Apple at Work

Seguridad de la plataforma

Diseñados para ser seguros.

En Apple nos tomamos muy en serio la seguridad de los usuarios y los datos corporativos. Nuestros productos están diseñados pensando en la seguridad desde el minuto uno, todo sin interferir en la experiencia del usuario y dándole libertad absoluta para trabajar como quiera. Solo Apple puede ofrecer este nivel de protección, ya que el hardware, el software y los servicios de todos nuestros productos están perfectamente integrados.

Seguridad del hardware
Un software seguro necesita basarse en un hardware de confianza, por eso los dispositivos Apple (con iOS, iPadOS, macOS, tvOS y watchOS) integran funcionalidades de seguridad en el propio chip.

Esto incluye características personalizadas de la CPU que hacen posibles las prestaciones de seguridad del sistema y el chip. Cuando el hardware está diseñado para ser seguro, se sigue el principio de admitir funciones limitadas y definidas al detalle. Así se reduce al mínimo la superficie de ataque con componentes como la ROM de arranque, que constituye la «raíz de confianza» del hardware para proteger el arranque, unos motores AES dedicados que proporcionan tecnologías de cifrado y descifrado eficientes y seguras, y un Secure Enclave.

El Secure Enclave es un sistema en chip (SoC) incluido en todas las generaciones recientes de los dispositivos iPhone, iPad, Apple Watch, Apple TV y HomePod, así como en los Mac con chips de fabricación propia y el chip T2 Security de Apple. Dicho sistema sigue el mismo principio de diseño que el SoC y contiene un motor de AES y una ROM de arranque propios. Además, proporciona las tecnologías básicas de generación y almacenamiento seguros de las claves de cifrado de datos en reposo, y protege y evalúa los datos biométricos de Touch ID y Face ID.

El cifrado del almacenamiento debe ser rápido y eficiente y, a su vez, impedir la exposición de los datos que utiliza para establecer las relaciones entre las claves criptográficas. El motor de hardware de AES resuelve este problema cifrando o

descifrando los archivos en el momento de la escritura y la lectura. Un canal especial del Secure Enclave proporciona al motor de AES todos los datos de claves que necesita sin exponer esta información al procesador de aplicaciones (o CPU) ni al sistema operativo en general. De esta forma, FileVault y las tecnologías de protección de datos de Apple salvaguardan los archivos del usuario sin revelar claves de cifrado de larga duración.

El arranque seguro de Apple garantiza que los programas de bajo nivel no se manipulen y que solo se cargue el software de sistema operativo autorizado por Apple. El arranque seguro comienza con un código inmutable llamado «ROM de arranque» que se incorpora durante la fabricación del SoC de Apple y se conoce como la raíz de confianza del hardware. En los ordenadores Mac con el chip T2, la confianza para el arranque seguro de macOS tiene su origen en el propio chip. Además, tanto el chip T2 como el Secure Enclave ejecutan procesos de arranque seguro mediante sus propias ROM de arranque independientes, exactamente igual que los chips de la serie A y el M1.

El Secure Enclave también procesa los datos dactilares y faciales recogidos por los sensores Touch ID y Face ID de los dispositivos Apple, lo que protege la autenticación mientras se mantienen a salvo la privacidad y la seguridad de los datos biométricos del usuario. También permite a los usuarios beneficiarse de la protección de contraseñas y claves de acceso más largas y complejas, así como de la comodidad de poder autenticarse rápidamente para iniciar sesión o comprar.

Estas prestaciones de seguridad de los dispositivos Apple son posibles gracias a un diseño conjunto del chip, el hardware, el software y los servicios que solo Apple es capaz de ofrecer.

Seguridad del sistema

La seguridad del sistema se basa en las características únicas del hardware de Apple, y se encarga de controlar el acceso a los recursos del sistema en los dispositivos sin afectar a la facilidad de uso. Dicha seguridad la conforma el proceso de arranque, las actualizaciones de software y la protección de los recursos del sistema informático, como la CPU, la memoria, el disco duro, los programas y los datos almacenados.

Las versiones más recientes de los sistemas operativos de Apple son las más seguras. Una parte importante de la seguridad de Apple es el arranque seguro, que protege el sistema del malware al encenderlo. El arranque seguro empieza en el hardware y crea una cadena de confianza a través del software en la que cada paso se asegura de que el siguiente funciona adecuadamente antes de cederle el control. Este modelo de seguridad no solo se aplica al arranque predeterminado de los dispositivos Apple, sino también a varios modos de recuperación y a las actualizaciones de los dispositivos Apple. Algunos subcomponentes, como el chip T2 y el Secure Enclave, realizan su propio arranque seguro para garantizar que solo se ejecuta código procedente de Apple. El sistema de actualización puede prevenir incluso aquellos ataques en los que los dispositivos retroceden a una versión anterior del sistema operativo como método para sustraer los datos del usuario.

Los dispositivos Apple también incluyen mecanismos de protección para el arranque y el tiempo de ejecución que permiten mantener la integridad durante toda la sesión. Los chips diseñados por Apple del iPhone, el iPad, el Apple Watch,

el Apple TV, el HomePod y el Mac proporcionan una arquitectura común que protege la integridad del sistema operativo. Además, macOS presenta un modelo informático único que está reforzado por un conjunto ampliado y configurable de prestaciones de seguridad, así como funciones admitidas en todas las plataformas de hardware del Mac.

Cifrado y protección de los datos
Los dispositivos Apple cuentan con prestaciones de cifrado que protegen los datos del usuario y permiten borrarlos en remoto en el caso de pérdida o robo del dispositivo.

La cadena de arranque seguro, la seguridad del sistema y la seguridad de las apps ayudan a garantizar que en un dispositivo solo se ejecuten código y apps de confianza. Los dispositivos Apple disponen de prestaciones de cifrado adicionales para proteger los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad están en peligro, por ejemplo, si el dispositivo se pierde o ejecuta código que no es fiable. Todas estas prestaciones benefician tanto a los usuarios como a los administradores de TI, ya que protegen la información personal y corporativa en todo momento y proporcionan métodos para borrar el dispositivo a distancia y de forma inmediata en caso necesario.

Los dispositivos iOS y iPadOS usan un método de cifrado de archivos llamado «protección de datos». Por su parte, la información de los ordenadores Mac con procesadores de Intel se protege mediante la tecnología FileVault de cifrado de volumen. Los Mac con chips de Apple utilizan un modelo híbrido compatible con la protección de datos, salvo dos excepciones: el nivel de protección más bajo (clase D) no está admitido, y el nivel predeterminado (clase C), que emplea una clave del volumen, y funciona como el FileVault en los Mac con procesadores Intel. En todos los casos, las jerarquías de gestión de claves se basan en el chip independiente del Secure Enclave. Un motor de AES, también independiente, permite el cifrado al instante y garantiza que las claves de cifrado de larga duración no se revelen nunca al sistema operativo del núcleo ni a la CPU, donde podrían correr peligro. (Los Mac con procesadores Intel y el chip T1 o aquellos sin un Secure Enclave, no utilizan un chip independiente para proteger las claves de cifrado de FileVault.)

Los núcleos del sistema operativo de Apple, además de usar la protección de datos y FileVault para evitar el acceso no autorizado, garantizan la protección y la seguridad. El núcleo utiliza controles de acceso a la zona protegida de apps (que restringe los datos a los que puede acceder una app) y un mecanismo llamado Data Vault que, en lugar de restringir las llamadas que puede realizar una app, limita el acceso a los datos de una aplicación desde cualquier otra que los solicite.

Seguridad de las apps
Las apps se cuentan entre los elementos más críticos de una arquitectura de seguridad. Aunque ayudan a los usuarios a mejorar su productividad, también pueden afectar negativamente a la seguridad del sistema, la estabilidad y los datos si no se gestionan de forma adecuada.

Por esa razón, las capas de protección de Apple se encargan de garantizar que las apps no contengan malware conocido ni se hayan manipulado de forma indebida. El acceso de las apps a los datos del usuario está regulado por otros mecanismos de protección. Estos controles de seguridad proporcionan una plataforma estable

y segura para las apps, y permiten que multitud de desarrolladores ofrezcan cientos de miles de apps para iOS, iPadOS y macOS sin poner en peligro la integridad del sistema. Así los usuarios pueden acceder a estas apps en sus dispositivos Apple sin miedo a los virus, al malware y a otros ataques.

En el iPhone, el iPad y el iPod touch, las apps se obtienen en el App Store y todas ellas están en una zona protegida de apps, por lo que el control es muy estricto.

En el Mac, muchas apps se obtienen en el App Store, pero los usuarios también pueden descargar y utilizar apps de internet. Para proteger las descargas de internet, macOS cuenta con mecanismos de control adicionales. En primer lugar, todas las apps para el Mac tienen que estar certificadas por Apple para poder abrirse a partir de macOS 10.15. Este requisito ayuda a asegurarse de que estas apps no contengan malware conocido sin necesidad de que se distribuyan a través del App Store. Además, macOS incluye mecanismos de protección antivirus innovadores para bloquear (y, si es necesario, eliminar) el malware.

La zona protegida de apps, como control adicional presente en todas las plataformas, impide que las apps accedan a los datos del usuario sin autorización. Además, los datos almacenados en zonas críticas de macOS están protegidos para que los usuarios puedan controlar el acceso de las apps, estén en la zona protegida de apps o no, a los archivos de Escritorio, Documentos, Descargas y otras partes del sistema.

Seguridad de los servicios
Los increíbles servicios de Apple están diseñados para ayudar a los usuarios a trabajar más y mejor con sus dispositivos. Estos servicios proporcionan funciones avanzadas para el almacenamiento en la nube, la sincronización, el almacenamiento de contraseñas, la autenticación, el pago, los mensajes, las comunicaciones y mucho más sin descuidar la privacidad de los usuarios y la seguridad de sus datos.

Entre ellos están iCloud, Iniciar de Sesión con Apple, Apple Pay, iMessage, el Chat para Clientes, FaceTime, Buscar y Continuidad, y pueden requerir el uso de un ID de Apple o un ID de Apple Gestionado. Hay determinados servicios, como Apple Pay, con los que no es posible utilizar ID de Apple Gestionados.

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

Descripción de la seguridad de la red
Además de las medidas que Apple incluye para proteger la información almacenada en sus dispositivos, las organizaciones disponen de muchas opciones para mantener la seguridad de los datos cuando se envían de un dispositivo a otro. Todo esto está relacionado con la seguridad de la red.

Los usuarios necesitan acceder a las redes corporativas desde cualquier lugar del mundo, así que es importante asegurarse de que cuentan con autorización y sus datos están protegidos durante las transmisiones. Para cumplir estos objetivos en materia de seguridad, iOS, iPadOS y macOS integran tecnologías consolidadas y los estándares más recientes para las conexiones de redes wifi y móviles. Por eso, los sistemas operativos de Apple utilizan protocolos de red estándar que dan acceso a los desarrolladores y protegen la autenticación, la autorización y el cifrado de las comunicaciones.

Más información sobre la seguridad con los dispositivos Apple.

apple.com/es/business/it

apple.com/es/macos/security

apple.com/es/privacy/features

apple.com/es/security

Ecosistema de socios

Los dispositivos Apple funcionan con las herramientas y los servicios de seguridad empresarial más extendidos para garantizar que tanto los dispositivos como los datos que contienen respetan las políticas. Todas las plataformas admiten los protocolos estándar de VPN (incluidas las conexiones VPN realizadas en iOS 14 y iPadOS 14) y de conexión wifi segura para proteger el tráfico de red, y se conectan de forma segura a las infraestructuras más utilizadas por las empresas.

La alianza de Apple con Cisco mejora la seguridad y la productividad. Las redes de Cisco refuerzan la seguridad a través de Cisco Security Connector y priorizan el tráfico de las aplicaciones empresariales.