Seguridad de macOS

Descripción para departamentos de TI

Apple diseñó la plataforma macOS con un enfoque integral en cuanto al hardware, el software y los servicios para garantizar la seguridad de todo el sistema desde su concepción y simplificar la configuración, la implantación y la gestión de los dispositivos. macOS incluye las tecnologías de seguridad fundamentales que el profesional de las TI necesita para salvaguardar los datos corporativos e integrar los sistemas con los entornos de red seguros de la empresa. Apple también ha colaborado con los organismos de normalización para garantizar la conformidad con las certificaciones más recientes en materia de seguridad informática. En este resumen se explican brevemente algunas de esas prestaciones.

Este documento se divide en los temas siguientes:

- **Seguridad del sistema:** el software integrado y seguro que constituye los cimientos de macOS.
- **Cifrado y protección de datos:** la arquitectura y el diseño que protegen los datos del usuario en caso de pérdida o robo del dispositivo.
- **Seguridad de las apps:** los sistemas que protegen el Mac del software dañino y que se ejecutan de forma segura sin poner en peligro la integridad de la plataforma.
- **Autenticación y firma digital:** las facilidades incluidas en macOS para gestionar las credenciales y funcionar con las tecnologías estándar del sector, como las tarjetas inteligentes y los certificados S/MIME.
- **Seguridad de las redes:** los protocolos de red estándar del sector que proporcionan autenticación segura y cifrado de los datos en tránsito.
- **Controles de dispositivo:** métodos que permiten gestionar los dispositivos Apple, impedir su uso no autorizado y borrar de forma telemática los datos de un dispositivo perdido o robado.

Para más información acerca de la implantación y la gestión de macOS, consulta la guía de referencia sobre la implantación de macOS en help.apple.com/deployment/macos.

Para más información acerca de las prestaciones de seguridad de los servicios de Apple que no queden cubiertas en este documento, consulta la «Guía de seguridad de iOS» en www.apple.com/es/business/docs/iOS_Security_Guide.pdf.

Seguridad del sistema

La seguridad del sistema macOS está pensada para que todos los componentes de hardware y software clave de los ordenadores Mac sean seguros. Este planteamiento es básico en macOS, donde más seguridad no es igual a más complicaciones para el usuario.

UNIX

El kernel de macOS —el núcleo del sistema operativo— está basado en la Berkeley Software Distribution (distribución de software de Berkeley, o BSD) y en el microkernel Mach. BSD ofrece servicios básicos de red y de sistemas de archivo, un esquema de identificación de usuarios y grupos, y muchas otras funciones de carácter fundacional. BSD también prescribe las restricciones de acceso a los archivos y los recursos del sistema en base a identidades de usuario y grupo.

Mach proporciona gestión de la memoria, control de hilos, abstracción de hardware y comunicación entre procesos. Los puertos Mach representan tareas y otros recursos, y Mach impone el acceso a los puertos controlando qué tareas pueden enviarles mensajes. Las políticas de seguridad de BSD y los permisos de acceso de Mach constituyen una parte esencial de la seguridad de macOS y son cruciales para aplicar la seguridad a nivel local.

La seguridad del kernel es fundamental para la seguridad del sistema operativo en general. La firma de código protege el kernel y las extensiones de kernel de terceros, así como otras bibliotecas y ejecutables del sistema desarrollados por Apple.

Modelo de permisos del usuario

La concesión o denegación de permisos de acceso —también conocidos como «derechos de acceso»— constituyen un aspecto importante de la seguridad de un Mac. Un permiso es la capacidad para realizar una acción determinada, como acceder a datos o ejecutar código. Los permisos se otorgan a nivel de carpetas, subcarpetas, archivos y apps, así como para datos específicos de archivos, capacidades de apps y funciones administrativas. Las firmas digitales identifican los derechos de acceso de las apps y de los componentes del sistema.

macOS controla los permisos en muchos niveles, incluidos los componentes Mach y BSD del kernel. Para controlar los permisos de las apps en red, macOS utiliza protocolos de red.

Controles de acceso obligatorios

macOS también utiliza controles de acceso obligatorios, es decir, políticas que establecen las restricciones de seguridad creadas por el desarrollador y que no se pueden obviar. Este enfoque difiere de los controles de acceso discrecionales, que permiten que los usuarios omitan ciertas políticas de seguridad de acuerdo con sus preferencias. Los controles de acceso obligatorios no son visibles para los usuarios, pero son la tecnología de base que ayuda a habilitar varias prestaciones importantes, como la zona protegida, los controles parentales, las preferencias gestionadas, las extensiones y la Protección de la Integridad del Sistema.

Protección de la Integridad del Sistema

OS X 10.11 y las versiones posteriores incluyen una tecnología de protección a nivel del sistema denominada Protección de la Integridad del Sistema que impide que, en determinadas ubicaciones los componentes modifiquen o sobrescriban archivos críticos del sistema para evitar que ningún código malicioso los modifique o ejecute. La Protección de la Integridad del Sistema es un ajuste del ordenador que está activado por omisión cuando se actualiza a OS X 10.11; si se desactiva, se elimina la protección de todas las particiones del dispositivo de almacenamiento físico. macOS aplica esta política de seguridad a todos los procesos que se ejecutan en el sistema, con independencia de si se están ejecutando en una zona protegida de apps o con privilegios administrativos.

Para más información acerca de estas áreas de solo lectura del sistema de archivos, consulta el artículo de soporte técnico de Apple «Acerca de la Protección de la Integridad del Sistema en tu Mac» en support.apple.com/HT204899.

Extensiones de kernel

macOS ofrece un mecanismo de extensión de kernel para permitir la carga dinámica del código en el kernel, sin necesidad de volver a compilar o enlazar. Dado que estas extensiones de kernel (KEXT) proporcionan tanto modularidad como capacidad de carga dinámica, son la opción más lógica para casi cualquier servicio relativamente autónomo que requiera acceso a las interfaces del kernel, como son los drivers de los dispositivos de hardware o las apps de VPN.

Con el fin de mejorar la seguridad del Mac, es necesario que el usuario dé su consentimiento para cargar las extensiones de kernel instaladas junto con macOS High Sierra o después. Esto se conoce como «carga de extensiones de kernel aprobadas por el usuario». Cualquier usuario puede aprobar una extensión de kernel, aunque no tenga privilegios administrativos.

Las extensiones de kernel no requieren autorización en los siguientes casos:

- Se instalaron en el Mac antes de actualizar a macOS High Sierra.
- Sustituyen extensiones aprobadas con anterioridad.
- Tienen permiso para cargarse sin el consentimiento del usuario utilizando el comando `spctl`, disponible al arrancar desde la partición de recuperación de macOS.
- Tienen permiso para cargarse mediante la configuración de una solución de gestión de dispositivos móviles (Mobile Device Management, MDM). A partir de la versión 10.13.2 de macOS High Sierra, es posible utilizar MDM para concretar una lista de extensiones de kernel que se cargarán sin el consentimiento del usuario. Esta opción requiere un Mac con macOS High Sierra 10.13.2 que esté inscrito en MDM, bien mediante el Programa de Inscripción de Dispositivos (Device Enrollment Program, DEP), bien mediante una inscripción en MDM aprobada por el usuario.

Para más información acerca de las extensiones de kernel, consulta el artículo de soporte técnico de Apple «Prepararse para los cambios en las extensiones de kernel en macOS High Sierra» en support.apple.com/HT208019.

Contraseña de firmware

macOS permite utilizar una contraseña para impedir modificaciones o ajustes de firmware no intencionados en un determinado sistema. Esta contraseña del firmware sirve para evitar las siguientes situaciones:

- Arrancar desde un volumen del sistema no autorizado
- Alterar el proceso de arranque, como arrancar en modo de usuario único
- Acceso no autorizado a Recuperación de macOS
- Acceso directo a la memoria (DMA) a través de interfaces como Thunderbolt
- Modo de disco de destino, que requiere DMA

Nota: el chip T2 de Apple instalado en el iMac Pro impide que los usuarios puedan restablecer la contraseña del firmware aunque tengan acceso físico al Mac. En un Mac que no tenga el chip T2 se deben tomar medidas adicionales si se quiere impedir que los usuarios tengan acceso físico a los componentes internos del Mac.

Recuperación por Internet

Los ordenadores Mac intentan iniciarse automáticamente desde Recuperación de macOS a través de Internet cuando no pueden arrancar desde el sistema de recuperación integrado. Cuando esto ocurre, durante el inicio aparece una esfera que da vueltas en lugar del logotipo de Apple. La recuperación por Internet permite al usuario reinstalar la versión más reciente de macOS o la versión que venía con su Mac.

Las actualizaciones de macOS se distribuyen a través del App Store y se ejecutan mediante el Instalador de macOS, que utiliza firmas de código para garantizar la integridad y la autenticidad del instalador y de sus paquetes antes de llevar a cabo la instalación. De modo parecido, el servicio Recuperación por Internet es el origen autorizado para el sistema operativo que venía con un Mac en particular.

Para más información acerca de Recuperación de macOS, consulta el artículo de soporte técnico de Apple «Acerca de Recuperación de macOS» en support.apple.com/HT201314.

Cifrado y protección de datos

Apple File System

Apple File System (APFS) es un nuevo sistema de archivos para macOS, iOS, tvOS y watchOS. Está optimizado para el almacenamiento flash/SSD e introduce un cifrado más robusto, metadatos de copiar al escribir, espacio compartido, clonación de archivos y directorios, instantáneas, redimensionamiento rápido de directorios, primitivas de guardado seguro atómico y mejora de los aspectos básicos del sistema de archivos, así como un diseño de copiar al escribir único que une las peticiones de E/S para proporcionar el máximo rendimiento mientras garantiza la fiabilidad de los datos.

APFS asigna espacio de disco a la carta. Cuando un solo contenedor de AFPS tiene varios volúmenes, el espacio libre del contenedor se comparte para poder asignarse a cualquiera de los volúmenes, según sea necesario. Cada volumen emplea una parte del contenedor general, de manera que el espacio disponible equivale al tamaño total del contenedor menos el espacio empleado en todos los volúmenes del contenedor.

En el caso de macOS High Sierra, un contenedor de APFS válido debe contener al menos tres volúmenes, los dos primeros de los cuales están ocultos al usuario:

- Volumen de prearranque: contiene datos necesarios para arrancar cada uno de los volúmenes del contenedor.
- Volumen de recuperación: contiene el disco de recuperación.
- Volumen del sistema: contiene macOS y la carpeta Usuario.

FileVault

Todos los Mac incluyen una tecnología de cifrado integrada llamada FileVault que sirve para proteger los datos en reposo. FileVault emplea el cifrado de datos XTS-AES-128 para proteger los datos en reposo de un Mac. Esto puede aplicarse a la protección de todo el volumen en los dispositivos de almacenamiento internos y externos. Si un usuario introduce un ID de Apple y su contraseña durante Asistente de Configuración, el asistente sugiere la activación de FileVault y el almacenamiento de la clave de recuperación en iCloud.

Cuando un usuario activa FileVault en un Mac, tiene que proporcionar credenciales válidas antes de continuar el proceso de arranque para tener acceso a los modos de inicio especializados, como Modalidad de Disco de Destino. A falta de unas credenciales válidas y de una clave de recuperación, el volumen seguirá totalmente cifrado y protegido de accesos no autorizados, aunque el dispositivo de almacenamiento físico se retire y se conecte a otro ordenador.

Para proteger los datos en un entorno empresarial, el departamento de TI debe definir e imponer políticas de configuración de FileVault a través de una solución de MDM. Las empresas tienen varias opciones para gestionar los volúmenes

cifrados, lo que incluye las claves de recuperación institucionales, las claves de recuperación personales (que pueden almacenarse o no con la solución de MDM para su custodia) o una combinación de ambas. Otra posibilidad es establecer la rotación de claves como política.

Cifrado de imágenes de disco

En macOS, las imágenes de disco cifradas sirven de contenedores seguros en los que los usuarios pueden almacenar o transferir documentos sensibles y otros archivos. Las imágenes de disco cifradas se crean por medio de Utilidad de Discos, que se encuentra en /Aplicaciones/Utilidades/. Pueden cifrarse con AES de 128 o 256 bits. Dado que la imagen de disco montada se trata como un volumen local conectado a un Mac, los usuarios pueden copiar, mover y abrir los archivos y carpetas almacenados en ella. Tal y como ocurre con FileVault, los contenidos de una imagen de disco se cifran y descifran en tiempo real. Gracias al cifrado de imágenes de disco, los usuarios pueden intercambiar documentos, archivos y carpetas fácilmente con solo guardar una imagen de disco cifrada en soportes extraíbles, adjuntarla a un mensaje de correo electrónico o almacenarla en un servidor remoto.

Certificaciones ISO 27001 y 27018

Apple ha recibido las certificaciones ISO 27001 y 27018 por implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) en la infraestructura, desarrollo y operaciones que soportan los siguientes productos y servicios: Apple School Manager, iCloud, iMessage, FaceTime, ID de Apple Gestionados y iTunes U, de conformidad con la Declaración de Aplicabilidad 2.1 del 11 de julio de 2017. El cumplimiento de la norma ISO por parte de Apple está certificado por el Organismo Nacional de Normalización del Reino Unido (British Standards Institution, BSI). Para consultar los certificados de cumplimiento de las normas ISO 27001 e ISO 27018, visita el sitio web de la BSI:

www.bsigroup.com/es-ES/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/es-ES/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Validación criptográfica (FIPS 140-2)

Desde la publicación de OS X 10.6, todas las versiones de los módulos criptográficos de macOS han recibido la validación de conformidad con los Estándares Federales de Procesamiento de la Información (Federal Information Processing Standards, FIPS) 140-2 de nivel 1 estadounidenses. Cada vez que se publica el sistema operativo del Mac, Apple procede del mismo modo que con el resto de las versiones principales y envía los módulos al CMVP para que vuelva a validarlas. Este programa acredita la integridad de las operaciones de cifrado de las apps de Apple y de terceros que utilizan los servicios criptográficos y los algoritmos aprobados de macOS. Todos los certificados de validación de la conformidad con la norma FIPS 140-2 de Apple se encuentran en la página de proveedores del CMVP. El CMVP mantiene el estado de validación de los módulos criptográficos en dos listas distintas, en función de cuál sea su estado vigente, en la página csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Certificación de los Criterios Comunes (ISO 15408)

En su día, Apple obtuvo las certificaciones de macOS con arreglo al programa Certificación de los Criterios Comunes y ahora está sometiendo macOS High Sierra a evaluación para conseguir la acreditación en el perfil de protección del

sistema operativo (Operating System Protection Profile) PP_OSv4.1. Apple continúa evaluando y trabajando por obtener certificaciones en versiones nuevas y actualizadas de los perfiles de protección colaborativos (Collaborative Protection Profiles, cPPs) disponibles actualmente. Apple ha desempeñado un papel activo en la comunidad técnica internacional (International Technical Community, ITC) en cuanto al desarrollo de cPPs dirigidos a evaluar las principales tecnologías de seguridad móvil.

Certificaciones de seguridad, validaciones y directrices

Apple ha colaborado con gobiernos de todo el mundo en el desarrollo de guías destinadas a ofrecer instrucciones y recomendaciones para mantener un entorno más seguro, también conocido como «endurecimiento de dispositivos» o «device hardening», para entornos de alto riesgo. Estas guías proporcionan información contrastada sobre la mejor forma de configurar y utilizar las prestaciones integradas de macOS para reforzar la seguridad.

Para obtener la información más reciente acerca de las certificaciones de seguridad, validaciones y directrices para macOS, consulta el artículo de soporte técnico de Apple «Certificaciones de seguridad de productos, validaciones y directrices para macOS» en support.apple.com/HT201159.

Seguridad de las apps

macOS incluye tecnologías que garantizan que solo se instalan las apps de confianza y ayudan a defender el sistema del software dañino. macOS también adopta un enfoque por capas formado por un sistema de zona protegida (sandboxing) que protege las apps en tiempo de ejecución y las firma para evitar que se manipulen.

Gatekeeper

A fin de controlar la procedencia de las apps que se pueden instalar en el sistema, macOS incluye Gatekeeper: una prestación que permite a los usuarios y a las empresas definir un nivel de seguridad mínimo para la instalación de apps.

Con la configuración más segura de Gatekeeper, los usuarios solo pueden instalar apps del App Store firmadas. El ajuste por omisión permite a los usuarios instalar apps del App Store y apps que tengan una firma de ID de Desarrollador válido. Esta firma indica que las apps están firmadas por un certificado emitido por Apple y que nunca se han modificado desde entonces. Gatekeeper también se puede desactivar por completo a través de un comando de Terminal si fuera necesario.

Además, Gatekeeper emplea una técnica de aleatorización de rutas en algunos casos, como cuando las apps se inician directamente desde una imagen de disco sin firmar o desde la ubicación en la que se descargaron y descomprimieron de forma automática. La aleatorización de rutas hace que las apps estén disponibles en un lugar al azar de solo lectura en el sistema de archivos antes de iniciarse. Esto no solo impide que las apps accedan al código o al contenido utilizando rutas relativas, sino que además evita que se actualicen automáticamente si se abren desde esta ubicación, que es de solo lectura. Cuando se utiliza el Finder para mover de sitio una app, por ejemplo, a la carpeta Aplicaciones, deja de aplicarse la aleatorización de rutas.

La mayor ventaja de seguridad del modelo de protección por omisión es que ofrece una protección del ecosistema amplia. Si el autor de un programa dañino trata de robar o de conseguir por algún otro medio la capacidad para firmar un ID de Desarrollador y la utiliza para distribuir software dañino, Apple puede responder rápidamente y revocar el certificado de firma. Esto impide la propagación del código dañino. Este tipo de protecciones socavan el modelo económico de la mayoría de las campañas de malware para el Mac y proporcionan medidas de protección amplias a todos los usuarios.

Los usuarios pueden obviar estos ajustes de forma temporal para instalar cualquier app. Las empresas pueden utilizar su solución de MDM para establecer e imponer ajustes de Gatekeeper, así como para añadir certificados a la política de confianza de macOS que evalúen la firma del código.

XProtect

macOS incorpora tecnología para la detección de código dañino basada en firmas. Apple vigila la aparición de nuevas infecciones o amenazas de código dañino, y actualiza las firmas de XProtect automáticamente —con independencia de las actualizaciones del sistema— para ayudar a proteger los sistemas Mac de las infecciones por software malicioso. XProtect detecta y bloquea automáticamente la instalación de malware conocido.

Herramienta de eliminación de código dañino

En el caso de que algún programa malicioso consiga acceder a un Mac, macOS también incluye tecnología para contener las infecciones. Además de vigilar la actividad del malware en el ecosistema para revocar los ID de Desarrollador que sean necesarios y de emitir actualizaciones de XProtect, Apple también publica actualizaciones de macOS para eliminar el código dañino de cualquier sistema

afectado que esté configurado para recibir actualizaciones de seguridad automáticas. Una vez que la herramienta de eliminación de código dañino recibe información actualizada, el malware se elimina tras el primer reinicio. La herramienta de eliminación de código dañino no reinicia el Mac automáticamente.

Actualizaciones de seguridad automáticas

Apple publica las actualizaciones de XProtect y la herramienta de eliminación de código dañino automáticamente. Por omisión, macOS comprueba si hay actualizaciones a diario. Para más información acerca de las actualizaciones de seguridad, consulta el artículo de soporte técnico de Apple «Mac App Store: Actualizaciones de seguridad automáticas» en support.apple.com/HT204536.

Protección en tiempo de ejecución

Los archivos del sistema, los recursos y el kernel están blindados del espacio de la app del usuario. Todas las apps del App Store tienen una zona protegida para restringir el acceso a los datos almacenados por otras apps. Si una app del App Store necesita acceder a datos de otra, solo puede hacerlo usando las API y los servicios ofrecidos por macOS.

Firma obligatoria del código de las apps

Todas las apps del App Store están firmadas por Apple para garantizar que no hayan sido manipuladas o alteradas. Apple firma todas las apps que vienen con los dispositivos Apple. Muchas apps distribuidas fuera del App Store están firmadas por el desarrollador utilizando un certificado de ID de Desarrollador emitido por Apple (en combinación con una clave privada) para que se ejecute respetando los ajustes predeterminados de Gatekeeper.

Las apps que no procedan del App Store también se suelen firmar con un certificado de desarrollador emitido por Apple para garantizar que la app es genuina y no se ha manipulado. Las apps desarrolladas de forma interna también deberían firmarse con un ID de Desarrollador emitido por Apple para que puedas validar su integridad.

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

Autenticación y firma digital

Para almacenar las credenciales y las identidades digitales de los usuarios de forma cómoda y segura, macOS incluye Llavero y otras herramientas compatibles con tecnologías de autenticación y firma digital como las tarjetas inteligentes y los certificados S/MIME.

Arquitectura de llavero

macOS ofrece un repositorio llamado Llavero que almacena de forma cómoda y segura los nombres de usuario y las contraseñas, incluidas las identidades digitales, las claves de cifrado y las notas seguras. Se puede acceder abriendo la app Acceso a Llaveros en /Aplicaciones/Utilidades/. Gracias a los llaveros, se puede prescindir de introducir —o incluso recordar— las credenciales de cada recurso. Aunque se crea un llavero predeterminado para cada usuario de un Mac, se pueden crear más para fines específicos.

Además de los de usuario, macOS usa unos llaveros del sistema en los se guardan los activos de autenticación genéricos, como las credenciales de red y las identidades de la infraestructura de clave pública (PKI). Uno de estos llaveros, Raíz del Sistema, es inmutable y almacena certificados de la autoridad

certificadora (AC) raíz de la PKI de Internet para facilitar tareas comunes, como son las operaciones de banca online y de comercio electrónico. Asimismo, puedes implantar certificados de una autoridad certificadora interna en ordenadores Mac gestionados para facilitar la validación de servicios y sitios internos.

Marco de autenticación seguro

Los datos de Llavero se particionan y protegen con listas de control de acceso (ACL) y por eso las apps con identidades diferentes carecen de acceso a las credenciales almacenadas por apps de terceros, a menos que el usuario lo permita de forma explícita. Esta protección proporciona el mecanismo de seguridad de las credenciales de autenticación de los dispositivos Apple en una amplia gama de apps y servicios de tu empresa.

Touch ID

Los sistemas Mac con un sensor Touch ID pueden desbloquearse con la huella dactilar. Pero Touch ID no sustituye la necesidad de utilizar una contraseña, que sigue siendo necesaria para iniciar sesión al encender, reiniciar o cerrar sesión en el Mac. Una vez iniciada la sesión, los usuarios pueden autenticarse rápidamente con Touch ID siempre que se les pida la contraseña.

Los usuarios también pueden utilizar Touch ID para desbloquear notas protegidas por contraseña en la app Notas, el panel Contraseñas de las preferencias de Safari y muchos paneles de preferencias de Preferencias del Sistema. Para reforzar la seguridad, los usuarios deben introducir una contraseña en lugar de utilizar Touch ID para desbloquear el panel Seguridad y Privacidad en Preferencias del Sistema. Si FileVault está activado, los usuarios también deben introducir una contraseña para gestionar las preferencias de Usuarios y Grupos. Si el Mac está compartido entre varios usuarios, estos pueden usar Touch ID para cambiar de cuenta.

Para más información acerca de Touch ID y su seguridad, consulta el artículo de soporte técnico de Apple «Acerca de la tecnología de seguridad avanzada de Touch ID» en support.apple.com/HT204587.

Desbloqueo Automático con el Apple Watch

Los usuarios que tengan un Apple Watch pueden utilizarlo para desbloquear el Mac de forma automática. Gracias a las tecnologías Bluetooth de bajo consumo (BLE) y Wi-Fi punto a punto, el Apple Watch puede desbloquear un Mac con seguridad cuando están lo suficientemente cerca. Esto requiere una cuenta de iCloud con la autenticación de doble factor (TFA) configurada.

Para ampliar los detalles acerca del protocolo y obtener más información sobre las prestaciones Continuidad y Handoff, consulta la «Guía de seguridad de iOS» en www.apple.com/es/business/docs/iOS_Security_Guide.pdf.

Tarjetas inteligentes

macOS Sierra y las versiones posteriores son compatibles de serie con las tarjetas de verificación de la identidad personal (PIV). El uso de estas tarjetas está muy extendido en empresas comerciales y públicas con fines de autenticación de doble factor, firma digital y cifrado.

Las tarjetas inteligentes incluyen una o varias identidades digitales con un par de claves pública y privada y un certificado asociado. Desbloquear una tarjeta inteligente con el número de identificación personal (PIN) proporciona acceso a las claves privadas utilizadas para las operaciones de autenticación, cifrado y firma. El certificado determina para qué se puede usar una clave, qué atributos están asociados a ella y si está validada (firmada) por una autoridad de certificación.

Las tarjetas inteligentes se pueden usar para la autenticación de doble factor. Los dos factores necesarios para desbloquear una tarjeta son «algo que tienes» (la tarjeta) y «algo que sabes» (el PIN). macOS Sierra y las versiones posteriores tienen compatibilidad nativa con autenticación con ventana de inicio de sesión con tarjeta inteligente y con autenticación con certificado de cliente en sitios web con Safari. Además, admite la autenticación Kerberos mediante pares de claves (PKINIT) para el inicio de sesión único en servicios de Kerberos compatibles.

Para más información acerca de la implantación de tarjetas inteligentes con macOS, consulta la guía de referencia sobre la implantación de macOS en help.apple.com/deployment/macos.

Firma digital y cifrado

En la app Mail, los usuarios pueden enviar mensajes cifrados y firmados digitalmente. Mail detecta automáticamente nombres de sujeto o nombres alternativos de sujeto de dirección de email con distinción entre mayúsculas y minúsculas RFC822 en certificados de firma digital y cifrado en identificadores PIV adjuntos a tarjetas inteligentes compatibles. Si una cuenta de email configurada coincide con una dirección de email en un certificado de firma digital o cifrado en un identificador PIV adjunto, Mail muestra automáticamente el botón de firma de correo electrónico en una barra de herramientas de mensaje nuevo. Si Mail tiene el certificado de cifrado de email del destinatario o puede detectarlo en la lista global de direcciones (GAL) de Microsoft Exchange, aparece el icono de un candado abierto en la barra de herramientas del mensaje nuevo. Si el candado del icono aparece cerrado, significa que el mensaje se enviará cifrado con la clave pública del destinatario.

S/MIME por mensaje

macOS es compatible con la tecnología S/MIME por mensaje. Esto significa que los usuarios de S/MIME pueden elegir firmar y cifrar los mensajes por omisión o firmar y cifrar según qué mensajes.

Las identidades empleadas con S/MIME se pueden enviar a los dispositivos Apple por medio de un perfil de configuración, una solución de MDM, Simple Certificate Enrollment Protocol (SCEP) o la autoridad de certificación de Microsoft Active.

Seguridad de la red

Además de las tecnologías de defensa integradas que Apple utiliza para proteger los datos almacenados en los ordenadores Mac, las empresas disfrutan de muchas otras medidas de seguridad de red que sirven para mantener a salvo la información mientras viaja hasta o desde un Mac.

Los usuarios de dispositivos móviles 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 su transmisión. macOS utiliza protocolos de red estándar —y permite su acceso a los desarrolladores— para garantizar la autenticación, la autorización y el cifrado de las comunicaciones. Para reunir estos objetivos en materia de seguridad, macOS integra tecnologías consolidadas y los estándares más recientes para las conexiones de datos en redes Wi-Fi.

TLS

macOS es compatible con los protocolos Transport Layer Security (TLS 1.0, TLS 1.1 y TLS 1.2) y DTLS. Admite tanto AES-128 como AES-256 y prefiere cifrar paquetes con confidencialidad directa total. Safari, Calendario, Mail y otras apps de Internet utilizan este protocolo automáticamente para establecer un canal de comunicación cifrado entre el dispositivo y los servicios de red.

Una serie de API de alto nivel (como CFNetwork) facilita a los desarrolladores la adopción del protocolo TLS en sus apps, mientras que las API de bajo nivel (como SecureTransport) proporcionan un control más preciso. CFNetwork deshabilita el uso de SSLv3 y las apps que utilizan WebKit (como Safari) no pueden establecer conexiones SSLv3.

A partir de macOS High Sierra y iOS 11, los certificados SHA-1 ya no están permitidos para las conexiones TLS, a menos que sean de la confianza del usuario. Los certificados con claves RSA inferiores a 2.048 bits tampoco están permitidos. En macOS Sierra y iOS 10, el paquete criptográfico simétrico RC4 queda descatalogado. Por omisión, los clientes o servidores TLS implantados con interfaces API SecureTransport carecen de paquetes criptográficos RC4 y, cuando este es el único paquete criptográfico disponible, no se pueden conectar. Como medida de seguridad extra, los servicios o apps que requieran RC4 deben actualizarse para utilizar paquetes criptográficos modernos y seguros.

App Transport Security

App Transport Security ofrece requisitos de conexión predeterminados para que las apps se adhieran a las prácticas recomendadas en materia de conexiones seguras al utilizar las API NSURLConnection, CFURL o NSURLSession. Por omisión, App Transport Security limita la selección del cifrador para incluir únicamente paquetes que proporcionen confidencialidad directa, en concreto ECDHE_ECDSA_AES y ECDHE_RSA_AES en el modo GCM o CBC. Las apps pueden desactivar el requisito de confidencialidad directa en función del dominio, en cuyo caso se añade RSA_AES al conjunto de cifradores disponibles.

Los servidores deben ser compatibles tanto con TLS 1.2 como con el método de confidencialidad directa, y los certificados deben ser válidos y estar firmados mediante SHA-256 o una versión superior con una clave que sea, como mínimo, bien RSA de 2.048 bits, bien de curva elíptica de 256 bits.

Las conexiones de red que no cumplan estos requisitos fallarán, a menos que la app deje App Transport Security sin efecto. Con los certificados no válidos siempre se producen fallos graves que imposibilitan la conexión. App Transport Security se aplica automáticamente a las apps que están compiladas para macOS 10.11 o versiones posteriores.

VPN

Los servicios de redes seguras, como las redes privadas virtuales (VPN), suelen requerir una configuración mínima compatible con macOS. Los ordenadores macOS funcionan con servidores VPN compatibles con los siguientes protocolos y métodos de autenticación:

- IKEv2/IPSec con autenticación mediante secreto compartido, certificados RSA y ECDSA, EAP-MSCHAPv2 o EAP-TLS
- VPN sobre SSL con la correspondiente app cliente del App Store
- Cisco IPSec con autenticación de usuario mediante contraseña, RSA SecurID o CRYPTOCard, y autenticación automática mediante secreto compartido y certificados
- L2TP/IPSec con autenticación de usuario mediante MS-CHAPV2 Password, RSA SecurID o CRYPTOCard, y autenticación automática mediante secreto compartido

Además de soluciones de VPN de terceros, macOS admite los siguientes servicios:

- **VPN por Petición** para redes que utilizan autenticación basada en certificados. Las políticas del departamento de TI deben especificar qué dominios requieren una conexión VPN mediante un perfil de configuración VPN.

- **VPN Individual por App** para facilitar las conexiones VPN con un control mucho más preciso. MDM puede especificar una conexión para cada app gestionada y determinados dominios en Safari a fin de garantizar la seguridad de los datos que entran y salen de la red corporativa. También es una forma de proteger la confidencialidad de los datos personales del usuario.

Wi-Fi

macOS es compatible con los protocolos Wi-Fi estándar del sector, como WPA2 Enterprise, para proporcionar acceso autenticado a las redes corporativas inalámbricas. WPA2 Enterprise utiliza cifrado AES de 128 bits, que ofrece a los usuarios las máximas garantías de que sus datos estarán protegidos al enviar y recibir comunicaciones a través de una conexión de red Wi-Fi. Los ordenadores Mac son compatibles con 802.1X y pueden integrarse con un amplio abanico de entornos de autenticación RADIUS. Estos son los métodos de autenticación inalámbrica para 802.1X: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 y LEAP.

La autenticación WPA/WPA2 Enterprise también puede utilizarse en la ventana de inicio de sesión de macOS para que el usuario tenga que iniciar sesión para autenticarse en la red.

El Asistente de Configuración de macOS admite la autenticación 802.1X con nombre de usuario y contraseña mediante TTLS o PEAP.

Firewall

macOS incluye un firewall integrado para proteger el Mac de los accesos por red o de los ataques por denegación del servicio. Es compatible con las siguientes configuraciones:

- Bloquear todas las conexiones entrantes, con independencia de la app
- Permitir de forma automática recibir conexiones entrantes al software integrado
- Permitir de forma automática recibir conexiones entrantes al software descargado y firmado
- Añadir o denegar el acceso en función de las apps especificadas por el usuario
- Impedir que el Mac responda a las solicitudes de sondeo ICMP y de exploración de puertos

Inicio de sesión único

macOS permite utilizar Kerberos para la autenticación en redes empresariales. Las apps pueden utilizar Kerberos para autenticar a usuarios en los servicios en los que tienen autorización de acceso. Kerberos también puede utilizarse para una amplia gama de actividades de red, como la protección de las sesiones de Safari y la autenticación en el sistema de archivos en red y en las apps de desarrolladores externos. La autenticación basada en certificados (PKINIT) es compatible, aunque es necesario que la app adopte una API del desarrollador.

Los identificadores GSS-API SPNEGO y el protocolo HTTP Negotiate funcionan con puertas de enlace de autenticación basada en Kerberos y sistemas de autenticación integrada de Windows compatibles con los tickets de Kerberos. La compatibilidad con Kerberos está basada en el proyecto de código abierto Heimdal.

Se admiten los siguientes tipos de cifrado:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Para configurar Kerberos, hay que adquirir tickets con la app Ticket Viewer, iniciar sesión en un dominio de Windows Active Directory o utilizar la herramienta de línea de comandos `kinit`.

Seguridad de AirDrop

Los ordenadores Mac compatibles con AirDrop utilizan BLE y la tecnología Wi-Fi de punto a punto desarrollada por Apple para enviar archivos e información a dispositivos que se encuentren cerca, incluidos los dispositivos iOS con iOS 7 o posterior que cuenten con la tecnología AirDrop. La radio Wi-Fi sirve para comunicar los dispositivos entre sí sin necesidad de una conexión a Internet o de un punto de acceso Wi-Fi. Esta conexión se cifra con TLS.

Para más información acerca de AirDrop, la seguridad de AirDrop y otros servicios de Apple, consulta el apartado «Seguridad de la red» de la «Guía de seguridad de iOS» en www.apple.com/es/business/docs/iOS_Security_Guide.pdf.

Controles de dispositivo

macOS es compatible con políticas y configuraciones de seguridad flexibles que facilitan su aplicación y gestión. Esto permite a las empresas proteger la información corporativa y asegurarse de que los empleados cumplen los requisitos de la empresa, aunque estén utilizando sus ordenadores personales (por ejemplo, en el marco de un programa en el que el empleado trabaja con su propio dispositivo).

Las empresas pueden utilizar diferentes recursos, como la protección mediante contraseña, los perfiles de configuración y las soluciones de MDM de terceros, para gestionar parques de dispositivos y ayudar a proteger los datos de la empresa, aunque los empleados accedan a ellos desde sus ordenadores Mac personales.

Protección mediante contraseña

En los ordenadores Mac con Touch ID, la contraseña debe tener ocho caracteres como mínimo. Siempre se recomiendan contraseñas largas y complejas porque son más difíciles de adivinar o atacar.

Los administradores pueden imponer el uso de contraseñas complejas y otras políticas por medio de la solución de MDM o exigiendo a los usuarios que instalen perfiles de configuración de forma manual. Para instalar la carga útil de políticas de códigos de acceso en macOS, es necesario introducir una contraseña de administrador.

Para ampliar los detalles acerca de cada una de las políticas disponibles en los ajustes de MDM, consulta help.apple.com/deployment/mdm/#/mdm4D6A472A.

Consulta la referencia sobre los perfiles de configuración para desarrolladores en developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Imposición de configuraciones

Un perfil de configuración es un archivo XML que permite a un administrador distribuir información de configuración a un ordenador Mac. Si el usuario elimina un perfil de configuración, todos los ajustes definidos por el perfil desaparecen del equipo. Los administradores pueden imponer ajustes vinculando las políticas al acceso Wi-Fi y a los datos. Por ejemplo, un perfil de configuración que prescriba una configuración de email puede especificar a su vez una política de contraseña que debe cumplir el dispositivo; por ejemplo, que un usuario no pueda acceder al correo electrónico a menos que la contraseña reúna los requisitos definidos por el administrador.

Un perfil de configuración de macOS contiene una serie de ajustes que se pueden modificar, por ejemplo:

- Políticas de código
- Restricciones en prestaciones del dispositivo (por ejemplo, desactivación de la cámara)
- Ajustes de Wi-Fi o VPN
- Ajustes del servidor de Mail o Exchange
- Ajustes del servicio de directorios LDAP
- Ajustes de firewall
- Credenciales y claves
- Actualizaciones de software

Para acceder a la lista actualizada de perfiles, consulta la guía de referencia sobre los perfiles de configuración en help.apple.com/deployment/mdm/#/mdm5370d089.

Los perfiles de configuración pueden firmarse y cifrarse para validar sus orígenes, garantizar su integridad y proteger sus contenidos. También es posible impedir la eliminación de un perfil de configuración de un Mac u obligar a introducir una contraseña para eliminarlo. Los perfiles de configuración que inscriben un Mac en una solución de MDM se pueden eliminar, lo que a su vez borra la información de configuración, los datos y las apps gestionados.

Los usuarios pueden instalar perfiles de configuración descargados desde Safari, enviados en un mensaje de email o sin cables a través de una solución de MDM. Cuando un usuario configura un Mac con el DEP o con Apple School Manager, el ordenador descarga e instala automáticamente un perfil para inscribirse en la solución de MDM.

MDM

La compatibilidad de macOS con MDM permite a las empresas configurar y gestionar de forma segura implantaciones de dispositivos Mac, iPhone, iPad y Apple TV a escala. Las funciones de MDM se basan en tecnologías de macOS ya existentes, como los perfiles de configuración, la inscripción inalámbrica y el servicio de notificaciones push de Apple (APNs). Por ejemplo, el APNs sirve para activar el dispositivo para que se comunique directamente con la solución de MDM a través de una conexión segura. El APNs no transmite ninguna información confidencial o privada.

MDM permite a los departamentos de TI inscribir ordenadores Mac en un entorno empresarial, configurar y actualizar los ajustes de forma inalámbrica, supervisar el cumplimiento de las políticas corporativas y hasta borrar o bloquear ordenadores Mac gestionados de forma telemática.

Inscripción de dispositivos

La inscripción de dispositivos, que es un servicio de Apple School Manager y de los Programas de Implantación de Apple, es una forma rápida y optimizada de implantar los ordenadores Mac comprados por una empresa directamente a Apple o a través de un Distribuidor Autorizado Apple participante.

Las empresas pueden hacer la inscripción en MDM de forma automática sin necesidad de preparar ni tocar físicamente los ordenadores antes de entregarlos a los usuarios. Tras la inscripción, los administradores inician sesión en el sitio web del programa para vincularlo a su solución de MDM. A partir de ahí, los ordenadores comprados pueden asignarse automáticamente con una solución de MDM. Una vez que un Mac está inscrito, las configuraciones, restricciones o controles de MDM se instalan automáticamente. Todas las comunicaciones que se establezcan entre los ordenadores y los servidores de Apple se cifran en tránsito con HTTPS (SSL).

El proceso de configuración que tienen que seguir los usuarios puede simplificarse al máximo eliminando pasos específicos de Asistente de Configuración, para que los usuarios puedan ponerse a trabajar sin demora. Los administradores también pueden controlar si el usuario puede eliminar o no el perfil de MDM del ordenador y asegurarse de que las restricciones del dispositivo se aplican desde el principio. El ordenador, una vez desembalado y activado, se inscribe en la solución de MDM de la empresa y todos los ajustes de gestión, apps y libros se instalan. Recuerda que la inscripción de dispositivos no está disponible en todos los países o regiones.

Para más información relativa a las empresas, consulta la ayuda de los Programas de Implantación de Apple en help.apple.com/deployment/business. Para más información relacionada con la educación, consulta la ayuda de Apple School Manager en help.apple.com/schoolmanager.

Restricciones

Los administradores pueden activar restricciones —o, en algunos casos, desactivarlas— para evitar que los usuarios accedan a determinada app, servicio o función del dispositivo. Las restricciones se envían a los dispositivos en la carga útil Restricciones del perfil de configuración. Las restricciones se pueden aplicar a dispositivos macOS, iOS y tvOS.

Aquí encontrarás una lista actualizada de las restricciones disponibles para los responsables de TI: help.apple.com/deployment/mdm/#/mdm2pHf95672

Borrado y bloqueo remotos

Un administrador o el propio usuario puede borrar los datos de un ordenador Mac de forma telemática. El borrado remoto instantáneo solo está disponible si el Mac tiene FileVault activado. Cuando se ejecuta un comando de borrado remoto con MDM o iCloud, el ordenador envía un acuse de recibo y realiza un borrado. Con un bloqueo remoto, MDM exige introducir un código de seis dígitos para poder acceder al Mac.

Privacidad

Apple considera que la privacidad es un derecho humano fundamental, por eso todos los productos Apple están pensados para procesar la información en el dispositivo siempre que sea posible, limitar la recopilación y el uso de los datos, proporcionarte transparencia y control sobre tu propia información, y crear unos cimientos seguros sólidos.

Apple incluye numerosas opciones y controles integrados que permiten a los usuarios de macOS decidir cómo y cuándo utilizar su información las apps, así como qué información se puede usar. Para más información, consulta www.apple.com/es/privacy.