicite un subconjunto específico de los elementos de datos presentes en el documento de identidad en la app Cartera y que el documento de identidad en la app Cartera responda con ese mismo subconjunto, compartiendo así solo los datos solicitados y maximizando la privacidad del usuario.

Vinculación del dispositivo

La autenticación de los documentos de identidad en la app Cartera usa una firma de dispositivo para protegerse frente a la clonación de un documento de identidad y la reproducción de una transacción de identidad. Al almacenar la clave privada para la autenticación del documento de identidad en el Secure Element del iPhone, el documento de identidad está vinculado al mismo dispositivo para el que la autoridad estatal emisora creó el documento de identidad.

Consentimiento informado

La autenticación del lector de documentos de identidad en la app Cartera usa el protocolo definido en los estándares ISO/IEC 18013-5. Durante la presentación, se le muestra un icono derivado del certificado del lector para dar al usuario la seguridad de que está interactuando con el tercero previsto.

Confidencialidad de los datos del usuario a través de enlaces de radio

La encriptación de la sesión ayuda a garantizar que toda la información de identificación personal (PII) que se intercambia entre el documento de identidad en la app Cartera y el lector de identidad está encriptada. La encriptación se realiza en la capa de la aplicación. Por lo tanto, la seguridad de la encriptación de la sesión no depende de la seguridad proporcionada por la capa de transmisión (por ejemplo, NFC, Bluetooth y wifi).

Los documentos de identidad en la app Cartera ayudan a mantener la privacidad de la información de los usuarios

Los documentos de identidad en la app Cartera se adhieren al proceso de "recuperación del dispositivo" descrito en los estándares ISO/IEC 18013-5. La recuperación del dispositivo evita la necesidad de hacer llamadas al servidor durante la presentación, protegiendo así a los usuarios de ser rastreados por Apple y el emisor.

iMessage

Descripción general de la seguridad de iMessage

iMessage de Apple es un servicio de mensajería para dispositivos iOS y iPadOS, para el Apple Watch y para ordenadores Mac. iMessage admite texto y archivos adjuntos tales como fotos, contactos, ubicaciones, enlaces y archivos que se adjuntan directamente a un mensaje, como, por ejemplo, un icono de pulgar hacia arriba. Puesto que los mensajes se muestran en todos los dispositivos registrados de un usuario, una conversación se puede continuar desde cualquiera de sus dispositivos. iMessage utiliza el [servicio de notificaciones push de Apple \(APNs\)](#) en gran medida. Apple no registra ni el contenido de los mensajes ni el de los archivos adjuntos, que está protegido mediante una encriptación de punto a punto, de modo que únicamente el emisor y el receptor pueden acceder a ellos, ya que Apple no puede desencriptar los datos.

Cuando un usuario activa iMessage en un dispositivo, el dispositivo genera pares de claves de encriptación y de firma para usarlas con el servicio. Para la encriptación, hay una clave RSA de 1280 bits, además de una clave de encriptación EC de 256 bits en la curva P-256 del NIST. Para las firmas, se usan claves de firma de 256 bits con el [algoritmo de firma digital de curva elíptica \(ECDSA\)](#). Las claves privadas se guardan en el llavero del dispositivo y solo están disponibles tras el primer desbloqueo. Las claves públicas se envían al [servicio de identidad \(IDS\) de Apple](#), donde se asocian al número de teléfono o la dirección de correo electrónico del usuario, junto con la dirección del APNs del dispositivo.

A medida que los usuarios activan otros dispositivos para usarlos con iMessage, las claves públicas de encriptación y firma, las direcciones del APNs y los números de teléfono asociados se añaden al servicio de directorio. Los usuarios también pueden añadir más direcciones de correo electrónico, que se verifican mediante el envío de un enlace de confirmación. La SIM y la red del operador verifican los números de teléfono. En algunas redes, esto requiere el uso de mensajes de texto (al usuario se le muestra un cuadro de diálogo de confirmación si el mensaje de texto no es gratuito). Además de iMessage, es posible que varios servicios del sistema requieran la verificación del número de teléfono, como FaceTime y iCloud. En todos los dispositivos registrados del usuario, se muestra un mensaje de aviso al añadir un dispositivo, número de teléfono o dirección de correo electrónico nuevos.

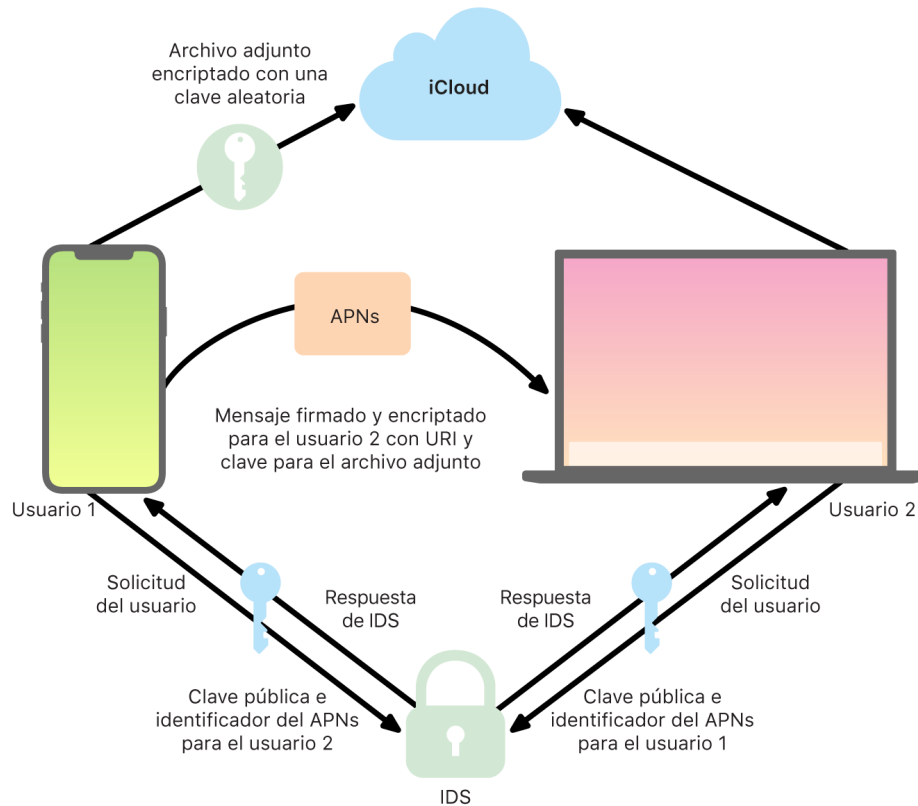
Cómo iMessage envía y recibe mensajes de forma segura

Los usuarios inician una nueva conversación de iMessage al introducir una dirección o un nombre. Si introducen un número de teléfono o una dirección de correo electrónico, el dispositivo se pone en contacto con el [servicio de identidad \(IDS\) de Apple](#) para recuperar las claves públicas y las direcciones del APNs de todos los dispositivos asociados al destinatario. Si el usuario introduce un nombre, el dispositivo usa primero la app Contactos del usuario para recopilar los números de teléfono y las direcciones de correo electrónico asociadas a ese nombre y, a continuación, obtiene las claves públicas y las direcciones del APNs del IDS de Apple.

El mensaje que envía el usuario se encripta de forma individual para cada uno de los dispositivos del destinatario. Las claves de encriptación públicas y las claves de firmas de los dispositivos receptores se obtienen del IDS. El dispositivo desde el que se envían los mensajes genera un valor aleatorio de 88 bits para cada dispositivo de destino y lo utiliza como clave HMAC-SHA256 para crear un valor de 40 bits derivado de la clave pública del emisor y receptor y del texto sin formato. La concatenación de los valores de 88 bits y de 40 bits constituye una clave de 128 bits, que encripta el mensaje utilizando el estándar AES en modo de contador (CTR). El dispositivo que recibe el mensaje utiliza el valor de 40 bits para verificar la integridad del texto sin formato desencriptado. Esta clave AES por mensaje se encripta con RSA-OAEP para la clave pública del dispositivo receptor. Con el texto del mensaje encriptado y la clave del mensaje encriptada se genera un hash SHA-1, que se firma con el [algoritmo de firma digital de curva elíptica \(ECDSA\)](#) utilizando la clave de firma privada del dispositivo emisor. En iOS 13 o posterior y iPadOS 13.1 o posterior, los dispositivos pueden usar una encriptación de esquema de encriptación integrado de curva elíptica (ECIES), en lugar de una encriptación RSA.

Los mensajes que se obtienen, uno para cada dispositivo receptor, están constituidos por el texto del mensaje encriptado, la clave del mensaje encriptada y la firma digital del emisor. A continuación, se mandan al APNs para que los envíe. Los metadatos, como la fecha y la información sobre el enrutamiento del APNs no se encriptan. La comunicación con el APNs se encripta utilizando un canal TLS de secreto-hacia-delante.

El APNs solo puede transmitir mensajes de 4 o 16 kB como máximo en función de la versión de iOS o iPadOS. Si el texto del mensaje es demasiado largo o si se incluye un archivo adjunto (por ejemplo, una foto), el archivo adjunto se encripta con AES en modo CTR utilizando una clave de 256 bits generada aleatoriamente y se carga a iCloud. A continuación, la clave AES para el archivo adjunto, su [identificador uniforme de recursos \(URI\)](#) y un hash SHA-1 de su forma encriptada se envían al destinatario como el contenido de un mensaje de iMessage, cuya confidencialidad e integridad están protegidas mediante la encriptación normal de iMessage, como se muestra en el diagrama siguiente.



En el caso de las conversaciones de grupo, este proceso se repite para cada destinatario y sus dispositivos.

En cuanto a la recepción, cada dispositivo recibe una copia del mensaje desde el APNs y, en caso necesario, recupera el archivo adjunto de iCloud. El número de teléfono o la dirección de correo electrónico del emisor del mensaje se cotejan con los contactos del receptor para que, cuando sea posible, se muestre el nombre.

Como sucede con todas las notificaciones push, el mensaje se elimina del APNs una vez enviado. Sin embargo, a diferencia de lo que sucede con otras notificaciones del APNs, los mensajes de iMessage se ponen en la cola para enviarlos a los dispositivos sin conexión. Los mensajes se almacenan en servidores de Apple durante un plazo máximo de 30 días.

Compartir nombre y foto en iMessage de forma segura

La opción de compartir nombre y foto en iMessage permite al usuario compartir un nombre y una foto mediante iMessage. El usuario puede seleccionar la información de "Mi tarjeta" o personalizar el nombre e incluir la imagen que quiera. La opción de compartir nombre y foto en iMessage utiliza un sistema de dos etapas para distribuir el nombre y la foto.

Los datos están subdivididos en campos y cada uno de ellos se encripta y autentica por separado, además de autenticarse juntos con el siguiente proceso. Hay tres campos:

- Nombre
- Foto
- Nombre de archivo de la foto

Uno de los primeros pasos en la creación de datos es generar aleatoriamente en el dispositivo el registro de una clave de 128 bits. A continuación, esta clave de registro deriva con HKDF-HMAC-SHA256 para crear tres subclaves: Clave 1:Clave 2:Clave 3 = HKDF(clave de registro, "alias"). Para cada campo, se genera un vector de inicialización (IV) de 96 bits aleatorio y los datos se encriptan usando AES-CTR y la Clave 1. A continuación, se calcula un código de autenticación de mensaje (MAC) con HMAC-SHA256 mediante la Clave 2, abarcando el nombre del campo, el campo IV y el texto cifrado del campo. Por último, el conjunto de valores MAC del campo individual se concatenan y su MAC se calcula con HMAC-SHA256 mediante la Clave 3. La MAC de 256 bits se almacena junto con los datos encriptados. Los primeros 128 bits de esta MAC se usan como RecordID.

A continuación, este registro encriptado se almacena en la base de datos pública CloudKit bajo RecordID. Este registro nunca se cambia y cada vez que un usuario decide cambiar su nombre y foto, se vuelve a generar un nuevo registro encriptado. Cuando el usuario 1 elige compartir su nombre y foto con el usuario 2, envía la clave de registro junto con el recordID dentro de la carga útil de su iMessage, que está [encriptada](#).

Cuando el dispositivo del usuario 2 recibe esta carga útil de iMessage, detecta que la carga útil contiene un recordID de Alias y Foto, y una clave. A continuación, el dispositivo del usuario 2 accede a la base de datos pública CloudKit para recuperar el nombre y la foto encriptados de recordID y lo envía en el iMessage.

Una vez recuperado el mensaje, el dispositivo del usuario 2 desencripta la carga útil y verifica la firma mediante el propio recordID. Si esto se aprueba, al usuario 2 se le muestra el nombre y la foto y puede añadir esta información a sus contactos o usarla para Mensajes.

Seguridad de Apple Messages for Business

Apple Messages for Business es un servicio de mensajería que permite a los usuarios comunicarse con empresas mediante la app Mensajes. Con Apple Messages for Business, el usuario siempre tiene el control de la conversación. También puede eliminar la conversación y bloquear a la empresa para impedir que pueda enviarle mensajes en el futuro. Para garantizar la privacidad, las empresas no reciben el número de teléfono, la dirección de correo electrónico ni la información de la cuenta de iCloud del usuario. En su lugar, el [servicio de identidad \(IDS\) de Apple](#) genera un identificador único personalizado, llamado *identificador opaco*, que se comparte con las empresas. El identificador opaco es exclusivo para la relación entre el ID de Apple del usuario y el identificador de la empresa. Un usuario tendrá un identificador opaco distinto para cada empresa con la que contacte mediante Apple Messages for Business. El usuario decide si quiere compartir información de identificación personal con la empresa y cuándo, y el servicio de Apple Messages for Business nunca almacena el historial de conversaciones.

Apple Messages for Business admite ID de Apple gestionados de [Apple Business Manager](#) y determina si están activados para iMessage y FaceTime en [Apple School Manager](#).

Los mensajes enviados a las empresas se encriptan entre el dispositivo del usuario y los servidores de mensajería de Apple, utilizando la misma seguridad y servidores de mensajería de Apple que iMessage. Los servidores de mensajería de Apple desencriptan estos mensajes en la RAM y los transmiten a la empresa a través de un enlace encriptado mediante TLS 1.2. Los mensajes nunca se almacenan en formato desencriptado mientras se transfieren al servicio de Apple Messages for Business. Las respuestas de las empresas también se envían mediante TLS 1.2 a los servidores de mensajería de Apple, donde se encriptan con las claves públicas únicas de cada dispositivo de destino.

Si el dispositivo del usuario está en línea, el mensaje se entrega inmediatamente y no se almacena en caché en los servidores de mensajería de Apple. Si el dispositivo del usuario no está en línea, el mensaje encriptado se almacena en caché durante un máximo de 30 días para permitir que el usuario lo reciba cuando el dispositivo vuelva a tener conexión. En el momento en el que el dispositivo vuelva a estar en línea, se entregará el mensaje y se eliminará de la caché. Transcurridos 30 días, un mensaje en caché sin entregar expirará y se eliminará de forma permanente.

Seguridad de FaceTime

FaceTime es el servicio de llamadas de audio y vídeo de Apple. Al igual que iMessage, las llamadas de FaceTime utilizan el [servicio de notificaciones push de Apple \(APNs\)](#) para establecer una conexión inicial con los dispositivos registrados del usuario. El contenido de audio/vídeo de las llamadas FaceTime se protege mediante la encriptación de punto a punto, con lo cual, únicamente el emisor y el receptor pueden acceder a él, ya que Apple no puede descifrar los datos.

La conexión inicial de FaceTime se realiza a través de una infraestructura de servidores de Apple, que transmite paquetes de datos entre los dispositivos registrados de los usuarios. Al usar las notificaciones push de Apple (APNs) y mensajes de Utilidades Transversales de Sesión para NAT (STUN) a través de la conexión transmitida, los dispositivos verifican sus certificados de identidad y establecen un secreto compartido para cada sesión. El secreto compartido se utiliza para derivar las claves por sesión para los canales de contenido multimedia, que se transmiten mediante el protocolo de transporte en tiempo real seguro (SRTP). Los paquetes SRTP se encriptan con AES-256 en modo de contador y se autentican con HMAC-SHA1. Después de la conexión inicial y la configuración de seguridad, FaceTime utiliza STUN y el estándar de establecimiento de conexión a internet (ICE) para establecer una conexión P2P entre los dispositivos, si es posible.

Con FaceTime en grupo, se admiten hasta 33 participantes a la vez en FaceTime. Al igual que las clásicas llamadas FaceTime individuales, las llamadas en grupo están encriptadas de punto a punto entre los dispositivos de los participantes invitados. Aunque las llamadas FaceTime en grupo reutilizan gran parte de la infraestructura y el diseño de las llamadas FaceTime individuales, estas llamadas en grupo incluyen un mecanismo de establecimiento de claves integrado, además de la autenticidad que proporciona el [servicio de identidad \(IDS\) de Apple](#). Este protocolo proporciona confidencialidad directa; de este modo, si el dispositivo de un usuario se viera comprometido, no se filtraría el contenido de las llamadas anteriores. Las claves de sesión se encapsulan mediante AES-SIV y se distribuyen entre los participantes con una construcción ECIES con claves P-256 ECDH efímeras.

Cuando se añade un nuevo número de teléfono o dirección de correo electrónico a una llamada FaceTime en grupo en curso, los dispositivos activos establecen nuevas claves de contenido y nunca comparten las claves utilizadas anteriormente con los nuevos dispositivos invitados.

Buscar

Seguridad de Buscar

La app Buscar para dispositivos Apple se ha diseñado sobre una base de criptografía de clave pública avanzada.

Descripción general

La app Buscar combina Buscar mi iPhone y Buscar a mis Amigos en una sola app en iOS, iPadOS y macOS. Buscar ayuda a los usuarios a localizar un dispositivo extraviado, incluso un Mac sin conexión. Un dispositivo que tenga conexión puede informar de su ubicación al usuario simplemente por iCloud. Buscar funciona con dispositivos sin conexión enviando señales Bluetooth de corto alcance desde el dispositivo extraviado que pueden ser detectadas por otros dispositivos Apple cercanos. Luego, dichos dispositivos cercanos retransmiten la ubicación detectada del dispositivo extraviado a iCloud para que los usuarios puedan localizarlo en la app Buscar, garantizando en todo momento la protección de la privacidad y la seguridad de todos los usuarios implicados. Buscar también permite encontrar ordenadores Mac que no tengan conexión y estén en reposo.

Mediante Bluetooth y los cientos de millones de dispositivos iOS, iPadOS y macOS en uso por todo el mundo, un usuario puede buscar un dispositivo perdido, incluso si no se puede conectar a una red móvil o wifi. Cualquier dispositivo iOS, iPadOS o macOS que tenga "Encontrar sin conexión" activado en los ajustes de Buscar puede actuar como "dispositivo localizador". Esto significa que el dispositivo puede detectar la presencia de otro dispositivo perdido que está desconectado de internet mediante Bluetooth y, a continuación, usar su conexión de red para informar al propietario de la ubicación aproximada. Cuando un dispositivo tiene la búsqueda sin conexión activada, también significa que otros participantes pueden localizarlo del mismo modo. Toda esta interacción es anónima, está encriptada de punto a punto y diseñada para ser eficiente a nivel de batería y de datos. Hay un impacto mínimo en la duración de la batería y en el uso del plan de datos móviles y, además, se protege mejor la privacidad del usuario.

Nota: Puede que Buscar no esté disponible en todos los países o regiones.

Encriptación de punto a punto

Buscar se ha diseñado sobre una base de criptografía de clave pública avanzada. Cuando se activa la búsqueda sin conexión en los ajustes de Buscar, se genera un par de claves de encriptación privada EC P-224 de la curva elíptica directamente en el dispositivo y marcadas como $\{d, P\}$, donde d es la clave privada y P es la clave pública. Además, un SK_0 secreto de 256 bits y un contador i se inicializan a 0. Este par de claves privadas y el secreto nunca se envían a Apple y solo se sincronizan con los otros dispositivos del usuario mediante la encriptación de punto a punto utilizando el llavero de iCloud. El secreto y el contador se usan para derivar la clave simétrica SK_i actual con la siguiente construcción recursiva: $SK_i = \text{KDF}(SK_{i-1}, \text{"update"})$.

En función de la clave SK_i , se calculan dos enteros grandes u_i y v_i con $(u_i, v_i) = \text{KDF}(SK_i, \text{"diversify"})$. Tanto la clave privada P-224 indicada como d y la correspondiente clave pública indicada como P se derivan mediante una relación afín que implica a los dos enteros para calcular un par de claves de corta duración: la clave privada derivada es d_i , donde $d_i = u_i * d + v_i$ (operación módulo del orden de la curva P-224) y la parte pública correspondiente es P_i y verifica que $P_i = u_i * P + v_i * G$.

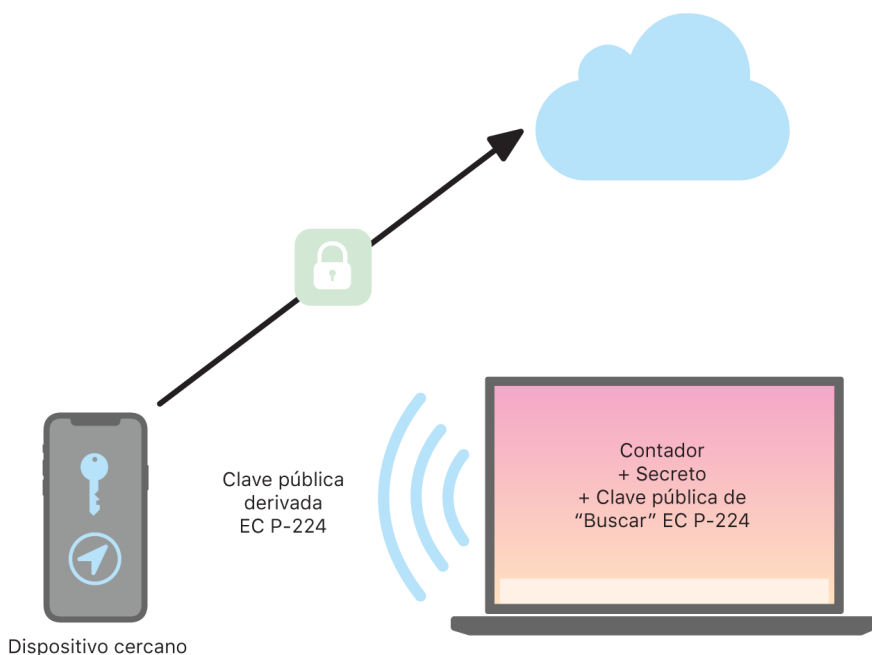
Cuando un dispositivo se pierde y no se puede conectar a una red móvil o wifi (por ejemplo, un MacBook Pro olvidado en el banco de un parque), comienza a difundir periódicamente la clave pública derivada P_i durante periodos de tiempo limitados en una carga útil de Bluetooth. Al usar P-224, la representación de clave pública puede encajar en una única carga útil de Bluetooth. A continuación, los dispositivos circundantes pueden ayudar en la búsqueda del dispositivo desconectado de internet encriptando su ubicación en la clave pública. Cada 15 minutos aproximadamente, la clave pública se sustituye por una nueva usando un valor incrementado del contador y el proceso anterior, para que un identificador persistente no pueda realizar un seguimiento del usuario. El mecanismo de derivación está diseñado para evitar que las distintas claves públicas P_i se puedan vincular al mismo dispositivo.

Mantener el anonimato de los usuarios y los dispositivos

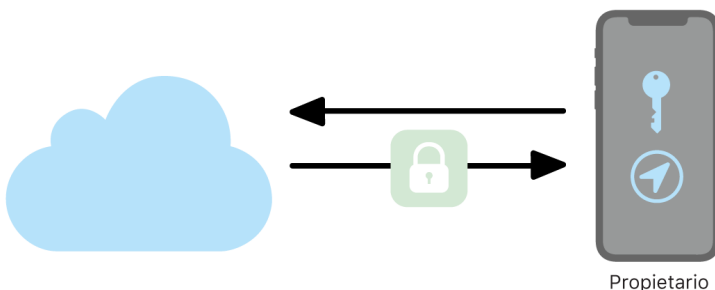
Además de garantizar que la información de la ubicación y otros datos estén totalmente encriptados, las identidades de los participantes se mantienen en privado, entre sí y de Apple. El tráfico que envían los dispositivos localizadores a Apple no contiene información de autenticación en el contenido ni en las cabeceras. Como resultado, Apple desconoce quién es el localizador o a quién pertenece el dispositivo encontrado. Además, Apple no registra ninguna información que pueda revelar la identidad del localizador y no conserva ninguna información con la que se pueda correlacionar el localizador y el propietario. El propietario del dispositivo solo recibe la información de ubicación encriptada que se descrypta y se muestra en la app Buscar sin ninguna indicación de quién ha encontrado el dispositivo.

Usar Buscar para localizar dispositivos Apple perdidos

Cualquier dispositivo Apple que se encuentre dentro del alcance de Bluetooth y tenga activada la opción de búsqueda sin conexión puede detectar la señal de otro dispositivo Apple configurado para permitir Buscar y leer la clave P_i de difusión actual. Con una construcción ECIES y la clave pública P_i de la difusión, los dispositivos localizadores encriptan la información de su ubicación actual y la transmiten a Apple. La ubicación encriptada se asocia con un índice de servidor que se calcula como el hash SHA256 de la clave pública P-224 P_i obtenida de la carga útil de Bluetooth. Apple nunca tiene la clave de desencriptación, por lo que no puede leer la ubicación encriptada por el dispositivo localizador. El propietario del dispositivo perdido puede reconstruir el índice y desencriptar la ubicación encriptada.



Al intentar localizar el dispositivo perdido, se estima un intervalo esperado de valores del contador para el periodo de búsqueda de la ubicación. Con el conocimiento de la clave P-224 privada original d y los valores secretos SK_i del intervalo de valores del contador del periodo de búsqueda, el propietario puede entonces reconstruir el conjunto de valores $\{d_i, \text{SHA256}(P_i)\}$ para todo el periodo de búsqueda. A continuación, el propietario del dispositivo utilizado para localizar el dispositivo perdido puede realizar consultas al servidor usando el conjunto de valores de índice $\text{SHA256}(P_i)$ y descargar las ubicaciones encriptadas del servidor. Luego, la app Buscar desencripta de forma local las ubicaciones encriptadas con las claves privadas coincidentes d_i y muestra una ubicación aproximada del dispositivo perdido en la app. La app del propietario combina los informes de ubicación de los distintos dispositivos localizadores para generar una ubicación más precisa.



Localizar dispositivos sin conexión

Si un usuario tiene Buscar mi iPhone activado en su dispositivo, la búsqueda sin conexión se activa por defecto al actualizar un dispositivo a iOS 13 o posterior, iPadOS 13.1 o posterior y macOS 10.15 o posterior. Esto está diseñado para garantizar que cada usuario tenga la mejor oportunidad posible de localizar su dispositivo si se pierde. Sin embargo, si el usuario prefiere no participar en cualquier momento, puede desactivar la búsqueda sin conexión en los ajustes de Buscar en su dispositivo. Al desactivar la búsqueda sin conexión, el dispositivo ya no actúa como localizador ni puede ser detectado por otros dispositivos localizadores. Sin embargo, el usuario puede seguir localizando el dispositivo siempre que se pueda conectar a una red móvil o wifi.

Cuando se localiza un dispositivo perdido desconectado de internet, el usuario recibe una notificación y un mensaje de correo electrónico para hacerles saber que se ha encontrado el dispositivo. Para ver la ubicación del dispositivo perdido, el usuario abre la app Buscar y selecciona la pestaña Dispositivos. En lugar de mostrar el dispositivo en un mapa en blanco, como lo haría antes de haber localizado el dispositivo, Buscar muestra una ubicación en el mapa con una dirección aproximada e información sobre cuánto tiempo hace que se ha detectado el dispositivo. Si llegan más informes de ubicación, la ubicación actual y la marca de tiempo se actualizan automáticamente. Aunque los usuarios no pueden reproducir un sonido en un dispositivo desconectado de internet ni borrarlo de forma remota, pueden usar la información de ubicación para volver sobre sus pasos o tomar otras medidas para poder recuperarlo.

Continuidad

Descripción general de la seguridad de Continuidad

Continuidad saca provecho de tecnologías como iCloud, Bluetooth y wifi para permitir a los usuarios continuar con una actividad en otro dispositivo, hacer y recibir llamadas telefónicas, enviar y recibir mensajes de texto, así como compartir la conexión a internet de un dispositivo móvil.

Seguridad de Handoff

Apple gestiona la seguridad de las transferencias con Handoff, ya sea desde un dispositivo a otro, entre una app y un sitio web o incluso transferencias de grandes cantidades de datos.

Cómo funciona Handoff de forma segura

Con Handoff, cuando los dispositivos iOS, iPadOS y macOS de un usuario están cerca, el usuario puede transferir automáticamente aquello en lo que esté trabajando de un dispositivo al otro. Handoff permite al usuario cambiar de dispositivo y continuar trabajando de forma instantánea.

Cuando un usuario inicia sesión en iCloud en un segundo dispositivo compatible con Handoff, los dos dispositivos establecen un enlace mediante una conexión Bluetooth LE (BLE) 4.2 fuera de banda a través del APNs. Los mensajes individuales están encriptados de forma similar a los mensajes de iMessage. Una vez que los dispositivos están enlazados, cada dispositivo genera una clave simétrica AES de 256 bits que se almacena en el [llavero](#) del dispositivo. Esta clave puede encriptar y autenticar los avisos de la conexión BLE que comunican la actividad actual del dispositivo con otros dispositivos enlazados de iCloud utilizando AES256 en el modo GCM con medidas de protección de reproducción.

La primera vez que un dispositivo recibe un aviso de una clave nueva, establece una conexión BLE con el dispositivo que origina la clave y genera un intercambio de claves de encriptación del aviso. Esta conexión se protege mediante la encriptación estándar BLE 4.2, así como mediante la encriptación de los mensajes individuales, que es parecida a la encriptación de iMessage. En algunas situaciones, estos mensajes se envían mediante APNs en lugar de hacerlo mediante la conexión BLE. La carga útil de la actividad se protege y se transfiere del mismo modo que con un iMessage.

Handoff entre apps nativas y sitios web

Handoff permite que una app nativa de iOS, iPadOS o macOS pueda reanudar la actividad del usuario en una página web en dominios controlados legítimamente por el desarrollador de la app. También permite reanudar la actividad del usuario de la app nativa en un navegador web.

Con el fin de ayudar a evitar que las apps nativas soliciten reanudaciones de sitios web no controlados por el desarrollador, las apps deben demostrar que disponen del control legítimo de los dominios web que quieren reanudar. El control de un sitio web se establece mediante el mecanismo para credenciales web compartidas. Para obtener información detallada, consulta [Acceso de las apps a las contraseñas guardadas](#). El sistema debe validar el control del nombre del dominio de una app antes de que esta tenga permiso para aceptar la continuidad de la actividad del usuario con Handoff.

El origen de Handoff de una página web puede ser cualquier navegador que haya aceptado las API de Handoff. Cuando el usuario visualiza una página web, el sistema anuncia el nombre del dominio de la página web en los bytes de aviso de Handoff encriptados. Únicamente los demás dispositivos del usuario pueden descifrar los bytes de aviso.

En un dispositivo receptor, el sistema detecta que una app nativa instalada acepta Handoff desde el nombre de dominio anunciado y muestra el icono de la app nativa como la opción de Handoff. Una vez abierta, la app nativa recibe la dirección URL completa y el título de la página web. No se transfiere ninguna otra información del navegador a la app nativa.

En el sentido inverso, una app nativa puede especificar una URL alternativa cuando el dispositivo que recibe Handoff no tiene instalada la misma app nativa. En este caso, el sistema muestra el navegador por defecto del usuario como opción de app de Handoff (si ese navegador ha adoptado las API de Handoff). Cuando se solicite el uso de Handoff, el navegador se abre y se le facilita la URL alternativa que haya proporcionado la app nativa. No es necesario que la URL alternativa se limite a los nombres de dominio que controle el desarrollador de la app nativa.

Handoff de datos de mayor tamaño

Como complemento al uso de la función básica de Handoff, es posible que algunas apps elijan usar API que sean compatibles con el envío de un mayor número de datos mediante la tecnología de red wifi P2P creada por Apple (de forma parecida a AirDrop). Por ejemplo, la app Mail utiliza esas API para poder utilizar Handoff con borradores de mensajes de correo, que podrían incluir archivos adjuntos de gran tamaño.

Cuando una app utiliza estas API, el intercambio entre los dos dispositivos se inicia como en Handoff. Pero, tras recibir la carga útil inicial mediante Bluetooth LE (BLE), el dispositivo receptor inicia una conexión nueva a través de la red wifi. Esta conexión está encriptada con TLS y obtiene la confianza mediante una identidad compartida a través del llavero de iCloud. La identidad de los certificados se coteja con la identidad del usuario. El resto de los datos de carga útil se envía mediante esta conexión encriptada hasta que se completa la transferencia.

Portapapeles Universal

El portapapeles universal aprovecha Handoff para transferir de forma segura el contenido del portapapeles de un usuario entre los dispositivos, de modo que se pueda copiar contenido de un dispositivo y pegarlo en otro. El contenido se protege del mismo modo que otros datos de Handoff y se comparte por defecto con Portapapeles Universal, a menos que el desarrollador de la app no permita que se comparta.

Las apps tienen acceso a los datos del portapapeles independientemente de si el usuario ha pegado el portapapeles en ellas. Con Portapapeles Universal, este acceso a los datos se extiende a las apps que se ejecutan en los demás dispositivos del usuario (tal y como se establece al iniciar sesión en iCloud).

Seguridad de la transmisión de llamadas telefónicas del iPhone

Cuando el Mac, iPad, iPod touch o HomePod de un usuario están en la misma red wifi que el iPhone, puede hacer y recibir llamadas de teléfono mediante la conexión a la red móvil del iPhone. La configuración requiere que en los dispositivos se haya iniciado sesión tanto en iCloud como en FaceTime con la misma cuenta de ID de Apple.

Al recibir una llamada entrante, todos los dispositivos configurados reciben una notificación mediante el [servicio de notificaciones push de Apple \(APNs\)](#). Con cada notificación se usará la misma encriptación de punto a punto que iMessage. Los dispositivos que estén en la misma red presentan la misma interfaz de usuario de notificación de llamada entrante. Cuando el usuario responde a la llamada, el audio se transmite sin interrupciones desde el iPhone del usuario mediante una conexión segura P2P entre los dos dispositivos.

Cuando se responde a una llamada desde un dispositivo, esta deja de sonar en los demás dispositivos cercanos enlazados a través de iCloud y se avisa de esta situación brevemente mediante Bluetooth de baja energía (BLE). Los bytes de aviso se encriptan con el mismo método que los avisos de Handoff.

Las llamadas salientes también se transmiten al iPhone mediante APNs y el audio se transmite de forma parecida mediante el enlace P2P seguro entre dispositivos. Los usuarios pueden desactivar la transferencia de llamadas telefónicas en un dispositivo desactivando "Llamadas telef. del iPhone" en los ajustes de FaceTime.

Seguridad del reenvío de mensajes de texto del iPhone

La opción "Reenvío de SMS" permite enviar automáticamente los mensajes de texto SMS recibidos en un iPhone al iPad, iPod touch o Mac inscrito del usuario. Cada dispositivo debe haber iniciado sesión en el servicio iMessage con la misma cuenta de ID de Apple. Cuando se activa la opción "Reenvío de SMS", la inscripción de los dispositivos que estén dentro del círculo de confianza del usuario es automática si tienen la autenticación de doble factor activada. En caso contrario, el iPhone genera un código numérico de seis dígitos aleatorio que se introduce en cada dispositivo para verificar su inscripción.

Una vez que los dispositivos están enlazados, el iPhone encripta y reenvía los mensajes de texto SMS entrantes a cada dispositivo mediante los métodos descritos en [Descripción general de la seguridad de iMessage](#). Las respuestas se envían de vuelta al iPhone utilizando el mismo método y, a continuación, el iPhone las envía como mensajes de texto con ayuda del mecanismo de transmisión de SMS del operador. La opción "Reenvío de SMS" se puede desactivar en los ajustes de Mensajes.

Seguridad de Instant Hotspot

Instant Hotspot conecta otros dispositivos Apple a un punto de acceso personal de iOS o iPadOS. Los dispositivos iOS y iPadOS compatibles con Instant Hotspot usan la tecnología Bluetooth LE (BLE) para descubrir y comunicarse con todos los dispositivos que hayan iniciado sesión en la misma cuenta individual de iCloud o en las cuentas de iCloud que usen "En familia" (en iOS 13 y iPadOS). Los ordenadores Mac compatibles con OS X 10.10 o posterior utilizan la misma tecnología para detectar dispositivos iOS y iPadOS, y comunicarse con ellos mediante Instant Hotspot.

Inicialmente, cuando un usuario accede a los ajustes de wifi en un dispositivo, este emite un aviso de BLE que contiene un identificador común para todos los dispositivos que han iniciado sesión en la misma cuenta de iCloud. El identificador se genera desde un identificador DSID (Destination Signaling Identifier) vinculado a la cuenta de iCloud y va rotando periódicamente. Si hay otros dispositivos que han iniciado sesión en la misma cuenta de iCloud cerca y son compatibles con la función de punto de acceso personal, detectan la señal y responden indicando su disponibilidad para usar Instant Hotspot.

Cuando un usuario que no forma parte de "En familia" selecciona un iPhone o iPad como punto de acceso personal, se envía una solicitud de activación del punto de acceso personal a dicho dispositivo. La solicitud se envía mediante un enlace que se encripta con la encriptación BLE y la solicitud se encripta mediante un proceso parecido al de la encriptación de iMessage. A continuación, el dispositivo responde a través del mismo enlace de BLE con la misma encriptación por mensaje con información de la conexión del punto de acceso personal.

Para los usuarios que forman parte de "En familia", la información de la conexión del punto de acceso personal se comparte de forma segura mediante un mecanismo similar al usado por los dispositivos de HomeKit para sincronizar la información. Concretamente, la conexión que comparte la información del punto de acceso entre los usuarios se protege mediante clave efímera ECDH (Curve25519) que se autentica con las claves públicas Ed25519 específicas de cada dispositivo de los usuarios. Las claves públicas que se utilizan son las que se habían sincronizado previamente entre los miembros de "En familia" mediante el IDS cuando se estableció el servicio "En familia".

Seguridad de la red

Descripción general de la seguridad de la red

Además de los métodos de protección integrados que Apple utiliza para proteger los datos almacenados en dispositivos Apple, existen muchas medidas que las organizaciones pueden poner en marcha para proteger la información durante su transferencia a un dispositivo o desde él. Todos estos métodos de protección y medidas se incluyen en la seguridad de red.

Dado que los usuarios necesitan acceso a redes corporativas desde cualquier parte del mundo, es importante garantizar que están autorizados y que sus datos están protegidos durante la transmisión. Para alcanzar estos objetivos de seguridad, iOS, iPadOS y macOS integran tecnologías probadas y los estándares más recientes para conexiones de red móvil y wifi. Por eso, nuestros sistemas operativos utilizan —y proporcionan acceso de desarrollador a— protocolos de red estándar para las comunicaciones autenticadas, autorizadas y encriptadas.

Seguridad de TLS

iOS, iPadOS y macOS son compatibles con la seguridad de la capa de transporte (TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3) y con Datagram Transport Layer Security (DTLS). El protocolo TLS es compatible con AES128 y AES256, y prefiere conjuntos de cifrado con confidencialidad directa. Las apps de internet, como Safari, Calendario y Mail, usarán automáticamente este protocolo para permitir un canal de comunicación encriptado entre el dispositivo y los servicios de red. Las API de alto nivel (como CFNetwork) facilitan a los desarrolladores la adopción de TLS en sus apps, mientras que las API de bajo nivel (como Network.framework) proporcionan un control muy preciso. CFNetwork no permite SSL 3 y las apps que utilizan WebKit (como Safari) tienen prohibido realizar una conexión SSL 3.

En iOS 11 o posterior, y macOS 10.13 o posterior, ya no se permiten los certificados SHA-1 para las conexiones TLS, a no ser que el usuario indique que son de confianza. Tampoco se permiten los certificados con claves RSA que tengan una longitud inferior a 2048 bits. En iOS 10 y macOS 10.12 ya no se usa el conjunto de cifrado simétrico RC4. Por defecto, los clientes o servidores TLS implementados con las API SecureTransport no disponen de conjuntos de cifrado simétrico RC4 y no pueden conectarse cuando el único conjunto de cifrado disponible es RC4. Si quieres aumentar la seguridad, los servicios o apps que requieren RC4 deberían actualizarse para usar conjuntos de cifrado seguros. En iOS 12.1, los certificados emitidos después del 15 de octubre de 2018 desde un certificado raíz de confianza del sistema deben registrarse en un registro de transparencia de certificados de confianza para que se permitan para las conexiones TLS. En iOS 12.2, las API Network.framework y NSURLSession tienen TLS 1.3 activado por defecto. Sin embargo, los clientes TLS que utilicen las API SecureTransport no pueden usar TLS 1.3.

Seguridad de transporte de las apps

La seguridad de transporte de las apps proporciona unos requisitos de conexión por defecto, de manera que las apps cumplan las buenas prácticas para conexiones seguras al utilizar las API `NSURLConnection`, `CFURL` o `NSURLSession`. Por defecto, la seguridad de transporte de las apps limita la selección de cifrados para incluir solo conjuntos que proporcionen la confidencialidad directa, concretamente:

- ECDHE_ECDSA_AES y ECDHE_RSA_AES en modo Galois/Counter (GCM)
- Modo de encadenamiento de bloques de cifrado (CBC)

Las apps pueden desactivar el requisito de confidencialidad directa por dominio, en cuyo caso se añade RSA_AES al conjunto de cifrados disponibles.

Los servidores deben ser compatibles con TLS 1.2 y con la confidencialidad directa, y los certificados deben ser válidos y estar firmados mediante SHA256 o algo más seguro, con un mínimo de una clave RSA de 2048 bits o una clave de curva elíptica de 256 bits.

Las conexiones de red que no cumplan estos requisitos darán error, a menos que la app omita la seguridad de transporte de las apps. Los certificados no válidos siempre dan como resultado un fallo grave e imposibilidad de conexión. La seguridad de transporte de las apps se aplica automáticamente a las apps compiladas para iOS 9 o posterior y macOS 10.11 o posterior.

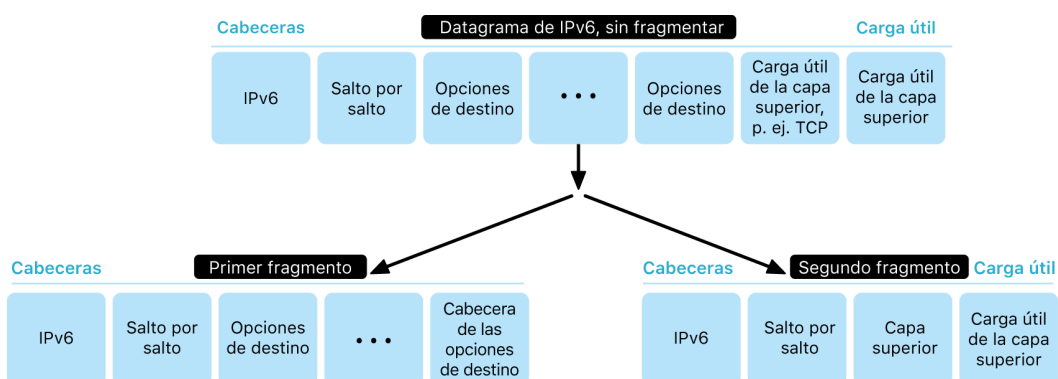
Comprobación de la validez del certificado

La evaluación del estado de confianza de un certificado TLS se lleva a cabo de acuerdo con los estándares establecidos del sector, como se establece en [RFC 5280](#), e incorpora estándares emergentes como el [RFC 6962](#) (transparencia de certificados). En iOS 11 o posterior y macOS 10.13 o posterior, los dispositivos Apple se actualizan de forma periódica con una lista actual de los certificados revocados y restringidos. La lista está compuesta por las listas de revocación de certificados (CRL, por sus siglas en inglés) que publican cada una de las autoridades de certificación básica integradas en las que confía Apple, además de los emisores secundarios de dichas autoridades de certificación. Apple, a su discreción, puede incluir otras limitaciones a la lista. Esta información se consulta cada vez que se usa una función API de red para establecer una conexión segura. Si hay demasiados certificados revocados de una autoridad de certificación como para enumerarlos individualmente, una evaluación de confianza puede requerir que se necesite una respuesta del estado del certificado en línea (OCSP, por sus siglas en inglés); si la respuesta no está disponible, la evaluación de confianza dará un error.

Seguridad de IPv6

Todos los sistemas operativos de Apple admiten IPv6, con la implementación de varios mecanismos para proteger la privacidad de los usuarios y la estabilidad de la pila de redes. Cuando se utiliza la configuración automática de direcciones sin estado (SLAAC), las direcciones IPv6 de todas las interfaces se generan de un modo que contribuye a impedir el rastreo de dispositivos a través de las redes y al mismo tiempo permite una buena experiencia de usuario al garantizar la estabilidad de las direcciones cuando no se producen cambios en la red. El algoritmo de generación de direcciones se basa en direcciones generadas criptográficamente a partir del [RFC 3972](#), mejorado por un modificador específico por interfaz para garantizar que incluso las distintas interfaces de la misma red acaben teniendo direcciones distintas. Además, las direcciones temporales se crean con una duración preferida de 24 horas y se usan por defecto para cualquier nueva conexión. En consonancia con la función de dirección wifi privada introducida en iOS 14, iPadOS 14 y watchOS 7, se genera una dirección local de enlace única para cada red wifi a la que se conecta un dispositivo. El SSID de la red se incorpora como un elemento adicional para la generación de direcciones, similar al parámetro Network_ID desde el [RFC 7217](#). Este enfoque se utiliza en iOS 14, iPadOS 14 y watchOS 7.

Para protegerse de los ataques basados en la fragmentación y los encabezados de extensión de IPv6, los dispositivos Apple incorporan medidas de protección especificadas en [RFC 6980](#), [RFC 7112](#) y [RFC 8021](#). Entre otras medidas, se inhiben aquellos ataques en los que el encabezado de la capa superior solo puede encontrarse en el segundo fragmento (como se muestra a continuación), lo que, a su vez, podría generar ambigüedades para los controles de seguridad, como el filtrado de paquetes sin estado.



Además, para ayudar a garantizar la fiabilidad de la pila IPv6 de los sistemas operativos de Apple, los dispositivos Apple aplican varios límites en las estructuras de datos relacionadas con IPv6, como el número de prefijos por interfaz.

Seguridad de la red privada virtual (VPN)

Los servicios de red segura, como las redes privadas virtuales, suelen requerir una configuración mínima para funcionar con dispositivos iOS, iPadOS y macOS.

Protocolos compatibles

Estos dispositivos funcionan con servidores VPN que admiten los siguientes protocolos y métodos de autenticación:

- IKEv2/IPsec con autenticación por secreto compartido, certificados RSA, [certificados de algoritmo de firma digital de curva elíptica \(ECDSA\)](#), EAP-MSCHAPv2 o EAP-TLS.
- VPN SSL con la app cliente adecuada de App Store.
- L2TP/IPsec con autenticación de usuario mediante contraseña de MS-CHAPv2 y autenticación de máquina mediante secreto compartido (iOS, iPadOS y macOS), y RSA SecurID o CRYPTOCARD (solo macOS).
- Cisco IPsec con autenticación de usuario mediante contraseña, RSA SecurID o CRYPTOCARD, y autenticación de máquina mediante secreto compartido y certificados (solo macOS).

Implementaciones de VPN compatibles

iOS, iPadOS y macOS son compatibles con lo siguiente:

- *VPN por petición:* Para las redes que utilizan la autenticación basada en certificados. Las políticas de TI utilizan un perfil de configuración VPN para especificar los dominios que requieren una conexión VPN.
- *VPN por app:* Para facilitar las conexiones VPN de forma mucho más granular. Las soluciones de [gestión de dispositivos móviles \(MDM\)](#) pueden especificar una conexión para cada app gestionada y para dominios específicos en Safari. Esto ayuda a garantizar que los datos seguros siempre entran en la red corporativa y salen de ella, pero no así los datos personales del usuario.

iOS y iPadOS son compatibles con lo siguiente:

- *VPN siempre activada:* Para dispositivos gestionados con una solución MDM y que se supervisan con Apple Configurator para Mac, [Apple School Manager](#) o [Apple Business Manager](#). Con el ajuste "VPN siempre activada" se elimina la necesidad de que los usuarios activen la red VPN para obtener protección al conectarse a redes wifi y móviles. Además, proporciona a la organización control absoluto sobre el tráfico del dispositivo al dirigir todo el tráfico IP de vuelta a la organización. El intercambio por defecto de parámetros y claves para la encriptación posterior, IKEv2, protege la transmisión de tráfico con encriptación de datos. La organización puede supervisar y filtrar el tráfico de estos dispositivos en ambas direcciones, proteger los datos en la red y restringir el acceso del dispositivo a internet.

Seguridad de la red wifi

Acceso seguro a redes inalámbricas

Todas las plataformas de Apple son compatibles con los protocolos de autenticación y encriptación de la red wifi estándar del sector, para así proporcionar acceso autenticado y confidencialidad al conectarse a las siguientes redes seguras inalámbricas:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 transicional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise con seguridad de 192 bits

WPA2 y WPA3 autentican cada conexión y proporcionan encriptación AES de 128 bits para ayudar a garantizar la confidencialidad de los datos que se envían de forma remota. Esto proporciona a los usuarios la máxima garantía de que sus datos están protegidos durante las comunicaciones a través de una conexión de red wifi.

Compatibilidad con WPA3

WPA3 es compatible con los siguientes dispositivos Apple:

- iPhone 7 o posterior
- iPad 5.^a generación o posterior
- Apple TV 4K o posterior
- Apple Watch Series 3 o posterior
- Ordenadores Mac (finales de 2013 o posterior, con 802.11ac o posterior)

Los dispositivos más nuevos son compatibles con la autenticación WPA3 Enterprise con seguridad de 192 bits e incluyen compatibilidad con la encriptación AES de 256 bits al conectarse a puntos de acceso inalámbrico compatibles. Esto proporciona protecciones más seguras para la confidencialidad del tráfico que se envía de forma remota. WPA3 Enterprise con seguridad de 192 bits es compatible con el iPhone 11, el iPhone 11 Pro, el iPhone 11 Pro Max y los dispositivos iOS y iPadOS posteriores.

Compatibilidad con PMF

Además de proteger los datos enviados de forma remota, las plataformas de Apple amplían las protecciones de nivel WPA2 y WPA3 a tramas de gestión de unidifusión y multidifusión mediante el servicio de trama de gestión protegida (PMF) al que se hace referencia en el estándar 802.11w. La compatibilidad con PMF está disponible en los siguientes dispositivos Apple:

- iPhone 6 o posterior
- iPad Air 2 o posterior
- Apple TV HD o posterior
- Apple Watch Series 3 o posterior
- Ordenadores Mac (finales de 2013 o posterior, con 802.11ac o posterior)

Los dispositivos Apple, compatibles con 802.1X, se pueden integrar en un amplio abanico de entornos de autenticación RADIUS. Los métodos de autenticación inalámbrica compatibles con 802.1X son los siguientes: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 y PEAPv1.

Protecciones de la plataforma

Los sistemas operativos de Apple protegen los dispositivos frente a las vulnerabilidades del firmware del procesador de red. Esto significa que los controladores de red con wifi tienen limitado el acceso a la memoria del procesador de aplicaciones.

- Cuando se utiliza USB o SDIO (entrada/salida de Secure Digital) para comunicarse con el procesador de red, este no puede iniciar transacciones de acceso directo a memoria (DMA) al procesador de aplicaciones.
- Cuando se utiliza PCIe, cada procesador de red está en su propio bus PCIe aislado. Hay una [unidad de gestión de memoria de entrada/salida \(IOMMU\)](#) en cada bus PCIe que limita aún más el acceso DMA del procesador de red a solo la memoria y los recursos que contengan sus paquetes de red y estructuras de control.

Protocolos en desuso

Los productos de Apple son compatibles con los siguientes protocolos en desuso de autenticación y encriptación de la red wifi:

- WEP abierta, con claves de 40 bits y de 104 bits;
- WEP compartida, con claves de 40 bits y de 104 bits;
- WEP dinámica;
- Protocolo de integridad de clave temporal (TKIP);
- WPA;
- WPA/WPA2 transicional.

Estos protocolos ya no se consideran seguros y se desaconseja encarecidamente su uso por razones de compatibilidad, fiabilidad, rendimiento y seguridad. Solo se ofrecen para garantizar la compatibilidad con las versiones anteriores y es posible que se eliminen en las futuras versiones de software.

Se recomienda migrar todas las implementaciones de redes wifi a WPA3 Personal o WPA3 Enterprise para proporcionar las conexiones wifi más robustas, seguras y compatibles posible.

Privacidad de la red wifi

Aleatorización de la dirección MAC

Las plataformas de Apple utilizan una dirección aleatorizada de control de acceso al medio (MAC) mientras se realiza una exploración de redes wifi cuando no están asociadas a ninguna red de este tipo. Estas exploraciones se pueden realizar para buscar una red wifi conocida y conectarse a ella o para ayudar a la función Localización en el caso de las apps que utilizan geocercas, como los recordatorios basados en la ubicación de Mapas de Apple. Ten en cuenta que las exploraciones de redes wifi que se realizan mientras se produce un intento de conexión a una red wifi preferida no se aleatorizan. Los dispositivos iPhone 5 posteriores son compatibles con la aleatorización de la dirección MAC wifi.

Las plataformas de Apple también utilizan una dirección MAC aleatorizada al realizar exploraciones de preferencia de descarga de red mejorada (ePNO) cuando un dispositivo no está asociado a una red wifi o su procesador está en reposo. Las exploraciones ePNO se ejecutan cuando un dispositivo utiliza la función Localización para apps con geocercas, como los recordatorios basados en la ubicación que determinan si el dispositivo se encuentra cerca de una ubicación específica.

La dirección MAC de un dispositivo cambia cuando se desconecta de una red wifi, por lo que no se puede utilizar para realizar un seguimiento continuo de un dispositivo con observadores pasivos del tráfico de la red wifi, incluso cuando el dispositivo está conectado a una red móvil. Apple ha informado a los fabricantes de wifi de que en las exploraciones de redes wifi de iOS y iPadOS se utiliza una dirección MAC aleatorizada, y de que ni Apple ni los fabricantes pueden predecir este tipo de direcciones.

En iOS 14 o posterior, iPadOS 14 o posterior y watchOS 7 o posterior, cuando un iPhone, iPad, iPod touch o Apple Watch se conecta a una red wifi, se identifica con una dirección MAC única (aleatoria) por red. El usuario puede desactivar esta función, que también puede desactivarse mediante una nueva opción en la carga útil de wifi. En determinadas circunstancias, el dispositivo recurrirá a la dirección MAC real.

Para obtener más información, consulta el artículo de soporte técnico de Apple [Usar direcciones wifi privadas en el iPhone, el iPad, el iPod touch y el Apple Watch](#).

Aleatorización de los números de la secuencia del marco de wifi

Los marcos de wifi incluyen un número de secuencia que utiliza el protocolo 802.11 de bajo nivel para obtener comunicaciones wifi eficientes y fiables. Dado que estos números de la secuencia aumentan en cada marco transmitido, se podrían utilizar para correlacionar la información transmitida durante las exploraciones de redes wifi con los otros marcos transmitidos por el mismo dispositivo.

Para evitar esto, los dispositivos Apple aleatorizan los números de la secuencia cada vez que se cambia una dirección MAC a una nueva dirección aleatorizada. Esto incluye aleatorizar los números de la secuencia para cada nueva petición de exploración que se inicia mientras el dispositivo no está asociado. Esta aleatorización es compatible con los siguientes dispositivos:

- iPhone 7 o posterior
- iPad 5.^a generación o posterior
- Apple TV 4K o posterior
- Apple Watch Series 3 o posterior
- iMac Pro (Retina 5K, 27 pulgadas, 2017) o posterior
- MacBook Pro (13 pulgadas, 2018) o posterior
- MacBook Pro (15 pulgadas, 2018) o posterior
- MacBook Air (Retina, 13 pulgadas, 2018) o posterior
- Mac mini (2018) o posterior
- iMac (Retina 4K, 21,5 pulgadas, 2019) o posterior
- iMac (Retina 5K, 27 pulgadas, 2019) o posterior
- Mac Pro (2019) o posterior

Conexiones wifi

Apple genera direcciones MAC aleatorizadas para las conexiones wifi P2P que se usan para AirDrop y AirPlay. Las direcciones aleatorizadas también se utilizan para la función de compartir internet en iOS y iPadOS (con una tarjeta SIM) y para "Compartir internet" en macOS.

Las nuevas direcciones aleatorias se generan cada vez que se inician estas interfaces de red y se generan direcciones únicas de forma independiente para cada interfaz, según sea necesario.

Redes ocultas

Las redes wifi se identifican mediante su nombre de red, lo que se conoce como *identificador de red (SSID)*. Algunas redes wifi se han configurado para ocultar su SSID y, como resultado, el punto de acceso inalámbrico no difunde el nombre de la red. Estas se conocen como *redes ocultas*. El iPhone 6s y los dispositivos posteriores detectan automáticamente si la red está oculta. Si una red está oculta, el dispositivo iOS o iPadOS realiza un sondeo con el SSID incluido en la petición (y no de otra manera). Esta medida ayuda a impedir que el dispositivo difunda el nombre de las redes ocultas a las que un usuario estaba conectado previamente y, por lo tanto, se asegura la privacidad aún más.

Seguridad del Bluetooth

Hay dos tipos de Bluetooth en los dispositivos Apple: Bluetooth clásico y Bluetooth de baja energía (BLE). El modelo de seguridad del Bluetooth para ambas versiones incluye las siguientes funciones de seguridad distintas:

- *Enlace*: El proceso para crear una o más claves secretas compartidas.
- *Vinculación*: El acto de almacenar las claves creadas durante el enlace para usarlas en conexiones posteriores y formar un par de dispositivos de confianza.
- *Autenticación*: Verificar que los dos dispositivos tienen las mismas claves.
- *Encriptación*: Confidencialidad del mensaje.
- *Integridad del mensaje*: Protección frente a la falsificación del mensaje.
- *Enlace sencillo seguro*: Protección frente a la interceptación pasiva y protección frente a los ataques con intermediarios.

Bluetooth 4.1 añadió la función de las conexiones seguras al transporte físico de Bluetooth clásico (BR/EDR).

Las funciones de seguridad para cada tipo de Bluetooth se indican a continuación.

Compatibilidad	Bluetooth clásico	Bluetooth de baja energía
Enlace	Curva elíptica de P-256	Algoritmos admitidos por la FIPS (AES-CMAC y curva elíptica de P-256)
Vinculación	Información de enlace almacenada en una ubicación segura en los dispositivos iOS, iPadOS, macOS, tvOS y watchOS	Información de enlace almacenada en una ubicación segura en los dispositivos iOS, iPadOS, macOS, tvOS y watchOS
Autenticación	Algoritmos admitidos por la FIPS (HMAC-SHA256 y AES-CTR)	Algoritmos admitidos por la FIPS
Encriptación	Criptografía AES-CCM realizada en el controlador	Criptografía AES-CCM realizada en el controlador
Integridad del mensaje	AES-CCM para la integridad del mensaje	AES-CCM para la integridad del mensaje
Enlace sencillo seguro: Protección frente a la interceptación pasiva	Intercambio de claves efímeras de Diffie-Hellman de curva elíptica (ECDHE)	Intercambio de claves de Diffie-Hellman de curva elíptica (ECDHE)
Enlace sencillo seguro: Protección frente a los ataques con intermediarios (MITM)	Dos métodos numéricos asistidos por el usuario: comparación numérica o introducción de la clave de paso	Dos métodos numéricos asistidos por el usuario: comparación numérica o introducción de la clave de paso Los enlaces requieren la respuesta de un usuario, incluidos todos los modos de enlace sin intermediarios
Bluetooth 4.1 o posterior	iMac de finales de 2015 o posterior MacBook Pro de principios de 2015 o posterior	iOS 9 o posterior iPadOS 13.1 o posterior macOS 10.12 o posterior tvOS 9 o posterior watchOS 2.0 o posterior

Compatibilidad	Bluetooth clásico	Bluetooth de baja energía
Bluetooth 4.2 o posterior	iPhone 6 o posterior	iOS 9 o posterior iPadOS 13.1 o posterior macOS 10.12 o posterior tvOS 9 o posterior watchOS 2.0 o posterior

Privacidad del Bluetooth de baja energía

Para ayudar a proteger la privacidad del usuario, BLE incluye las dos funciones siguientes: la aleatorización de la dirección y la derivación de claves entre transportes.

La *aleatorización de la dirección* es una función que reduce la capacidad de seguir un dispositivo BLE durante un tiempo al cambiar con frecuencia la dirección del dispositivo Bluetooth. Para que un dispositivo que usa la función de privacidad se vuelva a conectar a dispositivos conocidos, el otro dispositivo debe poder resolver la dirección del dispositivo (que se conoce como la *dirección privada*). La dirección privada se genera usando la clave de resolución de identidad del dispositivo intercambiada durante el proceso de enlace.

iOS 13 o posterior y iPadOS 13.1 o posterior tienen la capacidad de obtener claves de enlace entre transportes, una función que se conoce como *derivación de claves entre transportes*. Por ejemplo, una clave de enlace generada con BLE se puede usar para derivar una clave de enlace de Bluetooth clásico. Además, Apple añadió Bluetooth clásico a la compatibilidad con BLE para los dispositivos que admiten la función de las conexiones seguras introducida en Bluetooth Core Specification 4.1 (consulta [Bluetooth Core Specification 5.1](#)).

Seguridad de la banda ultraancha en iOS

El nuevo chip U1 que ha creado Apple utiliza la tecnología de la banda ultraancha para el posicionamiento espacial. Esto permite que el iPhone 11, el iPhone 11 Pro, el iPhone 11 Pro Max o modelos de iPhone posteriores puedan localizar con precisión otros dispositivos Apple equipados con el chip U1. La tecnología de la banda ultraancha usa la misma tecnología para aleatorizar los datos que se encuentran en otros dispositivos Apple compatibles:

- Aleatorización de la dirección MAC
- Aleatorización de los números de la secuencia del marco de wifi

Seguridad del inicio de sesión único

Inicio de sesión único

Seguridad del inicio de sesión único

iOS y iPadOS admiten la autenticación en redes empresariales mediante el inicio de sesión único (SSO). El SSO funciona con redes basadas en Kerberos para autenticar a usuarios en los servicios en los que tienen autorización de acceso. El SSO se puede utilizar para diferentes operaciones de red, desde la navegación segura en Safari hasta el uso de aplicaciones de terceros. También admite la autenticación basada en certificados (como PKINIT).

macOS admite la autenticación en redes empresariales mediante Kerberos. Las apps pueden usar Kerberos para autenticar a usuarios en los servicios en los que tienen autorización de acceso. Kerberos también se puede utilizar para diferentes operaciones de red, desde la navegación segura en Safari y la autenticación del sistema de archivos de red hasta el uso de apps de terceros. Admite la autenticación basada en certificados, aunque se requiere instalar la app de la API de un desarrollador.

En el SSO de iOS, iPadOS y macOS, se usan identificadores SPNEGO y el protocolo HTTP Negotiate para trabajar con puertos de enlace de autenticación basada en Kerberos y sistemas de autenticación integrada de Windows que admitan tickets de Kerberos. La compatibilidad con el SSO se basa en el proyecto de código abierto Heimdal.

Se admiten los siguientes tipos de encriptación en iOS, iPadOS y macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari admite el SSO, y las apps de terceros que utilizan API de conexión a redes de iOS y iPadOS estándar también se pueden configurar para que lo hagan. Para configurar el SSO, iOS y iPadOS admiten una carga útil de perfil de configuración que permite a las soluciones de [gestión de dispositivos móviles \(MDM\)](#) obtener los ajustes necesarios. Aquí se incluye el nombre del principal usuario (es decir, la cuenta de usuario de Active Directory) y los ajustes del dominio Kerberos, así como la configuración de las apps y direcciones URL web de Safari a las que se debe permitir el uso del SSO.

Para configurar Kerberos en macOS, tienes que obtener tiques con el Visor de Tiques, iniciar sesión en un dominio de Active Directory de Windows o usar la herramienta de línea de comandos `kinit`.

Inicio de sesión único extensible

Los desarrolladores de apps pueden ofrecer sus propias implementaciones de inicio de sesión único con las extensiones del SSO. Las extensiones del SSO se invocan cuando una app nativa o web necesita usar algún proveedor de identidad para la autenticación del usuario. Los desarrolladores pueden ofrecer dos tipos de extensiones: las que redirigen a HTTPS y las que usan un mecanismo de reto/respuesta como Kerberos. Esto permite que el inicio de sesión único extensible sea compatible con los esquemas de autenticación de OpenID, OAuth, SAML2 y Kerberos.

Para usar una extensión de inicio de sesión único, una app puede utilizar la API `AuthenticationServices` o bien confiar en el mecanismo de intercepción de URL que ofrece el sistema operativo. WebKit y CFNetwork proporcionan una capa de intercepción que permite una compatibilidad fluida del inicio de sesión único para cualquier app WebKit o nativa. Para que se invoque una extensión de inicio de sesión único, un administrador debe proporcionar la configuración que se instalará a través del perfil de una solución de gestión de dispositivos móviles (MDM). Además, las extensiones de tipo redirigir deben usar la carga útil de dominios asociados para probar que el servidor de identidad con el que son compatibles conoce su existencia.

La única extensión proporcionada con el sistema operativo es la extensión SSO de Kerberos.

Seguridad de AirDrop

Los dispositivos Apple compatibles con AirDrop utilizan Bluetooth de baja energía (BLE o Bluetooth LE) y la tecnología wifi P2P creada por Apple para enviar archivos e información a dispositivos cercanos, incluidos los dispositivos iOS y los dispositivos iPad compatibles con AirDrop que usen iOS 7 o posterior y los ordenadores Mac que usen OS X 10.11 o posterior. El radio de alcance wifi sirve para la comunicación directa entre dispositivos sin utilizar ningún tipo de conexión a internet ni punto de acceso inalámbrico. Esta conexión está encriptada con TLS.

El ajuste por defecto de AirDrop para compartir contenido es "Solo contactos". Los usuarios también pueden elegir entre utilizar AirDrop para compartir contenido con todos y desactivar la función por completo. Las organizaciones pueden restringir el uso de AirDrop para los dispositivos o apps gestionados mediante una solución de [gestión de dispositivos móviles \(MDM\)](#).

Operación de AirDrop

AirDrop usa los servicios de iCloud para ayudar a los usuarios a autenticarse. Cuando un usuario inicia sesión en iCloud, se guarda en el dispositivo un algoritmo de identidad RSA de 2048 bits y, cuando el usuario activa AirDrop, se crea un hash de identidad corto de AirDrop basado en las direcciones de correo electrónico y los números de teléfono asociados al ID de Apple del usuario.

Cuando un usuario elige AirDrop como método para compartir un ítem, el dispositivo emisor envía una señal de AirDrop a través de BLE que incluye el hash de identidad de AirDrop corto del usuario. Los dispositivos Apple que estén activados, se encuentren cerca y tengan AirDrop activado detectan la señal y responden utilizando la tecnología wifi P2P para que el dispositivo emisor descubra su identidad.

En el modo "Solo contactos", los hashes de identidad cortos de AirDrop recibidos se comparan con los hashes de las personas incluidas en la app Contactos del dispositivo receptor. Si se encuentra una coincidencia, el dispositivo receptor responde con información sobre su identidad a través de la tecnología wifi P2P. Si no se encuentra ninguna coincidencia, el dispositivo no responde.

En el modo Todos, en general se utiliza el mismo proceso. Sin embargo, el dispositivo receptor responde incluso si no hay ninguna coincidencia en la app Contactos del dispositivo.

A continuación, el dispositivo emisor inicia una conexión de AirDrop mediante la tecnología wifi P2P y, por medio de dicha conexión, envía un hash de identidad largo al dispositivo receptor. Si el hash de identidad largo coincide con el hash de una persona conocida de los contactos del receptor, este responde con sus hashes de identidad largos.

Si se han verificado los hashes, el nombre y la foto del destinatario (si se encuentra en Contactos) se muestran en la hoja de compartir contenido de AirDrop del emisor. En iOS y iPadOS, se muestran en la sección Personas o Dispositivos. Los dispositivos que no se han verificado o autenticado se muestran en la hoja de compartir contenido de AirDrop del emisor con un icono de silueta y el nombre del dispositivo, tal como se indica en Ajustes > General > Información > Nombre. En iOS y iPadOS se colocan en la sección "Otras personas" de la hoja de compartir contenido de AirDrop.

El usuario emisor puede entonces seleccionar a los usuarios con los que quiere compartir contenido. Al seleccionar al usuario, el dispositivo emisor inicia una conexión encriptada (TLS) con el dispositivo receptor, que intercambia sus certificados de identidad de iCloud. La identidad de los certificados se coteja con la información disponible en la app Contactos de cada usuario.

Si se han verificado los certificados, se solicita al usuario receptor que acepte la transferencia entrante del usuario o el dispositivo identificados. Si se han seleccionado varios destinatarios, este proceso se repite para cada destino.

Seguridad de las contraseñas wifi compartidas en el iPhone y el iPad

Los dispositivos iOS y iPadOS que permiten compartir la contraseña wifi utilizan un mecanismo similar a AirDrop para enviar una contraseña wifi de un dispositivo a otro.

Cuando un usuario selecciona una red wifi (solicitante) y se le pide que introduzca la contraseña wifi, el dispositivo Apple inicia un aviso de Bluetooth LE (BLE) indicando que quiere la contraseña wifi. Los dispositivos Apple que estén activos, se encuentren cerca y tengan la contraseña para la red wifi seleccionada se conectarán al dispositivo que realiza la petición mediante BLE.

El dispositivo que tiene la contraseña wifi (otorgante) requiere la información de contacto del solicitante y el solicitante debe demostrar su identidad utilizando un mecanismo similar a AirDrop. Una vez que se ha demostrado la identidad, el otorgante envía al solicitante el código, que se puede utilizar para acceder a la red.

Las organizaciones pueden restringir el uso compartido de la contraseña wifi para los dispositivos o apps gestionados mediante una solución de [gestión de dispositivos móviles \(MDM\)](#).

Seguridad del firewall en macOS

macOS incluye un firewall integrado para proteger al Mac del acceso a la red y de los ataques de denegación de servicio. Se puede configurar en el panel "Seguridad y privacidad" de las Preferencias del Sistema y admite las siguientes configuraciones:

- Bloquear todas las conexiones entrantes, independientemente de la app.
- Permitir que el software integrado reciba conexiones entrantes de forma automática.
- Permitir que el software descargado y firmado reciba conexiones entrantes de forma automática.
- Permitir o denegar el acceso en función de las apps especificadas por el usuario.
- Impedir que el Mac responda a solicitudes de sondeo y escaneo de puertos ICMP (protocolo de control de mensajes de internet).

Seguridad del kit de desarrollo

Descripción general de la seguridad del kit de desarrollo

Apple proporciona una serie de “kits” de estructuras para que los desarrolladores externos puedan ampliar los servicios de Apple. Estas estructuras se han diseñado en torno a la privacidad y la seguridad del usuario:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

Seguridad de HomeKit

Seguridad de las comunicaciones de HomeKit

HomeKit proporciona una infraestructura de automatización doméstica que usa la seguridad de iCloud y de iOS, iPadOS y macOS para proteger y sincronizar los datos privados sin exponerlos a Apple.

La identidad y la seguridad de HomeKit se basan en pares de claves Ed25519 constituidos por una clave pública y una privada. En el dispositivo iOS, iPadOS y macOS, se genera un par de claves Ed25519 para cada usuario de HomeKit, y este pasa a ser su identidad de HomeKit. Dicho par se utiliza para autenticar la comunicación entre dispositivos iOS, iPadOS y macOS, y entre accesorios y dispositivos iOS, iPadOS y macOS.

Las claves (que se almacenan en el [llavero](#) y solo se incluyen en las copias de seguridad encriptadas del llavero) se mantienen siempre actualizadas entre dispositivos utilizando el llavero de iCloud si está disponible. El HomePod y el Apple TV reciben claves al pulsar para configurar o mediante el modo de configuración que se describe más adelante. Las claves se comparten desde un iPhone con un Apple Watch enlazado mediante el [servicio de identidad \(IDS\) de Apple](#).

Comunicación entre accesorios de HomeKit

Los accesorios de HomeKit generan su propio par de claves Ed25519 para la comunicación con dispositivos iOS, iPadOS y macOS. Si el accesorio se restaura con los ajustes originales de fábrica, se genera un par de claves nuevo.

Para establecer una relación entre un dispositivo iOS, iPadOS y macOS y un accesorio de HomeKit, las claves se intercambian utilizando el protocolo de contraseña remota segura (3072 bits), que usa un código de ocho dígitos proporcionado por el fabricante del accesorio. El usuario lo introduce en el dispositivo iOS, iPadOS y macOS y, después, se encripta con ChaCha20-Poly1305 AEAD mediante claves derivadas de HKDF-SHA512. La certificación MFi del accesorio también se verifica durante la configuración. Los accesorios sin un chip MFi pueden integrar la compatibilidad con la autenticación de software en iOS 11.3 o versiones posteriores.

Cuando el dispositivo iOS, iPadOS y macOS y el accesorio de HomeKit se comunican durante el uso, se autentican entre sí mediante las claves intercambiadas en el proceso descrito más arriba. Todas las sesiones se establecen con el protocolo STS y se encriptan con claves derivadas de HKDF-SHA512 basadas en claves Curve25519 por sesión. Esto se aplica tanto a los accesorios basados en IP como a los accesorios Bluetooth de baja energía (BLE).

En el caso de los dispositivos BLE que admiten notificaciones de difusión, un dispositivo iOS, iPadOS y macOS enlazado proporciona al accesorio una clave de encriptación de difusión a través de una sesión segura. Esta clave se utiliza para encriptar los datos sobre los cambios de estado del accesorio, que se notifican mediante avisos de BLE. La clave de encriptación de difusión es una clave derivada de HKDFSHA-512 y los datos se encriptan con el algoritmo ChaCha20-Poly1305 AEAD. El dispositivo iOS, iPadOS y macOS cambia periódicamente la clave de encriptación de difusión, que se actualiza en otros dispositivos mediante iCloud, tal como se describe en el apartado [Seguridad de los datos de HomeKit](#).

HomeKit y Siri

Siri se puede utilizar para enviar consultas a los accesorios y controlarlos, y para activar ambientes. Siri recibe anónimamente información mínima sobre la configuración de la casa para facilitar los nombres de las habitaciones, accesorios y ambientes necesarios para el reconocimiento de comandos. El audio enviado a Siri puede hacer referencia a determinados accesorios o comandos, pero esos datos de Siri no se asocian a otras funciones de Apple, como HomeKit.

Accesorios de HomeKit compatibles con Siri

Los usuarios pueden habilitar nuevas funciones como Siri, y otras funciones del HomePod como los temporizadores, las alarmas, el intercomunicador y el timbre, en los accesorios compatibles con Siri usando la app Casa. Cuando se activan estas funciones, el accesorio se coordina con un HomePod enlazado en la red local que tiene estas funciones de Apple. El audio se intercambia entre los dispositivos a través de canales encriptados usando los protocolos de HomeKit y AirPlay.

Cuando "Al oír 'Oye Siri'" está activado, el accesorio escucha la frase "Oye Siri" utilizando un motor de detección de la frase de activación que se ejecuta localmente. Si este motor detecta la frase, envía el audio directamente a un HomePod enlazado usando el HomeKit. El HomePod realiza una segunda comprobación del audio y puede cancelar la sesión de audio si la frase no parece contener la frase de activación.

Cuando “Toca para Siri” está activado, el usuario puede pulsar un botón dedicado en el accesorio para iniciar una conversación con Siri. El audio se envía directamente al HomePod enlazado.

Cuando se detecta una invocación correcta de Siri, el HomePod envía el audio a los servidores de Siri y cumple la intención del usuario usando las mismas garantías de seguridad, privacidad y encriptación que el HomePod aplica a las invocaciones del usuario realizadas al propio HomePod. Si Siri tiene una respuesta de audio, la respuesta de Siri se envía a través de un canal de audio AirPlay al accesorio. Algunas peticiones de Siri requieren información adicional por parte del usuario (por ejemplo, preguntarle si quiere escuchar más opciones). En ese caso, el accesorio recibe una indicación de que se debe preguntar al usuario y el audio adicional se transmite al HomePod.

El accesorio debe tener un indicador visual para señalar al usuario cuándo está escuchando activamente (por ejemplo, un indicador LED). El accesorio no tiene conocimiento de la intención de la petición de Siri, salvo el acceso a los flujos de audio, y no se almacenan datos del usuario en el accesorio.

Seguridad de los datos de HomeKit

Los datos de HomeKit se pueden actualizar de forma segura entre los dispositivos iOS, iPadOS y macOS de un usuario mediante iCloud y el [llavero](#) de iCloud. Durante este proceso, los datos de HomeKit se encriptan con claves derivadas de la identidad de HomeKit del usuario y con un [nonce](#) aleatorio, y se gestionan como un objeto binario grande o *blob* opaco. El BLOB más reciente se almacena en iCloud, pero no se utiliza para ningún otro fin. Además, como está encriptado con claves que solo están disponibles en los dispositivos iOS, iPadOS y macOS del usuario, no es posible acceder a su contenido durante la transmisión y el almacenamiento en iCloud.

Los datos de HomeKit también se sincronizan entre varios usuarios de la misma casa. Este proceso utiliza los mismos métodos de autenticación y encriptación que se usan entre un dispositivo iOS, iPadOS y macOS y un accesorio de HomeKit. La autenticación se basa en las claves públicas Ed25519 que se intercambian entre dispositivos al añadir un usuario a una casa. Después de añadir un usuario nuevo a una casa, todas las comunicaciones se autentican y encriptan con el protocolo STS y claves por sesión.

El usuario que creó inicialmente el grupo de casa en HomeKit u otro usuario con permiso de edición son los que pueden añadir usuarios nuevos. El dispositivo del propietario configura los accesorios con la clave pública del nuevo usuario, de modo que el accesorio pueda autenticar y aceptar los comandos de dicho usuario. Cuando un usuario con permiso de edición añade a otro usuario, el proceso se delega a una central de accesorios de la casa para que complete la operación.

HomeKit y el Apple TV

El proceso para poder utilizar el Apple TV con HomeKit se lleva a cabo automáticamente cuando el usuario inicia sesión en iCloud. La cuenta de iCloud debe tener la autenticación de doble factor activada. El Apple TV y el dispositivo del propietario intercambian temporalmente las claves públicas Ed25519 a través de iCloud. Cuando el dispositivo del propietario y el Apple TV están conectados a la misma red local, se utilizan las claves temporales para proteger la conexión a través de la red local mediante el protocolo de estación a estación y las claves por sesión. Este proceso utiliza los mismos métodos de autenticación y encriptación que se usan entre un dispositivo iOS, iPadOS y macOS y un accesorio de HomeKit. A través de esta conexión local segura, el dispositivo del propietario transfiere el par de claves pública y privada Ed25519 del usuario al Apple TV. A continuación, estas claves se utilizan para proteger la comunicación entre el Apple TV y los accesorios de HomeKit, así como entre el Apple TV y otros dispositivos iOS, iPadOS y macOS que forman parte del grupo casa de HomeKit.

Si un usuario no tiene más de un dispositivo ni concede acceso a su casa a más usuarios, los datos de HomeKit no se transfieren a iCloud.

Apps y datos de Casa

El acceso de las apps a los datos de casa está controlado por los ajustes de privacidad del usuario. Para que las apps tengan acceso a estos datos cuando lo solicitan, los usuarios tienen que concedérselo, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS, iPadOS y macOS. Si el usuario lo autoriza, las apps tienen acceso a los nombres de las habitaciones, los nombres de los accesorios y la ubicación de cada accesorio, así como a otra información que se detalla en la documentación para desarrolladores de HomeKit en <https://developer.apple.com/homekit/>.

Almacenamiento local de datos

HomeKit almacena datos sobre casas, accesorios, ambientes y usuarios en los dispositivos iOS, iPadOS y macOS de un usuario. Estos datos almacenados se encriptan con claves derivadas de las claves de identidad de HomeKit del usuario y con un nonce aleatorio. Además, los datos de HomeKit se almacenan con la clase de [Protección de datos](#) "Protegido hasta la primera autenticación del usuario". Para los datos de HomeKit, solo se realizan copias de seguridad encriptadas, de modo que, por ejemplo, las copias de seguridad no encriptadas en el Finder (en macOS 10.15 o posterior) o en iTunes (en macOS 10.14 o anterior) a través de USB no contienen datos de HomeKit.

Routers seguros con HomeKit

Los routers compatibles con HomeKit permiten a los usuarios mejorar la seguridad de la red de su casa gestionando el acceso wifi que los accesorios de HomeKit tienen a la red local y a internet. Los routers también son compatibles con el sistema de autenticación mediante clave precompartida privada (PPSK), de modo que los accesorios pueden añadirse a la red wifi mediante una clave específica para dicho accesorio que puede revocarse cuando sea necesario. La autenticación mediante PPSK proporciona una mayor seguridad, ya que la contraseña principal de la red wifi no queda expuesta a los accesorios y, además, permite al router identificar a un accesorio de forma segura aunque tuviera que cambiar su dirección MAC.

En la app Casa, los usuarios pueden configurar distintas restricciones de acceso para los grupos de accesorios:

- *Sin restricciones*: Permite el acceso a internet y a la red local sin ningún tipo de restricción.
- *Automático*: Es el ajuste por defecto. Permite el acceso a internet y a la red local en función de una lista de sitios de internet y de puertos locales que el fabricante del accesorio proporciona a Apple. Esta lista incluye todos los sitios y puertos que necesita el accesorio para funcionar adecuadamente (el ajuste "Sin restricciones" se aplica hasta que dicha lista está disponible).
- *Restringir a casa*: No se permite el acceso a internet ni a la red local excepto para las conexiones que HomeKit requiere para detectar y controlar los accesorios desde la red local (incluida la conexión desde la central de accesorios de la casa para permitir el control remoto).

La autenticación mediante PPSK utiliza una contraseña WPA2 Personal segura y específica para cada accesorio que HomeKit genera automáticamente y que se revoca en el momento en el que el accesorio se elimina de la app Casa. Se usa la autenticación mediante PPSK cuando HomeKit añade un accesorio a la red wifi en una casa que se haya configurado con un router de HomeKit; esta adición aparece reflejada como "Credencial wifi: Gestionada por HomeKit" en la pantalla de ajustes del accesorio en la app Casa. Los accesorios que se hubieran añadido a la red wifi antes de la instalación del router se reconfiguran para usar la autenticación mediante PPSK si son compatibles con ella; de lo contrario, mantendrán sus credenciales actuales.

Como medida de seguridad adicional, los usuarios deben configurar el router de HomeKit mediante la app del fabricante del router para que dicha app pueda validar que los usuarios tienen acceso al router y que tienen permiso para añadirlo a la app Casa.

Seguridad de las cámaras de HomeKit

Las cámaras que tienen una dirección de protocolo de internet (IP) en HomeKit envían secuencias de audio y de vídeo directamente al dispositivo iOS, iPadOS, tvOS y macOS por la red local que accede a la secuencia. Las secuencias se encriptan con claves generadas de forma aleatoria en el dispositivo y en una cámara de protocolo de internet (o cámara IP), las cuales se intercambian en la sesión segura que establece HomeKit con la cámara. Cuando un dispositivo no se encuentra en la red local, recibe las secuencias encriptadas a través de la central de accesorios de la casa. Dicha central de accesorios no desencripta las secuencias; solo sirve para transmitir las entre el dispositivo y la cámara IP. Cuando una app muestra la visualización del vídeo de la cámara IP de HomeKit al usuario, HomeKit renderiza los fotogramas de vídeo de forma segura desde un proceso del sistema independiente. En consecuencia, la app no puede acceder a la secuencia de vídeo ni almacenarla. Además, las apps no pueden realizar capturas de pantalla de esta secuencia.

Vídeo seguro de HomeKit

HomeKit proporciona un mecanismo de punto a punto privado y seguro para grabar, analizar y revisar clips de vídeo grabados por las cámaras IP de HomeKit sin exponer dichas grabaciones a Apple ni a terceros. Cuando una cámara IP detecta movimiento, se envían los clips de vídeo grabados directamente a un dispositivo Apple que actúa como central de accesorios de la casa a través de una conexión de red local creada con ese fin entre la central de accesorios y la cámara IP. La conexión de red local se encripta con un par de claves derivadas de HKDF-SHA512 que se negocia a través de la sesión de HomeKit entre la central de accesorios de la casa y la cámara IP. HomeKit desencripta las transmisiones de audio y vídeo en la central de accesorios y analiza localmente los fotogramas de vídeo en busca de cualquier suceso significativo. Si se detecta algo significativo, HomeKit encripta el clip de vídeo con cifrado AES-256-GCM y una clave AES256 generada aleatoriamente. Asimismo, HomeKit genera fotogramas póster de cada clip, que a su vez se encriptan con la misma clave AES256. Una vez encriptados, los fotogramas póster y los datos de audio y vídeo se suben a los servidores de iCloud. Los metadatos relacionados con cada clip, que incluyen la clave de encriptación, se suben a CloudKit mediante el método de encriptación de punto a punto de iCloud.

Para la clasificación de caras, HomeKit almacena todos los datos que se usan para clasificar la cara de una determinada persona en CloudKit mediante la encriptación de punto a punto de iCloud. Los datos almacenados incluyen información sobre cada persona, como el nombre, así como imágenes de su cara. Estas imágenes faciales se pueden obtener de la app Fotos de un usuario si ha dado permiso para ello, o se pueden recopilar a partir del vídeo capturado por la cámara IP que se ha analizado previamente. Una sesión de análisis del vídeo de seguridad de HomeKit utiliza estos datos de clasificación para identificar caras en la secuencia de vídeo que recibe directamente de la cámara IP e incluye esa información de identificación en los metadatos del clip mencionados anteriormente.

Cuando se usa la app Casa para ver los clips grabados por las cámaras, se descargan los datos de iCloud y las claves necesarias para desencriptar las transmisiones se desencapsulan localmente mediante la encriptación de punto a punto de iCloud. El contenido de vídeo encriptado se transmite desde los servidores y se desencripta localmente en el dispositivo iOS antes de mostrarlo en el visor. Cada sesión de vídeo grabada puede descomponerse en subsecciones de modo que cada una de ellas encripte su contenido con su propia clave única.

Seguridad de HomeKit con el Apple TV

HomeKit conecta de forma segura accesorios de control remoto de terceros con el Apple TV y permite añadir perfiles de usuario al propietario del Apple TV de la casa.

Uso de accesorios de control remoto de terceros con el Apple TV

Algunos accesorios de control remoto de terceros envían eventos de diseño de interfaz humana (HID) y audio de Siri a un Apple TV asociado añadido con la app Casa. El mando a distancia envía los eventos de HID a través de la sesión segura al Apple TV. Un mando a distancia compatible con Siri envía datos de audio al Apple TV cuando el usuario activa explícitamente el micrófono en el mando a distancia mediante un botón específico de Siri. El mando a distancia envía el audio directamente al Apple TV a través de una conexión de red local dedicada. Para encriptar la conexión de red local, se utiliza un par de claves derivadas de HKDF-SHA512 que se negocia a través de la sesión de HomeKit entre el Apple TV y el mando a distancia. HomeKit desencripta el audio en el Apple TV y lo reenvía a la app Siri, donde se trata con las mismas medidas de protección de la privacidad que cualquier entrada de audio de Siri.

Perfiles del Apple TV para las casas con HomeKit

Cuando un usuario de una casa de HomeKit añade su perfil al del propietario del Apple TV de la casa, le da a ese usuario acceso a sus programas de televisión, música y podcasts. Los ajustes de cada usuario relativos a su uso del perfil en el Apple TV se comparten en la cuenta de iCloud del propietario usando la encriptación de punto a punto de iCloud. Los datos son propiedad de cada usuario y se comparten con el propietario como de solo lectura. Cada usuario de la casa puede cambiar estos valores en la app Casa y el Apple TV del propietario usa estos ajustes.

Cuando se activa un ajuste, la cuenta de iTunes del usuario pasa a estar disponible en el Apple TV. Cuando se desactiva un ajuste, toda la cuenta y los datos pertenecientes a ese usuario se borran del Apple TV. El dispositivo del usuario inicia el uso compartido inicial de CloudKit y el identificador para establecer que el uso compartido seguro de CloudKit se envía por el mismo canal seguro que se utiliza para sincronizar los datos entre los usuarios de la casa.

Seguridad de SiriKit en iOS, iPadOS y watchOS

Siri usa el sistema de las extensiones de app para comunicarse con apps de terceros. En un dispositivo, Siri puede acceder a los datos de contacto del usuario y a la ubicación actual del dispositivo. Sin embargo, antes de proporcionar información protegida a una app, Siri comprueba los permisos de acceso de la app controlados por el usuario. En función de esos permisos, Siri envía a la extensión de la app solo el fragmento pertinente de la frase original del usuario. Por ejemplo, si una app no tiene acceso a los datos de contacto, Siri no resolverá ninguna relación personal que aparezca en la petición de un usuario como, por ejemplo, en “Págale a mi madre 10 euros con App de Pago”. En ese caso, la app solo vería el término literal “mi madre”.

Sin embargo, si el usuario le ha dado a la app permiso para acceder a los datos de contacto, la app recibirá información resuelta sobre la madre del usuario. Si se ha mencionado una relación en la parte principal de un mensaje, por ejemplo “Dile a mi madre por app_para_mensajes que mi hermano es genial”, Siri no resuelve “mi hermano” independientemente de los permisos de la app.

Las apps compatibles con SiriKit pueden enviar vocabulario específico de la app o del usuario a Siri, como los nombres de los contactos del usuario. Esta información hace posible el reconocimiento de voz de Siri y la comprensión del lenguaje natural para reconocer el vocabulario de esa app, y está asociada con un identificador aleatorio. La información personalizada seguirá estando disponible siempre y cuando el identificador esté en uso, o hasta que el usuario desactive la integración de Siri de la app en Ajustes, o hasta que se desinstale la app compatible con SiriKit.

Para una frase como “Pídeme un coche para ir a casa de mi madre con AppDeVehículoCompartido”, la solicitud requiere los datos de la ubicación de los contactos del usuario. Solo para esa solicitud, Siri proporciona la información requerida a la extensión de la app, independientemente de los permisos que el usuario le haya dado a la app para acceder a la ubicación o a los datos de contacto.

Seguridad de DriverKit para macOS

DriverKit es la estructura que permite a los desarrolladores crear controladores de dispositivo que el usuario instala en el Mac. Los controladores creados con DriverKit se ejecutan en el espacio del usuario, en lugar de hacerlo como extensiones del kernel, para mejorar la seguridad y la estabilidad del sistema. Esto facilita la instalación y aumenta la estabilidad y seguridad de macOS.

El usuario solo tiene que descargar la app (no se necesitan instaladores si se usan las extensiones del sistema o DriverKit) y la extensión solo se activa cuando es necesario. Esto sustituye a las kexts en muchos casos de uso que requieren privilegios de administrador para instalar en `/Sistema/Librería` o `/Librería`.

Se recomienda a los administradores de TI que usan controladores de dispositivos, soluciones de almacenamiento en la nube, conexiones de red y apps de seguridad que requieren extensiones del kernel que se pasen a las versiones más recientes que estén creadas en extensiones del sistema. Estas versiones más recientes reducen significativamente la posibilidad de que se produzcan situaciones de "kernel panic" en el Mac, además de reducir la superficie de ataque. Estas nuevas extensiones se ejecutan en el espacio del usuario, no requieren privilegios especiales para la instalación y se eliminan automáticamente cuando la app que hospeda la extensión se traslada a la Papelera.

La estructura DriverKit proporciona clases de C++ para servicios de E/S, coincidencias de dispositivos, descriptores de memoria y colas de envío. También define tipos adecuados de E/S para números, colecciones, cadenas y otros tipos comunes. El usuario utiliza estos junto con las estructuras de controladores específicas para cada familia, como USBDriverKit y HIDDriverKit. Se puede usar la estructura de las extensiones del sistema para instalar y actualizar un controlador.

Seguridad de ReplayKit en iOS y iPadOS

ReplayKit es una estructura que permite a los desarrolladores añadir a sus apps la posibilidad de grabar contenido y retransmitirlo en directo. Además, permite a los usuarios comentar sus grabaciones y retransmisiones con el micrófono y la cámara frontal del dispositivo.

Grabación de vídeo

En la grabación de un vídeo, hay varias capas de seguridad integradas:

- *Cuadro de diálogo de permisos:* Antes de empezar a grabar, ReplayKit muestra un aviso de consentimiento del usuario en el que se solicita al usuario que confirme su intención de grabar la pantalla, el micrófono y la cámara frontal. Este aviso aparece una vez por cada proceso de la app y vuelve a aparecer si la app se deja en segundo plano durante más de 8 minutos.
- *Grabación de la pantalla y del audio:* La grabación de la pantalla y del audio no se incluye en el proceso de la app en el daemon `replayd` de ReplayKit, lo cual garantiza que dicho proceso no podrá acceder nunca al contenido grabado.
- *Grabación de la pantalla y del audio integrada en la app:* Esto permite que la app obtenga búferes de muestra y de vídeo que están protegidos por el cuadro de diálogo de permisos.
- *Creación del vídeo y almacenamiento:* El archivo de vídeo se guarda en un directorio al que solo pueden acceder los subsistemas de ReplayKit, por lo que ninguna app puede acceder a él. Esto contribuye a que ningún tercero pueda utilizar las grabaciones sin el consentimiento del usuario.
- *Previsualización y compartición por parte del usuario final:* El usuario puede previsualizar y compartir el vídeo con la interfaz de usuario que provee ReplayKit. La interfaz de usuario se presenta fuera del proceso mediante la infraestructura de extensiones de iOS y tiene acceso al archivo de vídeo generado.

Retransmisión con ReplayKit

En la retransmisión de un vídeo, hay varias capas de seguridad integradas:

- *Grabación de la pantalla y del audio:* El mecanismo de grabación de la pantalla y del audio durante la retransmisión es el mismo que el de la grabación de vídeo y se da en `replayd`.
- *Extensiones de retransmisión:* Para que los servicios de terceros puedan participar en la retransmisión de ReplayKit, es necesario que creen dos extensiones nuevas configuradas con el endpoint "com.apple.broadcast-services":
 - Una extensión de interfaz de usuario que permita al usuario configurar la retransmisión.
 - Una extensión de carga que gestione la carga de los datos de vídeo y audio en los servidores del servicio.

Esta arquitectura ayuda a garantizar que las apps de alojamiento no tengan privilegios sobre el contenido de vídeo y audio transmitido. Únicamente tienen acceso ReplayKit y las extensiones de retransmisión de terceros.

- *Selector de retransmisión:* Con el selector de retransmisión, los usuarios inician las retransmisiones del sistema directamente desde su app mediante la misma interfaz de usuario definida por el sistema que es accesible a través del centro de control. La interfaz de usuario se implementa mediante una API privada y es una extensión que se encuentra en la estructura de ReplayKit. No está incluida en el proceso de la app de alojamiento.
- *Extensión de carga:* La extensión que implementan los servicios de retransmisión de terceros para gestionar el contenido de audio y vídeo durante la retransmisión utiliza búferes de muestra no codificados en formato nativo. Cuando se utiliza este modo de gestión, los datos de audio y vídeo se serializan y envían a la extensión de carga de terceros en tiempo real a través de una conexión XPC directa. Los datos del vídeo se codifican mediante la extracción del objeto IOSurface del búfer de muestra del vídeo, la codificación de dicho objeto de forma segura como un objeto XPC, su envío por XPC a la extensión de terceros y su descodificación de forma segura como el objeto IOSurface inicial.

Seguridad de ARKit en iOS y iPadOS

ARKit es una estructura que permite a los desarrolladores crear experiencias de realidad aumentada en sus apps o juegos. Los desarrolladores pueden añadir elementos en 2D o 3D mediante la cámara delantera o trasera de un dispositivo iOS o iPadOS.

Apple ha diseñado las cámaras teniendo en cuenta la privacidad y, para que las apps de terceros puedan acceder a ellas, deben obtener primero el consentimiento del usuario. En iOS y iPadOS, cuando un usuario permite que una app acceda a la cámara, esa app puede acceder a las imágenes en tiempo real de las cámaras delantera y trasera. Las apps no pueden usar la cámara sin dejar claro que la cámara está en uso.

Las fotos y los vídeos que se toman con la cámara pueden contener otra información, como dónde y cuándo se tomaron, la profundidad de campo y la sobrecaptura. Si los usuarios no quieren que las fotos y vídeos tomados con la app Cámara incluyan la ubicación, pueden controlar esto en cualquier momento en Ajustes > Privacidad > Localización > Cámara. Si los usuarios no quieren que se incluya la ubicación al compartir las fotos y vídeos, pueden desactivar la ubicación en el menú Opciones de la hoja de compartir contenido.

Para posicionar mejor la experiencia de realidad aumentada del usuario, las apps que usan ARKit deben utilizar información de seguimiento facial o global desde la otra cámara. El seguimiento global usa algoritmos en el dispositivo del usuario para procesar la información de estos sensores con el fin de determinar su posición en relación con un espacio físico. El seguimiento global permite funciones como la dirección óptica en Mapas.

Gestión segura de dispositivos

Descripción general de la gestión segura de dispositivos

iOS, iPadOS, macOS y tvOS son compatibles con políticas de seguridad y configuraciones flexibles que se pueden aplicar y gestionar fácilmente. Gracias a ellas, las organizaciones pueden proteger su información corporativa y ayudar a garantizar que sus empleados cumplen con los requisitos de la empresa, incluso si utilizan sus propios dispositivos, por ejemplo, como parte de un programa "trae tu propio dispositivo" (BYOD, por sus siglas en inglés).

Las organizaciones pueden utilizar recursos como la protección mediante contraseña, los perfiles de configuración, el borrado remoto y las soluciones de [gestión de dispositivos móviles \(MDM\)](#) de terceros para gestionar conjuntos de dispositivos y ayudar a mantener la seguridad de los datos corporativos, incluso cuando los empleados acceden a dichos datos mediante sus propios dispositivos.

En iOS 13 o posterior, iPadOS 13.1 o posterior y macOS 10.15 o posterior, los dispositivos Apple son compatibles con una nueva opción de inscripción de usuarios específicamente diseñada para los programas BYOD. Las inscripciones de los usuarios proporcionan más autonomía a los usuarios que utilizan sus propios dispositivos, a la vez que se aumenta la seguridad de los datos de la empresa al almacenarlos en un volumen [APFS \(sistema de archivos de Apple\)](#) independiente y protegido mediante encriptación. Esto proporciona un mayor equilibrio de seguridad, privacidad y experiencia del usuario para los programas BYOD.

Seguridad del modelo de enlace en el iPhone y el iPad

iOS y iPadOS usan un modelo de enlace para controlar el acceso a un dispositivo desde un ordenador host. El enlace establece una relación de confianza entre el dispositivo y el host conectado, representada mediante el intercambio de claves públicas. iOS y iPadOS utilizan esta señal de confianza para activar otras funcionalidades con el host conectado, como la sincronización de datos. En iOS 9 o posterior, los servicios:

- que requieren enlace no pueden iniciarse hasta que el usuario haya desbloqueado el dispositivo;
- no se iniciarán a no ser que el dispositivo se haya desbloqueado recientemente;
- pueden requerir que el dispositivo esté desbloqueado para poder iniciarse (como con la sincronización de fotos).

Para que el proceso de enlace se lleve a cabo, es necesario que el usuario desbloquee el dispositivo y acepte la solicitud de enlace del host. En iOS 9 o posterior, el usuario también debe introducir su código, tras lo cual el host y el dispositivo intercambian y guardan claves públicas RSA de 2048 bits. A continuación, el host recibe una clave de 256 bits con la que puede desbloquear un repositorio de claves de custodia almacenado en el dispositivo. Las claves intercambiadas se utilizan para comenzar una sesión SSL encriptada, que el dispositivo necesita antes de enviar datos protegidos al host o de iniciar un servicio (sincronización con iTunes o Finder, transferencias de archivos, desarrollo con Xcode, etc.). A fin de utilizar esta sesión encriptada para todas las comunicaciones, el dispositivo precisa conexiones desde un host a través de la red wifi, con lo cual debe enlazarse previamente mediante USB. Además, el enlace también activa varias funciones de diagnóstico. En iOS 9, un registro de enlaces caduca si no se ha utilizado desde hace más de seis meses. En iOS 11 o posterior, este periodo de tiempo se reduce a 30 días.

Determinados servicios de diagnóstico, como `com.apple.mobile.pcapd`, solo pueden funcionar mediante USB. Además, el servicio `com.apple.file_relay` precisa la instalación de un perfil de configuración firmado por Apple. En iOS 11 o posterior, el Apple TV puede utilizar el protocolo de contraseña remota segura para establecer una relación de enlace por vía inalámbrica.

El usuario puede borrar la lista de hosts de confianza con las opciones “Restablecer ajustes de red” o “Restablecer localización y privacidad”.

Gestión de dispositivos móviles

Descripción general de la seguridad de la gestión de dispositivos móviles

Los sistemas operativos de Apple son compatibles con las soluciones de [gestión de dispositivos móviles \(MDM\)](#), que permiten a las organizaciones configurar y gestionar implementaciones de dispositivos Apple a gran escala.

Cómo funciona la solución MDM de forma segura

Las funciones de MDM están basadas en las tecnologías de los sistemas operativos existentes, como los perfiles de configuración, la inscripción remota y el [servicio de notificaciones push de Apple \(APNs\)](#). Por ejemplo, el APNs se utiliza para activar el dispositivo de manera que pueda comunicarse directamente con la solución MDM a través de una conexión segura. No se transmite información sensible ni privada con el APNs.

Con ayuda de una solución MDM, los departamentos de TI pueden inscribir dispositivos Apple en un entorno empresarial, configurar los ajustes y actualizarlos mediante una red inalámbrica, supervisar el cumplimiento de políticas corporativas, gestionar políticas de actualización de software e incluso borrar o bloquear de forma remota los dispositivos gestionados.

Además de las inscripciones de dispositivos tradicionales compatibles con iOS, iPadOS, macOS y tvOS, se ha añadido un tipo de inscripción en iOS 13 o posterior, iPadOS 13.1 o posterior y macOS 10.15 o posterior: la inscripción del usuario. Las inscripciones de los usuarios son inscripciones de MDM pensadas especialmente para las implementaciones de "trae tu propio dispositivo" (BYOD), en las que el dispositivo es personal pero se usa en un entorno gestionado. Las inscripciones de los usuarios otorgan a la solución MDM privilegios más limitados que las inscripciones de dispositivos no gestionados y ofrecen una separación criptográfica de los datos del usuario y de los datos corporativos.

Tipos de inscripción

- *Inscripción automatizada de dispositivos:* La inscripción automatizada de dispositivos permite a las organizaciones configurar y gestionar dispositivos desde el momento que se sacan del embalaje (un proceso que se conoce como *implementación de avance automático*). Estos dispositivos se convierten en *supervisados* y los usuarios tienen la posibilidad de establecer que el usuario no pueda eliminar el perfil MDM. La inscripción automatizada de dispositivos se ha diseñado para los dispositivos que son propiedad de la organización.
- *Inscripción de dispositivos:* La inscripción de dispositivos permite a los usuarios de las organizaciones inscribir dispositivos manualmente y gestionar numerosos aspectos del uso del dispositivo, incluyendo la posibilidad de borrarlo. La inscripción de dispositivos proporciona también un conjunto más amplio de cargas útiles y restricciones que pueden aplicarse al dispositivo. Cuando un usuario elimina un perfil de inscripción, todos los perfiles de configuración, sus ajustes y las apps gestionadas basadas en dicho perfil también se eliminan.

- *Inscripción del usuario:* La inscripción del usuario está diseñada para los dispositivos que son propiedad del usuario y está integrada en el ID de Apple gestionado para establecer la identidad de un usuario en el dispositivo. Los ID de Apple gestionados forman parte del perfil de inscripción del usuario y el usuario debe autenticarse correctamente para que se complete la inscripción. Los ID de Apple gestionados se pueden usar junto con un ID de Apple personal con el que el usuario ya haya iniciado sesión. Las cuentas y apps gestionadas utilizan un ID de Apple gestionado, mientras que las cuentas y apps personales usan un ID de Apple personal.

Restricciones del dispositivo

Los administradores pueden activar (o, en algunos casos, desactivar) las restricciones para ayudar a impedir que los usuarios accedan a una app, un servicio o una función específicos de un iPhone, iPad, Mac o Apple TV inscrito en una solución MDM. Las restricciones se envían a los dispositivos en una carga útil de restricciones, que forma parte de un perfil de configuración. Ciertas restricciones en un iPhone se pueden duplicar en un Apple Watch enlazado.

Gestión de los ajustes del código y de la contraseña

Por defecto, el código del usuario se puede definir como un PIN numérico. En dispositivos iOS y iPadOS con Face ID o Touch ID, la longitud mínima del código es de cuatro dígitos. Se recomiendan los códigos más largos y más complejos, puesto que son más difíciles de averiguar o atacar.

Los administradores pueden aplicar requisitos de uso de códigos complejos y otras políticas mediante soluciones MDM o Microsoft Exchange ActiveSync, o bien pidiendo a los usuarios que instalen perfiles de configuración manualmente. Se necesita una contraseña de administrador para instalar la carga útil de la política de código del macOS. Algunas políticas de código pueden requerir que el código tenga una determinada composición, longitud u otros atributos.

Aplicación de los perfiles de configuración

Los perfiles de configuración son la principal manera en la que una solución MDM aplica y gestiona políticas y restricciones en dispositivos gestionados. Si las organizaciones necesitan configurar muchos dispositivos o especificar una gran cantidad de certificados, ajustes de red o ajustes de correo personalizados en un número elevado de dispositivos, los perfiles de configuración te permiten hacer esto con seguridad.

Perfiles de configuración

Un *perfil de configuración* es un archivo XML (termina en .mobileconfig) que contiene cargas útiles que cargan los ajustes y la información de autorización en dispositivos Apple. Los perfiles de configuración automatizan la configuración de ajustes, cuentas, restricciones y credenciales. Estos archivos se pueden crear con una solución MDM, con Apple Configurator para Mac o manualmente. Antes de enviar un perfil de configuración a un dispositivo Apple, las organizaciones deben inscribir el dispositivo en la solución MDM mediante un perfil de inscripción.

Perfiles de inscripción

Un *perfil de inscripción* es un perfil de configuración con una carga útil de MDM que inscribe el dispositivo en la solución MDM indicada para dicho dispositivo, lo que permite a la solución MDM enviar comandos y perfiles de configuración al dispositivo y consultar ciertos aspectos sobre este. Cuando un usuario elimina un perfil de inscripción, todos los perfiles de configuración, sus ajustes y las apps gestionadas basadas en dicho perfil también se eliminan. Un dispositivo no puede tener más de un perfil de inscripción al mismo tiempo.

Ajustes de los perfiles de configuración

Un perfil de configuración contiene una serie de ajustes en determinadas cargas útiles que se pueden especificar, incluidos los siguientes (con carácter no limitativo):

- políticas de código y de contraseña;
- restricciones en las funciones del dispositivo (por ejemplo, la desactivación de la cámara);
- ajustes de red y VPN;
- ajustes de Microsoft Exchange;
- ajustes de Mail;
- ajustes de la cuenta;
- ajustes del servicio de directorio LDAP;
- ajustes del servicio de calendario CalDAV;
- credenciales y claves;
- actualizaciones de software.

Encriptación y firma del perfil

Los perfiles de configuración se pueden firmar para validar su origen y ayudar a encriptar para garantizar su integridad y proteger su contenido. Los perfiles de configuración para iOS y iPadOS se encriptan mediante el formato de sintaxis de mensajes criptográficos (CMS) que se especifica en la [RFC 5652](#) y son compatibles con 3DES y AES128.

Instalación del perfil

Los usuarios pueden instalar perfiles de configuración directamente en sus dispositivos mediante Apple Configurator para Mac, o bien pueden descargarlos con Safari, enviarlos como archivos adjuntos mediante un mensaje de correo electrónico, transferirlos mediante AirDrop o la app Archivos en iOS y iPadOS, o enviarlos de forma remota con ayuda de una solución de [gestión de dispositivos móviles \(MDM\)](#). Cuando un usuario configura un dispositivo en [Apple School Manager](#) o [Apple Business Manager](#), el dispositivo descarga e instala un perfil para la inscripción en la solución MDM. Para obtener información acerca de cómo eliminar perfiles, consulta [Introducción a la gestión de dispositivos móviles](#) en Implementación de las plataformas de Apple.

Nota: En dispositivos supervisados, los perfiles de configuración también pueden bloquearse en un dispositivo. Esto está diseñado así para impedir su eliminación o para permitirla solo con un código. Dado que muchas organizaciones disponen de sus propios dispositivos iOS y iPadOS, los perfiles de configuración que unen un dispositivo a una solución MDM se pueden eliminar. Sin embargo, al hacerlo, se elimina también toda la información de configuración, las apps y los datos gestionados.

Inscripción automatizada de dispositivos

Las organizaciones pueden inscribir automáticamente dispositivos iOS, iPadOS, macOS y tvOS en las soluciones de [gestión de dispositivos móviles \(MDM\)](#) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban. Tras inscribirse en uno de los servicios, los administradores inician sesión en el sitio web del servicio y enlazan el programa a su solución MDM. A continuación, los dispositivos que han comprado se pueden asignar a los usuarios mediante MDM. Durante el proceso de configuración del dispositivo, es posible aumentar la seguridad de los datos sensibles con la aplicación de medidas de seguridad apropiadas. Por ejemplo:

- Haz que los usuarios se autenticuen durante el proceso de configuración inicial en el asistente de configuración del dispositivo de Apple durante la activación.
- Proporciona una configuración preliminar con acceso limitado y requiere configuración adicional para acceder a los datos sensibles.

Una vez que al usuario se le ha asignado un dispositivo, todas las configuraciones, restricciones o controles específicos de MDM se instalan automáticamente. Las comunicaciones establecidas entre los dispositivos y los servidores de Apple se encriptan mediante HTTPS (TLS).

El proceso de configuración se puede simplificar todavía más para los usuarios al eliminar determinados pasos en el asistente de configuración para los dispositivos, de modo que los usuarios pueden poner sus dispositivos en marcha rápidamente. Los administradores también pueden controlar si los usuarios pueden o no eliminar el perfil MDM del dispositivo y ayudar a garantizar que las restricciones del dispositivo están establecidas a lo largo de su ciclo de vida. Una vez que el dispositivo se saca del embalaje y se activa, se puede inscribir en la solución MDM de la organización, de manera que se instalan todos los ajustes de gestión, apps y libros definidos por el administrador de MDM.

Apple School Manager, Apple Business Manager y Apple Business Essentials

Apple School Manager, Apple Business Manager y Apple Business Essentials son servicios que permiten a los administradores de TI implementar dispositivos Apple que una organización ha comprado directamente a Apple o a través de operadores o distribuidores de Apple autorizados participantes en el programa.

Cuando se usan con una solución MDM, los administradores pueden simplificar el proceso de configuración para los usuarios, configurar ajustes de los dispositivos y distribuir apps y libros comprados en estos servicios. Apple School Manager también se integra directamente o mediante SFTP con sistemas de información de alumnos (SIS). Además, los tres servicios pueden usar la autenticación federada o el sistema para la administración de identidades entre dominios (SCIM) con Microsoft Azure Active Directory (Azure AD) para que los administradores puedan crear cuentas rápidamente.

Apple mantiene certificaciones conformes a los estándares ISO/IEC 27001 y 27018 para permitir que sus clientes puedan cumplir con sus obligaciones regulatorias y contractuales. Estas certificaciones proporcionan a los clientes una acreditación independiente de las prácticas de privacidad y seguridad de la información de Apple para los sistemas pertinentes. Para obtener más información, consulta [Certificaciones de seguridad para servicios de internet de Apple](#) en Certificaciones de las plataformas de Apple.

Nota: Para saber si un programa de Apple está disponible en un determinado país o región, consulta el artículo de soporte técnico de Apple [Disponibilidad de los métodos de pago y programas de Apple para el sector educativo y empresarial](#).

Supervisión del dispositivo

Generalmente, la *supervisión* indica que el dispositivo es propiedad de la organización, lo que le proporciona un control adicional sobre la configuración y las restricciones del dispositivo. Para obtener más información, consulta [Acerca de la supervisión de dispositivos Apple](#) en Implementación de las plataformas de Apple.

Seguridad del bloqueo de activación

El modo en que Apple aplica el bloqueo de activación varía en función de si el dispositivo es un iPhone o un iPad, un Mac con chip de Apple o un Mac basado en Intel con el chip de seguridad T2.

Comportamiento en el iPhone y el iPad

En dispositivos iPhone y iPad, el bloqueo de activación se aplica mediante el proceso de activación posterior a la pantalla de selección de wifi en el asistente de configuración de iOS y iPadOS. Cuando el dispositivo indica que se está activando, envía una solicitud a un servidor de Apple para obtener un certificado de activación. Los dispositivos con bloqueo de activación solicitan en este momento al usuario las credenciales de iCloud con las que se ha activado el bloqueo. El asistente de configuración de iOS y iPadOS no progresará a menos que pueda obtenerse un certificado válido.

Comportamiento en un Mac con chip de Apple

En un Mac con chip de Apple, el LLB verifica que existe un archivo LocalPolicy válido para el dispositivo y que los valores del **nonce** de la política de LocalPolicy coinciden con los valores almacenados en el componente de almacenamiento seguro. El LLB arrancará en el sistema operativo de recuperación si:

- No hay un archivo LocalPolicy para la instancia de macOS actual.
- El archivo LocalPolicy no es válido para esa instancia de macOS.
- Los valores del hash del nonce de LocalPolicy no coinciden con los hashes de los valores almacenados en el componente de almacenamiento seguro.

El sistema operativo de recuperación detecta que el Mac no está activado y contacta con el servidor de activación para obtener un certificado de activación. Si el dispositivo tiene el bloqueo de activación, el sistema operativo de recuperación solicita en este momento al usuario las credenciales de iCloud con las que se ha activado el bloqueo de activación. Después de obtener un certificado de activación válido, esa clave del certificado de activación se emplea para obtener un certificado de RemotePolicy. El ordenador Mac usa la clave de LocalPolicy y el certificado de RemotePolicy para generar un archivo LocalPolicy válido. El LLB no permitirá arrancar macOS a menos que haya presente un archivo LocalPolicy válido.

Comportamiento en ordenadores Mac basados en Intel

En un Mac basado en Intel con un chip T2, el firmware del chip T2 verifica que hay un certificado de activación válido antes de permitir que el ordenador arranque en macOS. El firmware de UEFI cargado por el chip T2 es responsable de consultar el estado de activación del dispositivo desde este chip y de arrancar en el sistema operativo de recuperación en lugar de en macOS si no se encuentra un certificado de activación válido. El sistema operativo de recuperación detecta que el Mac no está activado y contacta con el servidor de activación para obtener un certificado de activación. Si el dispositivo tiene el bloqueo de activación, el sistema operativo de recuperación solicita en este momento al usuario las credenciales de iCloud con las que se ha activado el bloqueo de activación. El firmware de UEFI no permitirá arrancar macOS a menos que haya presente un certificado de activación válido.

Modo Perdido gestionado y borrado remoto

El modo Perdido gestionado permite localizar dispositivos supervisados que han sido robados. Una vez localizados, es posible bloquearlos o borrarlos de forma remota.

Modo Perdido gestionado

Si se pierde o alguien roba un dispositivo iOS o iPadOS supervisado con iOS 9 o posterior, un administrador de [gestión de dispositivos móviles \(MDM\)](#) puede activar el modo Perdido (llamado modo Perdido gestionado) de forma remota en ese dispositivo. Cuando se activa este modo, se cierra la sesión del usuario activo en ese momento y el dispositivo no se puede desbloquear. En la pantalla, se muestra un mensaje que puede personalizar el administrador, como un número de teléfono al que llamar si alguien encuentra el dispositivo. El administrador también puede solicitar al propio dispositivo que envíe su ubicación en ese momento (incluso si está desactivada la función de localización) y, de forma opcional, reproducir un sonido. Cuando un administrador desactiva el modo Perdido gestionado, que es la única forma de salir de este modo, se informa al usuario mediante un mensaje en la pantalla bloqueada o un aviso en la pantalla de inicio.

Borrado remoto

Los administradores o usuarios pueden borrar el contenido de los dispositivos iOS, iPadOS y macOS de forma remota (el borrado remoto instantáneo solo está disponible si se ha activado FileVault en el Mac). El borrado remoto instantáneo se consigue al descartar la [clave de contenido](#) de [almacenamiento borrrable](#): de forma segura, de modo que los datos dejan de poder leerse. En el caso del borrado remoto mediante Microsoft Exchange ActiveSync, el dispositivo se registra en Microsoft Exchange Server antes de realizar el borrado.

Cuando una solución MDM o iCloud activan un comando de borrado remoto, el iPhone, iPad, iPod touch o Mac devuelve una confirmación a la solución MDM y realiza el borrado.

El borrado remoto no es posible en las siguientes situaciones:

- con la inscripción del usuario;
- si se usa Microsoft Exchange ActiveSync cuando la cuenta se instaló con la inscripción del usuario;
- si se usa Microsoft Exchange ActiveSync cuando el dispositivo está supervisado.

Los usuarios también pueden borrar el contenido de sus dispositivos iOS y iPadOS mediante la app Ajustes. Por último, como se ha mencionado anteriormente, los dispositivos iOS y iPadOS se pueden configurar para que se realice un borrado automático del contenido tras una serie de intentos erróneos de introducir el código.

Seguridad del iPad compartido en iPadOS

El modo de iPad compartido es un modo multiusuario que se utiliza en las implantaciones del iPad. Permite a los usuarios compartir un iPad manteniendo los documentos y los datos de cada usuario separados. Cada usuario obtiene su propia ubicación de almacenamiento reservada y privada, que se implementa como un volumen [APFS \(sistema de archivos de Apple\)](#) protegido por la credencial del usuario. Los iPad compartidos requieren el uso de un ID de Apple gestionado que sea propiedad de la organización y haya sido emitido por la misma.

Con los iPad compartidos, un usuario puede iniciar sesión en cualquier dispositivo que sea propiedad de la organización y que esté configurado para que lo puedan utilizar varios usuarios. Los datos de los usuarios se separan en directorios independientes, cada uno de los cuales está en su propio dominio de protección de datos y protegido mediante permisos UNIX y aislamiento. En iPadOS 13.4 o versiones posteriores, los usuarios también pueden iniciar sesiones temporales. Cuando el usuario cierra una sesión temporal, su volumen APFS se elimina y el espacio que tenía reservado se devuelve al sistema.

Inicio de sesión en el iPad compartido

Los ID de Apple gestionados, ya sean nativos o federados, se admiten al iniciar sesión en el iPad compartido. Al usar una cuenta federada por primera vez, se redirige al usuario al portal de inicio de sesión del proveedor de identidad (IdP, por sus siglas en inglés). Después de haberse autenticado, se emite un identificador de acceso de corta duración para respaldar los ID de Apple gestionados (y el proceso de inicio de sesión avanza de forma similar al proceso de inicio de sesión nativo de los ID de Apple gestionados). Después de haber iniciado sesión, el asistente de configuración del iPad compartido pide al usuario que establezca un código (credencial) que se usa para proteger los datos locales del dispositivo y para autenticarse en la pantalla de inicio de sesión en el futuro. Al igual que un dispositivo con un único usuario, en el que el usuario inicia sesión una vez en su ID de Apple gestionado con su cuenta federada para luego desbloquear el dispositivo con su código, en el iPad compartido el usuario inicia sesión una vez con su cuenta federada y, a partir de ese momento, usa el código que se ha establecido.

Cuando un usuario inicia sesión sin la autenticación federada, el ID de Apple gestionado se autentica con el [servicio de identidad \(IDS\) de Apple](#) mediante el protocolo SRP. Si la autenticación se realiza correctamente, se otorga un identificador de acceso de corta duración específico para el dispositivo. En el caso de que el usuario haya utilizado el dispositivo con anterioridad, ya dispondrá de una cuenta de usuario local que se desbloqueará con la misma credencial.

Si, por el contrario, el usuario no ha usado el dispositivo anteriormente o está usando la función de sesión temporal, el iPad compartido proporciona un nuevo ID de usuario UNIX, un volumen APFS para almacenar los datos personales del usuario y un llavero local. Puesto que se debe asignar (reservar) un espacio de almacenamiento para el usuario al crear el volumen APFS, puede que no se disponga del espacio suficiente para crear un volumen nuevo. En este caso, el sistema identifica a un usuario ya existente cuyos datos ya se hayan sincronizado en la nube y lo desaloja del dispositivo para que el nuevo usuario pueda iniciar sesión. En el caso improbable de que todos los usuarios existentes aún no hayan terminado de subir sus datos a la nube, el nuevo usuario no podrá iniciar sesión. Para iniciar sesión, el nuevo usuario tendrá que esperar a que se complete la sincronización de uno de los otros usuarios o solicitar a un administrador que fuerce la eliminación de una cuenta de usuario existente, con los riesgos de pérdida de datos que eso implicaría.

Si el dispositivo no está conectado a internet (por ejemplo, si el usuario no tiene ningún punto de acceso a una red wifi), solo podrá autenticarse con la cuenta local durante un número limitado de días. En esa situación, solo podrán iniciar sesión los usuarios que dispongan de cuentas locales que ya existían anteriormente o que inicien sesiones temporales. Una vez transcurrido el plazo, los usuarios deben autenticarse en línea, incluso si ya existe una cuenta local.

Una vez desbloqueada o creada la cuenta local del usuario, si se ha autenticado de forma remota, el identificador de corta duración emitido por los servidores de Apple se convertirá en un identificador de iCloud que permitirá iniciar sesión en iCloud. A continuación, los ajustes del usuario se restaurarán y sus documentos y datos se sincronizarán desde iCloud.

Mientras la sesión del usuario esté activa y el dispositivo esté conectado, los documentos y datos que se creen o modifiquen se almacenarán en iCloud. Además, un mecanismo de sincronización en segundo plano ayuda a garantizar el envío de los cambios a iCloud, o a otros servicios web que utilicen sesiones NSURLSession en segundo plano, una vez que el usuario ha cerrado sesión. Una vez completada la sincronización en segundo plano para ese usuario, el volumen APFS del usuario se desmontará y no se podrá montar de nuevo sin que el usuario vuelva a iniciar sesión.

En las sesiones temporales no se sincronizan los datos con iCloud y, aunque en las sesiones temporales se puede acceder a servicios de sincronización de otros proveedores, como Box o Google Drive, no hay posibilidad de seguir sincronizando los datos una vez terminada la sesión temporal.

Cierre de sesión en el iPad compartido

Cuando un usuario cierra la sesión en el iPad compartido, el [repositorio de claves](#) de dicho usuario se bloquea inmediatamente y todas las apps se cierran. En el caso de que otro usuario vaya a iniciar sesión, para agilizar el proceso, iPadOS pospone temporalmente algunas acciones ordinarias de cierre de sesión y muestra una ventana de inicio de sesión al nuevo usuario. Si un usuario inicia sesión durante este tiempo (aproximadamente 30 segundos), el iPad compartido realiza la limpieza diferida como parte del proceso de inicio de sesión de la cuenta del nuevo usuario. Sin embargo, si el iPad compartido permanece inactivo, se desencadenará la limpieza diferida. Durante la fase de limpieza, la ventana de inicio de sesión se reinicia como si se hubiera producido otro cierre de sesión.

Cuando termina una sesión temporal, el iPad compartido ejecuta la secuencia completa de cierre de sesión y elimina el volumen APFS de la sesión temporal inmediatamente.

Seguridad de Apple Configurator

Apple Configurator para Mac ofrece un diseño flexible, seguro y centrado en el dispositivo que permite a un administrador configurar de forma rápida y sencilla uno o decenas de dispositivos iOS, iPadOS y tvOS conectados a un Mac mediante USB (o dispositivos tvOS enlazados por Bonjour) antes de entregarlos a los usuarios. Con Apple Configurator para Mac, un administrador puede actualizar software, instalar apps y perfiles de configuración, cambiar y renombrar el fondo de pantalla de los dispositivos, exportar la información del dispositivo y los documentos, y mucho más.

Apple Configurator para Mac también puede restablecer o restaurar los ordenadores Mac con chip de Apple y los que tienen el chip de seguridad T2 de Apple. Cuando se restablece o restaura un Mac de esta forma, el archivo que contiene las últimas actualizaciones menores de los sistemas operativos (macOS, sistema operativo de recuperación para el chip de Apple o sepOS para el chip T2) se descarga de forma segura desde los servidores de Apple y se instala directamente en el Mac. Tras realizar correctamente el restablecimiento o restauración, el archivo se elimina del Mac que ejecuta Apple Configurator. En ningún momento el usuario puede inspeccionar o usar este archivo fuera de Apple Configurator.

Los administradores también pueden añadir dispositivos a Apple School Manager, Apple Business Manager o Apple Business Essentials mediante Apple Configurator para Mac o Apple Configurator para iPhone, incluso si los dispositivos no se han comprado directamente a Apple o a distribuidores y tiendas autorizadas por Apple. Cuando el administrador configura un dispositivo que se ha inscrito manualmente, se comporta igual que cualquier otro dispositivo en uno de esos servicios, con inscripción en la solución de gestión de dispositivos móviles (MDM) y supervisión obligatorias. Para los dispositivos que no se han comprado directamente, el usuario tiene un periodo provisional de 30 días para eliminar el dispositivo de uno de estos servicios, de la supervisión y de la solución MDM.

Las organizaciones también pueden usar Apple Configurator para Mac para activar dispositivos iOS, iPadOS y tvOS que no tengan ninguna conexión a internet, conectándolos a un Mac anfitrión con conexión a internet mientras se configuran los dispositivos. Los administradores pueden restaurar, activar y preparar dispositivos con las configuraciones necesarias (apps, perfiles y documentos) sin necesidad de conectarse a redes wifi o móviles. Esta función no permite al administrador saltarse los requisitos de bloqueo de activación que normalmente son necesarios durante la activación sin una conexión compartida.

Seguridad de “Tiempo de uso”

“Tiempo de uso” es una función para ver y gestionar el tiempo que los adultos y sus niños pasan en apps, sitios web y demás. Hay dos tipos de usuarios: adultos y menores (gestionados).

Aunque “Tiempo de uso” no es una nueva función de seguridad del sistema, es importante entender cómo protege la privacidad y seguridad de los datos recopilados y cómo se comparten entre los dispositivos. “Tiempo de uso” está disponible en iOS 12 o posterior, iPadOS 13.1 o posterior, macOS 10.15 o posterior y watchOS 6 o posterior (para algunas funciones).

En la tabla siguiente se describen las principales funciones de “Tiempo de uso”.

Función	Sistema operativo compatible
Ver datos de uso.	iOS iPadOS macOS
Aplicar restricciones adicionales.	iOS iPadOS macOS watchOS
Definir límites de uso de internet.	iOS iPadOS macOS
Definir límites para apps.	iOS iPadOS macOS watchOS
Configurar un tiempo de inactividad.	iOS iPadOS macOS watchOS

En el caso de un usuario que gestiona su propio dispositivo, es posible sincronizar los datos de uso y los controles de tiempo de uso entre dispositivos asociados a la misma cuenta de iCloud con la encriptación punto a punto de CloudKit. Para ello, es necesario que la cuenta del usuario tenga activada la autenticación de doble factor (por defecto, la sincronización está activada). La función “Tiempo de uso” sustituye a la de Restricciones que había en las versiones anteriores de iOS y iPadOS, y a la de “Controles parentales” de las versiones anteriores de macOS.

En iOS 13 o posterior, iPadOS 13.1 o posterior y macOS 10.15 o posterior, los usuarios de “Tiempo de uso” y los niños que gestionan comparten su uso automáticamente en todos los dispositivos si su cuenta de iCloud tiene activada la autenticación de doble factor. Cuando un usuario borra el historial de Safari o elimina una app, los datos de uso correspondientes se eliminan del dispositivo y de todos los dispositivos sincronizados.

Tiempo de uso para padres

Los padres también pueden usar “Tiempo de uso” en dispositivos iOS, iPadOS y macOS para conocer y controlar el uso que hacen sus niños del dispositivo. Si el padre o madre es organizador de la familia (en “En familia” en iCloud), puede ver datos de uso y gestionar los ajustes de tiempo de uso de sus niños. Los niños reciben una notificación cuando sus padres activan “Tiempo de uso” y también pueden supervisar su propio uso del dispositivo. Cuando los padres activan “Tiempo de uso” para sus niños, definen un código para que los niños no puedan hacer cambios. Al cumplir la mayoría de edad (que varía según el país o la región), los niños pueden desactivar esta supervisión.

Los datos de uso y los ajustes de configuración se transfieren entre los dispositivos de los padres y de los niños mediante el protocolo del [servicio de identidad \(IDS\)](#) de Apple encriptado de punto a punto. Los datos encriptados pueden almacenarse brevemente en los servidores de IDS hasta que el dispositivo receptor los lee (por ejemplo, en cuanto se enciende el iPhone, iPad o iPod touch si se encontraba apagado). Apple no puede leer estos datos.

Análisis de tiempo de uso

Si el usuario activa “Compartir análisis del iPhone y el Apple Watch”, solo se recopilarán los siguientes datos de manera anónima para que Apple pueda comprender mejor cómo se utiliza “Tiempo de uso”:

- Si estaba “Tiempo de uso” activado durante el asistente de configuración o posteriormente en Ajustes.
- Si se ha producido un cambio en el uso de una categoría después de haber creado un límite para ella (en un plazo de 90 días).
- Si “Tiempo de uso” está activado.
- Si hay activado un tiempo de inactividad.
- Número de veces que se ha utilizado la consulta “Pedir más tiempo”.
- Número de límites de apps.
- Número de veces que los usuarios han consultado el uso en los ajustes de “Tiempo de uso”, por tipo de usuario y por tipo de visualización (local, remota, widget).
- Número de veces que han ignorado los usuarios un límite, por tipo de usuario.
- Número de veces que han eliminado los usuarios un límite, por tipo de usuario.

Apple no recopila datos de uso de internet o de apps específicos. Cuando un usuario ve una lista de apps en la información de uso de “Tiempo de uso”, los iconos de las apps se obtienen directamente de App Store, que no conserva ningún dato de estas solicitudes.

Glosario

acceso directo a memoria (DMA): función que permite que los subsistemas de hardware accedan a la memoria principal directamente, saltándose la CPU.

AES (Estándar de encriptación avanzada): un conocido estándar de encriptación global usado para encriptar datos y garantizar su privacidad.

AES-XTS: un modo de AES definido en IEEE 1619-2007 para encriptar los soportes de almacenamiento.

aleatorización del espacio de direcciones (ASLR): técnica que emplean los sistemas operativos para que sea mucho más complicado conseguir aprovecharse de una vulnerabilidad de seguridad en el software. Al garantizar la impredecibilidad de las direcciones y los desplazamientos de la memoria, el código de ataque no puede incrustar esos valores en el código fuente.

algoritmo de firma digital de curva elíptica (ECDSA): algoritmo de firma digital basado en criptografía de curva elíptica.

almacén seguro de datos: mecanismo aplicado por el kernel para proteger frente a accesos no autorizados a los datos independientemente de si la app que solicita el acceso está aislada en una zona protegida.

almacenamiento borrable: área del almacenamiento NAND dedicada, utilizada para almacenar claves criptográficas, que se pueden identificar directamente y borrar de forma segura. Aunque no ofrezca protección si un atacante dispone del dispositivo físicamente, las claves almacenadas en el almacenamiento borrable se pueden usar como parte de una jerarquía de claves para facilitar el borrado rápido y la consiguiente seguridad.

APFS (sistema de archivos de Apple): el sistema de archivos por defecto para iOS, iPadOS, tvOS, watchOS y ordenadores Mac con macOS 10.13 o posterior. APFS incluye encriptación de alta seguridad, uso compartido de espacio, instantáneas, reajuste rápido del tamaño del directorio y mejoras en los fundamentos del sistema de archivos.

Apple Business Manager: portal sencillo basado en web para administradores de TI que permite a las organizaciones implementar de manera rápida y optimizada dispositivos Apple que hayan comprado directamente de Apple o de un operador o distribuidor de Apple autorizado participante en el programa. Pueden inscribir automáticamente dispositivos en su solución de [gestión de dispositivos móviles \(MDM\)](#) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

Apple School Manager: portal sencillo basado en web para administradores de TI que permite a las organizaciones implementar de manera rápida y optimizada dispositivos Apple que hayan comprado directamente de Apple o de un operador o distribuidor de Apple autorizado participante en el programa. Pueden inscribir automáticamente dispositivos en su solución de [gestión de dispositivos móviles \(MDM\)](#) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

autorización del software del sistema: proceso que combina las claves criptográficas integradas en el hardware con un servicio en línea para comprobar que solo se proporciona y se instala el software legítimo de Apple, adecuado para los dispositivos compatibles, a la hora de actualizar.

bits semilla de software: bits dedicados en el motor AES de Secure Enclave que se añaden al UID al generar claves a partir del UID. Cada bit semilla de software tiene un bit de bloqueo correspondiente. El sistema operativo y la ROM de arranque de Secure Enclave pueden cambiar independientemente el valor de cada bit semilla de software siempre que no se haya establecido el bit de bloqueo correspondiente. Una vez establecido el bit de bloqueo, ni este ni el bit semilla de software se podrán modificar. Los bits semilla de software y sus bloqueos se restablecen cuando se reinicia Secure Enclave.

Boot Camp: utilidad de Mac que permite instalar Microsoft Windows en ordenadores Mac compatibles.

cargador de arranque de bajo nivel (LLB): en ordenadores Mac con una arquitectura de arranque de dos fases, el LLB contiene el código al que invoca la ROM de arranque y que, a su vez, carga iBoot como parte de la cadena de arranque seguro.

circuito integrado (IC): también conocido como *microchip*.

CKRecord: un diccionario de pares de clave-valor que contiene los datos guardados en u obtenidos de CloudKit.

clave de contenido: parte de la jerarquía de claves de encriptación que contribuye a proporcionar un método de borrado seguro e instantáneo. En iOS, iPadOS, tvOS y watchOS, la clave de contenido encapsula los metadatos del volumen de datos (y, por consiguiente, sin ellos el acceso a todas las claves por archivo es imposible, lo que hace que los archivos con Protección de datos sean inaccesibles). En macOS, la clave de contenido encapsula el material de las claves, todos los metadatos y los datos situados en el volumen protegido por FileVault. En cualquiera de los casos, el borrado de la clave de contenido hace que los datos encriptados sean inaccesibles.

clave del sistema de archivos: clave que encripta los metadatos de cada archivo, incluida la clave de clase correspondiente. Se guarda en el almacenamiento borrrable para facilitar el borrado rápido, en lugar de la confidencialidad.

clave derivada del código (PDK): clave de encriptación obtenida al intrincar la contraseña del usuario con la clave SKP a largo plazo y el UID de Secure Enclave.

clave por archivo: clave usada por Protección de datos para encriptar un archivo en el sistema de archivos. La clave por archivo se encapsula mediante una clave de clase y se almacena en los metadatos del archivo.

componente de almacenamiento seguro: un chip diseñado con código de ROM inmutable, un generador de números aleatorios de hardware, motores criptográficos y detección de manipulaciones físicas. En dispositivos compatibles, Secure Enclave se asocia con un componente de almacenamiento seguro para el almacenamiento del nonce antirreproducción. Para leer y actualizar los nonces, Secure Enclave y el chip de almacenamiento emplean un protocolo seguro que ayuda a garantizar el acceso exclusivo a los nonces. Existen varias generaciones de esta tecnología con diferentes garantías de seguridad.

controlador de memoria: el subsistema de un sistema en un chip que controla la interfaz que conecta el sistema en un chip con su memoria principal.

controlador SSD: subsistema de hardware que gestiona el soporte de almacenamiento (disco duro de estado sólido).

correspondencia de ángulos del patrón de arrugas: representación matemática de la dirección y la anchura de las arrugas extraída de una porción de una huella digital.

encapsulación de claves: encriptación de una clave con otra clave. iOS y iPadOS utilizan la encapsulación de claves AES del Instituto Nacional de Estándares y Tecnología (NIST), de acuerdo con la publicación [RFC 3394](#).

firmware de la interfaz de firmware extensible unificada (UEFI): tecnología que sustituye a la BIOS para conectar el firmware al sistema operativo de un ordenador.

Gatekeeper: en macOS, una tecnología diseñada para ayudar a garantizar que solo se ejecute software de confianza en el Mac de un usuario.

gestión de dispositivos móviles (MDM): un servicio que permite a un administrador gestionar de forma remota los dispositivos inscritos. Una vez que se inscribe un dispositivo, el administrador puede usar el servicio MDM a través de la red para configurar ajustes y realizar otras tareas en el dispositivo sin la interacción del usuario.

grupo de acción de pruebas conjuntas (JTAG): herramienta estándar de depuración de hardware, que usan programadores y desarrolladores de circuitos.

HMAC: código de autenticación de mensajes basado en una función de hash criptográfico.

iBoot: cargador de arranque de fase 2 para todos los dispositivos Apple. Código que carga XNU como parte de la cadena de arranque seguro. En función de la generación del sistema en un chip (SoC), iBoot puede cargarse mediante el cargador de arranque de bajo nivel o directamente mediante la ROM de arranque.

ID de grupo (GID): como el UID, pero común a todos los procesadores de una clase.

identificador único (UID): clave AES de 256 bits que se graba en cada procesador durante el proceso de fabricación. Ni el firmware ni el software la pueden leer y solamente la usa el motor AES del hardware del procesador. Para obtener la clave real, un atacante tendría que crear un ataque físico muy sofisticado y caro contra el procesador. El UID no está relacionado con ningún otro identificador del dispositivo como, por ejemplo, el UDID.

identificador único del dispositivo (ECID): identificador de 64 bits único en el procesador de cada dispositivo iOS y iPadOS. Cuando se responde a una llamada desde un dispositivo, esta deja de sonar en los demás dispositivos cercanos enlazados a través de iCloud y se avisa de esta situación brevemente mediante Bluetooth de baja energía (BLE) 4.0. Los bytes de aviso se encriptan con el mismo método que los avisos de Handoff. Se usa como parte del proceso de personalización y no se considera un secreto.

identificador uniforme de recursos (URI): cadena de caracteres que identifica un recurso basado en web.

intercambio de claves efímeras de Diffie-Hellman de curva elíptica (ECDHE):

mecanismo de intercambio de claves basado en curvas elípticas. ECDHE permite que dos partes acuerden una clave secreta de forma que se imposibilite que un tercero que esté observando los mensajes entre las dos partes descubra la clave.

interfaz de periféricos serie mejorada (eSPI): bus único diseñado para la comunicación síncrona en serie.

llavero: la infraestructura y un conjunto de API usadas por los sistemas operativos de Apple y por apps de terceros para almacenar y recuperar contraseñas, claves y otras credenciales delicadas.

modo de actualización del firmware del dispositivo (DFU): modo en el que el código de la ROM de arranque de un dispositivo espera su recuperación mediante USB. Al estar en el modo DFU, la pantalla está en negro; sin embargo, tras conectarse a un ordenador en el que se ejecuta iTunes o el Finder, se muestra el siguiente mensaje: "iTunes (o el Finder) ha detectado un (iPhone, iPad o iPod touch) en modo de recuperación. El usuario debe restaurar este (iPhone, iPad o iPod touch) para poder usarlo en iTunes (o el Finder)".

modo de recuperación: un modo de recuperación para restaurar muchos dispositivos Apple si no reconoce el dispositivo del usuario, de modo que el usuario pueda reinstalar el sistema operativo.

módulo de seguridad de hardware (HSM): ordenador especializado en seguridad a prueba de manipulaciones que protege y gestiona claves digitales.

motor criptográfico AES: un componente de hardware dedicado que implementa AES.

NAND: memoria flash no volátil.

nonce: un número único que se usa en varios protocolos de seguridad.

perfil de datos: una lista de propiedades (archivo .plist) firmada por Apple que contiene una serie de entidades y autorizaciones que permiten instalar y probar apps en un dispositivo iOS o iPadOS. Un perfil de datos de desarrollo contiene una lista de dispositivos seleccionados por un desarrollador para realizar una distribución a medida, y un perfil de datos de distribución contiene el ID de app de una app desarrollada por una empresa.

protección de clave sellada (SKP): tecnología de Protección de datos que protege (o *sella*) las claves de encriptación con medidas de software del sistema y claves disponibles solo en el hardware (como el UID de Secure Enclave).

protección de datos: mecanismo de protección de archivos y del llavero para dispositivos Apple compatibles. También puede referirse a las API que utilizan las apps para proteger los archivos y los ítems del llavero.

protección de la integridad del coprocesador del sistema (SCIP): mecanismo que utiliza Apple diseñado para impedir la modificación del firmware del coprocesador.

recompensa de seguridad de Apple: una bonificación que ofrece Apple a los investigadores que comunican una vulnerabilidad que afecta a la versión de sistema operativo más reciente y, si corresponde, al hardware más reciente.

registro de progreso de arranque (BPR): conjunto de indicadores de hardware del sistema en un chip (SoC) que el software puede usar para registrar los modos de arranque que el dispositivo ha utilizado, como el modo de actualización del firmware del dispositivo (DFU) y el modo de recuperación. Cuando se establece un indicador del registro de progreso de arranque, ya no se puede borrar. De este modo, un software posterior podrá obtener un indicador de confianza del estado del sistema.

repositorios de claves: estructura de datos que se utiliza para almacenar un conjunto de claves de clase. Cada tipo (usuario, dispositivo, sistema, copia de seguridad, custodia o copia de seguridad de iCloud) tiene el mismo formato.

Una cabecera que contiene: la versión (cuatro en iOS 12 o posterior); el tipo (sistema, copia de seguridad, custodia o copia de seguridad de iCloud); el UUID del repositorio de claves; un código HMAC si el repositorio de claves está firmado; el método usado para la encapsulación de las claves de clase: vinculado al UID o PBKDF2, junto con la sal y el recuento de iteraciones.

Una lista de claves de clase: el UUID de las claves; la clase (qué clase de Protección de datos de archivo o de llavero); el tipo de encapsulación (solo clave derivada del UID; la clave derivada del UID y la clave derivada del código); y la clave pública para clases asimétricas.

ROM de arranque: el primer código que ejecuta el procesador de un dispositivo al encenderse por primera vez. Como parte integral del procesador, ni Apple ni un intruso lo pueden modificar.

sepOS: el firmware de Secure Enclave, basado en una versión personalizada por Apple del microkernel L4.

servicio de identidad (IDS) de Apple: directorio de Apple de claves públicas de iMessage, direcciones del APNs, números de teléfono y direcciones de correo electrónico que se usan para buscar las claves y las direcciones de los dispositivos.

servicio de notificaciones push de Apple (APNs): servicio ofrecido por Apple a nivel mundial que envía notificaciones push a los dispositivos Apple.

sistema en un chip (SoC): circuito integrado (IC) que incorpora varios componentes en un único chip. El procesador de aplicaciones, Secure Enclave y otros coprocesadores son componentes del SoC.

unidad de gestión de memoria de entrada/salida (IOMMU): unidad de gestión de memoria de entrada/salida. Subsistema en un chip integrado que controla el acceso al espacio de direcciones desde otros periféricos y dispositivos de entrada/salida.

vinculación: proceso mediante el cual el código de un usuario se convierte en una clave criptográfica y se fortalece con el UID del dispositivo. Este proceso ayuda a garantizar que un ataque de fuerza bruta se deba realizar en un dispositivo determinado y, por lo tanto, la velocidad esté limitada y el ataque no se pueda realizar en paralelo. El algoritmo de vinculación es PBKDF2, que usa AES cifrado con el UID del dispositivo como la función pseudoaleatoria (PRF) para cada iteración.

xART: abreviatura de tecnología antirreproducción ampliada. Conjunto de servicios que proporcionan almacenamiento persistente encriptado y autenticado para Secure Enclave con funciones antirreproducción basadas en la arquitectura de almacenamiento físico. Consulta Componente de almacenamiento seguro.

XNU: kernel ubicado en el corazón de los sistemas operativos de Apple. Se presupone que es de confianza, y refuerza las medidas de seguridad tales como la firma de código, el aislamiento, la comprobación de las autorizaciones y la aleatorización del espacio de direcciones (ASLR).

XProtect: en macOS, una tecnología antivirus integrada para la detección y eliminación mediante firmas de software malicioso.

Historial de actualizaciones del documento

Historial de actualizaciones del documento

Fecha	Resumen
Diciembre de 2022	<p data-bbox="777 722 932 743">Temas añadidos:</p> <ul data-bbox="777 753 1192 779" style="list-style-type: none"><li data-bbox="777 753 1192 779">• Protección de datos avanzada para iCloud <p data-bbox="777 789 967 810">Temas actualizados:</p> <ul data-bbox="777 821 1295 982" style="list-style-type: none"><li data-bbox="777 821 1230 846">• Descripción general de la seguridad de iCloud<li data-bbox="777 856 1013 882">• Encriptación de iCloud<li data-bbox="777 892 1224 917">• Seguridad de la copia de seguridad de iCloud<li data-bbox="777 928 1295 953">• Seguridad del contacto de recuperación de la cuenta<li data-bbox="777 963 1130 989">• Seguridad del representante digital

Fecha	Resumen
Mayo de 2022	<p>Actualizado para:</p> <ul style="list-style-type: none"> • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 <p>Temas añadidos:</p> <ul style="list-style-type: none"> • Restricciones del sistema operativo de recuperación enlazado • Versión del sistema operativo local (love) • Función de compartir los datos de salud • Seguridad del contacto de recuperación de la cuenta • Seguridad del representante digital • Seguridad de "Tap to Pay on iPhone" • Acceder mediante la app Cartera • Tipos de credenciales de acceso • Documentos de identidad en Cartera • Accesorios de HomeKit compatibles con Siri <p>Temas actualizados:</p> <ul style="list-style-type: none"> • Magic Keyboard con Touch ID • Face ID, Touch ID, códigos y contraseñas • Seguridad del reconocimiento facial • Tarjetas exprés con reserva de energía • Modos de arranque para un Mac con chip de Apple • Contenido de un archivo LocalPolicy para un Mac con chip de Apple • Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS • Seguridad del sistema de watchOS • Dispositivo de investigación de seguridad de Apple • La función del sistema de archivos de Apple • Protección del acceso de las apps a los datos de usuario • Introducción a la seguridad de las apps para macOS • Protección frente al software malicioso en macOS • Descripción general de la seguridad de iCloud • Sincronización segura del llavero • Recuperación segura del llavero de iCloud • Pago con tarjetas mediante Apple Pay • Tarjetas sin contacto en Apple Pay • Inhabilitar las tarjetas con Apple Pay • Solicitar la tarjeta Apple Card • Seguridad de Apple Cash • Añadir tarjetas de transporte y de dinero electrónico a la app Cartera • Seguridad de Apple Messages for Business • Seguridad de FaceTime • Seguridad de la función de llave del coche en iOS • Seguridad de Apple Configurator <p>Temas eliminados:</p> <ul style="list-style-type: none"> • Accesorios de HomeKit y iCloud

Fecha	Resumen
Mayo de 2021	<p data-bbox="777 212 938 233">Actualizado para:</p> <ul data-bbox="777 247 915 407" style="list-style-type: none"><li data-bbox="777 247 878 268">• iOS 14.5<li data-bbox="777 283 915 304">• iPadOS 14.5<li data-bbox="777 319 911 340">• macOS 11.3<li data-bbox="777 354 894 375">• tvOS 14.5<li data-bbox="777 390 915 411">• watchOS 7.4 <p data-bbox="777 422 932 443">Temas añadidos:</p> <ul data-bbox="777 457 1256 579" style="list-style-type: none"><li data-bbox="777 457 1078 478">• Magic Keyboard con Touch ID.<li data-bbox="777 493 1256 514">• Intención segura y conexiones a Secure Enclave.<li data-bbox="777 529 1187 550">• Desbloqueo automático y el Apple Watch.<li data-bbox="777 564 1256 585">• Hash del manifiesto Image4 de CustomOS (coih). <p data-bbox="777 596 932 617">Temas editados:</p> <ul data-bbox="777 632 1459 802" style="list-style-type: none"><li data-bbox="777 632 1459 674">• Se han añadido dos nuevas transacciones del modo exprés en Tarjetas exprés con ahorro de batería.<li data-bbox="777 688 1370 709">• Se ha editado Resumen de características de Secure Enclave.<li data-bbox="777 724 1338 766">• Se ha añadido contenido de actualizaciones de software a Multiarranque seguro (smb3).<li data-bbox="777 781 1354 802">• Contenido adicional para Protección de clave sellada (SKP).

Fecha	Resumen
Febrero de 2021	<p data-bbox="777 212 938 233">Actualizado para:</p> <ul data-bbox="777 247 915 407" style="list-style-type: none"><li data-bbox="777 247 878 268">• iOS 14.3<li data-bbox="777 283 915 304">• iPadOS 14.3<li data-bbox="777 319 906 340">• macOS 11.1<li data-bbox="777 354 894 375">• tvOS 14.3<li data-bbox="777 390 915 411">• watchOS 7.2 <p data-bbox="777 422 932 443">Temas añadidos:</p> <ul data-bbox="777 457 1450 846" style="list-style-type: none"><li data-bbox="777 457 1235 478">• Implementación segura de iBoot en la memoria<li data-bbox="777 493 1289 514">• Proceso de arranque para un Mac con chip de Apple<li data-bbox="777 529 1276 550">• Modos de arranque para un Mac con chip de Apple<li data-bbox="777 564 1450 611">• Control de la política de seguridad de Disco de Arranque para un Mac con chip de Apple<li data-bbox="777 625 1300 646">• Creación y gestión de claves de firmas de LocalPolicy<li data-bbox="777 661 1430 682">• Contenido de un archivo LocalPolicy para un Mac con chip de Apple<li data-bbox="777 697 1435 718">• Seguridad del volumen del sistema firmado en iOS, iPadOS y macOS<li data-bbox="777 732 1276 753">• Dispositivo de investigación de seguridad de Apple<li data-bbox="777 768 1057 789">• Supervisión de contraseñas<li data-bbox="777 804 971 825">• Seguridad de IPv6<li data-bbox="777 840 1260 861">• Seguridad de la función de llave del coche en iOS <p data-bbox="777 871 964 892">Temas actualizados:</p> <ul data-bbox="777 907 1430 1423" style="list-style-type: none"><li data-bbox="777 907 943 928">• Secure Enclave<li data-bbox="777 942 1175 963">• Desconexión del micrófono de hardware<li data-bbox="777 978 1430 1024">• Sistema operativo de recuperación y entornos de diagnóstico de un Mac basado en Intel<li data-bbox="777 1039 1422 1060">• Protecciones de acceso directo a memoria en los ordenadores Mac<li data-bbox="777 1075 1110 1096">• Extensiones del kernel en macOS<li data-bbox="777 1110 1162 1131">• Protección de la integridad del sistema<li data-bbox="777 1146 1122 1167">• Seguridad del sistema de watchOS<li data-bbox="777 1182 1086 1203">• Gestión de FileVault en macOS<li data-bbox="777 1218 1252 1239">• Acceso de las apps a las contraseñas guardadas<li data-bbox="777 1253 1243 1274">• Recomendaciones de seguridad de contraseñas<li data-bbox="777 1289 1036 1310">• Seguridad de Apple Cash<li data-bbox="777 1325 1203 1346">• Seguridad de Apple Messages for Business<li data-bbox="777 1360 1024 1381">• Privacidad de la red wifi<li data-bbox="777 1396 1138 1417">• Seguridad del bloqueo de activación<li data-bbox="777 1432 1105 1453">• Seguridad de Apple Configurator

Fecha	Resumen
Abril de 2020	<p>Actualizado para:</p> <ul style="list-style-type: none"> • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 <p>Actualizaciones:</p> <ul style="list-style-type: none"> • Se ha añadido información sobre la desconexión del micrófono en el iPad a la sección Desconexión del micrófono de hardware. • Se han añadido los almacenes seguros de datos a Protección del acceso de las apps a los datos de usuario. • Se han actualizado los apartados Gestión de FileVault en macOS y Herramientas de línea de comandos. • Se ha añadido información sobre la herramienta de eliminación de software malicioso a la sección Protección frente al software malicioso en macOS. • Se ha actualizado el apartado Seguridad del iPad compartido en iPadOS.
Diciembre de 2019	<p>Fusión de Seguridad de iOS, Descripción general de la seguridad de macOS y Descripción general del chip de seguridad T2 de Apple</p> <p>Actualizado para:</p> <ul style="list-style-type: none"> • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 <p>Se ha eliminado la información sobre controles de privacidad, Siri y sugerencias de Siri y el sistema de antirrastreo inteligente de Safari. Para obtener la información más reciente sobre estas funciones, consulta https://www.apple.com/es/privacy/.</p>
Mayo de 2019	<p>Actualizado para iOS 12.3</p> <ul style="list-style-type: none"> • Compatibilidad con TLS 1.3 • Descripción revisada de la seguridad de AirDrop • Modo DFU y modo de recuperación • Requisitos de código para la conexión de accesorios
Noviembre de 2018	<p>Actualizado para iOS 12.1</p> <ul style="list-style-type: none"> • FaceTime en grupo
Septiembre de 2018	<p>Actualizado para iOS 12 Secure Enclave</p> <ul style="list-style-type: none"> • Protección de la integridad del sistema operativo • Tarjeta exprés con reserva de energía • Modo DFU y modo de recuperación • Accesorios de HomeKit TV Remote • Tarjetas sin contacto • Carnés de estudiante • Sugerencias de Siri • Atajos en Siri • App Atajos • Gestión de contraseñas de usuario • Tiempo de uso • Certificaciones de seguridad y programas

Fecha	Resumen
Julio de 2018	Actualizado para iOS 11.4 <ul style="list-style-type: none"> • Políticas biométricas • HomeKit • Apple Pay • Chat para clientes • Mensajes en iCloud • Apple Business Manager
Diciembre de 2017	Actualizado para iOS 11.2 <ul style="list-style-type: none"> • Apple Pay Cash
Octubre de 2017	Actualizado para iOS 11.1 <ul style="list-style-type: none"> • Certificaciones de seguridad y programas • Touch ID/Face ID • Notas compartidas • Encriptación de punto a punto de CloudKit • Actualización de TLS • Apple Pay, Pagos con Apple Pay en internet • Sugerencias de Siri • iPad compartido
Julio de 2017	Actualizado para iOS 10.3 <ul style="list-style-type: none"> • Secure Enclave • Protección de datos de archivo • Repositorios de claves • Certificaciones de seguridad y programas • SiriKit • HealthKit • Seguridad de la red • Bluetooth • iPad compartido • Modo Perdido • Bloqueo de activación • Controles de privacidad
Marzo de 2017	Actualizado para iOS 10 Seguridad del sistema <ul style="list-style-type: none"> • Clases de Protección de datos • Certificaciones de seguridad y programas • HomeKit, ReplayKit y SiriKit • Apple Watch • Wifi, VPN • Inicio de sesión único • Apple Pay, Pagos con Apple Pay en internet • Envío de datos de tarjetas de crédito, débito y prepago • Sugerencias de Safari

Fecha	Resumen
Mayo de 2016	Actualizado para iOS 9.3 <ul style="list-style-type: none">• ID de Apple Gestionados• Autenticación de doble factor para el ID de Apple• Repositorios de claves• Certificaciones de seguridad• Modo Perdido, Bloqueo de activación• Notas seguras• Apple School Manager• iPad compartido
Septiembre de 2015	Actualizado para iOS 9 Bloqueo de activación del Apple Watch <ul style="list-style-type: none">• Políticas de código• Compatibilidad con la API de Touch ID• Protección de datos en A8 mediante AES-XTS• Repositorios de claves para la actualización de software sin supervisión• Actualización de certificados• Modelo de confianza de apps empresariales• Protección de datos para los marcadores de Safari• Seguridad de transporte de las apps• Especificaciones de VPN• Acceso remoto a iCloud para HomeKit• Tarjetas de bonificación de Apple Pay y app de la entidad emisora de tarjetas de Apple Pay• Indexación de Spotlight en el dispositivo• Modelo de enlace de iOS• Apple Configurator 2• Restricciones

© 2022 Apple Inc. Todos los derechos reservados.

El uso del logotipo de Apple producido mediante el teclado (Opción + G) con fines comerciales sin el consentimiento previo por escrito de Apple puede ser una infracción de la marca comercial y constituir competencia desleal según las leyes federales y estatales.

Apple, el logotipo de Apple, AirDrop, AirPlay, Apple Books, Apple Card, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch, AppleScript, ARKit, Bonjour, Boot Camp, CarPlay, Face ID, FaceTime, FileVault, Finder, FireWire, Handoff, HealthKit, HomeKit, HomePod, HomePod mini, iMac, iMac Pro, iMessage, iPad, iPadOS, iPad Air, iPad Pro, iPhone, iPod touch, iTunes, Keychain, Lightning, Mac, Mac Catalyst, Mac mini, Mac Pro, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Objective-C, OS X, QuickType, Retina, Rosetta, Safari, Siri, Siri Remote, SiriKit, Swift, Spotlight, Touch ID, TrueDepth, tvOS, watchOS y Xcode son marcas comerciales de Apple Inc., registradas en EE. UU. y en otros países y regiones.

App Clips, Find My y Touch Bar son marcas comerciales de Apple Inc.

App Store, AppleCare, CloudKit, iCloud, iCloud Drive, iCloud Keychain y iTunes Store son marcas de servicio de Apple Inc., registradas en EE. UU. y en otros países y regiones.

Apple Messages for Business es una marca de servicio de Apple Inc.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

IOS es una marca comercial o una marca registrada de Cisco en EE. UU. y en otros países y se utiliza bajo licencia.

La marca denominativa y los logotipos de Bluetooth® son marcas comerciales registradas de Bluetooth SIG, Inc., y Apple dispone de licencia para usar dichas marcas.

Java es una marca comercial registrada de Oracle y sus filiales.

UNIX® es una marca comercial registrada de The Open Group.

Otros nombres de productos y empresas mencionados en el presente documento pueden ser marcas comerciales de las respectivas empresas.

En la realización de este manual se ha puesto el máximo cuidado para asegurar la exactitud de la información que en él aparece. Apple no se responsabiliza de los posibles errores de impresión o copia.

Algunas apps no están disponibles en todas las áreas. La disponibilidad de la app está sujeta a cambios.

E028-00625