Centro de cumplimiento y certificaciones de seguridad

Diciembre de 2021

Contenido

Introducción a la garantía de seguridad de Apple

Como parte de nuestro compromiso con la seguridad, Apple se involucra regularmente con organizaciones de terceros con la finalidad de certificar y afirmar la seguridad del hardware, software y los servicios. Estas organizaciones reconocidas a nivel internacional le brindan a Apple certificaciones que se encuentran alineadas con cada lanzamiento de una versión importante del sistema operativo. De esta forma, las certificaciones proporcionan una medida de confianza —es decir, una garantía de seguridad— de que se están satisfaciendo las necesidades de seguridad de un sistema. En el caso de las áreas técnicas que no están contempladas en los acuerdos de reconocimiento mutuo (MRA) o que carecen de estándares de certificación de seguridad afianzados, Apple se compromete con el desarrollo de estándares de seguridad adecuados. Nuestra misión es impulsar una cobertura integral y globalmente aceptada de la certificación de seguridad en todos los hardware, los sistemas operativos, las apps y los servicios de Apple.

Las certificaciones también suelen ser necesarias para cumplir con los requisitos de las normas de la industria, regulativas y legislativas. Servicios como Apple School Manager y Apple Business Manager están cubiertos bajo las certificaciones ISO/IEC 27001 y ISO/IEC 27018 de Apple. Todos los clientes, incluidas las agencias gubernamentales y organizaciones educativas y empresariales que implementan dispositivos Apple, pueden utilizar las certificaciones de hardware, sistema operativo, software y servicios para respaldar la demostración de conformidad de los estándares.

Certificaciones de hardware

Debido a que el software seguro requiere una base de seguridad integrada en el hardware, todos los dispositivos Apple, ya sea que ejecuten iOS, iPadOS, macOS, tvOS o watchOS, tienen funcionalidades de seguridad diseñadas en el propio silicio. Entre ellas se incluye un CPU que impulsa las funcionalidades de seguridad del sistema y un silicio dedicado a las funcionalidades de seguridad. El componente más importante es el coprocesador Secure Enclave, que se encuentra en todos los dispositivos iOS, iPadOS, watchOS y tvOS modernos, así como en las computadoras Mac con Apple Chip y las computadoras Mac basadas en Intel con el chip de seguridad T2 de Apple. El Secure Enclave ofrece una base para la encriptación de datos en reposo, el arranque seguro en macOS y las funcionalidades biométricas.

El compromiso de Apple con la garantía de seguridad comienza con la certificación de los componentes de seguridad fundamentales en el silicio, desde la raíz de confianza del hardware hasta la aplicación del arranque seguro, el Secure Enclave que proporciona almacenamiento seguro para las claves y la autenticación segura mediante Touch ID y Face ID. Las funcionalidades de seguridad de los dispositivos Apple son posibles gracias a la combinación del diseño del silicio, el hardware, el software y los servicios disponibles exclusivamente por parte de Apple. La certificación de estos componentes es una parte crucial para verificar la garantía que brinda Apple.

Para obtener información sobre 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 apps y software

Apple mantiene certificaciones y afirmaciones independientes sobre sus sistemas operativos y apps de conformidad con los Estándares Federales de Procesamiento de la Información (FIPS) 140-2/-3 de EE.UU. para módulos criptográficos, y los estándares de Criterios Comunes para los sistemas operativos, las apps y los servicios de los dispositivos. La cobertura de los sistemas operativos incluye iOS, iPadOS, macOS, sepOS, el firmware del chip T2, tvOS y watchOS. Para las apps, la certificación independiente incluye inicialmente el navegador Safari y la app Contactos, y se cuenta con planes para certificar más apps en el futuro.

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 las apps de Apple

Certificaciones del servicio

Apple mantiene certificaciones de seguridad para ofrecer soporte a nuestros clientes, desde aquellos en ámbitos empresariales hasta los de entornos educativos. Estas certificaciones permiten que los clientes de Apple solventen sus obligaciones contractuales y normativas al usar los servicios de Apple en conjunto con hardware y software de Apple. Estas certificaciones brindan a nuestros clientes una afirmación independiente sobre las prácticas de privacidad, entorno y seguridad de la información de Apple para sus sistemas.

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

- Certificaciones de seguridad de los servicios de Internet de Apple

Si tienes preguntas sobre las certificaciones de seguridad y privacidad de Apple, ponte en contacto 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 de procesamiento de información federal (FIPS, por sus siglas en inglés) 140-2/-3 de EE.UU. para el firmware del chip T2 y de sepOS, así como otras certificaciones. Apple utiliza como base *componentes básicos de certificación* que luego aplica en varias plataformas según sea adecuado. Uno de estos componentes básicos es la validación de la biblioteca Corecrypto, que se utiliza para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo componente es la certificación del Secure Enclave, que está integrado en muchos dispositivos Apple. Un tercer componente es la certificación del Secure Element (SE) que se encuentra en los dispositivos Apple con Touch ID y los dispositivos con Face ID. Estos componentes básicos de certificación de hardware forman una base para certificaciones de seguridad de plataforma más amplias.

Validaciones de los algoritmos criptográficos

La validación de la corrección de la implementación de muchos algoritmos criptográficos y funciones de seguridad relacionadas es un requisito previo para la validación FIPS 140-3 y es una base para otras certificaciones. La validación la administra el Programa de validación de algoritmos criptográficos (CAVP) del Instituto Nacional de Estándares y Tecnología (NIST). Los certificados de validación para las implementaciones de Apple se pueden encontrar utilizando la funcionalidad 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 de forma reiterada mediante el Programa de validación de módulos criptográficos (CMVP) de conformidad con el Estándar de procesamiento de información federal de EE.UU. para módulos criptográficos (FIPS 140-2) para cada lanzamiento importante de sistemas operativos desde 2012. Después de cada lanzamiento importante, Apple envía los módulos al CMVP para su validación de conformidad con el estándar. Además de ser utilizados por los sistemas operativos y las apps de Apple, estos módulos ofrecen funcionalidades criptográficas para los servicios proporcionados por Apple y están disponibles para que los utilicen apps de terceros.

Apple ha obtenido el **nivel de seguridad 1** cada año para los módulos basados en software "Módulo Corecrypto para Intel" y "Módulo Corecrypto Kernel para Intel" para macOS. En el caso de los Apple Chips, los módulos "Corecrypto para ARM" y "Corecrypto Kernel para ARM" se aplican a iOS, iPadOS, tvOS, watchOS y al firmware integrado en el chip de seguridad T2 de Apple en computadoras Mac.

En 2019, Apple logró por primera vez el **nivel de seguridad 2** del estándar FIPS 140-2 para el módulo criptográfico de hardware integrado identificado como "Módulo Corecrypto de Apple: Almacenamiento seguro de claves", lo que permite el uso aprobado por el gobierno de EE.UU. de claves generadas y administradas en el Secure Enclave. Apple sigue esforzándose por conseguir validaciones para el módulo de hardware criptográfico con cada lanzamiento importante de sistema operativo posterior.

El Departamento de comercio de EE.UU. aprobó la validación **FIPS 140-3** en 2019. El cambio más notable en esta versión del estándar es la especificación de los estándares ISO/IEC; en particular el ISO/IEC 19790:2015 y el estándar de pruebas asociado ISO/IEC 24759:2017. El CMVP inició un programa de transición e indicó que a partir de 2020, los módulos criptográficos se empezarán a validar usando FIPS 140-3 como base. Los módulos criptográficos de Apple buscarán cumplir y transicionar a la norma FIPS 140-3 tan pronto como sea practicable.

Para los módulos criptográficos que se encuentran actualmente en los procesos de prueba y validación, el CMVP mantiene dos listas separadas que pueden contener información sobre las validaciones propuestas. Para los módulos criptográficos que están a prueba con un laboratorio acreditado, la lista de implementación bajo prueba (IUT) podría incluir el módulo. Una vez que el laboratorio completa las pruebas y recomienda la validación por parte del CMVP, los módulos criptográficos de Apple aparecen en la lista de módulos en proceso. Actualmente, las pruebas de laboratorio ya se completaron y están a la espera de validación por parte del CMVP. Debido a que la duración del proceso de evaluación puede variar, consulta las dos listas de proceso anteriores para determinar el estado actual de los módulos criptográficos de Apple entre la fecha de lanzamiento de una versión importante del sistema operativo y la emisión del certificado de validación por parte del CMVP.

Certificaciones de productos: Criterios Comunes (ISO/IEC 15408)

Criterios Comunes (ISO/IEC 15408) es un estándar que utilizan muchas organizaciones como base para realizar evaluaciones de seguridad de productos de TI.

Para las certificaciones que podrían reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA) internacional, consulta el portal de Criterios Comunes. Los esquemas de validación nacionales y privados también pueden utilizar el estándar de Criterios Comunes fuera del CCRA. En Europa, el reconocimiento mutuo se rige tanto por el acuerdo SOG-IS como por el CCRA.

El objetivo, según lo declarado por la comunidad de Criterios Comunes, es que un conjunto de estándares de seguridad aprobados internacionalmente proporcione una evaluación clara y confiable de las funcionalidades de seguridad de los productos de tecnologías de la información. Al ofrecer una evaluación independiente de la capacidad de un producto para cumplir con los estándares de seguridad, la Certificación de Criterios Comunes brinda a los clientes más confianza en la seguridad de los productos de tecnologías de la información y conduce a decisiones más informadas.

A través del CCRA, los países que son miembros acordaron reconocer la certificación de los productos de tecnologías de la información con el mismo nivel de confianza. Las evaluaciones necesarias antes de obtener la certificación son extensas e incluyen:

- Perfiles de protección (PP)
- Objetivos de seguridad (ST)
- Requisitos funcionales de seguridad (SFR)
- Requisitos de garantía de seguridad (SAR)
- Niveles de garantía de evaluación (EAL)

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (como Movilidad) y que se utilizan con fines de comparación entre las evaluaciones de los productos de TI dentro de una misma clase. La membresía del CCRA, junto con una lista cada vez más larga de PP aprobados, continúa creciendo anualmente. Este acuerdo permite que un desarrollador de productos busque una certificación única bajo cualquiera de los esquemas de autorización de certificados y que sea reconocida por cualquiera de los signatarios que consumen el certificado.

Los objetivos de seguridad (ST) definen *qué* se evaluará cuando se está certificando un producto de TI. Los ST se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, los cuales se usan para evaluar los ST con más detalle.

Los Criterios Comunes (CC) también incluyen *requisitos de garantía de seguridad*. Una medida que se identifica comúnmente es el *nivel de garantía de evaluación (EAL)*. Los EAL agrupan conjuntos SAR frecuentes y pueden especificarse en los PP y ST para admitir la comparabilidad.

Muchos PP antiguos ya están archivados y se están reemplazando con PP dirigidos que se encuentran en desarrollo y están centrados en soluciones y entornos específicos. En un esfuerzo concertado por garantizar el reconocimiento mutuo continuo de todos los miembros del CCRA, se establecieron las Comunidades Técnicas Internacionales (iTC) con el fin de desarrollar y mantener perfiles de protección colaborativa (cPP) que se desarrollan desde el principio con la participación de esquemas de firma del CCRA. Las partes interesadas adecuadas siguen desarrollando los PP dirigidos a grupos de usuarios y los acuerdos de reconocimiento mutuo que no son el CCRA.

Apple comenzó a buscar certificaciones bajo este CCRA actualizado con PP selectos a partir de principios de 2015. Desde entonces, Apple ha conseguido las certificaciones de Criterios Comunes para cada lanzamiento importante de iOS y ha expandido la cobertura para incluir la garantía de seguridad proporcionada por los nuevos PP.

Apple asume un papel activo dentro de las comunidades técnicas centradas en evaluar las tecnologías de seguridad móvil. Estas incluyen las iTC que son responsables de desarrollar y actualizar los cPP. Apple continúa evaluando y buscando certificaciones para los PP y cPP actuales.

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

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

Certificaciones de seguridad para el procesador Secure Enclave

Antecedentes sobre la certificación del Secure Enclave

El módulo criptográfico de hardware (*Módulo criptográfico de almacenamiento seguro de claves del SEP de Apple*) viene integrado en el SoC de Apple que se encuentra en los siguientes productos: los chips de Apple de la serie A para iPhone y iPad, la serie M para computadoras Mac con Apple Chip, la serie S para Apple Watch y el chip de seguridad de la serie T que se encuentra en las computadoras Mac basadas en Intel a partir de la iMac Pro de 2017.

En 2018, Apple sincronizó la validación de los módulos criptográficos de software con los sistemas operativos lanzados en 2017: iOS 11, macOS 10.13, tvOS 11 y watchOS 4. El módulo criptográfico de hardware del SEP, identificado como el módulo criptográfico de almacenamiento seguro de claves del SEP de Apple 1.0 se validó inicialmente según los requisitos de nivel de seguridad 1 de FIPS 140-2.

En 2019, Apple validó el módulo de hardware según los requisitos de nivel de seguridad 2 de FIPS 140-2 y actualizó el identificador de la versión del módulo a 9.0 para sincronizarlo con las versiones de las validaciones correspondientes de los módulos Corecrypto User y Corecrypto Kernel. En 2019, esto incluyó iOS 12, macOS 10.14, tvOS 12 y watchOS 5.

En 2020 y 2021, Apple está intentando obtener validaciones de conformidad con la norma FIPS 140-3, y con garantía adicional para el nivel de seguridad 3 de los requisitos de seguridad física para los Apple Chips A13, A14, S6 y M1.

Apple también participa activamente en la validación de los módulos Corecrypto User y Corecrypto Kernel para cada versión importante de un sistema operativo. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

Estado de la validación del módulo criptográfico

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Certificaciones de FIPS 140-3

Estado actual

En la siguiente tabla, se muestran los módulos criptográficos de los años 2020 y 2021 que el laboratorio está probando actualmente para verificar su conformidad con FIPS 140-3.

Se completó la prueba de laboratorio del almacenamiento seguro de claves (SKS) asociado con los lanzamientos de sistemas operativos de 2020 y 2021, y el laboratorio los recomendó al CMVP para su validación. Actualmente se incluyen en la lista de módulos en proceso y, una vez que se hayan validado, se pasarán a la lista de módulos criptográficos validados.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de iOS 15 (2021). Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con los lanzamientos de 2021 de iOS, iPadOS, macOS, tvOS y watchOS *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, T2, M1, S3-S6) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con los lanzamientos de 2021 de iOS, iPadOS, macOS, tvOS y watchOS *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware(A13, A14, S6, M1) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con los lanzamientos de 2020 de iOS, iPadOS, macOS, tvOS y watchOS *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, T2, M1, S3-S6) *Nivel de seguridad general:* 2

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con los lanzamientos de 2020 de iOS, iPadOS, macOS, tvOS y watchOS *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware(A13, A14, S6, M1) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente en el laboratorio para verificar su conformidad con FIPS 140-2.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 10.0 de Apple *Sistema operativo:* sepOS para macOS 10.15 Catalina *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS para macOS 10.14 Mojave *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/09/2019	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS para macOS 10.13 High Sierra *Tipo:* Hardware *Nivel de seguridad:* 2

Certificaciones de Criterios Comunes (CC)

Apple participa de forma activa en evaluaciones de Criterios Comunes en las que los perfiles de protección cubren las funcionalidades de seguridad de la tecnología de Apple.

Estado de la certificación de Criterios Comunes (CC)

El esquema de EE.UU., operado por la NIAP, mantiene una lista de productos en evaluación que incluye aquellos que se están evaluando actualmente en los EE.UU. con un laboratorio de pruebas de Criterios Comunes (CCTL) aprobado por la NIAP y que han completado una evaluación inicial (o equivalente) mediante la cual la administración del CCEVS acepta oficialmente el producto para su evaluación.

Después de que certifican los productos, la NIAP enumera las certificaciones actualmente válidas en su lista de productos cumplidores. Después de 2 años, estas certificaciones se revisan para verificar que cumplan con la política de mantenimiento de garantía actual. Una vez vencida la fecha de mantenimiento de la garantía, la NIAP mueve el producto a la lista de productos archivados.

En el portal de Criterios Comunes, se enumeran las certificaciones que pueden reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años; y también mantiene registros para las certificaciones archivadas.

En la tabla de abajo, se muestran las certificaciones que se están evaluando actualmente en un laboratorio o aquellas que ya están certificadas de conformidad con Criterios Comunes.

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: sepOS *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* Secure Enclave de Apple [2020] *Perfiles de protección:* CPP_DSC_V1.0 *Hardware:* Secure Enclave ((A9-A14, M1, T2, S3-S6) *Software:* sepOS distribuido con iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Certificaciones adicionales

En la tabla de abajo, se muestran las certificaciones para el Secure Enclave que no pertenecen a Criterios Comunes ni a los FIPS 140-3.

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

Certificaciones de seguridad para el chip de seguridad T2 de Apple

Antecedentes sobre la validación del módulo criptográfico

Apple participa activamente en la validación de los módulos de hardware y software integrados de Apple para cada versión importante de un sistema operativo. La validación de conformidad sólo se puede realizar con una versión final del lanzamiento del módulo.

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

Además del CPU de Intel, la mayoría de las computadoras Mac desde 2017 también cuentan con un chip de seguridad T2 de Apple, que es un sistema en chip (SoC) basado en Apple Chips. Estas computadoras Mac con chip T2 utilizan los cinco módulos criptográficos para varios servicios en el dispositivo.

- Módulo Corecrypto User para Intel (usado por macOS en computadoras Mac basadas en Intel)
- Módulo Corecrypto Kernel para Intel (usado por macOS en computadoras Mac basadas en Intel)
- Módulo Corecrypto User para ARM (usado por el chip T2)
- Módulo Corecrypto Kernel para ARM (usado por el chip T2)
- Módulo criptográfico de almacenamiento seguro de claves (utilizado por el coprocesador integrado Secure Enclave en el chip T2)

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

Estado de la validación del módulo criptográfico

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.

- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

Certificaciones de FIPS 140-3

Estado actual

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para los módulos de 2020, y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de los módulos de 2021. Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* sepOS para macOS 12 Monterey *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* sepOS para macOS 12 Monterey *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* sepOS para macOS 12 Monterey *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (T2) *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS para macOS 11 Big Sur *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS para macOS 11 Big Sur *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS para macOS 11 Big Sur en Intel *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware *Nivel de seguridad:* 2

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente en el laboratorio para verificar su conformidad con FIPS 140-2.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3856 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 10.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.15 Catalina *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3855 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.15 Catalina *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves de Corecrypto 10.0 de Apple *Sistema operativo:* sepOS para macOS 10.15 Catalina *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 23/04/2019	*Certificados:* 3438 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.14 Mojave *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 11/04/2019	*Certificados:* 3433 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.14 Mojave *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS para macOS 10.14 Mojave *Tipo:* Hardware *Nivel de seguridad:* 2

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018	*Certificados:* 3148 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.13 High Sierra *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018	*Certificados:* 3147 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para ARM de Apple *Sistema operativo:* sepOS para macOS 10.13 High Sierra *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/07/2018	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS para macOS 10.13 High Sierra *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2828 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* sepOS para macOS 10.12 Sierra *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2827 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* sepOS para macOS 10.12 Sierra *Tipo:* Software *Nivel de seguridad:* 1

Certificaciones de seguridad del sistema operativo

Descripción general de las certificaciones de seguridad del sistema operativo de Apple

Apple mantiene certificados de validación de conformidad con el Estándar de procesamiento de información federal (FIPS, por sus siglas en inglés) 140-2/-3 de EE.UU. para el firmware del chip T2 y de sepOS, así como otras certificaciones. Apple utiliza como base *componentes básicos de certificación* que luego aplica en varias plataformas según sea adecuado. Uno de estos componentes básicos es la validación del Corecrypto, que se utiliza para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo componente es la certificación del Secure Enclave, que está integrado en muchos dispositivos Apple. Un tercer componente es la certificación del Secure Element (SE) que se encuentra en los dispositivos Apple con Touch ID y los dispositivos con Face ID. Estos componentes básicos de certificación de hardware forman una base para certificaciones de seguridad de plataforma más amplias.

Validaciones de los algoritmos criptográficos

La validación de la corrección de la implementación de muchos algoritmos criptográficos y funciones de seguridad relacionadas es un requisito previo para la validación FIPS 140-3 y es una base para otras certificaciones. La validación la administra el Programa de validación de algoritmos criptográficos (CAVP) del NIST. Los certificados de validación para las implementaciones de Apple se pueden encontrar utilizando la funcionalidad de búsqueda del CAVP.

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

Los módulos criptográficos en los sistemas operativos de Apple se han validado de forma reiterada mediante el Programa de validación de módulos criptográficos (CMVP) de conformidad con los Estándares Federales de Procesamiento de la Información de EE.UU. (FIPS) 140-2 para cada lanzamiento importante de sistemas operativos desde 2012. Después de cada lanzamiento importante, Apple envía los módulos al CMVP para la validación criptográfica completa. Estos módulos validados proporcionan operaciones criptográficas para los servicios ofrecidos por Apple y están disponibles para su uso por apps de terceros.

Apple ha obtenido el **nivel de seguridad 1** cada año para los módulos basados en software "Módulo Corecrypto para Intel" y "Módulo Corecrypto Kernel para Intel" para macOS. En el caso de los Apple Chips, los módulos "Corecrypto para ARM" y "Corecrypto Kernel para ARM" se aplican a iOS, iPadOS, tvOS, watchOS y al firmware integrado en el chip de seguridad T2 de Apple en computadoras Mac.

En 2019, Apple logró por primera vez el **nivel de seguridad 2** del estándar FIPS 140-2 para el módulo criptográfico de hardware integrado identificado como "Módulo Corecrypto de Apple: Almacenamiento seguro de claves", lo que permite el uso aprobado por el gobierno de EE.UU. de claves generadas y administradas en el Secure Enclave. Apple sigue esforzándose por conseguir validaciones para el módulo de hardware criptográfico con cada lanzamiento importante de sistema operativo posterior.

El Departamento de comercio de EE.UU. aprobó la validación **FIPS 140-3** en 2019. El cambio más notable en esta versión del estándar es la especificación de los estándares ISO/IEC; en particular el ISO/IEC 19790:2015 y el estándar de pruebas asociado ISO/IEC 24759:2017. El CMVP inició un programa de transición e indicó que a partir de 2020, los módulos criptográficos se empezarán a validar usando FIPS 140-3 como base. Los módulos criptográficos de Apple buscarán cumplir y transicionar a la norma FIPS 140-3 tan pronto como sea practicable.

Para los módulos criptográficos que se encuentran actualmente en los procesos de prueba y validación, el CMVP mantiene dos listas separadas que pueden contener información sobre las validaciones propuestas. Para los módulos criptográficos que están a prueba con un laboratorio acreditado, la lista de implementación bajo prueba (IUT) podría incluir el módulo. Una vez que el laboratorio completa las pruebas y recomienda la validación por parte del CMVP, los módulos criptográficos de Apple aparecen en la lista de módulos en proceso. Actualmente, las pruebas de laboratorio ya se completaron y están a la espera de validación por parte del CMVP. Debido a que la duración del proceso de evaluación puede variar, consulta las dos listas de proceso anteriores para determinar el estado actual de los módulos criptográficos de Apple entre la fecha de lanzamiento de una versión importante del sistema operativo y la emisión del certificado de validación por parte del CMVP.

Certificaciones de productos: Criterios Comunes (ISO/IEC 15408)

Criterios Comunes (ISO/IEC 15408) es un estándar que utilizan muchas organizaciones como base para realizar evaluaciones de seguridad de productos de TI.

Para las certificaciones que podrían reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA) internacional, consulta el portal de Criterios Comunes. Los esquemas de validación nacionales y privados también pueden utilizar el estándar de Criterios Comunes fuera del CCRA. En Europa, el reconocimiento mutuo se rige tanto por el acuerdo SOG-IS como por el CCRA.

El objetivo, según lo declarado por la comunidad de Criterios Comunes, es que un conjunto de estándares de seguridad aprobados internacionalmente proporcione una evaluación clara y confiable de las funcionalidades de seguridad de los productos de tecnologías de la información. Al ofrecer una evaluación independiente de la capacidad de un producto para cumplir con los estándares de seguridad, la Certificación de Criterios Comunes brinda a los clientes más confianza en la seguridad de los productos de tecnologías de la información y conduce a decisiones más informadas.

A través del CCRA, los países que son miembros acordaron reconocer la certificación de los productos de tecnologías de la información con el mismo nivel de confianza. Las evaluaciones necesarias antes de obtener la certificación son extensas e incluyen:

- Perfiles de protección (PP)
- Objetivos de seguridad (ST)
- Requisitos funcionales de seguridad (SFR)
- Requisitos de garantía de seguridad (SAR)
- Niveles de garantía de evaluación (EAL)

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (como Movilidad) y que se utilizan con fines de comparación entre las evaluaciones de los productos de TI dentro de una misma clase. La membresía del CCRA, junto con una lista cada vez más larga de PP aprobados, continúa creciendo anualmente. Este acuerdo permite que un desarrollador de productos busque una certificación única bajo cualquiera de los esquemas de autorización de certificados y que sea reconocida por cualquiera de los signatarios que consumen el certificado.

Los objetivos de seguridad (ST) definen *qué* se evaluará cuando se está certificando un producto de TI. Los ST se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, los cuales se usan para evaluar los ST con más detalle.

Los Criterios Comunes (CC) también incluyen *requisitos de garantía de seguridad*. Una medida que se identifica comúnmente es el *nivel de garantía de evaluación (EAL)*. Los EAL agrupan conjuntos SAR frecuentes y pueden especificarse en los PP y ST para admitir la comparabilidad.

Muchos PP antiguos ya están archivados y se están reemplazando con PP dirigidos que se encuentran en desarrollo y están centrados en soluciones y entornos específicos. En un esfuerzo concertado por garantizar el reconocimiento mutuo continuo de todos los miembros del CCRA, se establecieron las Comunidades Técnicas Internacionales (iTC) con el fin de desarrollar y mantener *perfiles de protección colaborativa (cPP)* que se desarrollan desde el principio con la participación de esquemas de firma del CCRA. Las partes interesadas adecuadas siguen desarrollando los PP dirigidos a grupos de usuarios y los acuerdos de reconocimiento mutuo que no son el CCRA.

Apple comenzó a buscar certificaciones bajo este CCRA actualizado con PP selectos a partir de principios de 2015. Desde entonces, Apple ha conseguido las certificaciones de Criterios Comunes para cada lanzamiento importante de iOS y ha expandido la cobertura para incluir la garantía de seguridad proporcionada por los nuevos PP.

Apple asume un papel activo dentro de las comunidades técnicas centradas en evaluar las tecnologías de seguridad móvil. Estas incluyen las iTC que son responsables de desarrollar y actualizar los cPP. Apple continúa evaluando y buscando certificaciones para los PP y cPP actuales.

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

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

Certificaciones de seguridad para iOS

Antecedentes sobre la certificación de iOS

Apple participa activamente en la validación de los módulos de hardware y software integrados de Apple para cada versión importante de un sistema operativo. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

Estado de la validación del módulo criptográfico de iOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Certificaciones de FIPS 140-3

Estado actual

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para iOS 14 (2020), y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de iOS 15 (2021). Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* iOS 15 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* iOS 15 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con iOS 15 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con iOS 15 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A13, A14, A15) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* iOS 14 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* iOS 14 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con iOS 14 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con iOS 14 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A13-A14) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente y los que ya se probaron para verificar su conformidad con FIPS 140-2.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3856 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 10.0 para ARM de Apple *Sistema operativo:* iOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3855 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para ARM de Apple *Sistema operativo:* iOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 10.0 de Apple *Sistema operativo:* sepOS distribuido con iOS 13 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 23/04/2019	*Certificados:* 3438 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para ARM de Apple *Sistema operativo:* iOS 12 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 11/04/2019	*Certificados:* 3433 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para ARM de Apple *Sistema operativo:* iOS 12 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS distribuido con iOS 12 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018	*Certificados:* 3148 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para ARM de Apple *Sistema operativo:* iOS 11 *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018	*Certificados:* 3147 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para ARM de Apple *Sistema operativo:* iOS 11 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/09/2019	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS distribuido con iOS 11 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2828 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* iOS 10 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2827 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* iOS 10 *Tipo:* Software *Nivel de seguridad:* 1

Versiones anteriores

El CMVP enlista los certificados con una antigüedad mayor a 5 años con un estado histórico: Estas versiones anteriores de iOS contaban con validaciones del módulo criptográfico:

- iOS 9 (módulos Corecrypto 6.0)
- iOS 8 (módulos Corecrypto 5.0)
- iOS 7 (módulos Corecrypto 4.0)
- iOS 6 (módulos Corecrypto 3.0)

Antecedentes sobre la certificación de Criterios Comunes (CC)

Apple participa activamente en la evaluación de iOS para cada versión importante del sistema operativo. La evaluación sólo se puede realizar en una versión final del sistema operativo lanzada públicamente. Antes de iPadOS 13.1, iPadOS se llamaba iOS.

Estado de la certificación de Criterios Comunes (CC)

El esquema de EE.UU., operado por la NIAP, mantiene una lista de productos en evaluación que incluye aquellos que se están evaluando actualmente en los EE.UU. con un laboratorio de pruebas de Criterios Comunes (CCTL) aprobado por la NIAP y que han completado una evaluación inicial (o equivalente) mediante la cual la administración del CCEVS acepta oficialmente el producto para su evaluación.

Después de que certifican los productos, la NIAP enumera las certificaciones actualmente válidas en su lista de productos cumplidores. Después de 2 años, estas certificaciones se revisan para verificar que cumplan con la política de mantenimiento de garantía actual. Una vez vencida la fecha de mantenimiento de la garantía, la NIAP mueve el producto a la lista de productos archivados.

El portal de Criterios Comunes enumera las certificaciones que pueden reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años; y también mantiene registros para las certificaciones archivadas.

En la tabla de abajo, se muestran las certificaciones que se están evaluando actualmente en un laboratorio o aquellas que ya están certificadas de conformidad con Criterios Comunes.

Estado actual

Actualmente se están realizando pruebas de laboratorio para las evaluaciones con la NIAP para iOS 15. Para obtener la información más actualizada, consulta las listas de productos en evaluación (NIAP) y de productos cumplidores.

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: iOS 15 *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* —	*Título:* iOS 15 de Apple: iPhone *Perfiles de protección:* Fundamentos de dispositivos móviles (módulos PP por confirmar)
Sistema operativo: iOS 14 *Fecha de certificación:* 01/09/2021	*ID del esquema:* 11146 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 14 de Apple: iPhone *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, Módulo PP de cliente WLAN, EP de Agente MDM
Sistema operativo: iOS 13 *Fecha de certificación:* 06/11/2020	*ID del esquema:* 11036 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 13 de Apple en iPhone *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, EP de clientes WLAN, EP de Agente MDM

Certificaciones archivadas de Criterios Comunes para iOS

Estas versiones anteriores de iOS contaban con validaciones de Criterios Comunes. Estas se encuentran archivadas por la NIAP de acuerdo con su política:

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: iOS 12 *Fecha de certificación:* 14/03/2019	*ID del esquema:* 10937 *Documentos:* Objetivo de seguridad Pautas	*Título:* iPhone con iOS 12 *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, EP de cliente LAN inalámbrico, EP de Agente MDM
Sistema operativo: iOS 11 *Fecha de certificación:* 17/07/2018	*ID del esquema:* 10851 *Documentos:* Objetivo de seguridad Pautas	*Título:* iOS 11 de Apple *Perfiles de protección:* Fundamentos de dispositivos móviles, EP de cliente LAN inalámbrico, EP de Agente MDM
Sistema operativo: iOS 10 *Fecha de certificación:* 27/07/2017	*ID del esquema:* 10782 *Documentos::* Objetivo de seguridad Pautas	*Título:* iOS 10.2 en dispositivos iPhone y iPad *Perfiles de protección:* Fundamentos de dispositivos móviles, EP de cliente LAN inalámbrico, EP de Agente MDM
Sistema operativo: iOS 10 *Fecha de certificación:* 27/07/2017	*ID del esquema:* 10792 *Documentos::* Objetivo de seguridad Pautas	*Título:* Cliente VPN de iOS 10.2 en dispositivos iPhone y iPad *Perfiles de protección:* PP de cliente VPN
Sistema operativo: iOS 9 *Fecha de certificación:* 14/10/2016	*ID del esquema:* 10725 *Documentos::* Objetivo de seguridad Pautas	*Título:* iOS 9.3.2 con Agente MDM *Perfiles de protección:* Fundamentos de dispositivos móviles, EP de Agente MDM
Sistema operativo: iOS 9 *Fecha de certificación:* 13/10/2016	*ID del esquema:* 10714 *Documentos::* Objetivo de seguridad Pautas	*Título:* Cliente VPN de sistema operativo en dispositivos iPhone y iPad *Perfiles de protección:* PP de cliente VPN
Sistema operativo: iOS 9 *Fecha de certificación:* 28/01/2016	*ID del esquema:* 10695 *Documentos::* Objetivo de seguridad Pautas	*Título:* iOS 9 *Perfiles de protección:* Fundamentos de dispositivos móviles

Certificaciones de seguridad para iPadOS

Antecedentes sobre la certificación de iPadOS

Apple participa de forma activa en la validación de sus sistemas operativos para cada lanzamiento importante mediante los perfiles de protección colaborativos adecuados y los niveles de seguridad de la norma FIPS 140-3. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

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

Estado de la validación del módulo criptográfico de iPadOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Certificaciones de FIPS 140-3

Estado actual

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para iPadOS 14 (2020), y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de iPadOS 15 (2021). Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* iPadOS 15 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* iPadOS 15 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con iPadOS 15 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, M1) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con iPadOS 15 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, M1) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* iPadOS 14 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* iPadOS 14 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con iPadOS 14 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, M1) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con iPadOS 14 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A9-A14, M1) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente y los que ya se probaron para verificar su conformidad con FIPS 140-2.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3856 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 10.0 para ARM de Apple *Sistema operativo:* iPadOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3855 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para ARM de Apple *Sistema operativo:* iPadOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves de Corecrypto 10.0 de Apple *Sistema operativo:* sepOS distribuido con iPadOS 13 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 23/04/2019	*Certificados:* 3438 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para ARM de Apple *Sistema operativo:* iOS 12 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 11/04/2019	*Certificados:* 3433 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para ARM de Apple *Sistema operativo:* iOS 12 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS distribuido con iOS 12 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018	*Certificados:* 3148 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para ARM de Apple *Sistema operativo:* iOS 11 *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018	*Certificados:* 3147 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para ARM de Apple *Sistema operativo:* iOS 11 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/09/2019	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS distribuido con iOS 11 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2828 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* iOS 10 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2016 *Fechas de validación:* 01/02/2017	*Certificados:* 2827 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 7.0 de iOS de Apple *Sistema operativo:* iOS 10 *Tipo:* Software *Nivel de seguridad:* 1

Versiones anteriores

El CMVP enlista los certificados con una antigüedad mayor a 5 años con un estado histórico: Estas versiones anteriores de iOS contaban con validaciones del módulo criptográfico:

- iOS 9 (módulos Corecrypto 6.0)
- iOS 8 (módulos Corecrypto 5.0)
- iOS 7 (módulos Corecrypto 4.0)
- iOS 6 (módulos Corecrypto 3.0)

Antecedentes sobre la certificación de Criterios Comunes (CC)

Apple participa activamente en la evaluación de iPadOS para cada versión importante del sistema operativo. La evaluación sólo se puede realizar en una versión final del sistema operativo lanzada públicamente.

Estado de la certificación de Criterios Comunes (CC)

El esquema de EE.UU., operado por la NIAP, mantiene una lista de productos en evaluación que incluye aquellos que se están evaluando actualmente en los EE.UU. con un laboratorio de pruebas de Criterios Comunes (CCTL) aprobado por la NIAP y que han completado una evaluación inicial (o equivalente) mediante la cual la administración del CCEVS acepta oficialmente el producto para su evaluación.

Después de que certifican los productos, la NIAP enumera las certificaciones actualmente válidas en su lista de productos cumplidores. Después de 2 años, estas certificaciones se revisan para verificar que cumplan con la política de mantenimiento de garantía actual. Una vez vencida la fecha de mantenimiento de la garantía, la NIAP mueve el producto a la lista de productos archivados.

El portal de Criterios Comunes enumera las certificaciones que pueden reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años; y también mantiene registros para las certificaciones archivadas.

En la tabla de abajo, se muestran las certificaciones que se están evaluando actualmente en un laboratorio o aquellas que ya están certificadas de conformidad con Criterios Comunes.

Estado actual

Actualmente se están realizando pruebas de laboratorio para las evaluaciones con la NIAP para iPadOS 15. Para obtener la información más actualizada, consulta las listas de productos en evaluación (NIAP) y de productos cumplidores.

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: iPadOS 15 *Fecha de certificación:* 14/03/2019	*ID del esquema:* — *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iPad con iOS 12 *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, EP de cliente LAN inalámbrico, EP de Agente MDM
Sistema operativo: iPadOS 14 *Fecha de certificación:* 01/09/2021	*ID del esquema:* 11147 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iPadOS 14 de Apple: iPad *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, EP de cliente LAN inalámbrico, EP de Agente MDM
Sistema operativo: iPadOS 13 *Fecha de certificación:* 06/11/2020	*ID del esquema:* 11036 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iPadOS 13 en dispositivos móviles iPad *Perfiles de protección:* Fundamentos de dispositivos móviles, Módulo de cliente VPN, EP de cliente LAN inalámbrico, EP de Agente MDM

Versiones anteriores

Estas versiones anteriores de iOS contaban con validaciones de Criterios Comunes. Estas se encuentran archivadas por la NIAP de acuerdo con su política:

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

Certificaciones de seguridad para macOS

Antecedentes sobre la certificación de macOS

Apple participa de forma activa en la validación de sus sistemas operativos para cada lanzamiento importante mediante los perfiles de protección colaborativos adecuados y los niveles de seguridad de la norma FIPS 140-3. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

Estado de la validación del módulo criptográfico de macOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Para las computadoras Mac de Apple, en la siguiente tabla se muestra qué módulos criptográficos son aplicables a qué tecnología Mac.

Módulo criptográfico	Computadoras Mac con Apple Chip	Computadoras Mac con el chip de seguridad T2 de Apple	Computadoras Mac basadas en Intel sin el chip de seguridad T2 de Apple
Espacio de usuario (Apple Chip)	✓		
Kernel (Apple Chip)	✓		
Espacio de usuario (Intel)		✓	✓
Kernel (Intel)		✓	✓
Almacenamiento seguro de claves	✓	✓	

Certificaciones de FIPS 140-3

En 2020, Apple lanzó computadoras Mac que están basadas en Apple Chip. La aplicabilidad de los módulos criptográficos en computadoras basadas en Apple Chip o en Intel se indica en la columna “Información del módulo” de la tabla de abajo.

Nota: los chips de seguridad T2 de Apple se incluyen en muchas computadoras Mac basadas en Intel. 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

Se puede configurar OpenSSH para usar módulos validados por el estándar FIPS 140-3 para algunos algoritmos de FIPS 140-3. Las organizaciones pueden ejecutar un instalador firmado y notariado que está disponible desde Apple con la contraseña *FIPS140Mode*. El instalador coloca dos archivos en la Mac:

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

Después, macOS utiliza estos archivos para limitar los algoritmos criptográficos disponibles para OpenSSH a sólo aquellos que tienen la validación del NIST, lo que garantiza que el cliente OpenSSH use el módulo criptográfico validado y 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 completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para macOS 11 Big Sur, y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de macOS 12 Monterey. Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* macOS 12 Monterey en Apple Chip *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* macOS 12 Monterey en Apple Chip *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* macOS 12 Monterey en Intel *Entorno:* Intel, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* macOS 12 Monterey en Intel *Entorno:* Intel, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* sepOS distribuido con macOS 12 Monterey en Apple Chip, sepOS distribuido con macOS 12 Monterey en Intel con T2 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (M1 y T2) *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12.0 de Apple *Sistema operativo:* sepOS distribuido con macOS 12 Monterey en Apple Chip *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (M1) *Nivel de seguridad:* 2 *Nivel de seguridad física:* 3
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* macOS 11 Big Sur en Intel *Entorno:* Intel, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* macOS 11 Big Sur en Intel *Entorno:* Intel, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* macOS 11 Big Sur en Apple Chip *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* macOS 11 Big Sur en Apple Chip *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con macOS 11 Big Sur en Apple Chip, sepOS distribuido con macOS 11 Big Sur en Intel *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (M1) *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con macOS 11 Big Sur en Apple Chip *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (M1) *Nivel de seguridad:* 2 *Nivel de seguridad física:* 3

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente y los que ya se probaron para verificar su conformidad con FIPS 140-2.

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para macOS 10.15 Catalina, y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Nota: los chips de seguridad T2 de Apple se incluyen en muchas computadoras Mac basadas en Intel. 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 *Fechas de validación:* 24/03/2021	*Certificados:* 3859 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User Space para Intel de Apple (ccv10) *Sistema operativo:* macOS 10.15 Catalina *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 24/03/2021	*Certificados:* 3858 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para Intel de Apple (ccv10) *Sistema operativo:* macOS 10.15 Catalina *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 12/04/2019	*Certificados:* 3402 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para Intel de Apple *Sistema operativo:* macOS 10.14 Mojave *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 12/04/2019	*Certificados:* 3431 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para Intel de Apple *Sistema operativo:* macOS 10.14 Mojave *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 22/03/2018	*Certificados:* 3155 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para Intel de Apple *Sistema operativo:* macOS 10.13 High Sierra *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 22/03/2018	*Certificados:* 3156 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para Intel de Apple *Sistema operativo:* macOS 10.13 High Sierra *Tipo:* Software *Nivel de seguridad:* 1

Versiones anteriores

Estas versiones anteriores de OS X y macOS contaban con validaciones del módulo criptográfico. El CMVP enlista aquellas con una antigüedad mayor de 5 años con un estado histórico:

- 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

Antecedentes sobre la certificación de Criterios Comunes (CC)

Apple participa activamente en la evaluación de macOS para cada versión importante del sistema operativo. La evaluación sólo se puede realizar en una versión final del sistema operativo lanzada públicamente.

Estado de la certificación de Criterios Comunes (CC)

El esquema de EE.UU., operado por la NIAP, mantiene una lista de productos en evaluación que incluye aquellos que se están evaluando actualmente en los EE.UU. con un laboratorio de pruebas de Criterios Comunes (CCTL) aprobado por la NIAP y que han completado una evaluación inicial (o equivalente) mediante la cual la administración del CCEVS acepta oficialmente el producto para su evaluación.

Después de que certifican los productos, la NIAP enumera las certificaciones actualmente válidas en su lista de productos cumplidores. Después de 2 años, estas certificaciones se revisan para verificar que cumplan con la política de mantenimiento de garantía actual. Una vez vencida la fecha de mantenimiento de la garantía, la NIAP mueve el producto a la lista de productos archivados.

El portal de Criterios Comunes enumera las certificaciones que pueden reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años; y también mantiene registros para las certificaciones archivadas.

En la tabla de abajo, se muestran las certificaciones que se están evaluando actualmente en un laboratorio o aquellas que ya están certificadas de conformidad con Criterios Comunes.

Estado actual

Actualmente se están realizando evaluaciones con la NIAP para macOS 11 y macOS 12 utilizando el sistema operativo de propósito general y los perfiles de protección de encriptación de disco completo (FDE) (AA y EE).

Para obtener la información más actualizada, consulta las listas de productos en evaluación (NIAP) y de productos cumplidores.

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: macOS 12 Monterey *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* —	*Título:* FileVault 2 de Apple con macOS 12 Monterey *Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (módulos PP por confirmar)
Sistema operativo: macOS 12 Monterey *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* —	*Título:* macOS 12 Monterey *Perfiles de protección:* PP_OS_V4.21 (módulos PP por confirmar)
Sistema operativo: macOS 11 Big Sur *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* FileVault 2 de Apple con macOS 11 Big Sur *Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Sistema operativo: macOS 11 Big Sur *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* macOS 11 Big Sur de Apple *Perfiles de protección:* PP_OS_V4.21
Sistema operativo: macOS 10.15 Catalina *Fecha de certificación:* 29/04/2021	*ID del esquema:* 11078 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* FileVault 2 de Apple en computadoras T2 con macOS 10.15 Catalina *Perfiles de protección:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: macOS 10.15 Catalina *Fecha de certificación:* 23/09/2020	*ID del esquema:* 11077 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* macOS 10.15 Catalina *Perfiles de protección:* PP_OS_V4.21

Certificaciones de seguridad para tvOS

Antecedentes sobre la certificación de tvOS

Apple participa de forma activa en la validación de los módulos criptográficos asociados con cada versión importante del sistema tvOS. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

Estado de la validación del módulo criptográfico de tvOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Certificaciones de FIPS 140-3

Estado actual

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para tvOS 14 (2020), y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de tvOS 15 (2021). Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* tvOS 15 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* tvOS 15 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con tvOS 15 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A10, A12) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* tvOS 14 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* tvOS 14 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con tvOS 14 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (A10, A12) *Nivel de seguridad general:* 2

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente y los que ya se probaron para verificar su conformidad con FIPS 140-2.

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para tvOS 13 (2019), y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3856 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 10.0 para ARM de Apple *Sistema operativo:* tvOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 23/03/2021	*Certificados:* 3855 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para ARM de Apple *Sistema operativo:* tvOS 13 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 10.0 de Apple *Sistema operativo:* sepOS distribuido con tvOS 13 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 23/04/2019	*Certificados:* 3438 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para ARM de Apple *Sistema operativo:* tvOS 12 *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 11/04/2019	*Certificados:* 3433 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para ARM de Apple *Sistema operativo:* tvOS 12 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS distribuido con tvOS 12 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018	*Certificados:* 3148 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para ARM de Apple *Sistema operativo:* tvOS 11 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018	*Certificados:* 3147 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para ARM de Apple *Sistema operativo:* tvOS 11 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/09/2019	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS distribuido con tvOS 11 *Tipo:* Hardware *Nivel de seguridad:* 2

Certificaciones de seguridad para watchOS

Antecedentes sobre la certificación de watchOS

Apple participa de forma activa en la validación de los módulos criptográficos asociados con cada versión importante del sistema watchOS. La validación de conformidad sólo se puede realizar con una versión final ya publicada.

Estado de la validación del módulo criptográfico de watchOS

El Programa de validación de módulos criptográficos (CMVP) mantiene el estado de la validación de los módulos criptográficos en tres listas separadas según su estado actual:

- Para aparecer en la lista de implementación bajo prueba del CMVP, el laboratorio debe estar bajo contrato de Apple para realizar las pruebas.
- Después de que el laboratorio haya completado la prueba, el CMVP haya recomendado su validación y se hayan pagado las cuotas del CMVP, el módulo se agrega a la lista de módulos en proceso (MIP). La lista MIP monitorea el progreso de los esfuerzos de validación de CMVP en cuatro fases:
  - *Revisión pendiente:* en espera a que se asignen recursos por parte del CMVP.
  - *En revisión:* los recursos del CMVP están realizando sus actividades de validación.
  - *Coordinación:* el laboratorio y el CMVP están resolviendo cualquier problema que se haya encontrado.
  - *Finalización:* las actividades y formalidades relacionadas con la emisión del certificado.
- Después de la validación por parte del CMVP, los módulos reciben un certificado de conformidad y se agregan a la lista de módulos criptográficos validados, la cual incluye:
  - Módulos validados que se marcan como activos.
  - Después de cinco años, los módulos se marcan como históricos.
  - Si el certificado del módulo se revoca por algún motivo, se marca como revocado.

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

Certificaciones de FIPS 140-3

Estado actual

Se completó la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario para watchOS 7 (2020), y el laboratorio los recomendó al CMVP para su validación. Se encuentran en la lista de módulos en proceso.

Actualmente se está realizando la prueba de laboratorio del espacio del kernel, el almacenamiento seguro de claves y el espacio de usuario de watchOS 8 (2021). Se encuentran en la lista de implementación bajo prueba.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* watchOS 8 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* watchOS 8 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con watchOS 8 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (S3, S4, S5, S6) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2021 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 12 de Apple *Sistema operativo:* sepOS distribuido con watchOS 8 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (S6) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* watchOS 7 *Entorno:* Apple Chip, Usuario, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* watchOS 7 *Entorno:* Apple Chip, Kernel, Software *Tipo:* Software *Nivel de seguridad general:* 1
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con watchOS 7 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (S3, S4, S5, S6) *Nivel de seguridad general:* 2
Fecha de lanzamiento del sistema operativo: 2020 *Fechas de validación:* —	*Certificados:* Aún no se certifica *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto 11.1 de Apple *Sistema operativo:* sepOS distribuido con watchOS 7 *Entorno:* Apple Chip, Almacenamiento seguro de claves, Hardware *Tipo:* Hardware (S6) *Nivel de seguridad general:* 2 *Nivel de seguridad física:* 3

Certificaciones de FIPS 140-2

En la siguiente tabla, se muestran los módulos criptográficos que se están probando actualmente y los que ya se probaron para verificar su conformidad con FIPS 140-2.

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* —	*Certificados:* 3856 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 10.0 para ARM de Apple *Sistema operativo:* watchOS 6 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* —	*Certificados:* 3855 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 10.0 para ARM de Apple *Sistema operativo:* watchOS 6 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2019 *Fechas de validación:* 05/02/2021	*Certificados:* 3811 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 10.0 de Apple *Sistema operativo:* sepOS distribuido con watchOS 6 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 23/04/2019	*Certificados:* 3438 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 9.0 para ARM de Apple *Sistema operativo:* watchOS 5 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 11/04/2019	*Certificados:* 3433 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 9.0 para ARM de Apple *Sistema operativo:* watchOS 5 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2018 *Fechas de validación:* 10/09/2019	*Certificados:* 3523 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 9.0 de Apple *Sistema operativo:* sepOS distribuido con watchOS 5 *Tipo:* Hardware *Nivel de seguridad:* 2
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 22/05/2018, 06/07/2018	*Certificados:* 3148 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto User 8.0 para ARM de Apple *Sistema operativo:* watchOS 4 *Tipo:* Software *Nivel de seguridad:* 1

Fechas	Certificados/Documentos	Información del módulo
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 09/03/2018, 17/05/2018, 03/07/2018	*Certificados:* 3147 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo Corecrypto Kernel 8.0 para ARM de Apple *Sistema operativo:* watchOS 4 *Tipo:* Software *Nivel de seguridad:* 1
Fecha de lanzamiento del sistema operativo: 2017 *Fechas de validación:* 10/09/2019	*Certificados:* 3223 *Documentos:* Certificado Política de seguridad Pautas para el criptocustodio	*Título:* Módulo criptográfico de almacenamiento seguro de claves 1.0 de Apple *Sistema operativo:* sepOS distribuido con watchOS 4 *Tipo:* Hardware *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 de procesamiento de información federal (FIPS, por sus siglas en inglés) 140-2/-3 de EE.UU. para el firmware del chip T2 y de sepOS, así como otras certificaciones. Apple utiliza como base *componentes básicos de certificación* que luego aplica en varias plataformas según sea adecuado. Uno de estos componentes básicos es la validación del Corecrypto, que se utiliza para las implementaciones de módulos criptográficos de software y hardware dentro de los sistemas operativos desarrollados por Apple. Un segundo componente es la certificación del Secure Enclave, que está integrado en muchos dispositivos Apple. Un tercer componente es la certificación del Secure Element (SE) que se encuentra en los dispositivos Apple con Touch ID y los dispositivos con Face ID. Estos componentes básicos de certificación de hardware forman una base para certificaciones de seguridad de plataforma más amplias.

Certificaciones de productos: Criterios Comunes (ISO/IEC 15408)

Criterios Comunes (ISO/IEC 15408) es un estándar que utilizan muchas organizaciones como base para realizar evaluaciones de seguridad de productos de TI.

Para las certificaciones que podrían reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA) internacional, consulta el portal de Criterios Comunes. Los esquemas de validación nacionales y privados también pueden utilizar el estándar de Criterios Comunes fuera del CCRA. En Europa, el reconocimiento mutuo se rige tanto por el acuerdo SOG-IS como por el CCRA.

El objetivo, según lo declarado por la comunidad de Criterios Comunes, es que un conjunto de estándares de seguridad aprobados internacionalmente proporcione una evaluación clara y confiable de las funcionalidades de seguridad de los productos de tecnologías de la información. Al ofrecer una evaluación independiente de la capacidad de un producto para cumplir con los estándares de seguridad, la Certificación de Criterios Comunes brinda a los clientes más confianza en la seguridad de los productos de tecnologías de la información y conduce a decisiones más informadas.

A través del CCRA, los países que son miembros acordaron reconocer la certificación de los productos de tecnologías de la información con el mismo nivel de confianza. Las evaluaciones necesarias antes de obtener la certificación son extensas e incluyen:

- Perfiles de protección (PP)
- Objetivos de seguridad (ST)
- Requisitos funcionales de seguridad (SFR)
- Requisitos de garantía de seguridad (SAR)
- Niveles de garantía de evaluación (EAL)

Los perfiles de protección (PP) son documentos que especifican los requisitos de seguridad para una clase de tipos de dispositivos (como Movilidad) y que se utilizan con fines de comparación entre las evaluaciones de los productos de TI dentro de una misma clase. La membresía del CCRA, junto con una lista cada vez más larga de PP aprobados, continúa creciendo anualmente. Este acuerdo permite que un desarrollador de productos busque una certificación única bajo cualquiera de los esquemas de autorización de certificados y que sea reconocida por cualquiera de los signatarios que consumen el certificado.

Los objetivos de seguridad (ST) definen *qué* se evaluará cuando se está certificando un producto de TI. Los ST se traducen en *requisitos funcionales de seguridad (SFR)* más específicos, los cuales se usan para evaluar los ST con más detalle.

Los Criterios Comunes (CC) también incluyen *requisitos de garantía de seguridad*. Una medida que se identifica comúnmente es el *nivel de garantía de evaluación (EAL)*. Los EAL agrupan conjuntos SAR frecuentes y pueden especificarse en los PP y ST para admitir la comparabilidad.

Muchos PP antiguos ya están archivados y se están reemplazando con PP dirigidos que se encuentran en desarrollo y están centrados en soluciones y entornos específicos. En un esfuerzo concertado por garantizar el reconocimiento mutuo continuo de todos los miembros del CCRA, se establecieron las Comunidades Técnicas Internacionales (iTC) con el fin de desarrollar y mantener perfiles de protección colaborativa (cPP) que se desarrollan desde el principio con la participación de esquemas de firma del CCRA. Las partes interesadas adecuadas siguen desarrollando los PP dirigidos a grupos de usuarios y los acuerdos de reconocimiento mutuo que no son el CCRA.

Apple comenzó a buscar certificaciones bajo este CCRA actualizado con PP selectos a partir de principios de 2015. Desde entonces, Apple ha conseguido las certificaciones de Criterios Comunes para cada lanzamiento importante de iOS y ha expandido la cobertura para incluir la garantía de seguridad proporcionada por los nuevos PP.

Apple asume un papel activo dentro de las comunidades técnicas centradas en evaluar las tecnologías de seguridad móvil. Estas incluyen las iTC que son responsables de desarrollar y actualizar los cPP. Apple continúa evaluando y buscando certificaciones para los PP y cPP actuales.

Las certificaciones de la plataforma de Apple para el mercado norteamericano generalmente se realizan con la Asociación nacional de la garantía de la información (NIAP) que mantiene una lista de proyectos actualmente en evaluación pero aún no certificados.

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

Certificaciones de seguridad para las apps de Apple

Antecedentes sobre la certificación de apps de Apple

Apple participa activamente en las certificaciones de seguridad de sus apps mediante los perfiles de protección (PP) de Criterios Comunes adecuados. Estas evaluaciones se basan en las certificaciones de hardware y sistema operativo que Apple ha obtenido.

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

Estado de la certificación del módulo criptográfico

Las apps de Apple indicadas aquí utilizan los módulos criptográficos para el sistema operativo aplicable. 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 de Criterios Comunes (CC)

El esquema de EE.UU., operado por la NIAP, mantiene una lista de productos en evaluación que incluye aquellos que se están evaluando actualmente en los EE.UU. con un laboratorio de pruebas de Criterios Comunes (CCTL) aprobado por la NIAP y que han completado una evaluación inicial (o equivalente) mediante la cual la administración del CCEVS acepta oficialmente el producto para su evaluación.

Después de que certifican los productos, la NIAP enumera las certificaciones actualmente válidas en su lista de productos cumplidores. Después de 2 años, estas certificaciones se revisan para verificar que cumplan con la política de mantenimiento de garantía actual. Una vez vencida la fecha de mantenimiento de la garantía, la NIAP mueve el producto a la lista de productos archivados.

En el portal de Criterios Comunes, se enumeran las certificaciones que pueden reconocerse mutuamente bajo el Acuerdo de Reconocimiento de Criterios Comunes (CCRA). El portal de CC puede mantener productos en la lista de productos certificados durante 5 años; y también mantiene registros para las certificaciones archivadas.

En la tabla de abajo, se muestran las certificaciones que se están evaluando actualmente en un laboratorio o aquellas que ya están certificadas de conformidad con Criterios Comunes.

Estado actual

- Las evaluaciones con la NIAP que se publican indicando que están en curso se enumeran en la lista de productos en evaluación (NIAP).
- Las evaluaciones que ya se han completado y están validadas se enumeran en la lista de productos cumplidores de la NIAP.

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: macOS 11 Big Sur *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* macOS 11 Big Sur: Contactos *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: macOS 11 Big Sur *Fecha de certificación:* —	*ID del esquema:* Aún no se certifica *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* macOS 11 Big Sur: Safari *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: iOS 14, iPadOS 14 *Fecha de certificación:* 20/08/2021	*ID del esquema:* 11191 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 14 y iPadOS 14 de Apple: Contactos *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: iOS 14, iPadOS 14 *Fecha de certificación:* —	*ID del esquema:* 11192 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 14 y iPadOS 14 de Apple: Safari *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: iOS 13, iPadOS 13 *Fecha de certificación:* 05/06/2020	*ID del esquema:* 11060 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 13 y iPadOS 13 de Apple: Safari *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: iOS 13, iPadOS 13 *Fecha de certificación:* 05/06/2020	*ID del esquema:* 11050 *Documentos:* Certificado Objetivo de seguridad Pautas Reporte de validación Reporte de actividad de garantía	*Título:* iOS 13 y iPadOS 13 de Apple: Contactos *Perfiles de protección:* PP para SW de aplicaciones

Certificaciones archivadas de Criterios Comunes para las apps de Apple

Sistema operativo/Fecha de certificación	ID del esquema/Documentos	Título/Perfiles de protección
Sistema operativo: iOS 12 *Fecha de certificación:* 12/06/2019	*ID del esquema:* 10960 *Documentos:* Objetivo de seguridad Pautas	*Título:* Safari para iOS 12 *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: iOS 12 *Fecha de certificación:* 28/02/2019	*ID del esquema:* 10961 *Documentos:* Objetivo de seguridad Pautas	*Título:* Contactos para iOS 12 *Perfiles de protección:* PP para SW de aplicaciones
Sistema operativo: iOS 11 *Fecha de certificación:* 09/11/2018	*ID del esquema:* 10916 *Documentos:* Objetivo de seguridad Pautas	*Título:* Safari para iOS 11 *Perfiles de protección:* PP para SW de aplicaciones; EP para navegadores web
Sistema operativo: iOS 11 *Fecha de certificación:* 13/09/2018	*ID del esquema:* 10915 *Documentos:* Objetivo de seguridad Pautas	*Título:* Contactos para iOS 11 *Perfiles de protección:* PP para SW de aplicaciones

Certificaciones de seguridad de los servicios de Internet de Apple

Apple mantiene certificaciones de conformidad con los estándares ISO/IEC 27001 y 27018 para permitir que los clientes de Apple cumplan con sus obligaciones regulatorias y contractuales. Estas certificaciones brindan a nuestros clientes una afirmación independiente sobre las prácticas de privacidad y seguridad de la información de Apple para sistemas incluidos.

ISO/IEC 27001 e ISO/IEC 27018 son parte de una familia de estándares del Sistema de administración 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 incluyen en la Declaración de aplicabilidad como se define en los estándares ISO/IEC 27001 e ISO/IEC 27018. Apple se somete a una afirmación independiente por parte de un registrador acreditado cada año.

ISO/IEC 27001

ISO/IEC 27001 es un estándar del sistema de administración de seguridad de la información que especifica los requisitos necesarios para establecer, implementar, mantener y mejorar de forma continua este sistema en una organización. El estándar ISO/IEC 27001 incluye los siguientes dominios de seguridad cubiertos por las certificaciones de ISO/IEC de Apple:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Administración de componentes
- Seguridad de recursos humanos
- Seguridad física y del entorno
- Administración de operaciones y comunicaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de la información
- Administración de incidentes de seguridad de la información
- Administración de la continuidad de negocio
- Cumplimiento

ISO/IEC 27018

El estándar ISO/IEC 27018 es un código de prácticas para la protección de la información de identificación personal (PII) en entornos de nube públicos. El estándar ISO/IEC 27018 incluye los siguientes dominios de seguridad cubiertos por las certificaciones de ISO/IEC de Apple:

- Consentimiento y elección
- Especificación y legitimidad del propósito
- Limitación de la recolección
- Minimización de los datos
- Limitación del uso, retención y divulgación
- Precisión y calidad
- Apertura, transparencia y avisos
- Acceso y participación individual
- Responsabilidad
- Seguridad de la información
- Cumplimiento relacionado con la privacidad

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

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

- 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
- Apple ID administrados
- Tareas Escolares
- Siri

Certificaciones

Los comprobantes de las certificaciones ISO/IEC 27001 y 27018 de Apple están disponibles en nuestro registro.

Para consultar las certificaciones de Apple, ve a la sección de búsqueda del directorio de clientes y certificados del sitio web del Instituto de Estándares Británicos (BSI), ingresa “Apple” en el campo de búsqueda Empresa, haz clic en Buscar y luego selecciona los resultados de búsqueda para ver los certificados.

Nota: la información sobre productos no fabricados por Apple, o sitios web independientes no controlados ni probados por Apple, se proporciona sin recomendación ni aprobación. Apple no asume responsabilidad con respecto a la selección, el rendimiento o el uso de sitios web o productos de terceros. Apple no realiza ninguna declaración sobre la precisión o fiabilidad de los sitios web de terceros. Ponte en contacto con el proveedor para obtener más información.

Proyecto de cumplimiento de seguridad de macOS

El proyecto de cumplimiento de seguridad de macOS (mSCP) es un esfuerzo de código abierto que tiene la finalidad de proporcionar un enfoque programático a la generación de pautas de seguridad. Se trata de un proyecto conjunto del personal de seguridad de TI operativa federal del 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). El proyecto utiliza un conjunto de controles probados y validados para macOS y los asigna a cualquier pauta de seguridad compatible con el proyecto. Además, este proyecto se puede utilizar como un recurso para crear fácilmente líneas de base para la seguridad personalizada de los controles seguridad técnica, haciendo uso de una biblioteca de operaciones atómicas (parámetros de configuración) probadas y validadas. El proyecto genera documentación, scripts, perfiles de configuración personalizados y una lista de verificación de auditoría basada en la línea de base utilizada.

El mSCP puede generar contenido de salida que puede usarse junto con herramientas de administración y seguridad para lograr el cumplimiento. Los parámetros de configuración de este proyecto admiten las siguientes líneas de base para las pautas:

Organización	Líneas de base compatibles
Publicación especial (SP) 800-53 del Instituto Nacional de Estándares y Tecnología (NIST): Controles de seguridad recomendados para organizaciones y sistemas de información federales (revisión 5)	Alta: 800-53; moderada: 800-53; baja: 800-53
Publicación especial (SP) 800-171 del Instituto Nacional de Estándares y Tecnología (NIST): Protección de la información no clasificada y controlada en organizaciones y sistemas no federales (revisión 2)	800-171
Guía de implementación técnica de seguridad (STIG) de macOS 11 de la Agencia de Sistemas de Información de Defensa (DISA), Guía de implementación técnica de seguridad de macOS 11 de Apple	Guía de implementación técnica de seguridad
Instrucción 1253 del Comité de Sistemas de Seguridad Nacional (CNSSI): Categorización de seguridad y selección de controles para sistemas de seguridad nacional	1253

Información adicional:

- En este enlace puedes consultar una línea base para revisar todas las reglas del proyecto.
- Para obtener más información sobre el proyecto y el uso, consulta la wiki del Proyecto de cumplimiento de seguridad de macOS
- Para configurar el proyecto para su uso, consulta: Introducción al Proyecto de cumplimiento de seguridad de macOS (parte 1) e Introducción al Proyecto de cumplimiento de seguridad de macOS (parte 2).
- Si te interesa apoyar el desarrollo del proyecto, consulta las pautas para contribuyentes.

Historial de revisiones del documento

Fecha	Resumen
27 de octubre de 2021	Temas actualizados: • Certificaciones de seguridad para el procesador Secure Enclave • Certificaciones de seguridad para iOS • Certificaciones de seguridad para macOS
17 de agosto de 2021	Temas actualizados: • Certificaciones de seguridad para el procesador Secure Enclave • Certificaciones de seguridad para el chip de seguridad T2 de Apple • 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 • Certificaciones de seguridad para las apps de Apple • Certificaciones de seguridad • Proyecto de cumplimiento de seguridad de macOS
26 de abril de 2021	Tema agregado: • Proyecto de cumplimiento de seguridad de macOS Temas actualizados: • Certificaciones de seguridad para el chip de seguridad T2 de Apple: información sobre la nueva certificación de FIPS 140-2 (3811) • Certificaciones de seguridad para el procesador Secure Enclave: información sobre la nueva certificación de FIPS 140-2 (3811) y una tabla nueva para las certificaciones adicionales. • Certificaciones de seguridad para iOS: información sobre las nuevas certificaciones de FIPS 140-2 (3811) y el ID del esquema de iOS 14 (11146) en proceso de evaluación • Certificaciones de seguridad para iPadOS: información sobre las nuevas certificaciones de FIPS 140-2 (3811) y el ID del esquema de iPadOS 14 (11147) en proceso de evaluación • Certificaciones de seguridad para macOS: información sobre la nueva certificación de FIPS 140-2 (3811). • Certificaciones de seguridad para tvOS: información sobre las nuevas certificaciones de FIPS 140-2 (3811). • Certificaciones de seguridad para watchOS: información sobre las nuevas certificaciones de FIPS 140-2 (3811). • Certificaciones de seguridad para las apps de Apple: actualizaciones sobre el estado de Criterios Comunes y una tabla nueva para las certificaciones archivadas de Criterios Comunes.

Glosario

Acuerdo de Reconocimiento de Criterios Comunes (CCRA) Acuerdo de reconocimiento mutuo que establece las políticas y requisitos para el reconocimiento internacional de los certificados emitidos de acuerdo con los estándares de Criterios Comunes o la serie de normas ISO/IEC 15408.

Administración de dispositivos móviles (MDM) Servicio que le permite al usuario administrar dispositivos inscritos de forma remota. Una vez que se inscribe un dispositivo, el usuario puede usar el servicio de MDM a través de la red para configurarlo y realizar otras tareas sin la interacción del usuario.

Apple Business Manager Portal basado en la web para administradores de TI que proporciona una forma rápida y optimizada de implementar dispositivos Apple que una organización haya comprado directamente de Apple o de un distribuidor o proveedor autorizado de Apple participante. Las organizaciones pueden inscribir automáticamente dispositivos en la administración de dispositivos móviles (MDM) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

Apple School Manager Portal basado en la web para administradores de TI que proporciona una forma rápida y optimizada de implementar dispositivos Apple que una organización haya comprado directamente de Apple o de un distribuidor o proveedor autorizado de Apple participante. Las organizaciones pueden inscribir automáticamente dispositivos en la administración de dispositivos móviles (MDM) sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban.

Asociación nacional de la garantía de la información (NIAP) Organización del gobierno de EE.UU. responsable de operar la implementación en EE.UU. del estándar Criterios Comunes y de administrar el Esquema de validación y evaluación de Criterios Comunes (CCEVS) de la NIAP.

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

Comunidad Técnica Internacional (iTC) Grupo responsable de desarrollar perfiles de protección o perfiles de protección colaborativos bajo el patrocinio del Acuerdo de Reconocimiento de Criterios Comunes (CCRA).

Corecrypto Biblioteca que ofrece implementaciones de primitivas criptográficas de bajo nivel. Toma en cuenta que Corecrypto no proporciona directamente interfaces de programación para desarrolladores y se utiliza a través de las API proporcionadas a los desarrolladores. El código fuente de Corecrypto está disponible de forma pública para permitir la verificación de sus características de seguridad y su correcto funcionamiento.

Criterios Comunes (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.

Declaración de aplicabilidad (SOA) Documento que describe los controles de seguridad implementados en el alcance de un ISMS, producido con el apoyo de una certificación ISO/IEC 27001.

Encriptación de disco completo (FDE) Encriptación de todos los datos en un volumen de almacenamiento.

Estándar federal de procesamiento de la información (FIPS) Publicaciones desarrolladas por el Instituto Nacional de Estándares y Tecnología, ya sea cuando lo requiera la ley o cuando existan requisitos obligatorios del gobierno federal para la seguridad cibernética, o ambos.

Implementación bajo prueba (IUT) Módulo criptográfico bajo prueba por parte de un laboratorio.

Instituto Nacional de Estándares y Tecnología (NIST) Parte del Departamento de Comercio de EE.UU. responsable de los avances en tecnología, estándares y metrología.

Módulo criptográfico Hardware, software y/o firmware que proporcionan funciones criptográficas y cumplen con los requisitos de un estándar de módulo criptográfico establecido.

Módulos en proceso (MIP) Lista gestionada por el Programa de validación de módulos criptográficos (CMVP) de los módulos criptográficos que están actualmente en el proceso de validación del CMVP.

Nivel de seguridad (SL) Los cuatro niveles de seguridad generales (1–4) que se definen en ISO/IEC 19790 y que describen los conjuntos de requisitos de seguridad aplicables. El nivel 4 es el más riguroso.

Objetivo de seguridad (ST) Documento que especifica el problema de seguridad y los requisitos de seguridad para un producto en particular.

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

Perfil de protección colaborativa (cPP) Perfil de protección desarrollado por una Comunidad técnica internacional, que es un grupo de expertos encargados de la creación de cPP.

Procesador Secure Enclave (SEP) Coprocesador fabricado dentro de un sistema en 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 EE.UU. y Canadá que tiene el fin de validar la conformidad con el estándar FIPS 140-3.

Secure Element (SE) Apple Chip integrado en muchos dispositivos Apple que soporta funcionalidades tales como Apple Pay.

Seguridad de los sistemas de información del grupo de altos funcionarios (SOG-IS) Grupo que administra un acuerdo de reconocimiento mutuo entre varias naciones europeas.

sepOS Firmware del Secure Enclave basado en una versión personalizada de 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 administración de seguridad de la información (ISMS) Conjunto de políticas y procedimientos de seguridad de la información que gobiernan los límites de un programa de seguridad diseñado para proteger un alcance de información y sistemas mediante la administración sistemática de la seguridad de la información a lo largo de la información o el ciclo de vida del sistema.

Sistema en chip (SoC) Circuito integrado (IC) que incorpora varios componentes en un solo chip.

T2 Chip de seguridad de Apple incluido en algunas computadoras Mac basadas en Intel desde 2017.

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

LA028-00499-B