# Centro de conformidad y certificaciones de seguridad

Diciembre 2021

# Contenido

# Introducción a la garantía de seguridad de Apple

En el marco de nuestro compromiso con la seguridad, Apple colabora periódicamente con organizaciones de terceros para certificar y verificar la seguridad del hardware, el software y los servicios de Apple. Estas organizaciones reconocidas a nivel internacional otorgan a Apple certificaciones para cada nueva versión principal de los sistemas operativos. De este modo, proporcionan una medida de confianza o, dicho de otro modo, una garantía de seguridad de que las necesidades de seguridad de un sistema se están cumpliendo. Para las áreas técnicas que no se recogen en acuerdos de reconocimiento mutuo (MRA) o que carecen de estándares de seguridad suficientemente desarrollados, Apple trabaja para desarrollar estándares de seguridad apropiados. Nuestra misión es impulsar una cobertura de las certificaciones de seguridad integral y aceptada a nivel internacional para todo el hardware, los sistemas operativos, las apps y los servicios de Apple.

A menudo se necesitan certificaciones para cumplir requisitos legales y normas del sector. Los servicios como Apple School Manager y Apple Business Manager se encuentran cubiertos por las certificaciones ISO/IEC 27001 e ISO/IEC 27018 de Apple. Todos los clientes, incluidos los organismos gubernamentales y las organizaciones empresariales y educativas con dispositivos Apple implementados, pueden usar las certificaciones de hardware, sistemas operativos, software y servicios para demostrar el cumplimiento.

# Certificaciones de hardware

Dado que un software seguro requiere una base de seguridad integrada en el hardware, todos los dispositivos Apple (ya sea con iOS, iPadOS, macOS, tvOS o watchOS) cuentan con funciones de seguridad diseñadas en el procesador. Entre estas se incluyen capacidades de la CPU que respaldan las funciones de seguridad del sistema y un chip dedicado a las funciones de seguridad. El componente más importante es el coprocesador Secure Enclave, incluido en todos los dispositivos iOS, iPadOS, watchOS y tvOS modernos, así como en todos los ordenadores Mac con chip de Apple y en los ordenadores Mac basados en Intel con el chip de seguridad T2 de Apple. Secure Enclave proporciona la base para encriptar datos en reposo, para el arranque seguro en macOS y para el uso de datos biométricos.

El compromiso de Apple con la garantía de seguridad comienza con la certificación de los componentes de seguridad básicos en el chip desde la raíz de confianza del hardware hasta la aplicación del arranque seguro y la capacidad de Secure Enclave de proporcionar un almacén seguro de claves para la autenticación segura con Touch ID y Face ID. Las funciones de seguridad de los dispositivos Apple son posibles gracias a la combinación del diseño del chip, el hardware, el software y los servicios exclusivos de Apple. La certificación de estos componentes es una parte importante de la verificación de la garantía que Apple proporciona.

Para obtener información sobre las certificaciones públicas relacionadas con el hardware y los componentes de firmware asociados, consulta:

- Certificaciones de seguridad para el chip de seguridad T2 de Apple
- Certificaciones de seguridad para el procesador Secure Enclave

# Certificaciones de software y apps

Apple mantiene certificaciones y acreditaciones independientes de su sistema operativo y sus apps de conformidad con las normas del estándar federal de procesamiento de información de Estados Unidos (FIPS) 140-2/-3 para módulos criptográficos y Common Criteria para sistemas operativos, apps y servicios de los dispositivos. Entre los sistemas operativos cubiertos se incluyen iOS, iPadOS, macOS, sepOS, el firmware del chip T2, tvOS, y watchOS. En el caso de las apps, la certificación independiente incluye inicialmente el navegador Safari y la app Contactos, y en el futuro se irán certificando más.

Para obtener información sobre las certificaciones públicas relacionadas con los *sistemas operativos* de Apple, consulta:

- Certificaciones de seguridad para iOS
- Certificaciones de seguridad para iPadOS
- Certificaciones de seguridad para macOS
- Certificaciones de seguridad para tvOS
- Certificaciones de seguridad para watchOS

Para obtener información sobre las certificaciones públicas relacionadas con las *apps* de Apple, consulta:

- Certificaciones de seguridad para apps de Apple

# Certificaciones de servicios

Apple mantiene certificaciones de seguridad para respaldar a nuestros clientes del ámbito empresarial y educativo. Estas certificaciones permiten a los clientes de Apple cumplir sus obligaciones legales y contractuales al usar los servicios de Apple con hardware y software de Apple. Estas certificaciones proporcionan a los clientes una acreditación independiente de las prácticas medioambientales, de privacidad y de seguridad de la información de Apple para los sistemas de Apple.

Para obtener información sobre las certificaciones públicas relacionadas con los *servicios de internet* de Apple, consulta:

- Certificaciones de seguridad para servicios de internet de Apple

Para cualquier duda acerca de las certificaciones de seguridad y privacidad de Apple, contacta con security-certifications@apple.com.

# Certificaciones de seguridad del hardware

## Descripción general de las certificaciones de seguridad del hardware de Apple

Apple mantiene certificados de validación de conformidad con el estándar federal de procesamiento de información (FIPS) 140-2/-3 de EE. UU. para sepOS y el firmware del chip T2, así como otras certificaciones. Apple parte de *elementos esenciales de certificación* que se aplican con carácter general a las diversas plataformas cuando procede. Uno de esos elementos esenciales es la validación de la biblioteca Corecrypto, que se usa para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo elemento esencial es la certificación de Secure Enclave, que está integrado en muchos de los dispositivos Apple. En tercer lugar está la certificación de Secure Element (SE), que se encuentra en los dispositivos Apple con Touch ID y con Face ID. Todos estos elementos básicos de la certificación de los productos de hardware constituyen la base para certificaciones de seguridad de plataformas más amplias.

### Validaciones de los algoritmos criptográficos

La validación de la correcta implementación de diversos algoritmos criptográficos y las funciones de seguridad relacionadas es un requisito previo para la validación FIPS 140-3 sobre el que se sustentan otras certificaciones. La validación está gestionada por el Programa de validación de algoritmos criptográficos (CAVP) del Instituto Nacional de Estándares y Tecnología (NIST). Los certificados de validación de las implementaciones de Apple pueden encontrarse mediante la herramienta de búsqueda del CAVP. Para obtener más información, consulta el sitio web del Programa de validación de algoritmos criptográficos (CAVP).

## Validaciones de los módulos criptográficos: FIPS 140-2/3 (ISO/IEC 19790)

Los módulos criptográficos de Apple se han validado varias veces a través del Programa de validación de módulos criptográficos (CMVP) para garantizar su conformidad con el estándar federal de procesamiento de información de Estados Unidos (FIPS) 140-2 después de cada versión principal de los sistemas operativos desde 2012. Tras cada versión principal, Apple envía todos los módulos al CMVP para validar su conformidad con el estándar. Además de usarse en los sistemas operativos y apps de Apple, estos módulos proporcionan funciones criptográficas para servicios proporcionados por Apple y están disponibles para que apps de terceros los usen.

Apple logra el **Nivel de seguridad 1** cada año para los módulos basados en software "Módulo Corecrypto para Intel" y "Módulo de kernel Corecrypto para Intel" para macOS. Para el chip de Apple, los módulos "Módulo Corecrypto para ARM" y "Módulo de kernel Corecrypto para ARM" son aplicables a iOS, iPadOS, tvOS, watchOS y el firmware del chip de seguridad T2 de Apple integrado en ordenadores Mac.

En 2019, Apple obtuvo el primer **Nivel de seguridad 2** de FIPS 140-2 para el módulo criptográfico de hardware integrado identificado como "Módulo Corecrypto de Apple: Almacén seguro de claves", lo que permite el uso autorizado por el gobierno de EE. UU. de las claves generadas y gestionadas en Secure Enclave. Apple sigue trabajando para obtener validaciones para el módulo criptográfico de hardware con cada nueva versión principal de los sistemas operativos.

El Departamento de Comercio de Estados Unidos aprobó la validación **FIPS 140-3** en 2019. El cambio más significativo en esta versión del estándar es la especificación de los estándares ISO/IEC, en particular ISO/IEC 19790:2015 y el correspondiente estándar de realización de pruebas ISO/IEC 24759:2017. El CMVP ha iniciado un programa de transición y ha indicado que, a partir de 2020, los módulos criptográficos comenzarán a validarse basándose en FIPS 140-3. Los módulos criptográficos de Apple procurarán cumplir con el estándar FIPS 140-3 y hacer la transición hacia él tan pronto como sea viable.

En el caso de los módulos criptográficos que actualmente se encuentran en fase de prueba y validación, el CMVP mantiene dos listas separadas que pueden contener información sobre las validaciones propuestas. En el caso de los módulos criptográficos que están en fase de prueba en un laboratorio acreditado, el módulo puede figurar en la lista de implementaciones en pruebas. Una vez que el laboratorio completa las pruebas y recomienda la validación del CMVP, los módulos criptográficos de Apple aparecen en la lista de módulos en curso. En este momento, las pruebas de laboratorio se han completado y están a la espera de la validación por parte del CMVP. Dado que la duración del proceso de evaluación puede variar, conviene consultar primero las dos listas anteriores para determinar el estado actual de los módulos criptográficos de Apple entre la fecha de lanzamiento de una versión principal del sistema operativo y la emisión del certificado de validación del CMVP.

## Certificaciones de productos: Common Criteria (ISO/IEC 15408)

Muchas organizaciones utilizan el estándar de criterios comunes o Common Criteria (ISO/IEC 15408) como base para llevar a cabo evaluaciones de seguridad de los productos de tecnologías de la información.

Para las certificaciones que pueden ser reconocidas mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA) internacional, consulta el portal de Common Criteria. El estándar de Common Criteria también puede usarse fuera del CCRA por parte de sistemas de validación nacionales y privados. En Europa, el reconocimiento mutuo se rige por el acuerdo SOG-IS, así como por el CCRA.

El objetivo, como se indica en la comunidad de Common Criteria, está enfocado a un conjunto de estándares de seguridad aprobado internacionalmente para proporcionar una evaluación clara y fiable de las capacidades de seguridad de los productos que pertenecen a las tecnologías de la información. Al proporcionar una valoración independiente sobre la capacidad de un producto para cumplir los estándares de seguridad, la certificación Common Criteria aporta a los clientes más confianza en la seguridad de los productos tecnológicos y les permite tomar decisiones mejor fundamentadas.

A través del CCRA, los países miembros han acordado reconocer la certificación de productos que pertenecen a las tecnologías de la información con el mismo nivel de confianza. Se requieren numerosas evaluaciones antes de la certificación, entre las que se incluyen las siguientes:

- Perfiles de protección
- Objetivos de seguridad
- Requisitos funcionales de seguridad
- Requisitos de garantía de seguridad
- Niveles de garantía de evaluación

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (por ejemplo, Movilidad) y que permiten comparar las evaluaciones de seguridad de los distintos productos de tecnologías de la información de la misma clase. Al igual que crece la lista de los perfiles de protección aprobados, los miembros del acuerdo CCRA continúan aumentando año a año. Este acuerdo permite que los desarrolladores de productos trabajen para lograr una sola certificación en virtud de cualquiera de los esquemas de autorización de certificados que esté reconocida por todos los firmantes consumidores de certificados.

Los objetivos de seguridad (ST) definen *qué* se evaluará al certificar un producto de TI. Los objetivos de seguridad se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, que se usan para evaluar los objetivos de seguridad en detalle.

El estándar Common Criteria (CC) también incluye *requisitos de garantía de seguridad*. Una medida que se identifica habitualmente es el *nivel de garantía de evaluación (EAL)*. Los niveles de garantía de evaluación agrupan conjuntos de requisitos de garantía de seguridad utilizados habitualmente y pueden especificarse en perfiles de protección y objetivos de seguridad para permitir la comparación.

Muchos de los perfiles de protección más antiguos se han archivado y se han comenzado a sustituir por perfiles de protección específicos desarrollados y centrados en torno a soluciones y entornos concretos. En un esfuerzo conjunto por garantizar el reconocimiento mutuo continuado de todos los miembros del CCRA, se han establecido comunidades técnicas internacionales a fin de desarrollar y mantener perfiles de protección colaborativos que se desarrollan desde el inicio con la aplicación de varios esquemas de firmantes del CCRA. Diversas partes interesadas siguen desarrollando perfiles de protección destinados a grupos de usuarios y acuerdos de reconocimiento mutuo distintos al CCRA.

A principios de 2015, Apple comenzó a trabajar para obtener las certificaciones en virtud del CCRA actualizado con determinados perfiles de protección colaborativos. Desde entonces, Apple ha conseguido las certificaciones de Common Criteria para cada versión principal de iOS y ha ampliado la cobertura para incluir la garantía de seguridad que proporcionan los nuevos perfiles de protección.

Apple adopta un papel activo dentro de las comunidades técnicas centradas en la evaluación de las tecnologías de seguridad móvil. Esto incluye a las comunidades técnicas internacionales responsables de desarrollar y actualizar perfiles de protección colaborativos. Apple sigue evaluando y trabajando para lograr certificaciones con los perfiles de protección y los perfiles de protección colaborativos actuales.

Las certificaciones de la plataforma Apple para el mercado de Norteamérica generalmente se realizan con la National Information Assurance Partnership (NIAP), que tiene una lista de proyectos actualmente en evaluación pero que aún no están certificados.

Además de los certificados de plataforma generales mencionados, se han emitido otros certificados para demostrar requisitos de seguridad específicos para algunos mercados.

# Certificaciones de seguridad para el procesador Secure Enclave

## Contexto de la certificación del procesador Secure Enclave

El módulo criptográfico de hardware (*Módulo criptográfico del almacén seguro de claves del SEP de Apple*) viene integrado en el SoC de Apple incluido en los siguientes productos: La serie A de Apple de iPhone y iPad, la serie M de ordenadores Mac con chip de Apple, la serie S de Apple Watch y el chip de seguridad de la serie T de los ordenadores Mac basados en Intel a partir del iMac Pro introducido en 2017.

En 2018, Apple sincronizó la validación de los módulos criptográficos de software con los sistemas operativos publicados en 2017: iOS 11, macOS 10.13, tvOS 11 y watchOS 4. El módulo criptográfico de hardware del SEP identificado como Módulo criptográfico del almacén seguro de claves del SEP de Apple v1.0 se validó originalmente con los requisitos del Nivel de seguridad 1 de FIPS 140-2.

En 2019, Apple validó el módulo de hardware con los requisitos del Nivel de seguridad 2 del FIPS 140-2 y actualizó el identificador de la versión del módulo a v9.0 para sincronizarlo con las versiones de las validaciones de los módulos de kernel y usuario Corecrypto correspondientes. Esto incluyó iOS 12, macOS 10.14, tvOS 12 y watchOS 5.

En 2020 y 2021, Apple está trabajando para obtener validaciones para determinar su conformidad con el estándar FIPS 140-3 y con la garantía adicional para el nivel de seguridad 3 de los requisitos de seguridad física para los chips de Apple: chips A13, A14, S6 y M1.

Apple también participa activamente en la validación de módulos integrados de kernel y usuario Corecrypto para cada versión principal de un sistema operativo. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

## Estado de la validación de módulos criptográficos

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

# Certificaciones FIPS 140-3

### Estado actual

En la tabla siguiente se muestran los módulos criptográficos de 2020 y 2021 que se están probando en el laboratorio actualmente para determinar su conformidad con el estándar FIPS 140-3.

Se han completado las pruebas en laboratorio del almacén de claves seguras (SKS) asociado con los sistemas operativos lanzados en 2020 y 2021, y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso y, una vez validados, se trasladarán a la lista de módulos criptográficos validados.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de iOS 15 (2021). Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con las versiones de 2021 de iOS, iPadOS, macOS, tvOS y watchOS<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, T2, M1, S3-S6)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con las versiones de 2021 de iOS, iPadOS, macOS, tvOS y watchOS<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A13, A14, S6, M1)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con las versiones de 2020 de iOS, iPadOS, macOS, tvOS y watchOS<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, T2, M1, S3-S6)<br>*Nivel de seguridad general:* 2 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con las versiones de 2020 de iOS, iPadOS, macOS, tvOS y watchOS<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A13, A14, S6, M1)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v10.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.15 Catalina<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.14 Mojave<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.13 High Sierra<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

## Certificaciones Common Criteria (CC)

Apple trabaja activamente en las evaluaciones de Common Criteria en las que los perfiles de protección pertinentes cubren las funciones de seguridad de la tecnología de Apple.

## Estado de la certificación Common Criteria (CC)

El esquema de EE. UU., operado por la National Information Assurance Partnership (NIAP), mantiene una lista de productos en evaluación que incluye productos que se encuentran actualmente en fase de evaluación en EE. UU. en un laboratorio de pruebas de Common Criteria (CCTL) autorizado por la NIAP y que han completado una reunión de evaluación inicial (o equivalente) en la que la dirección del CCEVS ha aceptado oficialmente el producto para su evaluación.

Tras la certificación de los productos, la NIAP incluye las certificaciones válidas actualmente en su lista de productos conformes. A los dos años, estas certificaciones se revisan para determinar su conformidad con la política de mantenimiento de garantía vigente. Una vez expirada la fecha de mantenimiento de la garantía, la NIAP transfiere la certificación a su lista de productos archivados.

En el portal de Common Criteria se enumeran certificaciones que pueden reconocerse mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años y conserva registros de las certificaciones archivadas.

La tabla siguiente muestra las certificaciones que están siendo evaluadas por un laboratorio o cuyo cumplimiento con el estándar Common Criteria se ha certificado.

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* sepOS<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* Procesador Secure Enclave de Apple [2020]<br>*Perfiles de protección:* CPP_DSC_V1.0<br>*Hardware:* Secure Enclave para (A9-A14, M1, T2, S3-S6)<br>*Software:* sepOS distribuido con iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14 y watchOS 7 |

## Certificaciones adicionales

En la tabla siguiente se muestran certificaciones para Secure Enclave que no usan Common Criteria ni FIPS 140-3.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* 07/12/2019 a 26/12/2022 | *Certificados:* CFNR201902910002 (R. P. China: Certificación tecnológica de servicios financieros móviles)<br>Versión en chino<br>Versión en inglés | *Título:* Entorno de ejecución de confianza de terminales móviles<br>*Sistema operativo:* iOS 13.5.1<br>*Especificación:* JR/T 0156-2017 |

# Certificaciones de seguridad para el chip de seguridad T2 de Apple

## Contexto de la validación de módulos criptográficos

Apple participa activamente en la validación de módulos integrados de hardware y software de Apple para cada versión principal de un sistema operativo. La validación de la conformidad solo puede llevarse a cabo en una versión final del módulo.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación con el estándar federal de procesamiento de información (FIPS) 140-3.

Además de la CPU de Intel, la mayoría de los ordenadores Mac a partir de 2017 también tienen un chip de seguridad T2 de Apple independiente que es un sistema en un chip (SoC) basado en chip de Apple. Estos ordenadores Mac con un chip T2 utilizan los cinco módulos criptográficos para varios servicios en el dispositivo.

- Módulo de usuario Corecrypto para Intel (usado por macOS en ordenadores Mac basados en Intel)
- Módulo de kernel Corecrypto para Intel (usado por macOS en ordenadores Mac basados en Intel)
- Módulo de usuario Corecrypto para ARM (usado por el chip T2)
- Módulo de kernel Corecrypto para ARM (usado por el chip T2)
- Módulo criptográfico del almacén seguro de claves (usado por el coprocesador Secure Enclave integrado en el chip T2)

*Nota:* Los módulos basados en chip de Apple que se ejecutan en el chip T2 son los mismos que se ejecutan en otros chips de Apple, como las series A, S y M de Apple.

## Estado de la validación de módulos criptográficos

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.

- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

## Certificaciones FIPS 140-3

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de los módulos de 2020 y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de los módulos de 2021. Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* sepOS para macOS 12 Monterey<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* sepOS para macOS 12 Monterey<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* sepOS para macOS 12 Monterey<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (T2)<br>*Nivel de seguridad:* 2 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS para macOS 11 Big Sur<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS para macOS 11 Big Sur<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS para macOS 11 Big Sur con Intel<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3856<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.15 Catalina<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3855<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.15 Catalina<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves Corecrypto v10.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.15 Catalina<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 23/04/2019 | *Certificados:* 3438<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.14 Mojave<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 11/04/2019 | *Certificados:* 3433<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.14 Mojave<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.14 Mojave<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018 | *Certificados:* 3148<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.13 High Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018 | *Certificados:* 3147<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* sepOS para macOS 10.13 High Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/07/2018 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS para macOS 10.13 High Sierra<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2828<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* sepOS para macOS 10.12 Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2827<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* sepOS para macOS 10.12 Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

# Certificaciones de seguridad de los sistemas operativos

## Descripción general de las certificaciones de seguridad de los sistemas operativos de Apple

Apple mantiene certificados de validación de conformidad con el estándar federal de procesamiento de información (FIPS) 140-2/-3 de EE. UU. para sepOS y el firmware del chip T2, así como otras certificaciones. Apple parte de *elementos esenciales de certificación* que se aplican con carácter general a las diversas plataformas cuando procede. Uno de esos elementos esenciales es la validación de Corecrypto, que se usa para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo elemento esencial es la certificación de Secure Enclave, que está integrado en muchos de los dispositivos Apple. En tercer lugar está la certificación de Secure Element (SE), que se encuentra en los dispositivos Apple con Touch ID y con Face ID. Todos estos elementos básicos de la certificación de los productos de hardware constituyen la base para certificaciones de seguridad de plataformas más amplias.

### Validaciones de los algoritmos criptográficos

La validación de la correcta implementación de diversos algoritmos criptográficos y las funciones de seguridad relacionadas es un requisito previo para la validación FIPS 140-3 sobre el que se sustentan otras certificaciones. La validación está gestionada por el Programa de validación de algoritmos criptográficos (CAVP) del Instituto Nacional de Estándares y Tecnología (NIST). Los certificados de validación de las implementaciones de Apple pueden encontrarse mediante la herramienta de búsqueda del CAVP.

## Validaciones de los módulos criptográficos: FIPS 140-2/3 (ISO/IEC 19790)

Los módulos criptográficos de los sistemas operativos de Apple se han validado varias veces a través del Programa de validación de módulos criptográficos (CMVP) para garantizar su conformidad con las normas del estándar federal de procesamiento de información de Estados Unidos (FIPS) 140-2 después de cada versión principal de los sistemas operativos desde 2012. Tras cada versión principal, Apple envía todos los módulos al CMVP para su validación criptográfica. Estos módulos validados proporcionan operaciones criptográficas para los servicios proporcionados por Apple y están disponibles para que los puedan usar apps de terceros.

Apple logra el **Nivel de seguridad 1** cada año para los módulos basados en software "Módulo Corecrypto para Intel" y "Módulo de kernel Corecrypto para Intel" para macOS. Para el chip de Apple, los módulos "Módulo Corecrypto para ARM" y "Módulo de kernel Corecrypto para ARM" son aplicables a iOS, iPadOS, tvOS, watchOS y el firmware del chip de seguridad T2 de Apple integrado en ordenadores Mac.

En 2019, Apple obtuvo el primer **Nivel de seguridad 2** de FIPS 140-2 para el módulo criptográfico de hardware integrado identificado como "Módulo Corecrypto de Apple: Almacén seguro de claves", lo que permite el uso autorizado por el gobierno de EE. UU. de las claves generadas y gestionadas en Secure Enclave. Apple sigue trabajando para obtener validaciones para el módulo criptográfico de hardware con cada nueva versión principal de los sistemas operativos.

El Departamento de Comercio de Estados Unidos aprobó la validación **FIPS 140-3** en 2019. El cambio más significativo en esta versión del estándar es la especificación de los estándares ISO/IEC, en particular ISO/IEC 19790:2015 y el correspondiente estándar de realización de pruebas ISO/IEC 24759:2017. El CMVP ha iniciado un programa de transición y ha indicado que, a partir de 2020, los módulos criptográficos comenzarán a validarse basándose en FIPS 140-3. Los módulos criptográficos de Apple procurarán cumplir con el estándar FIPS 140-3 y hacer la transición hacia él tan pronto como sea viable.

En el caso de los módulos criptográficos que actualmente se encuentran en fase de prueba y validación, el CMVP mantiene dos listas separadas que pueden contener información sobre las validaciones propuestas. En el caso de los módulos criptográficos que están en fase de prueba en un laboratorio acreditado, el módulo puede figurar en la lista de implementaciones en pruebas. Una vez que el laboratorio completa las pruebas y recomienda la validación del CMVP, los módulos criptográficos de Apple aparecen en la lista de módulos en curso. En este momento, las pruebas de laboratorio se han completado y están a la espera de la validación por parte del CMVP. Dado que la duración del proceso de evaluación puede variar, conviene consultar primero las dos listas anteriores para determinar el estado actual de los módulos criptográficos de Apple entre la fecha de lanzamiento de una versión principal del sistema operativo y la emisión del certificado de validación del CMVP.

## Certificaciones de productos: Common Criteria (ISO/IEC 15408)

Muchas organizaciones utilizan el estándar de criterios comunes o Common Criteria (ISO/IEC 15408) como base para llevar a cabo evaluaciones de seguridad de los productos de tecnologías de la información.

Para las certificaciones que pueden ser reconocidas mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA) internacional, consulta el portal de Common Criteria. El estándar de Common Criteria también puede usarse fuera del CCRA por parte de sistemas de validación nacionales y privados. En Europa, el reconocimiento mutuo se rige por el acuerdo SOG-IS, así como por el CCRA.

El objetivo, como se indica en la comunidad de Common Criteria, está enfocado a un conjunto de estándares de seguridad aprobado internacionalmente para proporcionar una evaluación clara y fiable de las capacidades de seguridad de los productos que pertenecen a las tecnologías de la información. Al proporcionar una valoración independiente sobre la capacidad de un producto para cumplir los estándares de seguridad, la certificación Common Criteria aporta a los clientes más confianza en la seguridad de los productos tecnológicos y les permite tomar decisiones mejor fundamentadas.

A través del CCRA, los países miembros han acordado reconocer la certificación de productos que pertenecen a las tecnologías de la información con el mismo nivel de confianza. Se requieren numerosas evaluaciones antes de la certificación, entre las que se incluyen las siguientes:

- Perfiles de protección
- Objetivos de seguridad
- Requisitos funcionales de seguridad
- Requisitos de garantía de seguridad
- Niveles de garantía de evaluación

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (por ejemplo, Movilidad) y que permiten comparar las evaluaciones de seguridad de los distintos productos de tecnologías de la información de la misma clase. Al igual que crece la lista de los perfiles de protección aprobados, los miembros del acuerdo CCRA continúan aumentando año a año. Este acuerdo permite que los desarrolladores de productos trabajen para lograr una sola certificación en virtud de cualquiera de los esquemas de autorización de certificados que esté reconocida por todos los firmantes consumidores de certificados.

Los objetivos de seguridad (ST) definen *qué* se evaluará al certificar un producto de TI. Los objetivos de seguridad se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, que se usan para evaluar los objetivos de seguridad en detalle.

El estándar Common Criteria (CC) también incluye *requisitos de garantía de seguridad*. Una medida que se identifica habitualmente es el *nivel de garantía de evaluación (EAL)*. Los niveles de garantía de evaluación agrupan conjuntos de requisitos de garantía de seguridad utilizados habitualmente y pueden especificarse en perfiles de protección y objetivos de seguridad para permitir la comparación.

Muchos de los perfiles de protección más antiguos se han archivado y se han comenzado a sustituir por perfiles de protección específicos desarrollados y centrados en torno a soluciones y entornos concretos. En un esfuerzo conjunto por garantizar el reconocimiento mutuo continuado de todos los miembros del CCRA, se han establecido comunidades técnicas internacionales a fin de desarrollar y mantener *perfiles de protección colaborativos* que se desarrollan desde el inicio con la aplicación de varios esquemas de firmantes del CCRA. Diversas partes interesadas siguen desarrollando perfiles de protección destinados a grupos de usuarios y acuerdos de reconocimiento mutuo distintos al CCRA.

A principios de 2015, Apple comenzó a trabajar para obtener las certificaciones en virtud del CCRA actualizado con determinados perfiles de protección colaborativos. Desde entonces, Apple ha conseguido las certificaciones de Common Criteria para cada versión principal de iOS y ha ampliado la cobertura para incluir la garantía de seguridad que proporcionan los nuevos perfiles de protección.

Apple adopta un papel activo dentro de las comunidades técnicas centradas en la evaluación de las tecnologías de seguridad móvil. Esto incluye a las comunidades técnicas internacionales responsables de desarrollar y actualizar perfiles de protección colaborativos. Apple sigue evaluando y trabajando para lograr certificaciones con los perfiles de protección y los perfiles de protección colaborativos actuales.

Las certificaciones de la plataforma Apple para el mercado de Norteamérica generalmente se realizan con la National Information Assurance Partnership (NIAP), que tiene una lista de proyectos actualmente en evaluación pero que aún no están certificados.

Además de los certificados de plataforma generales mencionados, se han emitido otros certificados para demostrar requisitos de seguridad específicos para algunos mercados.

# Certificaciones de seguridad para iOS


## Contexto de la certificación de iOS

Apple participa activamente en la validación de módulos integrados de hardware y software de Apple para cada versión principal de un sistema operativo. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

## Estado de la validación de módulos criptográficos de iOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

# Certificaciones FIPS 140-3

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de iOS 14 (2020) y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de iOS 15 (2021). Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* iOS 15<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* iOS 15<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con iOS 15<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con iOS 15<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A13, A14, A15)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* iOS 14<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* iOS 14<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con iOS 14<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con iOS 14<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A13-A14)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que se están probando actualmente y que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3856<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* iOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3855<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* iOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v10.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iOS 13<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 23/04/2019 | *Certificados:* 3438<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* iOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 11/04/2019 | *Certificados:* 3433<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* iOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iOS 12<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018 | *Certificados:* 3148<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* iOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018 | *Certificados:* 3147<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* iOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iOS 11<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2828<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* iOS 10<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2827<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* iOS 10<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

## Versiones anteriores

El CMVP incluye en la lista con estado histórico aquellos certificados que tienen más de 5 años: Estas versiones de iOS anteriores tenían validaciones de módulos criptográficos:

- iOS 9 (módulos Corecrypto v6.0)
- iOS 8 (módulos Corecrypto v5.0)
- iOS 7 (módulos Corecrypto v4.0)
- iOS 6 (módulos Corecrypto v3.0)

## Contexto de la certificación Common Criteria (CC)

Apple participa activamente en la evaluación de iOS para cada versión principal del sistema operativo. La evaluación solo puede llevarse a cabo en una versión pública final del sistema operativo. Antes de iPadOS 13.1, iPadOS se llamaba iOS.

## Estado de la certificación Common Criteria (CC)

El esquema de EE. UU., operado por la National Information Assurance Partnership (NIAP), mantiene una lista de productos en evaluación que incluye productos que se encuentran actualmente en fase de evaluación en EE. UU. en un laboratorio de pruebas de Common Criteria (CCTL) autorizado por la NIAP y que han completado una reunión de evaluación inicial (o equivalente) en la que la dirección del CCEVS ha aceptado oficialmente el producto para su evaluación.

Tras la certificación de los productos, la NIAP incluye las certificaciones válidas actualmente en su lista de productos conformes. A los dos años, estas certificaciones se revisan para determinar su conformidad con la política de mantenimiento de garantía vigente. Una vez expirada la fecha de mantenimiento de la garantía, la NIAP transfiere la certificación a su lista de productos archivados.

En el portal de Common Criteria se enumeran certificaciones que pueden reconocerse mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años y conserva registros de las certificaciones archivadas.

La tabla siguiente muestra las certificaciones que están siendo evaluadas por un laboratorio o cuyo cumplimiento con el estándar Common Criteria se ha certificado.

### Estado actual

Se están llevando a cabo las pruebas en laboratorio para las evaluaciones de iOS 15 por parte de la NIAP. Para obtener la información más reciente, consulta la lista de productos en evaluación y la lista de productos conformes de la NIAP.

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* iOS 15<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:* — | *Título:* iOS 15 de Apple: iPhone<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles (módulos de PP por confirmar) |
| *Sistema operativo:* iOS 14<br>*Fecha de certificación:* 01/09/2021 | *ID de esquema:* 11146<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 14 de Apple: iPhone<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, Módulo WLAN Clients PP, MDM Agent EP |
| *Sistema operativo:* iOS 13<br>*Fecha de certificación:* 06/11/2020 | *ID de esquema:* 11036<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 13 de Apple: iPhone<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, WLAN Clients EP, MDM Agent EP |

# Certificaciones de Common Criteria archivadas para iOS

Estas versiones de iOS anteriores tenían validaciones de Common Criteria. Están archivadas por la NIAP de acuerdo con la política de la NIAP:

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* iOS 12<br>*Fecha de certificación:* 14/03/2019 | *ID de esquema:* 10937<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* iPhone con iOS 12<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, Wireless LAN Client EP, MDM Agent EP |
| *Sistema operativo:* iOS 11<br>*Fecha de certificación:* 17/07/2018 | *ID de esquema:* 10851<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* iOS 11 de Apple<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Wireless LAN Client EP, MDM Agent EP |
| *Sistema operativo:* iOS 10<br>*Fecha de certificación:* 27/07/2017 | *ID de esquema:* 10782<br>*Documentos:* Objetivo de seguridad, Directrices | *Título:* iOS 10.2 en dispositivos iPhone y iPad<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Wireless LAN Client EP, MDM Agent EP |
| *Sistema operativo:* iOS 10<br>*Fecha de certificación:* 27/07/2017 | *ID de esquema:* 10792<br>*Documentos:* Objetivo de seguridad, Directrices | *Título:* Cliente VPN de iOS 10.2 en iPhone y iPad<br>*Perfiles de protección:* PP de cliente VPN |
| *Sistema operativo:* iOS 9<br>*Fecha de certificación:* 14/10/2016 | *ID de esquema:* 10725<br>*Documentos:* Objetivo de seguridad, Directrices | *Título:* iOS 9.3.2 con MDM Agent<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, MDM Agent EP |
| *Sistema operativo:* iOS 9<br>*Fecha de certificación:* 13/10/2016 | *ID de esquema:* 10714<br>*Documentos:* Objetivo de seguridad, Directrices | *Título:* Cliente VPN de SO en iPhone y iPad<br>*Perfiles de protección:* PP de cliente VPN |
| *Sistema operativo:* iOS 9<br>*Fecha de certificación:* 28/01/2016 | *ID de esquema:* 10695<br>*Documentos:* Objetivo de seguridad, Directrices | *Título:* iOS 9<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles |

# Certificaciones de seguridad para iPadOS


## Contexto de la certificación de iPadOS

Apple participa activamente en la validación de los sistemas operativos de Apple para cada versión principal de un sistema operativo con los perfiles de protección colaborativos pertinentes y los niveles de seguridad de FIPS 140-3. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

*Nota:* En 2019, se cambió el nombre del sistema operativo de los dispositivos iPad a iPadOS. Antes de iPadOS 13.1, iPadOS se llamaba iOS.

## Estado de la validación de módulos criptográficos de iPadOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

# Certificaciones FIPS 140-3

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de iPadOS 14 (2020) y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de iPadOS 15 (2021). Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* iPadOS 15<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* iPadOS 15<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con iPadOS 15<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, M1)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con iPadOS 15<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, M1)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* iPadOS 14<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* iPadOS 14<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con iPadOS 14<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, M1)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con iPadOS 14<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A9-A14, M1)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que se están probando actualmente y que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3856<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* iPadOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3855<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* iPadOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves Corecrypto v10.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iPadOS 13<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 23/04/2019 | *Certificados:* 3438<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* iOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 11/04/2019 | *Certificados:* 3433<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* iOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iOS 12<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018 | *Certificados:* 3148<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* iOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018 | *Certificados:* 3147<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* iOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS distribuido con iOS 11<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2828<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* iOS 10<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2016<br>*Fechas de validación:* 01/02/2017 | *Certificados:* 2827<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v7.0 para iOS de Apple<br>*Sistema operativo:* iOS 10<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

## Versiones anteriores

El CMVP incluye en la lista con estado histórico aquellos certificados que tienen más de 5 años: Estas versiones de iOS anteriores tenían validaciones de módulos criptográficos:

- iOS 9 (módulos Corecrypto v6.0)
- iOS 8 (módulos Corecrypto v5.0)
- iOS 7 (módulos Corecrypto v4.0)
- iOS 6 (módulos Corecrypto v3.0)

## Contexto de la certificación Common Criteria (CC)

Apple participa activamente en la evaluación de iPadOS para cada versión principal del sistema operativo. La evaluación solo puede llevarse a cabo en una versión pública final del sistema operativo.

## Estado de la certificación Common Criteria (CC)

El esquema de EE. UU., operado por la National Information Assurance Partnership (NIAP), mantiene una lista de productos en evaluación que incluye productos que se encuentran actualmente en fase de evaluación en EE. UU. en un laboratorio de pruebas de Common Criteria (CCTL) autorizado por la NIAP y que han completado una reunión de evaluación inicial (o equivalente) en la que la dirección del CCEVS ha aceptado oficialmente el producto para su evaluación.

Tras la certificación de los productos, la NIAP incluye las certificaciones válidas actualmente en su lista de productos conformes. A los dos años, estas certificaciones se revisan para determinar su conformidad con la política de mantenimiento de garantía vigente. Una vez expirada la fecha de mantenimiento de la garantía, la NIAP transfiere la certificación a su lista de productos archivados.

En el portal de Common Criteria se enumeran certificaciones que pueden reconocerse mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años y conserva registros de las certificaciones archivadas.

La tabla siguiente muestra las certificaciones que están siendo evaluadas por un laboratorio o cuyo cumplimiento con el estándar Common Criteria se ha certificado.

### Estado actual

Se están llevando a cabo las pruebas en laboratorio para las evaluaciones de iPadOS 15 por parte de la NIAP. Para obtener la información más reciente, consulta la lista de productos en evaluación y la lista de productos conformes de la NIAP.

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* iPadOS 15<br>*Fecha de certificación:* 14/03/2019 | *ID de esquema:* —<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iPad con iOS 12<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, Wireless LAN Client EP, MDM Agent EP |
| *Sistema operativo:* iPadOS 14<br>*Fecha de certificación:* 01/09/2021 | *ID de esquema:* 11147<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iPadOS 14 de Apple: iPad<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, Wireless LAN Client EP, MDM Agent EP |
| *Sistema operativo:* iPadOS 13<br>*Fecha de certificación:* 06/11/2020 | *ID de esquema:* 11036<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iPadOS 13 en dispositivos móviles iPad<br>*Perfiles de protección:* Conceptos básicos de los dispositivos móviles, Módulo VPN Client, Wireless LAN Client EP, MDM Agent EP |

## Versiones anteriores

Estas versiones de iOS anteriores tenían validaciones de Common Criteria. Están archivadas por la NIAP de acuerdo con la política de la NIAP:

- iOS 12 (ID de esquema: 10937)
- iOS 11 (ID de esquema: 10851)
- iOS 10 (ID de esquema: 107782, 10792)
- iOS 9 (ID de esquema: 10725, 10714, 10695)

# Certificaciones de seguridad para macOS


## Contexto de la certificación de macOS

Apple participa activamente en la validación de los sistemas operativos de Apple para cada versión principal de un sistema operativo con los perfiles de protección colaborativos pertinentes y los niveles de seguridad de FIPS 140-3. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

## Estado de la validación de módulos criptográficos de macOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

Para los ordenadores Mac de Apple, la tabla siguiente muestra qué módulos criptográficos son aplicables a qué tecnología de Mac.

| Módulo criptográfico | Ordenadores Mac con chip de Apple | Ordenadores Mac con chip de seguridad T2 de Apple | Ordenadores Mac basados en Intel sin chip de seguridad T2 de Apple |
|---|---|---|---|
| Espacio de usuarios de chip de Apple | ✓ | | |
| Kernel de chip de Apple | ✓ | | |
| Espacio de usuarios de Intel | | ✓ | ✓ |
| Kernel de Intel | | ✓ | ✓ |
| Almacén seguro de claves | ✓ | ✓ | |

## Certificaciones FIPS 140-3

En 2020, Apple lanzó ordenadores Mac basados en un chip de Apple. La aplicación de los módulos criptográficos en ordenadores Mac basados en el chip de Apple o en Intel se indica en la columna “Información del módulo” de la tabla siguiente.

*Nota:* En muchos ordenadores Mac basados en Intel se incluyen chips de seguridad T2 de Apple. Para obtener información sobre las certificaciones del chip T2, consulta Certificaciones de seguridad para el chip de seguridad T2 de Apple.

**Cliente ssh de macOS**

OpenSSH se puede configurar para usar módulos validados por FIPS 140-3 para determinados algoritmos FIPS 140-3. Las organizaciones pueden ejecutar un instalador firmado y certificado disponible de Apple con la contraseña *FIPS140Mode*. El instalador coloca dos archivos en el Mac:

- *fips_ssh_config:* Ubicado en /private/etc/ssh/ssh_config.d/
- *fips_sshd_config:* Ubicado en /private/etc/ssh/sshd_config.d/

A continuación, macOS utiliza estos archivos para limitar los cifrados disponibles para OpenSSH a aquellos validados por el NIST y garantiza que el cliente OpenSSH use el módulo criptográfico validado proporcionado por la plataforma. Los administradores también pueden crear sus propios archivos. Para obtener más información, consulta la página “man” `apple_ssh_and_fips` en macOS 12.0.1 o posterior.

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de macOS 11 Big Sur y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de macOS 12 Monterey. Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* macOS 12 Monterey con chip de Apple<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* macOS 12 Monterey con chip de Apple<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* macOS 12 Monterey con Intel<br>*Entorno:* Intel, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* macOS 12 Monterey con Intel<br>*Entorno:* Intel, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* sepOS distribuido con macOS 12 Monterey con chip de Apple, sepOS distribuido con macOS 12 Monterey en Intel con chip T2<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (M1 y T2)<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12.0<br>*Sistema operativo:* sepOS distribuido con macOS 12 Monterey con chip de Apple<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (M1)<br>*Nivel de seguridad:* 2<br>*Nivel de seguridad físico:* 3 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* macOS 11 Big Sur con Intel<br>*Entorno:* Intel, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* macOS 11 Big Sur con Intel<br>*Entorno:* Intel, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* macOS 11 Big Sur con chip de Apple<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* macOS 11 Big Sur con chip de Apple<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con macOS 11 Big Sur con chip de Apple, sepOS distribuido con macOS 11 Big Sur con Intel<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (M1)<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con macOS 11 Big Sur con chip de Apple<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (M1)<br>*Nivel de seguridad:* 2<br>*Nivel de seguridad físico:* 3 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que se están probando actualmente y que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de macOS 10.15 Catalina y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

*Nota:* En muchos ordenadores Mac basados en Intel se incluyen chips de seguridad T2 de Apple. Para obtener información sobre las certificaciones del chip T2, consulta Certificaciones de seguridad para el chip de seguridad T2 de Apple.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 24/03/2021 | *Certificados:* 3859<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de espacio del usuario Corecrypto para Intel de Apple (ccv10)<br>*Sistema operativo:* macOS 10.15 Catalina<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 24/03/2021 | *Certificados:* 3858<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para Intel de Apple (ccv10)<br>*Sistema operativo:* macOS 10.15 Catalina<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 12/04/2019 | *Certificados:* 3402<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para Intel de Apple<br>*Sistema operativo:* macOS 10.14 Mojave<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 12/04/2019 | *Certificados:* 3431<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para Intel de Apple<br>*Sistema operativo:* macOS 10.14 Mojave<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 22/03/2018 | *Certificados:* 3155<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para Intel de Apple<br>*Sistema operativo:* macOS 10.13 High Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 22/03/2018 | *Certificados:* 3156<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para Intel de Apple<br>*Sistema operativo:* macOS 10.13 High Sierra<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

## Versiones anteriores

Estas versiones de OS X y macOS anteriores tenían validaciones de módulos criptográficos. El CMVP incluye en la lista con estado histórico aquellas que tienen más de 5 años:

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

## Contexto de la certificación Common Criteria (CC)

Apple participa activamente en la evaluación de macOS para cada versión principal del sistema operativo. La evaluación solo puede llevarse a cabo en una versión pública final del sistema operativo.

## Estado de la certificación Common Criteria (CC)

El esquema de EE. UU., operado por la National Information Assurance Partnership (NIAP), mantiene una lista de productos en evaluación que incluye productos que se encuentran actualmente en fase de evaluación en EE. UU. en un laboratorio de pruebas de Common Criteria (CCTL) autorizado por la NIAP y que han completado una reunión de evaluación inicial (o equivalente) en la que la dirección del CCEVS ha aceptado oficialmente el producto para su evaluación.

Tras la certificación de los productos, la NIAP incluye las certificaciones válidas actualmente en su lista de productos conformes. A los dos años, estas certificaciones se revisan para determinar su conformidad con la política de mantenimiento de garantía vigente. Una vez expirada la fecha de mantenimiento de la garantía, la NIAP transfiere la certificación a su lista de productos archivados.

En el portal de Common Criteria se enumeran certificaciones que pueden reconocerse mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años y conserva registros de las certificaciones archivadas.

La tabla siguiente muestra las certificaciones que están siendo evaluadas por un laboratorio o cuyo cumplimiento con el estándar Common Criteria se ha certificado.

### Estado actual

Se están llevando a cabo evaluaciones de macOS 11 y macOS 12 por parte de la NIAP utilizando el sistema operativo de uso genérico y perfiles de protección (AA y EE) de encriptación total del disco (FDE).

Para obtener la información más reciente, consulta la lista de productos en evaluación y la lista de productos conformes de la NIAP.

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* macOS 12 Monterey<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:* — | *Título:* FileVault 2 de Apple con macOS 12 Monterey<br>*Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (PP por confirmar) |
| *Sistema operativo:* macOS 12 Monterey<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:* — | *Título:* macOS 12 Monterey<br>*Perfiles de protección:* PP_OS_V4.21 (PP por confirmar) |
| *Sistema operativo:* macOS 11 Big Sur<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* FileVault 2 de Apple con macOS 11 Big Sur<br>*Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E |
| *Sistema operativo:* macOS 11 Big Sur<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* macOS 11 Big Sur de Apple<br>*Perfiles de protección:* PP_OS_V4.21 |
| *Sistema operativo:* macOS 10.15 Catalina<br>*Fecha de certificación:* 29/04/2021 | *ID de esquema:* 11078<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* FileVault 2 de Apple en ordenadores con chip T2 con macOS 10.15 Catalina<br>*Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E |

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
| --- | --- | --- |
| *Sistema operativo:* macOS 10.15 Catalina<br>*Fecha de certificación:* 23/09/2020 | *ID de esquema:* 11077<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* macOS 10.15 Catalina<br>*Perfiles de protección:* PP_OS_V4.21 |

# Certificaciones de seguridad para tvOS

## Contexto de la certificación de tvOS

Apple participa activamente en la validación de los módulos criptográficos asociados con cada versión principal de tvOS. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

## Estado de la validación de módulos criptográficos de tvOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

# Certificaciones FIPS 140-3

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de tvOS 14 (2020) y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de tvOS 15 (2021). Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* tvOS 15<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* tvOS 15<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con tvOS 15<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A10, A12)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* tvOS 14<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* tvOS 14<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con tvOS 14<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (A10, A12)<br>*Nivel de seguridad general:* 2 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que se están probando actualmente y que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de tvOS 13 (2019) y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3856<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* tvOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 23/03/2021 | *Certificados:* 3855<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* tvOS 13<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v10.0 de Apple<br>*Sistema operativo:* sepOS distribuido con tvOS 13<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 23/04/2019 | *Certificados:* 3438<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* tvOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 11/04/2019 | *Certificados:* 3433<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* tvOS 12<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS distribuido con tvOS 12<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018 | *Certificados:* 3148<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* tvOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018 | *Certificados:* 3147<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* tvOS 11<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS distribuido con tvOS 11<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

# Certificaciones de seguridad para watchOS


## Contexto de la certificación de watchOS

Apple participa activamente en la validación de los módulos criptográficos asociados con cada versión principal de watchOS. La validación de la conformidad solo puede llevarse a cabo en una versión pública final.

## Estado de la validación de módulos criptográficos de watchOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de validación de los módulos criptográficos en tres listas independientes en función de su estado actual:

- Para figurar en la lista de implementaciones en pruebas del CMVP, el laboratorio debe haber suscrito con Apple un contrato para llevar a cabo pruebas.
- Una vez completadas las pruebas, el laboratorio recomienda la validación del CMVP y, tras pagar las tarifas del CMVP, se añade el módulo a la lista de módulos en curso. La lista de módulos en curso controla el progreso de las labores de validación del CMVP en cuatro fases:
  - *Pendiente de revisión:* En espera de que se asigne el recurso del CMVP.
  - *En revisión:* Los recursos del CMVP están llevando a cabo sus actividades de validación.
  - *Coordinación:* El laboratorio y el CMVP están resolviendo los problemas detectados.
  - *Finalización:* Actividades y formalidades en relación con la emisión del certificado.
- Tras la validación del CMVP, los módulos reciben un certificado de conformidad y se incluyen en la lista de módulos criptográficos validados. Esto incluye lo siguiente:
  - Módulos validados marcados como activos.
  - Después de 5 años, los módulos se marcan como históricos.
  - Si la certificación del módulo se revoca por alguna razón, se marca como revocado.

En 2020, el CMVP adoptó el estándar internacional ISO/IEC 19790 como base para la validación FIPS 140-3.

# Certificaciones FIPS 140-3

### Estado actual

Se han completado las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de watchOS 7 (2020) y el laboratorio ha recomendado al CMVP su validación. Se incluyen en la lista de módulos en curso.

Se están realizando las pruebas en laboratorio del espacio de usuario, el espacio del kernel y el almacén seguro de claves de watchOS 8 (2021). Se incluyen en la lista de implementaciones en pruebas.

| Fechas | Certificados/Documentos | Información del módulo |
|---|---|---|
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* watchOS 8<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* watchOS 8<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con watchOS 8<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (S3, S4, S5, S6)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2021<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v12<br>*Sistema operativo:* sepOS distribuido con watchOS 8<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (S6)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* watchOS 7<br>*Entorno:* Chip de Apple, usuario, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* watchOS 7<br>*Entorno:* Chip de Apple, kernel, software<br>*Tipo:* Software<br>*Nivel de seguridad general:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con watchOS 7<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (S3, S4, S5, S6)<br>*Nivel de seguridad general:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2020<br>*Fechas de validación:* — | *Certificados:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo Apple Corecrypto v11.1<br>*Sistema operativo:* sepOS distribuido con watchOS 7<br>*Entorno:* Chip de Apple, almacén seguro de claves, hardware<br>*Tipo:* Hardware (S6)<br>*Nivel de seguridad general:* 2<br>*Nivel de seguridad físico:* 3 |

## Certificaciones FIPS 140-2

En la tabla siguiente se muestran los módulos criptográficos que se están probando actualmente y que ya se han probado en el laboratorio para determinar su conformidad con el estándar FIPS 140-2.

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* — | *Certificados:* 3856<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* watchOS 6<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* — | *Certificados:* 3855<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v10.0 para ARM de Apple<br>*Sistema operativo:* watchOS 6<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |

| Fechas | Certificados/Documentos | Información del módulo |
| --- | --- | --- |
| *Fecha de lanzamiento del sistema operativo:* 2019<br>*Fechas de validación:* 05/02/2021 | *Certificados:* 3811<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v10.0 de Apple<br>*Sistema operativo:* sepOS distribuido con watchOS 6<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 23/04/2019 | *Certificados:* 3438<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* watchOS 5<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 11/04/2019 | *Certificados:* 3433<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v9.0 para ARM de Apple<br>*Sistema operativo:* watchOS 5<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2018<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3523<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v9.0 de Apple<br>*Sistema operativo:* sepOS distribuido con watchOS 5<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018 | *Certificados:* 3148<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de usuario Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* watchOS 4<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018 | *Certificados:* 3147<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo de kernel Corecrypto v8.0 para ARM de Apple<br>*Sistema operativo:* watchOS 4<br>*Tipo:* Software<br>*Nivel de seguridad:* 1 |
| *Fecha de lanzamiento del sistema operativo:* 2017<br>*Fechas de validación:* 10/09/2019 | *Certificados:* 3223<br>*Documentos:*<br>Certificado<br>Política de seguridad<br>Directrices para los responsables del cifrado | *Título:* Módulo criptográfico del almacén seguro de claves v1.0 de Apple<br>*Sistema operativo:* sepOS distribuido con watchOS 4<br>*Tipo:* Hardware<br>*Nivel de seguridad:* 2 |

# Certificaciones de seguridad del software

## Descripción general de las certificaciones de seguridad del software de Apple

Apple mantiene certificados de validación de conformidad con el estándar federal de procesamiento de información (FIPS) 140-2/-3 de EE. UU. para sepOS y el firmware del chip T2, así como otras certificaciones. Apple parte de *elementos esenciales de certificación* que se aplican con carácter general a las diversas plataformas cuando procede. Uno de esos elementos esenciales es la validación de corecrypto, que se usa para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo elemento esencial es la certificación de Secure Enclave, que está integrado en muchos de los dispositivos Apple. En tercer lugar está la certificación de Secure Element (SE), que se encuentra en los dispositivos Apple con Touch ID y con Face ID. Todos estos elementos básicos de la certificación de los productos de hardware constituyen la base para certificaciones de seguridad de plataformas más amplias.

### Certificaciones de productos: Common Criteria (ISO/IEC 15408)

Muchas organizaciones utilizan el estándar de criterios comunes o Common Criteria (ISO/IEC 15408) como base para llevar a cabo evaluaciones de seguridad de los productos de tecnologías de la información.

Para las certificaciones que pueden ser reconocidas mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA) internacional, consulta el portal de Common Criteria. El estándar de Common Criteria también puede usarse fuera del CCRA por parte de sistemas de validación nacionales y privados. En Europa, el reconocimiento mutuo se rige por el acuerdo SOG-IS, así como por el CCRA.

El objetivo, como se indica en la comunidad de Common Criteria, está enfocado a un conjunto de estándares de seguridad aprobado internacionalmente para proporcionar una evaluación clara y fiable de las capacidades de seguridad de los productos que pertenecen a las tecnologías de la información. Al proporcionar una valoración independiente sobre la capacidad de un producto para cumplir los estándares de seguridad, la certificación Common Criteria aporta a los clientes más confianza en la seguridad de los productos tecnológicos y les permite tomar decisiones mejor fundamentadas.

A través del CCRA, los países miembros han acordado reconocer la certificación de productos que pertenecen a las tecnologías de la información con el mismo nivel de confianza. Se requieren numerosas evaluaciones antes de la certificación, entre las que se incluyen las siguientes:

- Perfiles de protección
- Objetivos de seguridad
- Requisitos funcionales de seguridad
- Requisitos de garantía de seguridad
- Niveles de garantía de evaluación

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (por ejemplo, Movilidad) y que permiten comparar las evaluaciones de seguridad de los distintos productos de tecnologías de la información de la misma clase. Al igual que crece la lista de los perfiles de protección aprobados, los miembros del acuerdo CCRA continúan aumentando año a año. Este acuerdo permite que los desarrolladores de productos trabajen para lograr una sola certificación en virtud de cualquiera de los esquemas de autorización de certificados que esté reconocida por todos los firmantes consumidores de certificados.

Los objetivos de seguridad (ST) definen *qué* se evaluará al certificar un producto de TI. Los objetivos de seguridad se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, que se usan para evaluar los objetivos de seguridad en detalle.

El estándar Common Criteria (CC) también incluye *requisitos de garantía de seguridad*. Una medida que se identifica habitualmente es el *nivel de garantía de evaluación (EAL)*. Los niveles de garantía de evaluación agrupan conjuntos de requisitos de garantía de seguridad utilizados habitualmente y pueden especificarse en perfiles de protección y objetivos de seguridad para permitir la comparación.

Muchos de los perfiles de protección más antiguos se han archivado y se han comenzado a sustituir por perfiles de protección específicos desarrollados y centrados en torno a soluciones y entornos concretos. En un esfuerzo conjunto por garantizar el reconocimiento mutuo continuado de todos los miembros del CCRA, se han establecido comunidades técnicas internacionales a fin de desarrollar y mantener perfiles de protección colaborativos que se desarrollan desde el inicio con la aplicación de varios esquemas de firmantes del CCRA. Diversas partes interesadas siguen desarrollando perfiles de protección destinados a grupos de usuarios y acuerdos de reconocimiento mutuo distintos al CCRA.

A principios de 2015, Apple comenzó a trabajar para obtener las certificaciones en virtud del CCRA actualizado con determinados perfiles de protección colaborativos. Desde entonces, Apple ha conseguido las certificaciones de Common Criteria para cada versión principal de iOS y ha ampliado la cobertura para incluir la garantía de seguridad que proporcionan los nuevos perfiles de protección.

Apple adopta un papel activo dentro de las comunidades técnicas centradas en la evaluación de las tecnologías de seguridad móvil. Esto incluye a las comunidades técnicas internacionales responsables de desarrollar y actualizar perfiles de protección colaborativos. Apple sigue evaluando y trabajando para lograr certificaciones con los perfiles de protección y los perfiles de protección colaborativos actuales.

Las certificaciones de la plataforma Apple para el mercado de Norteamérica generalmente se realizan con la National Information Assurance Partnership (NIAP), que tiene una lista de proyectos actualmente en evaluación pero que aún no están certificados.

Además de los certificados de plataforma generales mencionados, se han emitido otros certificados para demostrar requisitos de seguridad específicos para algunos mercados.

# Certificaciones de seguridad para apps de Apple

## Contexto de la certificación de las apps de Apple

Apple trabaja activamente para obtener certificaciones de seguridad de las apps de Apple con los perfiles de protección (PP) de Common Criteria pertinentes. Estas evaluaciones se basan en las certificaciones del hardware y los sistemas operativos que Apple ha obtenido.

En 2018, Apple puso en marcha una serie de evaluaciones de la seguridad de las aplicaciones clave de iOS 11 empezando por el navegador Safari y la app Contactos. Apple continuó estas evaluaciones en apps de iOS 12, iOS 13 y iPadOS 13.1. En 2021, se ha añadido cobertura para apps que se ejecutan en macOS 11.

## Estado de la certificación de módulos criptográficos

Las apps de Apple indicadas aquí usan módulos criptográficos para el sistema operativo correspondiente. Para obtener más información, consulta Certificaciones de seguridad para iOS, Certificaciones de seguridad para iPadOS y Certificaciones de seguridad para macOS.

## Estado de la certificación Common Criteria (CC)

El esquema de EE. UU., operado por la National Information Assurance Partnership (NIAP), mantiene una lista de productos en evaluación que incluye productos que se encuentran actualmente en fase de evaluación en EE. UU. en un laboratorio de pruebas de Common Criteria (CCTL) autorizado por la NIAP y que han completado una reunión de evaluación inicial (o equivalente) en la que la dirección del CCEVS ha aceptado oficialmente el producto para su evaluación.

Tras la certificación de los productos, la NIAP incluye las certificaciones válidas actualmente en su lista de productos conformes. A los dos años, estas certificaciones se revisan para determinar su conformidad con la política de mantenimiento de garantía vigente. Una vez expirada la fecha de mantenimiento de la garantía, la NIAP transfiere la certificación a su lista de productos archivados.

En el portal de Common Criteria se enumeran certificaciones que pueden reconocerse mutuamente en virtud del acuerdo de reconocimiento de Common Criteria (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años y conserva registros de las certificaciones archivadas.

La tabla siguiente muestra las certificaciones que están siendo evaluadas por un laboratorio o cuyo cumplimiento con el estándar Common Criteria se ha certificado.

### Estado actual

- Las evaluaciones de la NIAP en curso se incluyen en la lista de productos en evaluación (NIAP).
- Las evaluaciones que se han completado y validado se incluyen en la lista de productos conformes de la NIAP.

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* macOS 11 Big Sur<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* macOS 11 Big Sur: Contactos<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistema operativo:* macOS 11 Big Sur<br>*Fecha de certificación:* — | *ID de esquema:* Aún no está certificado<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* macOS 11 Big Sur: Safari<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistemas operativos:* iOS 14, iPadOS 14<br>*Fecha de certificación:* 20/08/2021 | *ID de esquema:* 11191<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 14 y iPadOS 14 de Apple: Contactos<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistemas operativos:* iOS 14, iPadOS 14<br>*Fecha de certificación:* — | *ID de esquema:* 11192<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 14 y iPadOS 14 de Apple: Safari<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistemas operativos:* iOS 13, iPadOS 13<br>*Fecha de certificación:* 05/06/2020 | *ID de esquema:* 11060<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 13 y iPadOS 13 de Apple: Safari<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistemas operativos:* iOS 13, iPadOS 13<br>*Fecha de certificación:* 05/06/2020 | *ID de esquema:* 11050<br>*Documentos:*<br>Certificado<br>Objetivo de seguridad<br>Directrices<br>Informe de validación<br>Informe de actividad de garantía | *Título:* iOS 13 y iPadOS 13 de Apple: Contactos<br>*Perfiles de protección:* PP para SW de aplicación |

## Certificaciones de Common Criteria archivadas para apps de Apple

| Sistema operativo/Fecha de certificación | ID de esquema/Documentos | Título/Perfiles de protección |
|---|---|---|
| *Sistema operativo:* iOS 12<br>*Fecha de certificación:* 12/06/2019 | *ID de esquema:* 10960<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* Safari de iOS 12<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistema operativo:* iOS 12<br>*Fecha de certificación:* 28/02/2019 | *ID de esquema:* 10961<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* Contactos de iOS 12<br>*Perfiles de protección:* PP para SW de aplicación |
| *Sistema operativo:* iOS 11<br>*Fecha de certificación:* 09/11/2018 | *ID de esquema:* 10916<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* Safari de iOS 11<br>*Perfiles de protección:* PP para SW de aplicación, EP para navegadores web |
| *Sistema operativo:* iOS 11<br>*Fecha de certificación:* 13/09/2018 | *ID de esquema:* 10915<br>*Documentos:*<br>Objetivo de seguridad<br>Directrices | *Título:* Contactos de iOS 11<br>*Perfiles de protección:* PP para SW de aplicación |

# Certificaciones de seguridad para servicios de internet de Apple

Apple mantiene certificaciones conformes a los estándares ISO/IEC 27001 e ISO/IEC 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 seguridad y privacidad de la información de Apple para los sistemas pertinentes.

ISO/IEC 27001 e ISO/IEC 27018 forman parte de la familia de estándares del Sistema de gestión de seguridad de la información (ISMS) publicados por la Organización Internacional de Normalización (ISO). Como parte del ISMS de Apple, todos los requisitos de control del Anexo A se han incluido en la Declaración de aplicabilidad, tal y como se define en los estándares ISO/IEC 27001 e ISO/IEC 27018. Apple se somete anualmente a una acreditación independiente que lleva a cabo un organismo de certificación acreditado.

## ISO/IEC 27001

ISO/IEC 27001 es un estándar del Sistema de gestión de seguridad de la información que especifica requisitos para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información de una organización. El estándar ISO/IEC 27001 incluye los siguientes dominios de seguridad que cubren las certificaciones de ISO/IEC de Apple:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de recursos humanos
- Seguridad física y medioambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad de las operaciones empresariales
- Conformidad

# ISO/IEC 27018

ISO/IEC 27018 es un código de prácticas para la protección de datos personales en entornos de nube pública. El estándar ISO/IEC 27018 incluye los siguientes dominios de seguridad que cubren las certificaciones de ISO/IEC de Apple:

- Consentimiento y elección
- Legitimidad y especificación de los objetivos
- Limitación de la recopilación
- Minimización de los datos
- Uso, retención y limitación de divulgación
- Exactitud y calidad
- Transparencia
- Participación individual y acceso
- Responsabilidad
- Seguridad de la información
- Conformidad de privacidad

# Servicios de Apple cubiertos por los estándares ISO/IEC 27001 e ISO/IEC 27018

Las certificaciones ISO/IEC 27001 e ISO/IEC 27018 de Apple cubren los siguientes servicios:

- Chat para clientes de Apple
- Apple Business Manager
- Servicio de notificaciones push de Apple (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- Servicios de iWork
- ID de Apple gestionados
- Tareas de Clase
- Siri

# Certificaciones

En nuestro registro hay disponibles evidencias de las certificaciones ISO/IEC 27001 e ISO/IEC 27018 de Apple.

Para ver las certificaciones de Apple, ve a la búsqueda en el directorio de clientes y de certificados del sitio web de BSI (British Standards Institution), escribe “Apple” en el campo de búsqueda Compañía, haz clic en el botón Buscar y selecciona los resultados para los certificados.

*Nota:* Apple no promociona ni recomienda los productos no fabricados por Apple ni los sitios web independientes no controlados ni probados por Apple sobre los que se proporciona información. Apple declina toda responsabilidad en lo que respecta a la selección, el rendimiento o el uso de sitios web o productos de terceros. Apple no se hace responsable de la exactitud o fiabilidad de los sitios web de terceros. Ponte en contacto con el proveedor para más información.

# Proyecto de conformidad de seguridad de macOS

El proyecto de conformidad de seguridad de macOS (mSCP) es una iniciativa de código abierto que tiene por objeto proporcionar una estrategia de programación para la generación de directrices de seguridad. Se trata de un proyecto conjunto entre el personal de seguridad de TI operativa de los siguientes organismos de EE. UU.: el Instituto Nacional de Estándares y Tecnología (NIST), la Administración Nacional de Aeronáutica y el Espacio (NASA), la Agencia de Sistemas de Información de Defensa (DISA) y el Laboratorio Nacional de Los Álamos (LANL). En el proyecto se emplea una serie de controles probados y validados para macOS y se asignan estos controles a cualquier directriz de seguridad admitida por el proyecto. Además, este proyecto puede usarse como recurso para crear fácilmente bases de referencia de seguridad personalizadas de controles de seguridad técnica al aprovechar una biblioteca de medidas atómicas probadas y validadas (ajustes de configuración). El proyecto genera documentación personalizada, scripts, perfiles de configuración y una lista de comprobación para auditorías basada en las bases de referencia utilizadas.

El mSCP puede crear contenido que se usará junto con herramientas de gestión y seguridad para lograr la conformidad. Los ajustes de configuración de este proyecto admiten las siguientes bases de referencia para las directrices:

| Organización | Bases de referencia admitidas |
| --- | --- |
| Publicación especial (SP) 800-53 del Instituto Nacional de Estándares y Tecnología (NIST): Security and Privacy Controls for Federal Information Systems and Organizations, Rev. 5 | 800-53 alta, 800-53 moderada, 800-53 baja |
| Publicación especial (SP) 800-171 del Instituto Nacional de Estándares y Tecnología (NIST): Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev. 2 | 800-171 |
| Agencia de Sistemas de Información de Defensa (DISA) macOS 11 STIG, Manual de implementación técnica de seguridad (STIG) del macOS 11 de Apple | STIG |
| Instrucción del Comité de Sistemas de Seguridad Nacional (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems | 1253 |

Información adicional:

- Puedes consultar una base de referencia para revisar todas las reglas del proyecto aquí.
- Para obtener más información sobre el proyecto y cómo usarlo, consulta la wiki del proyecto de conformidad de seguridad de macOS.
- Para configurar el proyecto para usarlo, consulta: Familiarizarse con el proyecto de conformidad de seguridad de macOS, parte 1 y Familiarizarse con el proyecto de conformidad de seguridad de macOS, parte 2.
- Si quieres contribuir al desarrollo del proyecto, consulta la guía para colaboradores.

# Historial de versiones del documento

| Fecha | Resumen |
| --- | --- |
| 27 de octubre de 2021 | Temas actualizados:<br>• Certificaciones de seguridad para el procesador Secure Enclave<br>• Certificaciones de seguridad para iOS<br>• Certificaciones de seguridad para macOS |
| 17 de agosto de 2021 | Temas actualizados:<br>• Certificaciones de seguridad para el procesador Secure Enclave<br>• Certificaciones de seguridad para el chip de seguridad T2 de Apple<br>• Certificaciones de seguridad para iOS<br>• Certificaciones de seguridad para iPadOS<br>• Certificaciones de seguridad para macOS<br>• Certificaciones de seguridad para tvOS<br>• Certificaciones de seguridad para watchOS<br>• Certificaciones de seguridad para apps de Apple<br>• Certificaciones de seguridad<br>• Proyecto de conformidad de seguridad de macOS |
| 26 de abril de 2021 | Tema añadido:<br>• Proyecto de conformidad de seguridad de macOS<br>Temas actualizados:<br>• Certificaciones de seguridad para el chip de seguridad T2 de Apple: Nueva certificación FIPS 140-2, 3811.<br>• Certificaciones de seguridad para el procesador Secure Enclave: Nueva certificación FIPS 140-2, 3811, y nueva tabla para certificaciones adicionales.<br>• Certificaciones de seguridad para iOS: Nueva certificación FIPS 140-2, 3811, ID de esquema 11146 para iOS 14 en evaluación.<br>• Certificaciones de seguridad para iPadOS: Nueva certificación FIPS 140-2, 3811, ID de esquema 11147 para iPadOS 14 en evaluación.<br>• Certificaciones de seguridad para macOS: Nueva certificación FIPS 140-2, 3811.<br>• Certificaciones de seguridad para tvOS: Nueva certificación FIPS 140-2, 3811.<br>• Certificaciones de seguridad para watchOS: Nueva certificación FIPS 140-2, 3811.<br>• Certificaciones de seguridad para apps de Apple: Actualizaciones del estado de Common Criteria y una nueva tabla para certificaciones Common Criteria archivadas. |

# Glosario

**Acuerdo de reconocimiento de Common Criteria (CCRA)** Acuerdo de reconocimiento mutuo que establece las políticas y los requisitos para el reconocimiento internacional de los certificados emitidos en virtud de la serie ISO/IEC 15408 o los estándares Common Criteria.

**Apple Business Manager** Un 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** Un 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.

**Cliente VPN IPsec** En un perfil de protección, un cliente que proporciona una conexión IPsec segura entre una plataforma de host física o virtual y una ubicación remota.

**Common Criteria (CC)** Estándar que establece los conceptos y principios generales de la evaluación de la seguridad de TI y especifica un modelo general de evaluación. Incluye catálogos de requisitos de seguridad en un lenguaje estandarizado.

**Comunidad técnica internacional (iTC)** Grupo responsable del desarrollo de perfiles de protección o perfiles de protección colaborativos en virtud del Acuerdo de reconocimiento de Common Criteria (CCRA).

**Corecrypto** Biblioteca que proporciona implementaciones de primitivas criptográficas de bajo nivel. Corecrypto no proporciona directamente interfaces de programación para desarrolladores y se utiliza mediante API proporcionadas a los desarrolladores. El código fuente de Corecrypto está disponible públicamente para permitir la verificación de sus características de seguridad y su correcto funcionamiento.

**Declaración de aplicabilidad** Documento que describe los controles de seguridad implantados en el ámbito de un ISMS, elaborado para respaldar una certificación ISO/IEC 27001.

**Encriptación total del disco (FDE)** Encriptación de todos los datos de un volumen de almacenamiento.

**Estándar federal de procesamiento de información (FIPS)** Publicaciones elaboradas por el Instituto Nacional de Estándares y Tecnología cuando así lo exige la ley o si existen requisitos federales obligatorios de ciberseguridad, o en ambos casos.

**Gestión de dispositivos móviles (MDM)** Un servicio que permite al usuario gestionar de forma remota los dispositivos inscritos. Una vez que se inscribe un dispositivo, el usuario 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.

**Implementación en pruebas (IUT)** Módulo criptográfico que se está sometiendo a pruebas en un laboratorio.

**Instituto Nacional de Estándares y Tecnología (NIST)** Parte del Departamento de Comercio de EE. UU. responsable del desarrollo de la ciencia, los estándares y la tecnología de medición.

**Módulo criptográfico** El hardware, el software y el firmware que proporcionan funciones criptográficas y cumplen los requisitos de un estándar de módulo criptográfico aplicable.

**Módulos en curso (MIP)** Lista elaborada por el Programa de validación de módulos criptográficos (CMVP) de módulos criptográficos que se encuentran actualmente en el proceso de validación del CMVP.

**National Information Assurance Partnership (NIAP)** Organización del gobierno de EE. UU. responsable de dirigir la implementación en EE. UU. del estándar Common Criteria y de gestionar el esquema de evaluación y validación de Common Criteria (CCEVS) de la NIAP.

**Nivel de seguridad (SL)** Los cuatro niveles de seguridad (1 a 4) globales se definen en el estándar ISO/IEC 19790 para describir conjuntos de requisitos de seguridad aplicables. El nivel 4 es el más restrictivo.

**Objetivo de seguridad (ST)** Documento que especifica el problema de seguridad y los requisitos de seguridad de un producto determinado.

**Perfil de protección (PP)** Documento que especifica el problema de seguridad y los requisitos de seguridad de una determinada clase de productos.

**Perfil de protección colaborativo (cPP)** Un perfil de protección desarrollado por una comunidad técnica internacional, un grupo de expertos encargado de la creación de perfiles de protección colaborativos.

**Procesador Secure Enclave (SEP)** Coprocesador integrado en un sistema en un chip (SoC)

**Programa de validación de algoritmos criptográficos (CAVP)** Organización operada por el NIST para proporcionar pruebas de validación de algoritmos criptográficos aprobados (por ejemplo, aprobados por el FIPS y recomendados por el NIST) y sus componentes individuales.

**Programa de validación de módulos criptográficos (CMVP)** Organización operada por los gobiernos de Canadá y EE. UU. para validar el cumplimiento del estándar FIPS 140-3.

**Secure Element (SE)** Chip de silicio integrado en muchos dispositivos Apple que permite funciones como Apple Pay.

**Senior Officials Group Information Systems Security (SOG-IS)** Grupo que gestiona un acuerdo de reconocimiento mutuo entre diversas naciones europeas.

**sepOS** El firmware de Secure Enclave, basado en una versión personalizada por Apple del microkernel L4.

**Servicio de notificaciones push de Apple (APNs)** Servicio ofrecido por Apple a nivel mundial que envía notificaciones push a los dispositivos Apple.

**Sistema de gestión de seguridad de la información (ISMS)** Conjunto de procedimientos y directivas de seguridad de la información que rigen los límites de un programa de seguridad diseñado para proteger un ámbito de información y sistemas mediante la gestión sistemática de la seguridad de la información en todo el ciclo de vida de la información y el sistema.

**Sistema en un chip (SoC)** Circuito integrado que incorpora diversos componentes en un solo chip.

**T2** Chip de seguridad de Apple incluido en algunos ordenadores Mac basados en Intel desde 2017.

Apple
One Apple Park Way
Cupertino, CA 95014
USA
apple.com

E028-00499-B